Social Changes and the Evolution of Crime Patterns: Taking China's "Digital Transformation" as an Example

Yanan Qu[1*], Jiayuan Zhang[1]

[1]School of Ocean Law and Humanities, Dalian Ocean University, Dalian, China
**Corresponding Author. Email: 709117713@qq.com*

Abstract. Against the backdrop of China's rapid "digital transformation", crime patterns have exhibited a distinct characteristic of "dual variation": traditional contact crimes such as theft, robbery, and fraud have continued to decline due to the popularization of mobile payments and the strengthening of technical prevention and control measures like the Skynet Project. Meanwhile, new types of crimes using the internet as a tool, platform, or target—such as telecom fraud, data theft, and online black industry—have grown rapidly, exposing problems including legislative lag, inadequate supervision, and the digital divide. This evolution stems from technology's reshaping of social structures and criminal opportunities, driving criminal activities toward remoteness, technicalization, and cross-regionalization. To address these challenges, it is necessary to construct a "resilient governance" system, promote legislative and regulatory innovation, strengthen smart law enforcement and platform responsibilities, deepen international cooperation, and enhance national digital literacy, thereby transforming crime governance from passive response to proactive early warning and systematic prevention and control.

Keywords: digital transformation, evolution of crime patterns, cybercrime, resilient governance

1. Introduction: research background

The digital economy is a new economic form following the agricultural and industrial economies.[1] Entering the 21st century, the application of new technologies such as 5G, the Internet of Things (IoT), cloud computing, big data, artificial intelligence (AI), and blockchain has brought profound changes to social life. The relatively single physical attribute of traditional society has been impacted, and cultural awareness, social structures, and legal systems are facing new adjustments.[2] In China, this process of "digital transformation" is particularly rapid and in-depth. According to reports from the China Internet Network Information Center (CNNIC), the scale of China's netizen population and internet penetration rate have continued to rise, while the penetration rate of mobile payments ranks among the highest in the world. This transformation is far more than an upgrade at the technical level; it is a comprehensive social change touching on social structures, economic models, and daily lifestyles. Social interactions have shifted from offline to online, economic activities from physical to virtual, and a new form of "digital society" closely coupled with the real society is taking shape. This requires social science researchers to re-examine many traditional

social issues, and crime, as a "pathological" indicator of society, has been at the forefront of morphological evolution. In this transformation process, a highly tense criminological phenomenon has emerged. On the one hand, statistical data from public security organs at all levels shows that the incidence of traditional contact crimes such as theft, robbery, and fraud, which have long accounted for a high proportion, has continued to decline, and the public security situation has continued to improve at the traditional level. On the other hand, new types of crimes targeting, using, or leveraging the internet have experienced explosive growth. Cases such as telecom and cyber fraud, online gambling, data theft and trafficking, and cyber hacking attacks have emerged one after another, involving huge amounts of money and causing increasingly serious social harm. This "dual variation"—the decline of traditional crimes and the surge of cybercrimes—constitutes the core empirical phenomenon of this research. It indicates that criminal energy has not disappeared but has been transferred and transformed amid social structural changes. Faced with the above drastic changes, existing theoretical explanations and governance strategies are facing challenges. At the theoretical level, traditional criminological theories are mostly based on the premise of relatively stable physical space and social structures, making them inadequate in explaining the anonymity of cyberspace, the cross-regional nature of criminal acts, and the novelty of criminal motives. There is an urgent need to integrate the macro and meso perspectives of sociology on social change, social structure, and social interaction with the micro perspective of criminology on criminal opportunities and decision-making to construct a more explanatory analytical framework. At the practical level, the public security governance system is undergoing a difficult transformation from offline to online and from responding to traditional threats to managing digital risks. Understanding the social mechanisms through which digital transformation affects crime patterns—rather than merely relying on technical blocking and legal punishment—is the key to promoting the transformation of crime governance models from post-event crackdowns to pre-event early warning and from departmental management to systematic social governance.

2. Presentation and analysis of domestic cases

2.1. Significant decline in traditional crimes

According to the Work Report of the Supreme People's Court and data from the Ministry of Public Security, since the mid-2010s, the number of registered cases of traditional "theft, robbery, and fraud" crimes nationwide has shown a continuous downward trend. Especially in urban central areas, the decline in such cases is more pronounced. Previously common crimes such as "pickpocketing on buses" and "street snatching on motorcycles" have decreased significantly, even becoming "memories of an era" for a generation. The decline of traditional crimes is not due to the disappearance of criminal motives, but to the profound transformation of the "social soil" and "opportunity structure" for their occurrence brought about by digital transformation. Firstly, the popularization of mobile payments has made society enter a "cashless era." People no longer carry cash but smartphones locked with passwords, fingerprints, or facial recognition. This has drastically reduced the "benefits" of street theft while significantly increasing the "risks" (device tracking). A thief may not obtain any economic benefits from a modern smartphone, but instead be quickly located and arrested due to the phone's built-in security system, which constitutes the most direct crime prevention. Secondly, China's "Skynet Project" and "Sharp Eyes Project" have built the world's largest public security video surveillance system. Combined with facial recognition technology and big data analysis, the anonymity of physical space has been greatly reduced. Every move of criminals in public places is exposed to "digital sky eyes," and the probability of being

arrested after committing a crime is extremely high, forming a strong deterrent. The solution to many theft cases has benefited from the precise restoration of suspects' movement trajectories through surveillance videos, making traditional crime models unsustainable.

2.2. Rapid growth of new types of crimes

In sharp contrast to the decline of traditional crimes, data from the Ministry of Public Security shows that the number of telecom and cyber fraud cases has remained at a high level, becoming one of the fastest-growing crime types with the strongest public reactions. At the same time, frequent data leakage incidents of various apps and platforms have spawned a huge black and gray industrial chain. For example, "pig-butchering scams," fake customer service fraud, illegal theft of public data, and digital pyramid schemes. Most of these crimes rely on emerging operation models and digital technologies, concealing their pyramid scheme essence—where rebates are calculated based on the number of downstream members recruited—through complex system designs and platform gameplay, making it impossible to correspond to the requirement of expanding downstream members.[3] In today's highly developed internet, emerging new types of crimes may take root in unknown places. The virtuality of cyberspace and the lag of early legal supervision have formed a "normative vacuum." Taking advantage of this, criminals have developed a set of neutralizing technologies to justify their actions, such as: "I'm just playing an online game (referring to fraud)," "They were too greedy/foolish themselves," and "This is not real theft." While bringing convenience, digital transformation has also created a digital divide based on age, educational level, and region. Groups such as the elderly and rural residents who are unfamiliar with online operations and have weak anti-fraud knowledge have become "suitable targets" in the eyes of criminals. For example, "pension fraud" and "fake public security, procuratorate, and court fraud" targeting the elderly often succeed precisely because they exploit the elderly's trust in official authority and their lack of ability to distinguish complex network technologies. The core of social networks is trust and connection, which are precisely exploited by criminals. For instance, illegally obtained personal data (shopping records, social relationships, etc.) is a digital mapping of personal social connections. Criminals use this data for "precision profiling," making fraudulent information highly deceptive. For example, fake customer service fraud is credible precisely because the fraudster can accurately state your shopping information, which essentially misappropriates the trust relationship you established in commercial activities.

3. Causes of the evolution of crime patterns

3.1. The lag of legislation

With the massive accumulation of information and the rise of digital and intelligent technologies, the governance value of data information has made it an important strategic resource. The instrumental significance of data has gradually become prominent, and information has been endowed with instrumental power in the criminological sense.[4] Traditional laws are established based on physical territories and clear rights and responsibilities, while cybercrimes are characterized by cross-regionalization, anonymization, and chainization, leading to difficulties in case filing, major jurisdictional disputes, and inconsistent standards for identifying electronic evidence. The speed of legal updates is far behind the iteration of criminal methods. Traditional laws regulate "people, acts, and objects" in the physical world, but in cyberspace, these elements have become blurred. For example, is duplicating virtual currency in a game using loopholes "destroying computer

information systems" or "theft"? What is the legal nature of virtual property? How to convict has become a major problem today. In the era of digital transformation, the speed of social changes has posed a huge challenge to the stability of laws.

3.2. The stimulation of digital development on crime patterns

Digital development has not merely "moved" traditional crimes online, but has fundamentally stimulated, spawned, and upgraded crimes. Firstly, the popularization of digital technology has created highly valuable criminal targets that did not exist in traditional society, such as issues of data security and privacy leakage, digital technology discrimination, the digital divide, and governance failures caused by excessive technological dependence.[5] Criminal targets have shifted from physical property to virtual data; digital assets such as cryptocurrencies, NFTs (Non-Fungible Tokens), and game virtual property have become the focus of hacking, fraud, and extortion due to their anonymity and high value; the digitalization and networking of fields such as energy, finance, transportation, and healthcare have made them high-value targets for cyberattacks, spawning destructive and terrorist crimes aimed at paralyzing social operations. Secondly, digital technology has provided criminals with unprecedented capabilities, lowering the threshold for crimes and improving criminal efficiency. For example, encrypted communication software provides criminal organizations with hidden communication channels; artificial intelligence (AI) is used to create counterfeit voiceprints and faces for identity fraud (deepfakes), or to automatically generate phishing emails and crack verification codes; big data analysis is used by criminals to accurately screen fraud targets, realizing "precision crimes." Thirdly, digitalization has also stimulated the evolution of criminal organizations themselves, making them more flexible and resilient. For example, traditional hierarchical and regionally concentrated criminal gangs are evolving into flat, distributed, and node-based cybercriminal organizations. Members may be scattered around the world, connected only through the internet, and the destruction of one node does not affect the operation of the entire network; the internet has made individual extremist crimes possible. Criminals can radicalize themselves online, learn violence techniques, and announce their actions on social media, with extremely high concealment and randomness. The core logic of digital development's stimulation of crime patterns lies in its comprehensive "empowerment" and "upgrading" of the criminal ecosystem through "creating new targets, providing new tools, spawning new models, and reshaping new organizations." This has made criminal activities exhibit the following characteristics: remote non-contact, breaking geographical restrictions; multiplied harm: a single crime can affect tens of thousands of targets; technology-intensive: the integration of technology and crime is increasingly close; concealed and anonymous: identity identification and traceability are extremely difficult.

3.3. Jurisdictional issues of transnational cybercrimes

A country's laws exercise supreme power within its territorial boundaries. The place of the criminal act and the place of the result are the basis for determining jurisdiction. This situation of the spillover of domestic legal effect formed based on the internet and digitalization has, to a certain extent, exceeded the dividing line between traditional domestic law and international law. Its essence is that the institutional construction originally purely for domestic law has produced a strong and unilateral foreign-related attribute.[6] For example, a hacker in Country A uses a server located in Country B to attack data of a company in Country C, causing losses to citizens of Country D. The place of the criminal act and the place of the result are scattered around the world. Which country's

court has jurisdiction? All countries may claim jurisdiction based on "part of the act or result occurring in their own territory," leading to positive conflicts of jurisdiction; on the contrary, they may also shirk responsibility due to the complexity of the case and evidence being located abroad, resulting in negative conflicts of jurisdiction. The most typical example is the fraud problem in northern Myanmar—even if Chinese police accurately locate fraud dens in Myanmar, they cannot directly go there to arrest, search, or seize evidence. Due to issues of judicial sovereignty, different countries have different standards for the legality, completeness, and relevance of electronic evidence. A remote evidence collection method that is legal in one country may be regarded as illegal intrusion in another, leading to the evidence not being admitted in court. All actions must rely on international judicial cooperation, which is often a slow, complex, and uncertain process.

4. Countermeasures for the evolution of crime patterns

4.1. From "lagging legislation" to "rapid governance"

The lag of legislation cannot be completely resolved, which is determined by the limitations of law. To reduce the huge losses caused by "lagging legislation," we need to change our thinking and focus more on "governance." For example, establish security pilot zones in key areas such as finance and data, allowing regulatory authorities and enterprises to jointly test new technologies, new formats, and their regulatory rules in real scenarios, realizing "standardization in development and development in standardization." Transform the legislative process from "desk conception" to "practical trial and error," providing true and reliable first-hand basis for formal legislation and avoiding "isolated decision-making." On this basis, strive to cultivate new legal science researchers in the fields of the internet, digital economy, and information technology industry. Excellent legal talents are required to be high-end legal professionals who are proficient in legal rules, familiar with information technology, and have cross-disciplinary integration thinking.[7] At the same time, clearly define the property rights of cryptocurrencies, virtual property, and data products in law, providing a solid legal basis for combating related crimes. Clarify the safety obligations of AI developers, the responsibility boundaries of users, and implement mandatory algorithmic transparency and ethical reviews for high-risk AI systems. An independent institution composed of legal experts, technical experts, and sociologists can also be established to conduct systematic evaluations of key digital laws regularly (e.g., every two years), analyze their effectiveness, side effects, and compatibility with technology, and put forward clear revision suggestions. Transform legislation from a "completed" product to an "ongoing" dynamic process to ensure that laws can be continuously optimized.

4.2. Responding to the stimulation of crime by digitalization

Firstly, develop "defensive AI," using artificial intelligence and machine learning to analyze network traffic, financial transactions, and social dynamics in real time, and establish a crime prevention mechanism coordinated by digital technology and credit evaluation mechanisms. Build a unified financial credit data platform to provide banks and other financial institutions with richer credit information,[8] automatically identify phishing websites, fraud scripts, money laundering patterns, and abnormal access behaviors, and realize "in-event" intervention and even "pre-event" early warning. Research and deploy dedicated algorithms that can quickly and accurately identify fake audio and video generated by AI face-swapping and voice-simulation technologies, curbing their application in fraud and disinformation dissemination. At the same time, promote trusted digital

identities based on biometrics or multi-factor authentication to reduce the risks of fraud, money laundering, etc., caused by the abuse of virtual identities. This is equivalent to establishing a unique and difficult-to-forge "ID card" for everyone in the online world. Furthermore, blockchain technology can be widely applied to evidence preservation scenarios such as electronic contracts, transaction records, and judicial documents. Its tamper-proof and traceable characteristics can greatly improve the reliability of electronic evidence and the efficiency of judicial trials. Secondly, strengthen the main responsibilities of platforms. Internet platforms, telecom enterprises, and financial institutions are the "critical information infrastructure" of digital society and must assume main responsibilities. Adopt strict technical and management measures to ensure real-name authentication for account backends, and proactively inspect and clean up illegal and criminal information on the platforms (such as fraud diversion and black industry advertisements). Establish a cross-platform "blacklist" database. Fraudulent numbers, malicious URLs, and fraud-related accounts identified by one platform should be shared with other platforms and financial institutions in real time, realizing joint blocking of "fraud involvement in one place leading to restrictions everywhere." Thirdly, promote cyber anti-fraud knowledge. Target vulnerable groups such as the elderly, students, and rural residents, and conduct "precision drip irrigation" publicity and education through community lectures, short videos, public service advertisements, and other forms. Establish convenient national reporting channels (such as official anti-fraud apps) and reward informants who provide important clues. At the same time, publicly disclose and feedback the handling results to enhance the sense of gain and trust of public participation. Encourage industry associations in various fields to formulate industry standards for anti-fraud and data security that are higher than legal requirements, and share best practices among members to form a self-purification mechanism within the industry.

4.3. Systematic strategies for addressing jurisdictional issues of transnational cybercrimes

The core contradiction in the jurisdiction of transnational cybercrimes lies in the conflict between "territorialized" judicial sovereignty and "globalized" criminal activities. Therefore, solutions must focus on "building consensus, simplifying processes, pre-positioning defense, and taking proactive actions." Firstly, in bilateral and multilateral negotiations, actively promote "substantial connection" as the main principle for determining jurisdiction. That is, as long as a criminal act causes a "substantial, direct, and foreseeable impact" on a country's sovereignty, security, social order, or citizens' rights and interests, that country has jurisdiction. At the same time, cultivate cross-industry legal talents. For example, relying on the Institute of Marine Rule of Law and Culture, Dalian Maritime University has set up courses such as Research on the Construction of a Marine Rule of Law System with Chinese Characteristics, Research on the Protection of Marine Rights and Interests and Dispute Resolution, and Research on the Legal Guarantee for Marine Sustainable Development. Through interdisciplinary training methods, it reserves compound international marine-related talents for the formation of new quality productive forces.[9] This can effectively resolve jurisdictional disputes caused by the separation of the place of criminal act and the place of result, providing a more reasonable and flexible international legal basis for countries to exercise jurisdiction. Secondly, advocate that countries "restrain" or "entrust" part of their sovereign powers under certain conditions when combating specific major cybercrimes. For example, with the authorization of the country where the evidence is located, law enforcement agencies of the victim country can conduct remote electronic evidence collection. This is a pragmatic innovation to address the geographical limitations of law enforcement power while respecting sovereignty. Thirdly, for major and complex transnational cybercrime cases (such as large-scale fraud groups and state-

sponsored hacking attacks), establish "joint investigation teams" with relevant countries. Law enforcement personnel from two or more parties share intelligence, take synchronized actions, and conduct joint evidence collection under a joint command framework, realizing in-depth cooperation in the form of "one case, one authorization."

5. Conclusion

Digital transformation is reshaping Chinese society with unprecedented depth and breadth. This is not only a technological revolution but also a profound social change. In this process, crime patterns have undergone significant structural evolution, presenting a "dual variation" pattern where traditional crimes decline and new types of crimes surge. Traditional contact crimes such as theft and robbery have decreased significantly due to changes in the "opportunity structure"—the popularization of mobile payments has made the "cashless society" a reality, technologies such as the Skynet Project and facial recognition have strengthened social control, and people's daily activities have shifted online, reducing the physical scenarios for crimes. However, at the same time, new types of crimes targeting, using, or leveraging the internet have experienced explosive growth. Their roots lie in the normative vacuum caused by social anomie in the digital age, the new social vulnerability created by the digital divide, and the trust crisis caused by the malicious abuse of social capital in cyberspace. The evolution of this crime pattern has exposed the systematic inadequacy of the traditional governance system in responding to the challenges of the digital age. Firstly, there is a contradiction between the lag of legislation and the subversiveness of technology. The traditional legal system based on the physical world is difficult to effectively regulate new types of criminal acts in virtual space, and the long legislative cycle cannot keep up with the iteration speed of criminal methods. Secondly, there is a conflict between national judicial sovereignty and the borderless nature of the internet. The principle of territorial jurisdiction is ineffective in the face of cross-border cybercrimes, and criminals exploit gaps in judicial jurisdiction to establish "safe havens." In addition, the "double-edged sword" effect of technology has become increasingly prominent. Defensive technologies and criminal technologies coexist and develop competitively, forming a cycle of "as virtue rises one foot, vice rises ten." More profoundly, the digital divide is exacerbating the differentiation of social structures. Vulnerable groups face greater criminal risks in the digital age, while the widespread existence of cybercrimes continues to erode the foundation of social trust. Faced with these severe challenges, piecemeal responses are no longer sufficient to solve the problem. It is necessary to construct a forward-looking and collaborative "resilient governance" system. This system needs to be built on four pillars: firstly, promote the transformation of legislation from "precision strikes" to "framework governance," enhancing the adaptability and learning ability of the legal system through mechanisms such as regulatory sandboxes and sunset clauses; secondly, comprehensively improve the level of smart law enforcement, strengthen the "digital combat capability" construction of law enforcement teams, build cross-departmental collaborative platforms, and realize the transformation from passive response to proactive early warning; thirdly, deepen global collaboration, actively participate in the formulation of international rules, establish rapid channels for cross-border electronic evidence collection, and break down judicial jurisdiction barriers; finally, build a pattern of social co-governance, consolidate the "gatekeeper" responsibilities of internet platforms and financial institutions, and systematically enhance national digital literacy to build a solid social immune system. The relationship between digital transformation and the evolution of crime patterns is essentially a concentrated manifestation of the mutual construction process between society and technology. Criminal energy will not disappear but will only find new outlets in the changes of social structures. Therefore, the ultimate

goal of governance is not to pursue absolute security, but to construct a governance ecosystem that can continuously learn, dynamically adapt, and effectively collaborate through the joint efforts of the government, market, and society. This system should be able to guide technology for good, curb its evil, and control various risks within an acceptable range while fully releasing the dividends of digital civilization. This is not only related to the maintenance of public security but also the cornerstone of building a safe, fair, and trustworthy digital future. In this process, we need to transcend traditional governance thinking and meet the comprehensive challenges of the digital age with greater courage in institutional innovation.

References

[1] Wei, C. D. (2024). The supply, demand, and response of criminal law on intellectual property in the era of digital economy. Journal of National Prosecutors College, 32(03), 49-64.

[2] Han, H. (2024). Theoretical review and standardized governance of the digital transformation of duty-related crime investigation. Jurist, (05), 128-141+194-195.

[3] Yin, B., & Yang, Z. J. (2025). Digital iteration and adaptive governance of pyramid selling crimes. Hebei Academic Journal, 45(05), 181-191.

[4] Wu, H. Q. (2024). Institutional response to the digital and intelligent transformation of crime governance models: From the perspective of privacy protection. Journal of People's Public Security University of China (Social Sciences Edition), 40(01), 25-34.

[5] Shi, Y. C. (2025). Paradigm shift and institutional response of digital empowerment in environmental rule of law. Gansu Political Science and Law University Journal, (05), 1-12.

[6] Pei, W. (2024). The digital approach to criminal procedure from the perspective of foreign-related rule of law. Chinese Journal of Criminal Law, (02), 124-142.

[7] Wang, X. G., & Liu, J. (2023). On the construction of an experimental teaching system for digital law courses. China University Teaching, (12), 46-55.

[8] Jiang, H., & Ning, Z. Y. (n.d.). Can the digital transformation of banks curb loan fraud crimes? Financial Economics Research, 1-19. Retrieved November 7, 2025.

[9] Cao, X. G., & Chu, B. P. (2023). On the construction of marine rule of law under the background of new liberal arts. Journal of Shandong University (Philosophy and Social Sciences), (01), 182-192.