Proceedings of the 2nd International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7048/73/2024.BO17847

Public Law Regulation and Joint Regulation of Cross-border Online Fraud: A Criminal Perspective

Xinyuan Chen[1,a,*]

[1]*Law school, Zhejiang Normal University, Jinhua, Zhejiang, 321000, China*
a. Nagisacxy@zjnu.edu.cn
**corresponding author*

Abstract: To handle cross-border online fraud, a global and significant issue, countries have adopted different legislative attitudes and enforcement methods. Existing theories address many issues of legal application and interpretation, whereas there are still some leaks in public law and systematic regulation. Therefore, this research, using this as a leverage point, from a criminal perspective, tries to discover how to regulate this issue efficiently. The main methodologies that this research chose are comparative law and crime script. This study found distinguishing differences between China, the United States and the Philippines, for instance, whether there is a dedicated responsible agency and whether there are specific laws in place, and the views of the European Union (hereinafter referred to as the EU) and African Union (hereinafter referred to as the AU) on this issue are definitely instructive. Through research, it has been found that to confirm criminal jurisdiction, the principle of territory and the principle of most significant relationship should be insisted. The protection of personal information should be based on the principles of legality, legitimacy, necessity, and integrity, with the explicit consent of the information owner as a prerequisite for obtaining and using the information. After de-identification, the information can be used within a certain scope without the provider's consent.

Keywords: cross-border online fraud, personal information, criminal jurisdiction, cross-border enforcement.

1. Introduction

Recently, with the deep socialization of cyberspace, cross-border online fraud has exhibited a trend of increasing frequency. Its features such as concealment, cross-border nature, and difficulty in obtaining evidence, heighten the challenge of regulating this issue. To better respond to the voice that the government should have full-chain, source-based and comprehensive regulation of people, the Law of the People's Republic of China on Combating Telecom and Online Fraud (hereinafter referred to as the Anti-Fraud Law) have adopted at the 36th Session of the Standing Committee of the Thirteenth National People's Congress of the People's Republic of China on September 2, 2022 [1]. Moreover, the Supreme People's Court and the Supreme People's Procuratorate presented some juridical interpretations, such as Interpretations 1 and 2 of the Supreme People's Court and the Supreme People's Procuratorate on the specific application of laws in handling criminal fraud cases (hereinafter referred to as Opinion (I) and Opinion (II)), which unified some important points related to online fraud [2,3]. Existing theories, most of them are based on legal doctrine, from the connection

DOI: 10.54254/2753-7048/73/2024.BO17847

of traditional and online fraud, making criminal analyses. For instance, some scholars may argue that non-amount circumstance of cross-border online fraud aren't appropriate connected current criminal and administrative law, meanwhile others hold that government should explore how to convict and joint prevention efficiently according to the non-contact feature when government take spatio-temporal property into its consideration [4,5]. Above these academicist, starting from Chinese criminal law, have responded to many difficulties about cross-border online fraud. However, this challenge isn't only in China, but the world. Countries have adopted different measures to prevent and counter it, whereas objectively, the distinguishing differences in enforcement abilities and resources between nations have imposed a negative impact on international practices of prevention and countering cross-border fraud. The resolution of these questions could help government to coordinate international and domestic law and foster relating public law and joint regulations.

This research based on national legislation and international public law, adopts comparative law, from criminal perspective, presenting relating resolutions to the leaks of existing international joint countering online fraud system.

2. The Current Situation of Cross-border Online Fraud

2.1. Definition and Classification

Cross-border fraud, refers to the act of defrauding public or private property by various means, using telecommunications network technology and other means, for the purpose of illegal possession [6]. As a typical cybercrime, the Budapest Convention stipulates that computer fraud: when committed intentionally and without right, the causing of a loss of property to another person by (a) any input, alteration, deletion or suppression of computer data, (b) any interference with the functioning of a computer system, this behaviour should be regulated [7]. In the Interpol 2022 report, it emphasized this as a typical representative of important cybercrime, which should be paid more attention [8].

Cheaters make the use of anonymity and concealment of telecommunication to fabricate identity or transaction, escaping supervision and combat. The specific forms of this crime are diverse, for example, (a) without the right to invade the computer system to interfere with or destroy computer function or data;(b) making use of virtual or disguised identities;(c) providing untrue financial and investment services;(d) offering fake services and transaction;(e) feigning online dating or friendship; and(f) utilizing undisclosed or false information. According to the report, fraud types represented by order brushing, false investment schemes, and impersonating customer service account for nearly 88.4% of the cases in the second and third categories of telecom network fraud [9].

2.2. Character and Trend

The contradiction between the rapid development of information online technology and the lack of efficient supervision, constitutes the crux of the difficulties in coping with cross-border online fraud. Cross-border online fraud is a special fraud in the information era, characterized by the following features:

First, concealment. The unique character of online measures, resulted in more hidden identity and purpose of cheaters than traditional cheaters. Criminals can use VoIP to fabricate fake communication locations. Moreover, fraudsters with strong counter-surveillance awareness would erase their criminal evidence and tools to avoid supervision.

Second, cross-border. Cybercrime has a natural cross-border even international character, which only can be appropriately handled with international cooperation. Since 2009, online fraud groups have started to relocate to Southeast Asian countries like Thailand, Cambodia, Indonesia, the Philippines, and Vietnam, as well as Arab countries, exhibiting a trend toward globalization.

DOI: 10.54254/2753-7048/73/2024.BO17847

Third, difficulty in obtaining evidence [10]. Given that cross-border online fraud cross territory, it requires coordination and joint investigation between the country where the act occurs and the country where the consequences manifest, which demands significant negotiation time and extra energy. Moreover, owing to the necessity of cross-border enforcement, the concrete enforcement activities are subject to local circumstances, ultimately investigators couldn't obtain evidence and solve cases timely.

3. Existing Public Law Regulation on Cross-border Online Fraud

As an emerging global criminal form, the regulation of cross-border online fraud is a great popular demand, so many countries have successively issued legal documents to clarify the boundaries of it. Meanwhile, the voice of unified legal standards about how to regulate this crime of the international community has dramatically been growing.

3.1. Public Law in Various Countries

In China, apart from the Anti-Fraud Law, some legal documents such as Opinion (I) and Opinion (II) provide basic regulation for criminal methods, relating to property, evidence collection, jurisdiction determination, and sentencing standards, to counter increasing cross-border online fraud by online communication, virtual figure, and fake base stations. In the United States of America, the Computer Fraud and Abuse Act presented in 1986 stipulates that whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains particular informations should be regarded as a crime [11]. In the Philippines, though the Cybercrime Prevention Act recognized and clarified the basic prevention and control routes for cross-border online fraud in the text presented in 2012, it ultimately was frozen owing to concerns about its potential impact on online privacy [12].

In comparison, China's legislative attitude centered around Criminal law and Anti-Fraud Law, supplemented by juridical interpretation and policy documents, while the United States prefers to adopt a comprehensive approach with multiple laws regulating the issue. Furthermore, in order to combat cross-border online fraud, China has established a specialized Anti-Fraud center, enforcing under the guidance of the Ministry of Public Security, in contrast, the USA tends to interagency collaboration, primarily involving FBI and FTC, whereas, the Philippines entrusts its National Bureau of Investigation (NBI) and Anti-Fraud Division with handling such cases.

In addition, to a certain extent, the Chinese government's legislation and enforcement of countering cross-border online fraud focus on protecting ordinary citizens, especially through nationwide special crackdown activities and targeted funding. However, the American government prefers to protect itself and critical infrastructure. For example, in May, 2021, the American president signed an executive order aimed to prevent the security of national information from threats, in October, 2021, the Department of Justice issued Civil Cyber-Fraud Initiative designed to combat illegal behaviors that threaten sensitive information. As for the Philippines, its legal system is still relatively young, and the Cybercrime Prevention Act of 2012 still suspended, so there is room for development.

3.2. Regional and International Public Law Regulation

In 2001, the European Union led the negotiation and conclusion of the Budapest Convention, but the number of parties are still limited, preventing the formation of a relatively unified international standard for judicial and law enforcement cooperation [13]. The Convention on Cyber Security and Personal Data Protection stipulated by AU faces similar questions. Both conventions have regulated

DOI: 10.54254/2753-7048/73/2024.BO17847

regional cybercrime, to a certain extent, however, the international community still has leaked a unified international law developed by the United Nations that addresses cross-border cybercrime.

Until the draft of the International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes gained consensus among related countries on August 8, 2024, the gap was filled. It's worth noting that some scholars and the public have negative attitudes towards the influence of the draft on online privacy and the right to a fair trial. They worry that the data supervision will be harmful to basic human rights, especially, since some countries suspect the inclusion of human rights protection clauses [14]. However, the convention remains the most significant legal document for the public law and joint regulation of cross-border online fraud, which holds considerable research value. Especially its positive response and practical solution to the drawbacks of the existing system, could help us handle cross-border online fraud better.

4. Exploring and Anticipating Feasible Approaches to Regulating Cross-border Online Fraud

4.1. Drawbacks of Existing System

To begin with, unclear attribution of criminal jurisdiction is the current difficult situation.

First, the claim of criminal jurisdiction should be based on reasonable grounds. Jurisdiction, refers to a power of government based on sovereign management matters within territory scope. Extraterritorial jurisdiction, refers to the government extending its influence territory of law application or judicial and administrative powers beyond its physics territory.

The Legitimacy and rationality of domestic jurisdiction are from the sovereign's right to completely control their territory, without extra proof, whereas extraterritorial jurisdiction, grounded in the principle of equality in the international community, should be based on specific legal or political reasons. Without this vital ground, criminal jurisdiction would extend disorderly, undermining the principle of international comity.

Second, the criminal jurisdiction of cross-border online fraud, cannot be determined by physical space. Owing to telecommunication online space is a virtual domain that transcends physical boundaries and distances, characterized by virtuality, remoteness, and borderlessness. The traditional principle of territory relying on physics space cannot straight apply on concealment and high-tech cross-border online fraud [15].

In addition, the contradiction between expanding extraterritorial criminal jurisdiction and the restrained objective requirements of criminal law must be resolved during the process of clarifying criminal jurisdiction. On one hand, if cybercrime is regarded as a global crime, universal jurisdiction might replace territorial jurisdiction as the primary principle. On the other hand, the boundaries of criminal jurisdiction are vague, leading to overlaps and conflicts in the exercise of jurisdiction for the same criminal acts. Furthermore, this problem would result in jurisdictional conflicts including between subjective territorial jurisdiction and objective territorial jurisdiction, jurisdiction based on the effects principle, and jurisdiction asserted under the protective principle.

Finally, the application of the principles of international comity and reasonableness, as provided in the Tallinn Manual 2.0, remains problematic. The principle of international comity points, a nation's jurisdiction should be restricted within its territory scope in normal situations, except specific reasons that justify recognizing the extraterritorial effect of foreign laws. The principle of reasonableness emphasizes that extraterritorial jurisdiction should have a significant relationship as a premise. Ian Brownlie argues: "If there is one fundamental principle, it is that there must be a real connection between the matter in question and the territorial basis or reasonable interests of the jurisdiction asserting authority." Ideally, government, could implement the principle of international cooperation and the principle of national sovereignty equality by applying these principles. However,

DOI: 10.54254/2753-7048/73/2024.BO17847

in practices, on the one hand, because of conflict between the essence of judicial enforcement and the principle of international comity, the judger couldn't be a decision-maker, otherwise this will result in judicial decisions being unpredictable. On the other hand, the ambiguity in defining the reasonableness principle, particularly the concept of "significant relationship," diminishes the practical effectiveness of the principle [16].

Then, Inadequate Criminal Law Protection of Personal Information. In most online fraud cases, the leak of victims' personal information constitutes a crime root. The existing criminal law framework lacks sufficient legal protection for citizens' personal information, fostering the increase in fraud. Cheaters frequently exploit key personal privacy information obtained in advance to impersonate others or fabricate events, thereby engaging in fraudulent activities. These incidents are rampant and difficult to eradicate, underscoring the urgent need for more comprehensive criminal law protections for personal information.

Articles 25, 26, 27, 28, and 29 of the draft United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purpose respectively stipulate the rapid preservation of stored electronic data, the expedited preservation and partial disclosure of traffic data, production orders, search and seizure of stored electronic data, and orders for real-time collection of traffic data. However, in the process of practices, if it ultimately could pass, to relevant parties, even irrelated parties' personal information, there remains a gap that needs more practical and sufficient precautions. Although these measures successfully address the major challenge of cross-border law enforcement, they are likely to lead to more crime caused by the leakage of citizens' personal privacy.

4.2. Exploration of Anticipating Feasible Approaches

First, clarify the attribution of criminal jurisdiction. To begin with, in the process of constituting criminal jurisdiction, countries should address the tension between jurisdictional expansion and the principle of restraint in criminal law, between what should be and what is, and between politics and law. Under beholding the principle of cyber sovereignty, nations should promote friendly consultations, and mutual assistance, and actively sign bilateral or multilateral agreements to jointly resolve jurisdictional issues in cross-border online fraud. Then, on the basics of insisting on the principle of territory, emphasizing the principle of reasonableness, and using the principle of significant relationship to clarify attribution of criminal jurisdiction. When determining a significant relationship, the government should keep a balance between the principle of quantity and the principle of quality, with a focus on what best promotes international social order stability, protects the legitimate rights and reasonable expectations of the parties involved, and maintains the consistency and fairness of judicial proceedings [17]. Before applying the principle of a significant relationship, the legitimate behaviours in their countries should be excluded from consideration to save juridical resources and boost judicial efficiency. Last, the government should make an effort under the guidance of the UN to promote the adoption and implementation of the United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes to control costs. In the basics of deep understanding and respecting the objective difference between national enforcement abilities, countries should have more international cooperation and judicial assistance, with judicial precedents potentially serving as sources for determining jurisdiction.

Second, establishing a more mature criminal law protection institution for citizen's information is a practical solution. According to the Interpretation on Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringing Citizens' Personal Information (hereinafter referred to as the Interpretation), "citizen's information" refers to various types of information, recorded electronically or other means, can distinguish specific natural person identity or reflect personal activities in combination or independently, including name, identity card, communication details, financial status, account password, location and so on. According to the Personal Information

DOI: 10.54254/2753-7048/73/2024.BO17847

Protection Law of the People's Republic of China, the application of personal information should obey the principle of legality, legitimacy, necessity, and good faith. To put it another way, the application of personal information must be restricted by the existing necessity of criminal law regulation. The usage of personal information, especially private sensitive information, should be limited in the scope of the principle of reasonableness. For one thing, the government should prevent and punish the abuse of personal information of individuals or entities, for another, preventing the disorder and expansion of authority that invades personal privacy rights and freedom of information is necessary.

Establishing a mature criminal law protection system for citizen's information should uphold the principle of responsibility and consent.

The government should adhere to the principle of responsibility, holding the individuals and organizations that illegally leak citizen's information accountable resolutely. Those who leak information without authorization or beyond authorization should be punished with relevant laws and regulations. According to Interpretation, if an individual knowingly or should have known that personal information would be used to commit a crime, yet still sells or provides the information, it should be considered a "serious circumstance" under Article 253 of the Criminal Law and be punished accordingly. Relatively, if an individual is forced to leak or based on legitimate reason to provide, owing to he or she leak alternative possibilities, the individual responsible for the disclosure should be exempted or given a reduced penalty.

The government should adhere to the principle of consent, and the premise of the use of knowing and application of citizen's information is explicit consent. The contradiction between the sharing of public information and the protection of personal information is an unavoidable question in every cyberspace activity. Since the development of the internet, the knowing and consent of the information owner is not only the premise of using information, but also is minimum protection demand for citizen's citizens' personal information. Although the premise of data creating value is free flow, this value should be restricted when facing basic human rights. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data points, there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject [18]. The EU has continued this requirement in the GDPR. The acquisition and application of citizens' personal information, not only needs noticed and gained consent but also grants the information owner the right of erase and the right of objection. Once they object to the usage of their information, entities must stop all use instantly.

For instance, Japan has restricted this requirement, and the USA firmly object to excessive supervision of data from the perspective of date-free flow. To be honest, it's a tough social choice. But overall, to regulate the acquisition and application of citizen's information, the sovereign should constitute criminal regulation system at the core of the right of knowing and consent, only accept some exceptions in certain situations to break the barriers of the principle of consent, for example from the contract clauses that are in coordination with public order and good customs, or the life interest and other major legal interests of the information owner cannot be guaranteed timely without possibility to gain consent. At the same time, when applying the principle to establish restrictions for entities to acquire personal information, the government couldn't excessively emphasize personal rights and interests. While maintaining control over the decision to transfer information, a certain degree of autonomy should also be granted to enterprises. For instance, after de-identification, the information can be used within a certain scope without the provider's consent.

5. Conclusions

Current prevention and combat of cross-border online fraud, primarily based on its unique characteristics such as concealment and cross-border, have relied on Interpol. Whereas these activities

DOI: 10.54254/2753-7048/73/2024.BO17847

have been subject to objective differences in enforcement resources and ability between nations, it's challenging to joint regulation efficiently. In order to regulate, in the process of jurisdiction determination, the principle of territory and the principle of reasonableness can be insisted, using the existence of the principle of most significant relationship to determine the substantive jurisdiction. In the process of regulating illegal leaks and unauthorized obtaining of personal information, the precedent of EU, USA, and Japan should be taken into consideration. Based on upholding the principles of responsibility and consent, balance two vital values between the free flow of data resources and efficient protection of personal information. As this research emphasized, the coordination between the principle of consent and the character of the free flow of data in personal information application and protection remains a social choice. This issue of how to reconcile these two elements could be a subject for further discussion in the future.

References

[1] *Xinhua News Agency. The Law of the People's Republic of China on Combating Telecom and Online Fraud. September, 2, 2022. Retrieved on September, 24, 2024. Retrieved from https://www.gov.cn/xinwen/2022-09/02/content_5708119.htm*

[2] *Xinhua News Agency. Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on the specific application of laws in handling criminal fraud cases. December, 20, 2016. Retrieved on September, 24, 2024. Retrieved from https://www.cac.gov.cn/2016-12/20/c_1120155376.htm*

[3] *The People's Courts News and Communication Agency. Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on the specific application of laws in handling criminal fraud cases. June, 17, 2021. Retrieved on September, 24, 2024. Retrieved from https://www.chinacourt.org/article/detail/2021/07/id/6129192.shtml*

[4] *Huo, J. (2023). Layered application of non-amount circumstances in cross-border telecom network fraud crimes. Journal of Chongqing University (Social Sciences Edition).*

[5] *Li, H. (2024). The legal logic and control of temporal and spatial standards in crime identification: A perspective on new standards for telecom network fraud crimes. Law Science, (07), 78-93.*

[6] *Li, K. (2024). Research on cross-border telecom fraud crimes and their governance. Law Science, 12(2), 749-755.*

[7] *Council of Europe. (2001). Budapest Convention on Cybercrime, Article 8 – Computer-related fraud. Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185*

[8] *Interpol. (2022). Report on Cybercrime: Trends and Developments. Retrieved from: https://www.interpol.int/*

[9] *Xinhua News Agency. The Ministry of Public Security has released a list of the top ten most common types of telecom network fraud. December, 25, 2024. Retrieved on September, 24, 2024. Retrieved from http://www.news.cn/politics/20240625/4499f6a5376f44b4ae43086b44562510/c.html*

[10] *Yin, J., & Tao, Y. (2022). Dilemmas and countermeasures in combating cross-border telecom network fraud crimes. People's Forum: Academic Frontiers, (16), 109-111.*

[11] *Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986).*

[12] *Kittima (Hu, H. L.). (2019). Research on the legal issues of cross-border data flow [Master's thesis, Wuhan University].*

[13] *Zhou, Z. (2019). Major disputes in the jurisdiction of cybercrime and China's position. China Information Security, (05), 32-34.*

[14] *Huang, Z., & Wang, X. (2023). Negotiation disputes and prospects of the United Nations Convention on Cybercrime. China Information Security, (03), 50-53.*

[15] *Yu, W. (2022). On the international conflict and regulation of criminal jurisdiction in cybercrime. Global Legal Review, 44(05), 178-192.*

[16] *Zheng, Y. (2023). Conflicts and responses in foreign-related criminal jurisdiction of cybercrime. Dispute Resolution, 9(5), 2086-2092.*

[17] *Weng, J. (2017). Judicial application of the principle of closest connection: Focusing on Article 2 of the Law on the Application of Laws for Foreign-related Civil Relations. Legal Science (Journal of Northwest University of Political Science and Law), 35(06), 194-199.*

[18] *Organization for Economic Co-operation and Development (OECD). (1980). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Retrieved from https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en*