Vol. 26 (2026): Proceedings of the 2nd International Conference on Social Sciences and Cultural Studies (ICSSCS 2026)
ISSN: 3105-0522 P-ISSN：3105-0514
DOI: https://doi.org/10.70267/icsscs.2026020917

AIGC-Enabled Cyber Sexual Offenses: Technological Logic and Legal Regulation

Xinting Hu*

Department of Law, School of Political Science and Law, Jiangxi Normal University, Nanchang 330022, China

**Corresponding author: Xinting Hu.*

Abstract

With the advent of the digital era, Artificial Intelligence Generated Content (AIGC) has come to play an increasingly important role in daily life. However, technological development inevitably brings new challenges. Some offenders have begun to exploit AIGC tools for criminal purposes, seriously infringing upon individual rights and public security. This study begins at the technological foundation and systematically examines the three core layers—data, algorithms, and computing power—each of which can be exploited by malicious actors. It then identifies and analyzes the two most common forms of AIGC-enabled cyber sexual offenses: face forgery and psychological manipulation. Building on this analysis, the paper proposes a tripartite analytical framework of "subject–tool–object" to clarify the underlying logic of these crimes. Within this framework, perpetrators are categorized into three levels: technology developers, tool distributors, and direct offenders. The criminal process is divided into four sequential stages: information collection, content generation, dissemination, and psychological manipulation. This structured deconstruction transforms previously fragmented phenomena into a clear and coherent picture. AIGC-enabled cyber sexual offenses are characterized by low barriers to entry, high concealment, and severe harm. Current legal frameworks struggle to address them effectively due to lagging definitions, difficulties in evidence recognition, insufficient platform accountability, and challenges in cross-border enforcement. Effective governance requires a coordinated approach that integrates legal measures with technological solutions, while mobilizing the joint efforts of platforms, society, and the international community.

Keywords

AIGC technology, cyber sexual offenses, crime model, legal regulation, collaborative governance, deepfake

1. Introduction

The rapid advancement of Artificial Intelligence-Generated Content (AIGC) technology is profoundly reshaping the paradigm of digital content production. AIGC systems are now capable of autonomously generating highly realistic multimodal content, encompassing text, images, audio, and video. Concurrently, everyday activities shared on social media platforms, such as selfies, voice recordings, and status updates, serve as readily available training data for these models. In the absence of effective regulation governing data collection and utilization, the potential risks associated with this technology cannot be overlooked.

In October 2025, Mou Qianwen, a top-performing sales professional at the Qingdao Porsche Center, discovered a proliferation of malicious, AI-synthesized illicit videos of herself online. These fabricated videos were created with the intent to defame and humiliate her, causing severe disruption to her personal life [5]In the same year, Daniel Weatherly, a 42-year-old man from Texas, United States, was sentenced to two years in prison and three years of supervised release for utilizing AI to generate child sexual abuse material (CSAM) [11]. Although occurring in vastly different geographical locations, these two incidents highlight a common issue: AIGC is being weaponized as a novel tool for cyber sexual violence. Such cases are far from isolated. According to statistics from international organizations, 98% of deepfake videos available online contain sexually explicit material, with 99% of these targeting women [15]. Furthermore, in 2025 alone, the Internet Watch Foundation (IWF) in the United Kingdom reported a 400% increase in cases involving AI-generated CSAM [9].

These figures indicate that cyber sexual offenses driven by AIGC technology are proliferating on a massive scale. A review of the existing literature reveals that current research tends to focus either on technical aspects, such as identification and detection, or on legal dimensions, such as the application of normative frameworks. Few studies have successfully integrated these two perspectives. Consequently, this paper seeks to examine the underlying technical logic of AIGC to analyze the coupling relationship between its technological characteristics and criminal motivations. By categorizing these emerging forms of criminality and constructing a comprehensive analytical framework, this study ultimately aims to explore feasible pathways for a synergistic governance model that integrates both legal and technological solutions.

2. The Rationale Behind the Weaponization of AIGC in Criminal Activities

2.1 The Three-Dimensional Structure and Risk Exposure of AIGC Technology

The foundational pillars of AIGC technology consist of three core elements: data, algorithms, and computing power. These elements interact to construct the operational framework of AIGC systems. However, when exploited maliciously, they can form a closed loop of technological alienation. This exploitation widens the risk exposure for technology-facilitated crimes and catalyzes the emergence of novel cyber offenses.

The first technological layer is data. The capacity of artificial intelligence to generate highly realistic, indistinguishable human faces stems from its exposure to vast datasets of facial imagery. The majority of these images are harvested from publicly available social media activities, including personal selfies, voice messages, and interaction logs. As Professor Xu Guanghua notes, web crawling technology has emerged as the primary mechanism for the automated collection of personal information, achieving data acquisition speeds at the millisecond level. Consequently, normative failures in the data collection phase have become a critical conduit for personal information breaches [1]. Such unregulated practices in data acquisition pose a direct threat to the security of citizens' personal information and broader public order.

The second technological layer is the algorithm. Once data is inputted, algorithms automatically process and assimilate the information. The mechanism by which AI autonomously identifies patterns from massive datasets is known as deep learning. In facial generation, greater exposure to facial data allows the model to better understand the alignment of facial musculature, thereby producing highly deceptive imagery. A similar principle applies to voice cloning. The fundamental issue, however, lies in the opaque nature of this learning process: the mechanisms and outcomes of the training are entirely invisible to external observers. This lack of transparency inherently leads to a lack of regulatory control. Recent research conducted jointly by the Alan Turing Institute and the UK Artificial Intelligence Safety Institute reveals that merely 250 malicious documents are sufficient to successfully poison the training data of a language model, and this attack efficacy is model-agnostic. This indicates that the cost associated with algorithmic poisoning is exceptionally low, and this reduction in technical barriers directly amplifies criminal risks. Consequently, if an algorithm is subjected to malicious training, such as utilizing obscene and explicit content as training data, it can be exploited for the mass production of fabricated pornographic material [2]. Compounding this issue is the algorithm's capacity for self-optimization. As the generated content becomes increasingly realistic, the difficulty of detection and authentication escalates accordingly.

The final technological layer is computing power. As noted by Wei Hong and Zhang Kui, computing power has emerged as a quintessential representation of novel productive forces in the era of the digital economy. Alongside algorithms and data, it constitutes the foundational bedrock of digital economic development [16]. With the widespread adoption of cloud computing services, computational resources have been decentralized, shifting from exclusive professional institutions to ordinary users. This democratization of technology directly translates into a significant reduction in the costs associated with executing criminal activities.

These three technological layers are highly interdependent and mutually reinforcing, ultimately forming a closed technological loop. Specifically, data supplies the essential training elements for algorithms, algorithms are entirely reliant on computing power for execution, and advancements in computing power facilitate faster and more accurate data processing. Should vulnerabilities emerge in any single link, the entire technological continuum becomes susceptible to malicious exploitation. Therefore, the governance of such technology cannot be confined to an isolated layer. Instead, it necessitates a synergistic approach that advances governance mechanisms across technological, legal, and societal dimensions simultaneously.

2.2 The Coupling of Technological Characteristics and Criminal Demands

The difficulty in preventing AIGC-driven crimes lies not only in the technology's inherent characteristics but also in its precise exploitation of human vulnerabilities. Furthermore, several specific attributes of AIGC perfectly align with the operational demands of perpetrators.

a) High Degree of Hyper-realism. AIGC is capable of generating content that is virtually indistinguishable from reality. It can precisely replicate a victim's face, voice, and physical movements in scenarios that never actually occurred. This profound sense of authenticity is crucial for perpetrators. Li Mingze conceptualizes this effect as a “hyper-realistic infringement scenario.” Specifically, when victims observe their own likenesses in fabricated videos, their initial reaction is often not anger, but rather profound fear and self-doubt [3]. The psychological impact of such an experience far exceeds that of traditional defamation, making it significantly easier to dismantle the victim's psychological defenses.

b) Exceptionally Low Barriers to Entry. Historically, the production of such sophisticated content required specialized equipment and technical training, entailing high costs in terms of both time and financial resources. The widespread accessibility of AIGC tools has fundamentally altered this landscape. Open-source models are available free of charge, and the generation process is highly automated. Consequently, operational barriers have been drastically lowered, and production costs have been compressed to near zero. This reduction in economic and technical thresholds directly expands the demographic pool of potential offenders.

c) Precision Customization. AIGC possesses the capability to generate highly targeted content based on the personal information of a specific subject. Perpetrators merely need to acquire the victim's social data, such as personal preferences, social networks, workplace environments, and daily routines. With this information, they can deploy customized psychological manipulation to successfully breach the victim's psychological defenses [4].

These three characteristics are mutually reinforcing. A higher degree of content realism correlates with a greater likelihood of breaking down the victim's psychological defenses. Lower technical barriers broaden the scope of potential criminal actors. Enhanced customization capabilities directly increase the success rate of criminal activities. This cyclical mechanism ensures that AIGC-driven cyber sexual offenses exhibit the overarching characteristics of low entry barriers, high concealment, and severe harm.

A comprehensive review of the aforementioned cases reveals two archetypal criminal methodologies. The first is “fabrication,” which involves the creation of fictitious sexual assault content that forces the victim into involuntary participation. The second is “manipulation,” characterized by the establishment of a deceptive relationship of trust to gradually control and exploit the victim. The subsequent sections will provide an in-depth analysis of these two specific forms of criminality.

3. Two Emerging Typologies: Fabrication and Manipulation

3.1 The Generation and Dissemination of Fabricated Sexual Assault Content

Fabrication-based crimes can be categorized into two primary modalities: facial replacement and the creation of entirely fictitious entities. Facial replacement, commonly known as deepfakes, involves the synthesis of a victim's facial imagery onto another individual's body, effectively forcing the victim into involuntary participation in pornographic material. In the aforementioned Qingdao Porsche Center case, Ms. Mou, a legitimate and successful sales professional, was abruptly confronted by a client inquiring about her purported presence in a sexually explicit video. She discovered that while the face in the video was hers, the body belonged to someone else; however, proving this discrepancy proved exceedingly difficult [5]. Victims of such crimes often face insurmountable hurdles at every stage of the legal process, including severe difficulties in securing evidence, highly complex judicial procedures, and the ambiguous liability of online platforms.

The second modality involves the generation of AI-CSAM (Artificial Intelligence-Generated Child Sexual Abuse Material), which presents a more insidious threat. AI systems are capable of generating virtual depictions of children from scratch. These images appear entirely photorealistic but do not depict any actual, living child. The critical issue is that such material inevitably infiltrates illicit markets and continues to incentivize further criminal activity. Current legal frameworks are severely constrained by the traditional prerequisite of an "actual victim." Consequently, establishing criminal liability in the absence of a real, identifiable victim presents a profound legal conundrum [6].

3.2 AI-Driven Manipulative Cyber Sexual Offenses

The defining characteristic of manipulation-based crimes is the fabrication of interpersonal relationships rather than the fabrication of content. Perpetrators utilize AI to analyze the victim's social data, encompassing personal interests, social networks, behavioral routines, and emotional fluctuations. Subsequently, they generate highly personalized manipulative discourse. When targeting isolated adolescents, the AI can assume the persona of an empathetic friend. Conversely, when targeting youth infatuated with celebrities, the AI can adopt the identity of an affectionate idol. During the initial stages, victims feel understood and gradually establish trust. As their psychological defenses are systematically dismantled, sexual grooming or extortion ensues [7].

The proliferation of the Metaverse concept has rendered such crimes even more difficult to prevent. Virtual avatars can be designed with extraordinary realism, enabling real-time interaction with victims. Within these immersive experiences, the boundary between the virtual and real worlds becomes increasingly blurred. Minors may believe they are interacting with an idol, while in reality, they are being groomed to engage in illicit activities. An empirical analysis conducted by Lei Hao, based on 52 criminal verdicts, reveals that this type of manipulative grooming accounts for over 60% of online remote molestation cases targeting minors [7]. Victims often remain oblivious to the deceptive nature of their "friend" until they are threatened with the exposure of their private information. Research by Li Luyan further indicates that the dissemination of such manipulative information exhibits a "pulsatile" characteristic. Once a critical threshold is breached, the content spreads exponentially within a condensed timeframe, rendering timely intervention practically impossible [8].

4. A Full-Chain Analytical Framework: Actors, Tools, Targets, and Processes

4.1 Core Elements

Based on a systematic review of typical cases, this category of crime can be distilled into three core elements: criminal actors, illicit tools, and targeted victims. Clarifying these three components is essential for fully comprehending the operational logic of such offenses.

a) Criminal Actors. The perpetrators exhibit a typical three-tiered division of labor. The upstream tier consists of technology developers who provide the technical foundation for criminal activities by creating or circumventing the safeguards of AIGC generation tools. While these individuals may not directly engage in criminal acts, their technological outputs are highly susceptible to being misappropriated as criminal instruments. The midstream tier is composed of underground cybercrime facilitators. They construct

operational platforms, traffic in personal information, and offer one-click generation services, thereby enabling the commercialized circulation of these technologies. The downstream tier comprises ordinary users who purchase these services and utilize the tools to directly perpetrate crimes. With each tier fulfilling its distinct function, this structure transforms isolated criminal acts into an industrialized supply chain.

b) Illicit Tools. The instruments used for these crimes are highly accessible. For instance, models like Stable Diffusion are open-source, applications such as DeepFaceLab are readily available through public channels, and ChatGPT offers open API access. Non-expert users can execute face-swapping operations merely by uploading a few photographs. Similarly, generating cloned voices requires only a few seconds of audio recording, and customizing manipulative scripts involves inputting a few basic keywords. More notably, these tools are frequently distributed through encrypted communication channels and dark web forums, making it exceedingly difficult for regulatory authorities to achieve effective traceability and tracking.

c) Targeted Victims. Any individual living in the digital age is a potential victim. The scope of targets has expanded from public figures to ordinary individuals, from real-world natural persons to virtual identities, and from localized offenses to cross-border dissemination. The digital footprints left by individuals online, including photographs, voice recordings, and social media updates, can all be exploited as source material.

These three elements interlock to form a complete criminal chain, following a trajectory from technology provision to tool circulation, and ultimately to victim infringement. Achieving effective governance and combating these criminal activities requires targeted interventions at every link to construct a full-chain prevention and control system.

4.2 The Criminal Process

In specific cases, the execution process of such crimes can be deconstructed into a four-step, closed-loop model.

The first step is information acquisition. Perpetrators utilize web crawlers and data scraping techniques on social media platforms to collect the target's photographs, voice samples, and social activity logs. A larger volume of acquired data directly correlates with higher fidelity in subsequent fabrications. In certain documented cases, the information collection coverage rate has exceeded 85% [11].

The second step is content generation. Perpetrators employ AIGC tools to transform the harvested information into fabricated evidence, encompassing facial replacement, voice cloning, and video synthesis. Empirical data indicates that facial replacement accuracy can reach 95%, voice synthesis similarity can achieve 90%, and overall visual realism can hit 92% [11]. Such high-fidelity content is virtually indistinguishable from reality to the naked eye.

The third step is dissemination. The fabricated content is distributed across social media platforms, dark web forums, and encrypted group chats. In some instances, the dissemination volume has surpassed 100,000 views within a 24-hour period [11]. Once the momentum of public pressure and reputational damage is established, any attempts by the victim to clarify the situation are frequently futile.

The final step involves psychological manipulation. Perpetrators threaten the victim with further exposure, coerce interactions, or extort financial assets. Statistical data reveals that the incidence rate of psychological trauma resulting from such manipulation reaches as high as 78% [11]. Consequently, victims may suffer from severe depression, be forced to withdraw from their academic institutions, or in extreme cases, commit suicide. The completion of these four steps solidifies the criminal loop. The intervention of AIGC technology renders this cycle significantly faster, highly concealed, and exceedingly difficult for law enforcement to disrupt.

5. The Regulatory Deficit: Challenges in Legal Governance

5.1 The Conundrum of Authentication and Evidentiary Classification

In the aforementioned Qingdao case, the victim's facial imagery was subjected to widespread dissemination. However, determining the precise criminal charge presents a significant challenge: should it

be classified as the dissemination of obscene materials, defamation, or the infringement of personal information? The judiciary frequently encounters profound adjudicative dilemmas when presiding over such cases. The primary cause is the absence of explicit statutory provisions addressing novel forms of infringement, such as AI-facilitated deepfakes [13]. Traditional jurisprudence operates on a foundational premise: evidence must possess authenticity, and facts must remain strictly objective. Conversely, content generated by AIGC fundamentally blurs the line between reality and fabrication. An image or a video clip may appear entirely authentic to the observer while being entirely synthetic in origin. Applying the charge of disseminating obscene materials is legally precarious because the content is entirely fabricated. Invoking defamation is equally problematic given the explicit sexual nature of the material. Furthermore, prosecuting under the infringement of personal information is debatable, as the perpetrators primarily "utilized" rather than directly compromised data systems.

A prominent counterargument posits that since AI-generated virtual CSAM does not inflict harm upon a real, identifiable child, regulatory intervention is unjustified. While superficially plausible, this assertion fails under rigorous legal and sociological scrutiny. Although an actual child may not be physically harmed, the existence of such material actively stimulates criminal ideation. These synthetic materials circulate extensively within illicit dark-web markets, serving as a medium for offenders to satiate illicit desires, exchange methodologies, and even pioneer new modalities of abuse. The absence of a tangible minor victim does not negate the fact that this material fosters a robust illicit industry. This underground economy comprises specialized tool developers, black-market distributors, and end-consumers. Ultimately, the systemic proliferation of such content inevitably endangers children, albeit through a more insidious and indirect mechanism.

5.2 Institutional Vacuums Regarding Platform Liability and International Cooperation

The determination of platform liability constitutes a central jurisprudential challenge. Current legal frameworks predominantly adhere to the principle of "technological neutrality," positioning platforms merely as passive "information conduits." Consequently, platforms are legally presumed to bear no proactive obligation to moderate or censor content published by users. While theoretically equitable, this paradigm becomes highly problematic in practice. When algorithms actively curate and recommend content, and when platforms derive substantial commercial profit from its dissemination, the assertion of strict neutrality is no longer tenable. Research conducted by Lao Peining emphasizes that the determination of complicity in cybercrime hinges on the presence of substantive facilitation. By designing engagement-driven algorithms and maintaining operational systems, platforms may implicitly constitute indirect facilitation of criminal acts. However, establishing legal accountability remains exceedingly difficult due to the protective shield of technological neutrality.

Furthermore, international cooperation presents an even more formidable obstacle. While AIGC content transcends geographical boundaries seamlessly, legal jurisdictions remain strictly territorial. Different sovereign states exhibit significant divergence in the legal classification of deepfakes, the evidentiary standards for digital authentication, and the regulatory frameworks governing cross-border data flows. This fragmentation allows perpetrators to exploit jurisdictions with lenient regulatory oversight, a phenomenon that Wei Zixiang conceptualizes as "regulatory arbitrage" [12].

6. Governance Pathways: Synergistic Regulation Through Law and Technology

6.1 Synergistic Governance Between Legal and Technological Frameworks

The governance of AIGC-driven cyber sexual offenses must be fundamentally anchored in the synergy between legal and technological mechanisms. On the legal front, several foundational questions must first be clarified: how should deepfakes be categorically classified within criminal law? Do they primarily infringe upon the right to reputation, the right to privacy, or other legally protected interests? Furthermore, how should legal liability be accurately apportioned? Research by Tang He and colleagues emphasizes that explicit legislative responses to these questions are imperative to prevent an overreliance on judicial discretion in legal practice [13]. Evidentiary rules must also be updated accordingly. The judiciary can no

longer rely solely on traditional paradigms of "original documents"; instead, specific criteria for forensic technological authentication must be codified into law.

Concurrently, technological countermeasures are indispensable. For instance, mandatory labeling systems must be implemented. AI-generated content should be required to embed immutable watermarks within its metadata, enabling users to immediately identify its synthetic origins. Additionally, platforms must deploy automated detection systems utilizing recognition models to preemptively intercept suspected deepfake content before dissemination. Furthermore, traceability technologies are critical. In the event of a violation, investigators must be able to utilize algorithmic traceability to ascertain the identity of the perpetrator, the exact time of creation, and the specific tools employed. The foundational technologies for these countermeasures are already mature; the primary bottleneck lies in the financial considerations and operational willingness of platform enterprises [14].

6.2 A Collaborative Governance System: Platform Liability, Public Participation, and International Cooperation

At the platform level, the principle of "technological neutrality" can no longer be invoked as a liability shield. Given that platforms generate substantial web traffic and advertising revenue from user-generated content, claiming to be mere passive conduits when violations occur is both legally and ethically untenable. Proactive content moderation, prompt removal of illicit material, and full cooperation with law enforcement investigations must become fundamental operational obligations. Platforms that excel in these duties could be granted regulatory incentives or safe harbor protections, whereas those guilty of dereliction of duty must be held strictly accountable.

At the societal level, governance cannot rely solely on governments and corporate platforms. Proactive public education is paramount, particularly for primary and secondary school students. While this demographic interacts with AI from an early age, they often lack awareness of its capacity to fabricate reality. Schools, communities, and the media must collaborate to cultivate a critical cognitive framework among the public, emphasizing that visual and auditory digital evidence is no longer inherently trustworthy. Moreover, reporting mechanisms must be streamlined. Currently, the reporting procedures on many platforms are overly convoluted, which deters ordinary users from submitting complaints. This operational friction must be eliminated.

International cooperation remains the most formidable challenge, yet it is utterly indispensable. AIGC content transcends borders seamlessly, prompting perpetrators to exploit jurisdictions with lenient regulatory oversight. Divergent national evidentiary standards mean that obtaining cross-border data can entail protracted bureaucratic procedures lasting months, severely hindering case progression. Therefore, it is imperative to harmonize international legal standards and normalize cross-border law enforcement collaboration, ensuring that territorial boundaries no longer serve as a jurisdictional sanctuary for cybercriminals.

7. Conclusion

This study acknowledges certain limitations. Given that AIGC-facilitated offenses represent an emerging typology of crime, the limited availability of public case data may restrict the comprehensiveness of this analysis. Furthermore, this paper approaches the issue primarily from a jurisprudential perspective, leaving room for a deeper exploration of the underlying technical mechanisms. Future research could conduct broader empirical studies to validate the proposed analytical framework with a larger dataset. Additionally, scholars could explore the psychological trauma inflicted upon victims and the amplification dynamics within online communities from the perspectives of psychology and sociology.

Ultimately, while technology itself is inherently neutral, the individuals who wield it are not. When technological innovations are weaponized to inflict harm upon others, the law must decisively intervene. The objective of such regulation is not to stifle the advancement of artificial intelligence, but rather to steadfastly defend a fundamental societal baseline: human dignity must never be deconstructed by algorithms.

References

[1] Xu, G. H. (2025). The practical status and theoretical reshaping of the "over-criminalization" of personal information crawling behavior in the context of information flow. Politics and Law, (7), 78-94.

[2] The Alan Turing Institute. (2025, October 9). LLMs may be more vulnerable to data poisoning than we thought. https://www.turing.ac.uk/blog/llms-may-be-more-vunerable-data-poisoning-we-thought

[3] Li, M. Z. (2024). New characteristics of metaverse crime. Juvenile Delinquency Prevention Research, (5), 78-85.

[4] Ma, F. (2012). Criminal network analysis: Application of social network analysis in organized crime research. Journal of Southwest University of Political Science and Law, (2), 34-43.

[5] Shi, H. X. (2025, October 15). Behind the false rumors about the Porsche female sales champion. China News Weekly. https://www.inewsweek.cn/society/2025-10-15/27113.shtml

[6] Zhao, J., & Li, Z. M. (2024). The criminal regulation dilemma and solution of AI-generated child sexual abuse materials. China Legal Science, (2), 187-208.

[7] Lei, H. (2024). Difficulties and countermeasures in preventing and controlling online child molestation crimes. Juvenile Delinquency Prevention Research, (3), 40-47.

[8] Zhou, B. H., & Zhang, S. Y. (2024). The "pulse" communication mechanism and intervention strategies of online grooming information: An analysis based on online child sexual abuse cases. Journal of News and Communication Research, (5), 52-70.

[9] Internet Watch Foundation. (2025, July 11). AI-generated child sexual abuse videos surge as synthetic imagery makes "huge leaps" in sophistication. IWF.org.uk. https://www.iwf.org.uk/news-media/news/ai-generated-child-abuse-videos-surge-as-synthetic-imagery-huge-leaps-in-sophistication/

[10] Shen, R. (2023). Dynamic analysis of node-based two-layer network SIRS epidemic model[Master's thesis, Huaqiao University].

[11] MoreLaw. (2025, August 5). United States of America v. Daniel Weatherly. https://www.morelaw.com/verdicts/case/FL/194950/

[12] Wei, Z. X. (2023). Research on public opinion evolution analysis and prediction model on social networks [Master's thesis, University of Electronic Science and Technology of China].

[13] Tang, H., & Zhao, M. (2022). Evolution of "pig butchering" telecom network fraud crime model. Journal of China People's Police University, 38(12), 12-17.

[14] Xu, Y. C. (2024). Stock return analysis integrating generative adversarial networks and statistical inference models [Master's thesis, Shandong University of Finance and Economics].

[15] Global Partnership for Action on Gender-Based Online Harassment and Abuse. (2025, December 10). Joint statement on preventing and responding to non-consensual intimate image (NCII) abuse. GOV.UK.

[16] Wei, H., & Zhang, K. (2025). Reflections on the connotation of "computing power" and its criminal law protection in the digital economy era. Journal of Guizhou University (Social Sciences Edition), (1), 95-105.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgment

This paper is an output of the science project.