The Practical Challenges and Responses of Local Anti-Fraud Legislation from the Perspective of Responsive Governance: A Case Study of Zhejiang Province

Linchen Huang

College of Criminal Investigation, Zhejiang Police College, Hangzhou, China
18058338657@163.com

Abstract. In the context of social digital transformation, telecom and online fraud has emerged as a complex governance challenge. Implementation Measures of Zhejiang Province for the Anti-Telecom and Online Fraud Law of the People's Republic of China (hereinafter referred to as "the Implementation Measures" came into effect on December 1, 2025. This marks a new phase in Zhejiang's anti-fraud efforts. Against this backdrop, this study adopts the theoretical lens of "Responsive Governance." It constructs a "dynamic response model" with three dimensions: technical response, collaborative response, and adaptive response. This model serves as an analytical framework for understanding anti-fraud governance. The study explores how Zhejiang can move from "having laws to adhere to" to "good laws and governance" under the new regulations. Based on this foundation, the paper focuses on Zhejiang's first local legislative measure against telecom and online fraud. The primary challenges center on four key areas: institutional barriers, a lack of accountability in collaborative efforts, inadequate capabilities and data interoperability in technical responses, and inflexible legal provisions with underdeveloped adaptive mechanisms. "The Implementation Measures" directly address these challenges. They enhance collaboration through joint governance systems, driving the modernization of governance capabilities through technological empowerment, and improve the adaptation of laws and technology through refined local regulations. This helps improve adaptive mechanisms. The study aims to provide theoretical references and practical recommendations to optimize Zhejiang's anti-fraud governance system under the new law. It also offers insights for other regions to develop anti-fraud governance models suited to the digital age.

Keywords: Law of the People's Republic of China on Combating Telecom and Online Fraud, Responsive Governance, Legal Safeguards, Implementation Effects

© The Author(s) 2026
C. F. Peng et al. (eds.), *Proceedings of the 2026 5th International Conference on Humanities, Wisdom Education and Service Management (HWESM 2026)*, Advances in Social Science, Education and Humanities Research 1024,
https://doi.org/10.2991/978-2-38476-593-5_10

1 Introduction

The Fourth Plenary Session of the 20th Central Committee of the Communist Party of China, standing at the strategic height of comprehensively building a modern socialist country, put forward the critical proposition of advancing the modernization of the national security system and capabilities, made important arrangements for improving the social governance system, and called for the prevention and resolution of major risks such as cybersecurity threats. The core essence of modernizing national governance lies in governance by institutions, driving governance transformation through legal reforms to achieve a fundamental shift from pre-modern to modern governance (Liu Yanhong, 2023). Against this grand backdrop, the digital transformation of society has not only reshaped economic forms and lifestyles but also given rise to new types of crime represented by telecommunications and online fraud, posing severe challenges to traditional national governance paradigms. In the face of rapidly evolving criminal methods and models, static and passive legal regulation has proven insufficient, making more adaptive concepts and practices of "responsive governance" an imperative of the times.

On September 2, 2022, the 36th Session of the Standing Committee of the 13th National People's Congress reviewed and adopted the Anti-Telecommunications and Online Fraud Law of the People's Republic of China (hereinafter referred to as the Anti-Telecommunications and Online Fraud Law), providing legal safeguards for combating and governing telecommunications and online fraud. The promulgation of this law embodies the concept of "responsive legislation," oriented toward addressing the risks of telecommunications and online fraud and actively adapting to the needs of social governance. It marks a crucial step in the legal transformation of China's governance in the field of cybercrime. Zhejiang Province, as a pioneer in digital economic development, has also enacted the nation's first local regulation in the field of anti-fraud, "the Implementation Measures" of Zhejiang Province for the Anti-Telecom and Online Fraud Law of the People's Republic of China(hereinafter referred to as "the Implementation Measures"), which took effect on December 1, 2025, showcasing proactive exploration at the local level. With the formal implementation of these local regulations, Zhejiang's anti-fraud efforts have entered a new stage characterized by "having laws to abide by and rules to follow." However, the prevalence and high incidence of telecommunications and online fraud in the province remain severe. How to further enhance governance effectiveness, address deep-seated challenges under the legal framework of "the Implementation Measures", and advance anti-fraud work from "having laws to abide by" to "good laws and sound governance" remains a central issue in current social governance.

Based on the theoretical perspective of "responsive governance," this study conducts a systematic analysis of the implementation of the Anti-Telecommunications and Online Fraud Law, rather than merely offering a superficial evaluation of its effectiveness. To this end, the research constructs a "dynamic response model" comprising three dimensions—technological response, collaborative response, and adaptive response—as the core analytical framework to systematically examine the internal logic and practical challenges of anti-fraud governance. Within this

framework, the study takes "the Implementation Measures" as a specific case to analyze its practical pathways in addressing governance dilemmas and to assess the institutional innovations and optimization directions reflected in these three dimensions.

2 Literature Review

2.1 Theoretical Origins

The theoretical foundation of "responsive governance" originates from “government responsiveness” in public administration.In Western countries, it originates from social contract and popular sovereignty, with emphasis on how governments provide timely and effective feedback to a public demand and preference.In China, the idea has evolved from a “people oriented” thinking, and was developed, under the influence of the Communist Party of China's fundamental “serving the people” as well as their development philosophy of putting people at the center, towards a ”responsive governance" philosophy. Wang Kuojian (2023) defines it as follows: for better performance of governance, government, guided by the “putting people first,” takes public needs as the base, government roles as primary, government services as an integral, supply-demand alignment as the key, and intelligent platforms as a supporting mechanism to allow interaction among the government, the public, society, and enterprises in public governance. However, when dealing with highly complex new types of crime, such as telecommunications and online fraud, classical theories are not powerful enough. Telecommunications and online Fraud are not only public security issues, but also governance challenges involving communications, finance, web, personal information, and even cross-border crime.Traditional “pressure-response” or “expression-response models,” that model, are no good when confronting highly complex new forms of crime. We therefore develop a ’responsive governance' in this article. It is an extension of traditional theory in the digital society, in that the response is not just a passive response to reported public victims of crimes, but a proactive response to potential criminal risks. In particular, cooperation between the government and social organizations, the government is needed to turn the more complex a system, from after a crime crackdown to front-end prevention, and from a government “solo performance” to a “societal chorus.”

2.2 Constructing a "Dynamic Response Model"

Effective responsive governance involves not only the speed of response but also a profound change of governance structures, processes, and rules.In order to get a better understanding of the inner logic of anti-fraud governance, the theory of the social collaborative governance, is developed with the emphasis on “ technological response,” “collaborative response,” and “adaptive response.” As shown in Figure 1, this dynamic response model covers the three core dimensions of anti-fraud responsive governance, which forms a complete logical system for analyzing anti-fraud governance practice.

The theory of social collaborative governance, in which the more complicated a social system is, the more cooperation among the government, social organizations and the public is crucial and active (Emerson K, Nabatchi T, et al.,2012). The theory of social collaborative governance is widely applied in fields such as community governance and judicial practice. Jin Yuqian and Tang Jun (2023) note that urban community governance faces challenges, including a single dominant stakeholder and an ambiguous delineation of responsibilities and authorities. Applying collaborative governance theory in practice helps enhance governance efficacy effectively through multi-stakeholder participation and platform-based collaboration. Sun Yu (2025) proposes that the operational logic of social collaborative governance inherently aligns with the jurisprudential requirements of juvenile justice, and this theory has been gradually integrated into the practice of juvenile judicial protection.Given the problem of social governance for telecom and online fraud, the government, financial institutions, telecom providers and public must not just take ad-hoc campaign-style joint actions but also establish a institutionalized and sustainable multi-stakeholder co-governance system. In this paper, we suggest the idea of “collaborative response” to address the basic questions of ” who answers and “how to collaborate.” It should be more of a phrase of ‘break-down” from departments, officials and individuals by institutional design and build a “governance community” with clear responsibilities, smooth procedures and interconnected information.

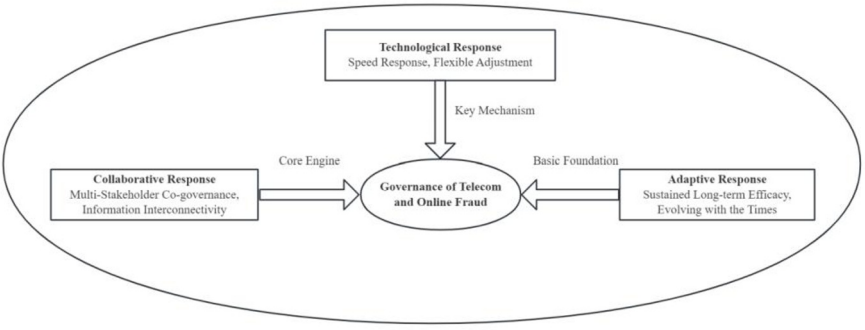

Fig. 1. Dynamic Response Model

Technological approach can provide legal practice with modern scientific and technological approaches. Huang Yuxi (2023) reviewed the electronic evidence collection norms for the cross-border telecommunications fraud from 2014 to 2022, and presented technical pathways to facilitate the global judicial assistance. Xu Jing and Wang Ying (2024) report that current technology governance is not sufficient to deal with AI-enabled fraud. They propose that personal information protection should be upgraded at the legislative level and platform accountability at the enforcement level to achieve synchronized improvements of technology and law. Institutional governance often regulates behavior with rule-making. However, when dealing with the ever-increasing crime methods, such as telecommunications and online,

institutional management might not be able to respond quickly and flexibly. Technological response should alleviate this disadvantage. By fully exploiting the enabling role of digital technologies, it allows real-time risk perception, decision making, and actions to be performed on a coordinated basis.

Adaptive governance theory is that in highly uncertain and dynamic environments, governance rules and institutions must be able to both to learn, experiment, and adapt to keep the system effective and moving with the times.(Chen Kun,2025) Xie Xiao and Luo Shijie (2025) note that as technology evolves rapidly, legal systems must be constantly learning but that legal systems will fail to "correct" new types of crime. Hu Dengfeng, Wu Hao, et al. (2025) say that law can also be a support for adaptive governance with mechanisms like "soft law" instruments and experimental legislative sandboxes, allowing bidirectional adaptation between institutions and technology. The stability and law is not limited by the rapid variation of fraud techniques such as AI face-swapping, virtual currencies, or GOIP devices—and the inherent stability and procedural nature of law. Because fraud practices change so quickly, the law is not yet responding to them. This can pose problems in the social order and citizens' property. Thus, "adaptive response" comes to the fore. The law requires that the law – especially the law and regulatory regimes – have good learning abilities and resilience. Thus "Adaptive response," the law's law and regulation regimes require the law to have good learnable and robust mechanisms to tackle the long-term "how to respond continuously and efficiently."

3 Implementation Effectiveness of the Anti-Telecommunications and Online Fraud Law

Modernizing national management can lead to better laws and effective governance. The enactment and implementation of the Anti-Telecommunications and Online Fraud Law is the practice of "responsive governance" at the country level. The first results of the implementation show its positive contribution to criminal activities. But from practice in Zhejiang Province, while the law has changed governance models, it also objectively revealed the flaws of uniform national legislation to local specialties and other contextual factors. These issues motivate the formulation and implementation for the other local regulations, such as Zhejiang Province implementation measures of the anti-Telecommunication and Online fraud Law.

Since the implementation of the Anti-Telecommunications and Online Fraud Law, Zhejiang Province has achieved significant governance results in its anti-fraud efforts. Changes in key governance indicators have shown a positive trend overall since the law took effect, characterized by the effective containment of case incidence, a reduction in economic losses, and enhanced enforcement efficacy. As shown in Figure 2, a comparison of data from before and after the law's implementation (average values for 2021-2022 versus 2023-2024) reveals: a simultaneous decline in the number of cases accepted and the amount of losses involved, reflecting the law's effective compression of the operational space for criminal activities; meanwhile, the case resolution rate and the number of suspects apprehended have maintained stable

growth, indicating that, based on the preliminary control of the criminal situation, the precision strike capability and sustained governance capacity of law enforcement agencies have been further consolidated. This "decline-increase" trend systematically illustrates the substantive role played by the law's implementation across both the prevention and control, as well as the enforcement, dimensions.

Since the implementation of law, Zhejiang Province has achieved good governance and anti-fraud activity. Changes in key governance indicators have been positive in general, which includes a good containment of the number of cases, a smaller economic loss, and improved enforcement efficiency. As illustrated from Figure 2, based on both before and after implementation (average (2021-2022 vs 2023-2024))data, a decrease in the number accepted cases and the amount of losses is reflected by the effective compression of the space of activity for criminal activities, while a stable increase in the case resolution rate and the number in seized cases, which implies that, based on the early control of the criminal situation, the precision strike capability and the robustness of the law enforcement agencies has also been enhanced. This “decline-up” phenomenon shows that the substantive value of the enforced laws, both in prevention and control, and in enforcement, has been fully appreciated. As we also show in Figure 2 with the case from Zhejiang Province implementation.

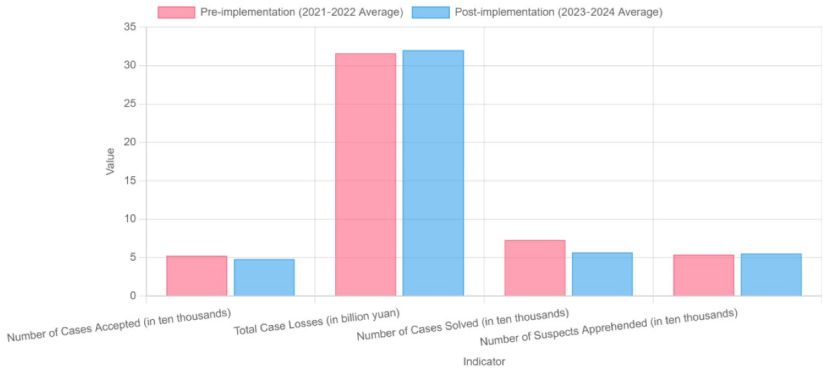

Fig. 2. Comparison of Key Indicators Before and After the Implementation of the Anti-Telecommunications and Online Fraud Law

As an example, the anti-Telecommunication and Online Fraud Law gave a clear legal account for fighting crime but also led to a transformation in governance models. For instance, 3 decline and 3 increase in key indicators are reflected in the data provided by the Zhejiang Provincial People Procuratorate in 2024. According to the figures released by the state government in 2024, the number of accepted cases and the amount of losses decrease by 12.2% and 35.7% year-on-year, respectively, while the number of major cases decreases by 51.8%. While the numbers of solved cases, the numbers of suspects and the amounts of recovered losses increase by 12.1%, 17.7%, and 37.1%, respectively.

This variation of “declines versus increases” can be observed as a sign of the law's ability to dampen criminal activities and to improve governance performance. As explained by the recent data of the administration in Zhejiang Province, the recent development of technical countermeasure capabilities has been crucial to the evolution of the governance model. The passive procedure of ”case occurrence → case filing → investigation → case solving” has rapidly evolved into a proactive prevention and control model of ‘monitoring → warning → dissuasion → interception’ and it is clear that this change is reflected in recent governance performances of Zhejiang Province. As illustrated by Figure 3, in the first half of 2025, Zhejiang Province prevented public losses and intercepted funds in 67.12 billion yuan cases from early warning, dissuasion, and technical countermeasures, much larger than the losses recovered by “case solving & asset recovery” (9.32 billion yuan). This data comparison highlights the benefit of front-end governance, indicating a significant strategic shift from “post-incident punishment” to “pre-incidents and in-process prevention and control.”

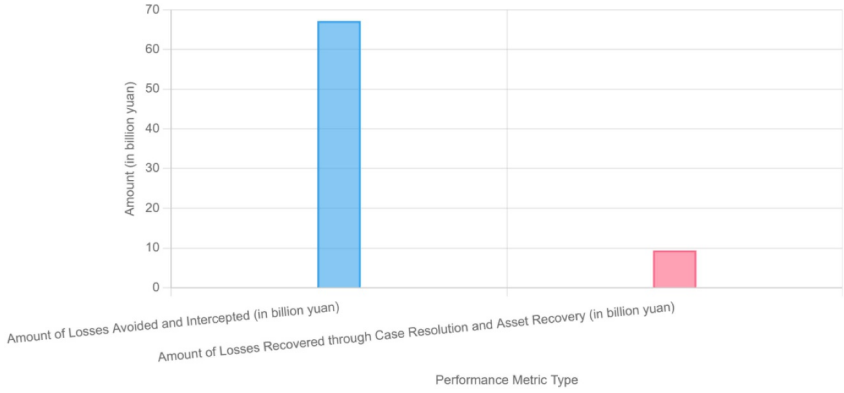

Fig. 3. Comparative Analysis of Selected Governance Performance Metrics for Telecommunications and Online Fraud in Zhejiang Province (First Half of 2025)

Its success is heavily dependent on the leap-frog development of technology countermeasures. The Anti-Telecommunications and Online Fraud Law and its local implementation has significantly cleared legal challenges for the institutionalized usage of technology, which has also been corroborated by recent technical interception data: according to Figure 4, in the first half of 2025, the volume of fraud-related SMS messages intercepted, scam calls blocked, and fake websites removed in Zhejiang Province reached millions or billions. Among them, intercepted SMS messages became even more relevant. This surge represents not merely a quantitative leap but signifies a systemic transition of the countermeasure framework—from "case-by-case response" to "mass filtering," and from "manual analysis" to "intelligent screening." It is precisely this robust technical support that underpins the prevention of substantial financial losses and demonstrates the effective

operation of a high-efficiency responsive mechanism that leverages technology to combat technology within the legal framework.

Although many important achievements have been achieved, telecommunications and online fraud remain a constant phenomenon.Gathering as it is, macro trends in Fig. 2 show the challenges even though such improvements are positive. While the total monetary losses are lower, their overall size remains high.On the other hand, the increase in solved cases and arrests of criminal organizations remains present. They together show that although enforcement and prevention efforts have increased, criminal gangs are adapting to governance pressures, they are adopting covert organizational structure and diversifying techniques. Criminals are utilizing new types of crimes such as AI face-swapping, virtual currencies and cross-border settlement. This makes study and fund tracing more challenging. This shows that just using a single measure of government are not sufficient. It needs to incorporate multi-stakeholder efforts through a "collaborative response" and flexibly adapt legal and policy tools via an "adaptive response" mechanism in order to build a more resilient and comprehensive governance system.

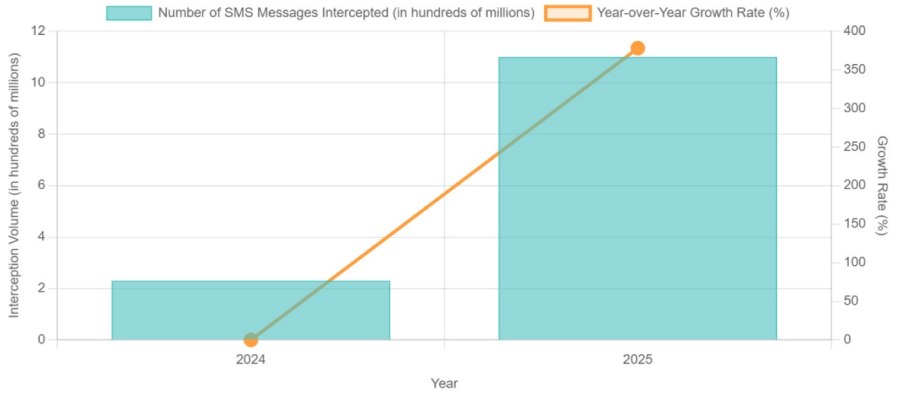

Fig. 4. Year-over-Year Growth in Technology-Based Interception of Fraud-Related Information in Zhejiang Province (2024 vs. 2025)

4 Deep-Seated Challenges in Legal Safeguards Against Fraud from the Perspective of Responsive Governance

Currently, the Anti-Telecommunications and Online Fraud Law is fully implemented. It gives basic rules on the governance system and provides sufficient support against possible illegal and criminal activities. However, when considered from the perspective of "responsive governance," the law still presents practical challenges, primarily reflected in three aspects: insufficient coordination, insufficient technical support and insufficient legal adaptability. These challenges constrain one another and collectively constitute the deep bottlenecks that need to be overcome to improve the effectiveness of anti-fraud governance.

4.1 Issues in Collaborative Response: Institutional Barriers and Lack of Stakeholder Engagement

Collaborative response aims to develop an institutionalized framework for multi-level co-governance. But in practice, it is constrained by institutional barriers and insufficient stakeholder engagement. In practice, current efforts to fight the telecommunications and the online fraud are not well-coordinated, due to shortcomings in joint prevention and control and more professional-training.

On one hand, existing mechanisms for cross-department coordination and collaboration are not effective, and they result in gaps in front-end supervision and insufficient source-level governance measures. While Zhejiang has developed a relatively complete cross-level and cross-regional law enforcement coordination system, the interdepartmental cooperation is lacking. Agencies such as cyberspace administration, telecommunications regulators, financial regulator and market supervision departments are among those with major deficiencies in cooperation.In practice, the success of current efforts still suffer from practical challenges such as a lack of joint prevention and less professional-level supervision.

On the other hand, public participation plays an important role in the fight against fraud. The public's awareness of telecommunications and online fraud directly affects prevention and enforcement, however, the existing public awareness issues are not sufficiently developed. The lack of awareness among citizens about their role as active players in a rule of law society. Co-governance campaigns of anti-fraud awareness campaigns have yet to fully mobilize the public. Although anti-fraud publicity teams have been established in the sub-district offices, organizations, communities, and volunteer service groups, the public's knowledge of their role in combating telecommunications and internet fraud is still not broad enough. This is due to the lack of long-term cooperation with well-established groups which makes it difficult for anti-fraud publicity teams to ensure reliable and effective management of this type of crime. The victims of telecommunications, online fraud often lack awareness of their rights and available legal options. The public's willingness to report fraudulent activities remains low and many people do not know where to report it. So the victims are left silent when receiving fraud, not reporting any incidents to police or agencies, and the criminals can still be executed with impunity.

4.2 The Issue of Technological Response: Conflict Between Technological Dynamism and Legal Normative Stability

Technological response is a main mechanism of “responsive governance,” which aims to effectively handle the problem of governance by technological empowerment. While for combating telecommunications, and online, this mechanism has a limited governance capability and inadequate data-sharing mechanism.

The delay in updating law enforcement personnel makes it hard for them to keep up with technologically motivated crimes. Telecom and online crime has been highly professional and intelligent recently. Clandestine groups exploit high-level technologies such as GoIP devices, virtual currencies, and AI-generated deepfakes,

making their methods covert and robust. On the other side, grassroots law enforcement officers often have to lag in knowledge updating, electronic forensics, data analysis, and cyber analysis, which often leaves them short time to disrupt criminal networks and recover losses. Data-sharing issues also impede the success of technology. Real-time early warning, analysis and handling of data sharing and combining analysis in key areas (for finance, telecommunications, Internet, and logistics) can be difficult to achieve. Even with advanced analytics models, the amount of information from other areas can be inadequate.

4.3 Dilemmas in Adaptive Response: Legal Rigidity and Institutional Deficiencies

Despite the increasing digital influence of cyberspace, cyber security and technicality can be considered as two different characteristics. Technology has been involved in social development of cybereism from its infancy and it is necessary for the government to manage the social development. But the continuous development of network technology also affects traditional social governance models and their associated legal and regulatory mechanisms (Xu Hanming, 2018). As a derivative of cyber security, the main question of telecommunications and online fraud is that the dynamic development of the information technology has an interference with the stability of legal norms of the Anti-Telecommunications and Online Fraud Law

While Chinese law and law enforcement practices for telecommunications and the online fraud have been relatively good with current laws and regulations, they are insufficient to deal with new crimes and complex cases and must be improved. Currently, the legal definitions of online fraud crimes are insufficient and the law is hard to correctly detect and apply the law under specific circumstances when the law was applied. For new criminal tactics including traffic hijacking and virtual currency fraud, the existing laws and rules are not correct enough for effective crackdowns. Moreover, legal measures for rapid freezing and recovering the assets involved in the cases remain not very suitable and cannot work properly as in telecommunications and Online fraud cases, which involve fast fund transfers and high concealment. This will have the effect of giving criminals an opportunity to recover their illicit gains with the help of a relatively weak legal structure.

Furthermore, the laws for protecting the rights and interests of victims still need to be improved in practice. Implementing efficient victim relief and compensation laws requires systematic research and development of corresponding institutional designs. Meanwhile, the provisions for civil litigation and public interest litigation in Articles 46 and 47 of the Anti-Telecommunications and Online Fraud Law need to also be implemented and revised in practice (Xu Lingbo and Zang Xueqing, 2023). In particular, if the perpetrators in associated crimes should be indicted for the breach of victims' property losses and the types and types of liability, or whether such a fine-grained lawsuit is also to be pursued through criminal incidental civil proceedings in the existing system of procuratorial public interest lawsuits, for example, through further improvement of related legal support mechanisms. Releasing enforcement and refinement of the articles will help the administration of

the judiciary as the last safeguard in terms of protecting the legitimate rights and the interests of victims.

5 Conclusion：Pathways for Optimizing the Anti-Fraud Governance System

With these challenges, Zhejiang Province did not just have national laws, but in fact its measures of Zhejiang Province for the Anti-Telecommunications and Online Fraud Law of China. This was a “second response” at the local level. As the nation’s first local policing of anti-fraud, this paper not only complicates the national law, but puts forward specific definitions in Zhejiang as well as follows the “dynamic response model”. Institutionalizing new innovations that are focused on “responsive governance” can give a “Zhejiang Solution” to legal security issues.

5.1 Optimizing Collaborative Response: Building a Multi-Stakeholder Co-Governance Framework

To deal with inadequate coordination between agencies and poor participation from the public. "The Implementation Measures" clarify rights and responsibilities, enabling collaborative governance. Chapter II of "the Implementation Measures", Public Awareness and Education, publishes anti-fraud knowledge and clear ways for the public to cooperate in governance. This shifts people from being merely protected to actively participating in governance. People are encouraged to actively participate in the system. Having community members and set up the system corrects misconceptions that fraudsters are simple or do not have the sophistication and increases the awareness of the problem(Yuan Jiayun and Yuan Yonghang, 2023). Article 7 establishes “96110” as the anti-fraud hotline and the public can report and supervise for the first time. This will enhance confidence and participation while checking the authority of the public and thus support cooperation.

"The Implementation Measures" set out specific legal duties and rules for inter-agency collaboration. Article 31 requires departments to work together efficiently and allows provincial public security to establish a unified anti-fraud data platform. Ten sectors, such as finance and telecom, must join this platform. The law mandates data sharing and joint action, not optional, providing sufficient enforcement to break down data silos.

5.2 Optimization of Technical Response: Driving the Modernization of Governance Capabilities

Article 32 of Chapter VI of “the Implementation Measures” establishes a province-wide unified early warning and dissuasion system. It formalizes “in-process intervention” a mandatory legal process which has to follow standard procedures. This move is a significant shift from a response measure which only relied on the experience of law enforcement personnel. This not only is an improvement in the

policing perspective from post-incident punishment to in-process interventions, but also, through institutionalized constraints, forces law enforcement capabilities to keep pace with the rapid development of criminal techniques and reduce response delays due to lack of expertise in the field.

To address collaboration barriers between agencies, Article 31 of Chapter VI “the Implementation Measures” mandate Zhejiang Provincial Public Security Authorities to provide a unified electronic data-sharing platform that integrates data from these key sectors such as finance, telecommunications, internet, and logistics. This presents a theoretical basis for risk early warning, and it also provides a legal responsibility for cross-department collaboration. It thus transforms the situation of “fragmented efforts” to a first “integrated and coordinated” governance scheme, which takes into account challenges in technologies based on the isolation of data.

Moreover, Implementation Measures support a fundamental shift of governance policy from “post-incident handling” and “preventive intervention”. In Article 31 of Chapter VI, the department should not only be able to handle missed cases, but also be able use big data models to analyze crime patterns, to identify risk targets, and detect emerging patterns. Using big data to analyze criminal trends, find high risk targets and identify new modus operandi, anti-fraud could move from ”universal awareness campaigns” towards “targeted prevention and control.” Last but not least, Implementation Techniques are intended to further regulate the technology tools and financial channels used for these crime activities.

5.3 Optimizing Adaptive Response: Achieving Dynamic Adaptation Between Law and Technology

“The Implementation Measures” are especially tailored to the region of Zhejiang Province, with rapid digital growth and the emergence of new business models, and provide tailored additions and modifications to the legal rules of the national law.

Due to the rapid development of criminal methods and slow time in legal definitions, "the Implementation Measures" do not attempt to redefine crimes themselves, only to better regulate the tools and channels required to accomplish these crime activities.Starting from the widespread implementation of user real name registration systems, Article 13 of Chapter IV makes strict rules concerning the control of voice-dedicated lines, SMS ports and sales agents, and increases source-level governance capabilities.The main idea is to close the domain of fraudsters which use new technologies, and effectively control the very channels they operate on.

In order to reduce the number of instances where freeze and recover property have not been performed, Articles 19 to 21 of Chapter V permit financial institutions to set classified, tiered restrictions and thresholds on abnormal accounts given risk information. This leads to the rapid use of asset preservation operations by allowing to block funds prior to cross borders. This helps in real-time tracking of asset seizures. The anti-fraud data sharing platform promoted by these regulations is also used to provide the essential data for real- time tracking of fund flows. It lifts a weak link from recovering illegal assets.

Regarding the lack of protection for victims and their interests, "the Implementation Measures" seek to create a system of effective process-based governance that will support their case.In law, the reasons why the civil litigation and public interest litigation clauses for articles 46 and 47 of the Anti-Telecommunications and Online Fraud Law are difficult to implement for victims are the difficulties of obtaining evidence and loss analysis.The early warning and dissuasion system and data sharing platform, which are provided by articles 31 and 32 of "the Implementation Measures", can help prevent preemptive intervention.In addition to their prevention, they can be recorded and stored to facilitate the monitoring of the fraud activities during the intervention process. These structured evidentiary materials can be helpful to follow legal actions by aiding victims to establish legal links for damages or helping judges and the courts in initiating public interest lawsuits. This greatly contributes to the transformation of the relevant litigation clauses from court text into law.

The adaptive relevance of “the Implementation Measures” is not necessarily to directly and fully resolve all the macro-level legal challenges, but rather to show the application of a local governance approach using technology to make legal application more flexible. By focusing on critical points, improving process supervision, and improving data sharing, “the Implementation Measures” translate principle-based legal provisions into executable and traceable operational rules, thereby building a buffer and adaptation mechanism that allows for dynamic response and flexible variation between relative stability in the national law and rapid improvement of the criminal technique. This practice is the essence of “responsive regulation” and a good basis for exploring and refining the governance system for telecommunications and online fraud at the national level.

Acknowledgment

This research was supported by 2024 National College Student Innovation and Entrepreneurship Training Program Project “Anti-Fraud Index: Constructing a More Scientific Measurement Standard for telecom and online fraud Crime Governance” (202411483024).

References

1. Chen Kun. “Four Laws in Parallel”: Towards an Adaptive Governance Paradigm in Artificial Intelligence Legislation[J]. Legal Forum, 2025, 40(04): 41–54.
2. Emerson K, Nabatchi T, Balogh S. An Integrative Framework for Collaborative Governance[J]. Journal of Public Administration Research and Theory, 2012, 22(1): 1–29.
3. Huang, Y. The Dilemma of Electronic Forensics of Cross-Border Telecom Network Fraud Crime and Its Treatment Path. Open Journal of Law Science, 2023, 11(5), 4184-4191. https://doi.org/10.12677/ojls.2023.115594
4. Hu Dengfeng, Wu Hao, Wang Jiayi. Research on Government Adaptive Governance in the Era of Artificial Intelligence—Based on a “Technology-Institution-Value”

Three-Dimensional Analytical Framework[J]. Academic Monthly, 2025, 57(06): 83–94.https://doi.org/10.19862/j.cnki.xsyk.001109.
5. Jin Yuqian, Tang Jun. Research on the Dilemmas and Coping Strategies of Urban Community Collaborative Governance from the Perspective of Complex Adaptive Systems[J]. Journal of Beijing University of Technology (Social Sciences Edition), 2023, 23(02): 38–47.
6. Liu Yanhong. The Transformation to Rule of Law in Cyber Violence Governance and the Construction of a Legislative System[J]. Chinese Journal of Law, 2023, 45(05): 79–95.
7. Sun Yu. On Collaborative Governance of Risk Assessment for Juvenile Delinquents in the Digital Age[J]. Journal of People's Public Security University of China (Social Sciences Edition), 2025, 41(01): 59–69.
8. Wang Kuojian. On Responsive Governance in the Process of Chinese Modernization[J]. Jianghai Academic Journal, 2023, (06): 135–141+256.
9. Xu Jing & Wang Ying. Research on Governance of AI Telecom Network Fraud in the Era of Artificial Intelligence. Open Journal of Law Science, 2024, 12(7), 4591-4595. https://doi.org/10.12677/ojls.2024.127655
10. Xu Hanming. The Experience and Enlightenment of China's Cyber Rule of Law[J]. China Legal Science, 2018, (03): 51–70. https://doi.org/10.14111/j.cnki.zgfx.2018.03.003.
11. Xu Lingbo, Zang Xueqing. The Convergence of Criminal and Civil Liability for Personnel Involved in Telecommunications and Online Fraud-Related Crimes[J]. Chinese Prosecutors, 2023, (17): 15–18.
12. Xie Xiao, Luo Shijie. On the Dynamic Risks of Generative Artificial Intelligence and Adaptive Governance[J]. Journal of Beijing University of Technology (Social Sciences Edition), 2025, 25(01): 112–125.
13. Yuan Jiayun, Yuan Yonghang. Problems and Optimization Strategies in Police Station Publicity Against Telecommunications and Online Fraud[J]. Journal of Political Science and Law, 2023, 40(04): 16–25.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.