

Legal Application Issues of Generative AI-Driven Emerging Intelligent Crimes

Yue Tan*

Law School, Wuhan University, Hubei, China

**Author to whom correspondence should be addressed.*

Copyright: © 2026 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

Abstract: The advancement and widespread application of generative AI technology have transformed traditional forms of crime, giving rise to new types of intelligent offenses such as deepfakes, AI-powered fraud, and AI-related intellectual property infringement. These crimes are characterized by concealed conduct, virtual perpetrators, and complex causal relationships, thereby challenging the framework and logic of conventional criminal law regulation. In judicial practice, issues such as rigid application of traditional criminal charges, unclear attribution of liability, difficulties in establishing causality, and an incomplete legal regulatory system have led to gaps or misalignments in addressing certain emerging intelligent crimes. This article analyzes the challenges arising from the judicial application of generative AI-related offenses by examining their unique characteristics, clarifies the boundaries of responsibility among involved parties, and explores appropriate legal principles and improvement strategies suited to the intelligent era. The article aims to provide a theoretical foundation for effectively regulating AI-induced crimes and achieving a balance between technological development and legal security.

Keywords: Generative AI; New forms of intelligent crime; Legal application; Criminal liability; Judicial regulation

Online publication: August 14, 2026

1. Introduction

Due to autonomous production, simulated intelligent operations, and batch processing, generative artificial intelligence has become widely involved in social activities and industrial economies. While actively contributing to societal development, it has also been exploited by criminals, giving rise to a series of new forms of intelligent crime. Unlike traditional human-perpetrated offenses, intelligent crimes involving generative AI weaken the traceability of human involvement and blur the causal relationship between actions and resulting harms. This undermines the traditional criminal law framework, which relies on subjective fault, elements of criminal conduct, and causality to establish liability and determine punishment. Current legal provisions primarily address conventional criminal forms, making them clearly inadequate when dealing with the emerging characteristics of intelligent crimes. Common challenges include difficulties

in conviction, ambiguity in assigning responsibility, and regulatory lag. Therefore, accurately addressing the legal application issues arising from AI-driven intelligent crimes, refining relevant judicial rules, and improving the criminal justice system are essential for managing legal risks in the age of artificial intelligence and achieving balanced development between technological advancement and legal governance.

2. Key characteristics of new types of intelligent crime enabled by generative AI

The emergence of new intelligent crimes driven by generative AI does not necessarily require the creation of entirely new criminal offenses in criminal law. Rather, these crimes represent a digital and intelligent evolution of traditional offenses—incorporating artificial intelligence technologies into conventional criminal acts. While retaining the essential nature of traditional crimes, they differ significantly in three aspects: methods of commission, patterns of offender involvement, and causal relationships. These differences are precisely why traditional criminal regulations cannot be directly applied, leading to a series of challenges. By analyzing the technical features of generative AI and potential criminal scenarios arising in judicial practice, it becomes clear that this new form of intelligent crime primarily exhibits three distinct characteristics.

2.1. The highly concealed nature of criminal acts

Traditional criminal offenses are primarily committed by individuals who directly and personally carry out the actions, with the entire process being tangible, traceable, and visible. Evidence such as physical items, written documents, and audiovisual materials can be used to fix and reflect subjective intent, procedures, and methods. However, the automated operation mode of generative AI has fundamentally disrupted conventional methods of committing crimes, significantly enhancing the concealment of illegal activities. Offenders no longer need to be directly involved; they merely input instructions and set a few parameters to generate fake audio and video content, forge official documents, precisely craft fraudulent scripts, or synthesize infringing images and text. At the core of these actions is algorithmic automation, requiring minimal human involvement, leaving almost no traceable evidence in the traditional sense. Currently, generative AI possesses remarkable simulation capabilities—deepfaked facial images, voice recordings, contracts, and identity documents appear highly authentic, making them nearly indistinguishable from real ones for ordinary individuals and standard technical verification methods. This greatly reduces the likelihood of detection. From a judicial perspective, the non-contact nature of these operations weakens traditional elements of evidence collection. With limited digital footprints, low identifiability, and virtual execution, law enforcement agencies face increased challenges in investigation, evidence gathering, and judicial assessment ^[1].

2.2. Ambiguity in the boundaries of criminal actors

Traditional criminal acts are characterized by a single, clear, and direct subject—the offender is clearly identifiable, with a defined identity, distinct conduct, and unambiguous liability. In contrast, crimes involving generative AI arise from a complex, multi-party structure encompassing algorithm design, data training, and service invocation. Multiple parties—including algorithm developers, AI platform providers, end users, and third-party operators—participate throughout the process. Their actions intertwine and cascade through layers, collectively contributing to the criminal outcome, thereby completely overturning the traditional model of singular criminal responsibility. From a technical standpoint, algorithm designers determine output outcomes through model development and parameter configuration; AI platform providers offer support and

services via technological infrastructure, computational power, and operational maintenance; while end users carry out specific illegal activities by inputting prompts. Each actor plays an indispensable role in this chain of causation. However, in judicial practice, the perceived “neutrality” of AI technology has become a primary defense for platform providers and algorithm developers seeking to evade criminal liability. They argue that as mere technology suppliers, they only provide neutral tools and online services, did not directly commit the crime, and thus should not be held responsible for users’ malicious use ^[2]. Meanwhile, actual users often downplay their own subjective culpability and influence, attributing the consequences to the autonomous functions of AI systems. As a result, the boundaries among these actors remain blurred, their respective contributions indistinct, making it easy for core offenders to escape accountability, for secondary participants to blur their roles, and for certain actions to go unpunished.

2.3. Difficulty in establishing causality

The traditional criminal justice system’s mechanisms for conviction and sentencing are based on causality, where conventional criminal acts have a direct, necessary, and clear logical connection to the resulting harm. In such cases, the commission of an offense directly leads to harmful consequences, enabling judicial authorities to clearly assign liability and precisely determine penalties by applying the principle of direct causation. However, crimes involving generative AI involve multiple layers of technological transmission, actions by multiple actors, and algorithmic probabilistic outputs—factors that completely undermine the traditional model of single, direct causation. The harmful outcomes in these cases are not caused by a single act but may instead result from a combination of factors, including flaws in algorithm design, inadequate platform monitoring and review, insufficient risk control mechanisms, malicious user exploitation of AI tools, and deviations arising from autonomous algorithm evolution. This multi-factorial causation is highly evident. Moreover, due to the inherent characteristics of large-scale generative AI models—such as self-learning, iterative improvement, and probabilistic content generation—the output of these models carries a degree of uncertainty or autonomy. As a result, certain illegal outcomes do not entirely depend on user input instructions but may emerge from the algorithm’s independent operation or deviations during its iterative process. This further weakens the direct link between human actions and harmful consequences, rendering traditional principles of direct and substantial causation ineffective. It also hinders judicial authorities from accurately assessing the contribution of each actor’s conduct to the damage, thereby complicating the processes of conviction and sentencing ^[3].

3. Legal challenges in applying criminal law to new forms of AI-driven intelligent crime

China’s criminal legal system has been developed based on traditional social structures, establishing rules and judicial frameworks primarily for conventional natural crimes and routine cybercrimes. However, intelligent crimes arising from generative AI present unique technical characteristics that differ fundamentally from past forms of crime, resulting in inadequate adaptability of existing legal norms. This manifests in multiple difficulties, including challenges related to criminal charges, liability, mens rea, and the coordination of regulatory mechanisms.

3.1. Traditional criminal offenses are rigid, leading to regulatory misalignment

The current Chinese Criminal Code's substantive provisions are primarily structured around traditional violent crimes and generalized cybercrimes. The criminal law and its judicial interpretations regarding cybercrimes, intellectual property offenses, and fraud are more suited to crimes committed manually in conventional online environments, failing to account for the new characteristics of generative AI—such as automation, intelligence, and mass production—resulting in a situation where legal charges are inadequately applicable. In current judicial practice, there is a lack of appropriate criminal charges to address emerging issues such as AI deepfake fraud, AI-generated infringing works, AI-driven dissemination of false information, and data theft by AI web crawlers. As a result, these acts can only be loosely regulated under traditional offenses like fraud, copyright infringement, illegal use of information networks, and unlawful acquisition of citizens' personal information. The elements, conduct standards, and requirements for subjective fault of these traditional offenses are all based on conventional criminal patterns, which clearly deviate significantly from the behavioral models and harmful characteristics of AI-related crimes. For instance, traditional fraud requires active acts such as fabricating false facts or concealing the truth to obtain property through deception. In contrast, AI-powered fraud involves algorithms automatically generating fraudulent content and mass-distributing it, thereby weakening the characteristic of human agency typically associated with deliberate fraudulent acts. Traditional copyright infringement offenses target individuals who copy or distribute works and are not applicable to AI's bulk generation of content. In judicial practice, it is common to encounter situations where certain AI behaviors do not meet the traditional elements of criminal offenses, or where subjective components fail to be established, making it difficult to convict. Alternatively, there are instances where convictions are stretched to achieve punitive goals, or even minor offenses are punished excessively. Such practices lead to regulatory gaps and judicial misjudgments, violate the principles of legality of crimes and punishments and proportionality between guilt and penalty, undermine judicial fairness, and erode judicial authority ^[4-5].

3.2. Unclear division of responsibilities among multiple parties, with a lack of standards for assigning liability

The multi-layered structure of participants involved in generative AI-related crimes has created unprecedented challenges in criminal liability attribution under traditional criminal law, as current legal frameworks have yet to establish differentiated liability mechanisms tailored to the diverse applications of artificial intelligence technology. From a judicial practice perspective, end users who directly and maliciously employ AI tools to commit fraud, infringement, or defamation clearly demonstrate intent, engage in concrete and direct conduct, and thus face uncontroversial liability determination with well-defined accountability pathways. However, algorithm developers and platform providers remain contentious figures in current judicial rulings due to ongoing debate over their criminal responsibility. Most AI service providers currently invoke the “technological neutrality” defense, arguing that they merely supply foundational, tool-like AI services without direct involvement in users' specific actions and lack control over subsequent usage, thereby claiming no liability for users' misconduct or criminal acts. Yet, in reality, certain algorithmic platforms fail to fulfill basic obligations such as risk assessment, content moderation, early warning systems, and access control during algorithm development, model deployment, and daily operations. They overlook the potential for illegal content generation by algorithms and the risks of model misuse, thereby providing critical

technological conditions and channels for criminals to exploit AI for unlawful purposes^[6]. Meanwhile, existing criminal laws and AI regulatory standards have not yet established clear criteria regarding the duty of safety assurance and risk prevention for AI service providers. The boundaries concerning technological neutrality, negligent performance, and intentional disregard remain ambiguous, making it difficult for courts to determine fault on the part of algorithm platforms or designers. As a result, a prevailing pattern has emerged in judicial practice: users are held accountable while providers escape liability, leading to extremely low legal costs for higher-level technical actors. This results in widespread cases where technology enables crime but remains unaccountable—a situation that profoundly violates the principles of personal responsibility and proportionate punishment.

3.3. Difficulty in establishing subjective fault and lack of support for criminal elements

Subjective fault is a core component of criminal liability. Traditional criminal law determines an offender's intent or negligence by comprehensively examining factors such as conduct, criminal purpose, pre- and post-event behavior, and awareness of harmful consequences—these serve as crucial bases for establishing criminal responsibility. However, in crimes involving generative artificial intelligence, the intelligent and automated nature of criminal activities significantly dilutes the manifestation of the actor's will and psychological state, making it difficult to establish subjective elements. Without sufficient evidence of subjective intent, many unlawful acts become hard to prosecute. First, criminals exploit the autonomous operation of AI algorithms to conceal their malicious motives within technical processes. By issuing simple commands, they trigger entire criminal sequences, after which all illegal content generation, dissemination, and rights violations are carried out automatically by the algorithm. This greatly weakens the behavioral indicators of human will, rendering it impossible to infer subjective intent through the chain of actions. Second, the probabilistic nature and self-generative characteristics of generative AI mean that outputs are inherently uncertain. As a result, there may be discrepancies between the actor's original intentions and the actual harmful outcomes. Consequently, defendants often argue that the results were due to technical errors or that they were unaware of the risks, claiming no knowledge of the consequences and thus denying both intent and negligence. Third, some offenders take full advantage of AI's strong concealment and difficulty in tracing origins to carry out large-scale illegal activities, cloaking their personal intentions behind technological operations to evade legal accountability. In sum, these circumstances lead to numerous AI-related offenses being unable to be prosecuted due to the absence of this essential element—subjective fault—leaving significant gaps in judicial oversight.

3.4. Incomplete legal regulatory system and poor coordination with criminal penalties

Currently, China's governance of generative artificial intelligence exhibits an imbalance characterized by “strict administrative oversight but lagging criminal regulation,” with particular prominence given to the incomplete legal regulatory framework and poor coordination between administrative and criminal enforcement. In recent years, China has successively issued regulatory documents such as the Interim Measures for the Management of Generative Artificial Intelligence Services, aiming to ensure AI compliance, prevent technological risks, and standardize content. These measures have established a preliminary comprehensive administrative supervision system for AI service providers and clarified administrative liability for violations related to AI services. However, corresponding criminal laws remain

severely inadequate. There are no specialized regulations specifically targeting intelligent crimes involving generative AI, nor are there clear standards or boundaries defined for criminal accountability. This results in a significant disconnect between administrative regulations and criminal law provisions: certain behaviors that violate AI service compliance requirements and cause social harm can only be punished administratively through corrective orders, fines, or temporary suspension of operations, failing to meet the threshold for criminal prosecution and thus leaving serious socially harmful acts without adequate legal consequences. On the other hand, due to the lack of uniform standards for criminal adjudication, courts across different regions often differ significantly in applying charges, determining liability, and imposing sentences for similar cases, leading frequently to inconsistent outcomes—“same cases, different judgments; same crimes, different penalties.” As a result, judicial consistency and authority are difficult to ensure, undermining the effectiveness of criminal deterrence.

4. A pathway to improve legal application for new types of AI-driven intelligent crimes

The core challenge in judicial regulation of new forms of AI-related intelligent crimes does not stem from a fundamental failure of traditional criminal law to adapt to technological advancements, but rather from insufficient adaptability. Therefore, there is no need to overturn or discard the existing criminal legal framework and blindly create new categories of offenses. Instead, within the current legal system, effective regulation of emerging intelligent crimes can be achieved by refining specific application rules based on the technical characteristics of AI-related offenses and addressing practical difficulties encountered in judicial practice. This includes clarifying liability attribution, improving standards for determination, and strengthening the regulatory framework—ultimately enabling precise and proportionate oversight while safeguarding both technological innovation and public safety.

4.1. Clarify the application of traditional criminal offenses to address regulatory gaps

Criminal acts involving generative artificial intelligence do not necessarily require the creation of new, independent offenses. The key lies in refining the scope of application, conduct standards, and criteria for criminal liability of existing offenses through judicial interpretations and guiding cases. By leveraging traditional criminal charges as tools, officials can extend their reach to cover AI-related intelligent crimes, thereby resolving issues of rigid or misaligned application. Judicial authorities should match specific traditional offenses to different forms of AI-related crimes—such as deepfakes, AI-powered fraud, mass copyright infringement via AI, and automated rumor dissemination—clarifying the conduct standards applicable to each offense in AI contexts. For instance, regarding AI-generated deepfake-based fraud and extortion, the standards defining fraudulent acts and extortion must be further clarified, specifying that AI-generated content may serve as both a tool and factual basis for such crimes. With regard to AI’s large-scale generation and dissemination of copyrighted works, the criteria for establishing copyright infringement and illegal use of information networks should be made clearer, with explicit guidelines on sentencing for extensive automated violations. Additionally, provisions concerning the offense of disturbing public order and fabricating false information should be refined to address AI-generated misinformation disrupting social stability. At the same time, specialized judicial interpretations targeting AI-related crimes could standardize

the conduct criteria for AI-enabled offenses, clearly defining how criminal liability should be determined in cases of technological automation. This would eliminate overly rigid and unreasonable requirements from traditional criminal law that are ill-suited to intelligent crimes, preventing unjustified convictions or excessive penalties. Strict adherence to the principles of legality of crime and punishment and proportionality between guilt and penalty will ensure seamless integration between emerging AI-related offenses and existing legal frameworks, effectively filling current regulatory gaps and shortcomings in this area.

4.2. Tiered liability allocation to clarify responsibility

Given the complex and multi-party involvement structure in generative AI-related crimes, traditional one-way liability models should be abandoned in favor of a differentiated criminal liability mechanism based on “tiered and categorized assessment, proportionality of wrongdoing, and commensurate punishment.” This approach aims to reasonably allocate responsibility among users, algorithm developers, and platform providers, resolving issues of ambiguous accountability and imbalanced enforcement.

First, end users should be fully held criminally liable as direct perpetrators of harmful outcomes, strictly according to the subjective malice and direct actions required by relevant criminal charges. They must be convicted and sentenced accordingly under the law, with no excuse allowed for evading liability by claiming they merely used a tool.

Second, criminal liability for algorithm developers should strictly adhere to the principle of technological neutrality. Developers should not face criminal liability for normal algorithm development without fault. However, if they intentionally introduce algorithmic vulnerabilities, deliberately retain features enabling illegal content generation, or knowingly design algorithms intended for criminal use and then allow such designs to be upgraded, they may be held liable as accomplices or separately punished depending on their role—balancing innovation protection with effective enforcement against misconduct.

Third, the specific obligations of generative AI platform providers regarding security review and risk control must be clearly defined. If platforms fail to fulfill reasonable supervisory duties, allow unlawful AI-generated content to proliferate, or negligently disregard risks of technology abuse, they should be held criminally liable for negligence. The platform’s responsibilities in algorithm auditing, content moderation, risk early warning, user management, and vulnerability remediation should be further specified. Through this tiered liability framework, the previous imbalance—where users bear all blame while providers remain unaccountable—can be fundamentally transformed, ensuring that each party bears appropriate liability in proportion to its fault and receives just punishment.

4.3. Refining standards for causation and subjective fault

Given the technical characteristics of generative AI-related crimes, traditional approaches to legal determination must be transcended. A new judicial framework for assessing causation and subjective fault in the age of artificial intelligence should be established. To address challenges in determining causal efficacy, the conventional one-dimensional and direct causality standard should be abandoned in favor of objective liability as the foundational criterion. The focus should be on whether each actor’s conduct created a legally impermissible risk, whether that risk materialized within the specific criminal context, and whether the resulting harm can be attributed to such risk. This approach enables precise identification of the legal causal relationship between each individual’s actions and the outcome, even in cases involving multiple causes

leading to a single effect, while also quantifying the degree of each party's contribution.

Regarding the assessment of subjective fault, a mechanism should be developed whereby “objective conduct proves subjective intent.” This replaces the outdated reliance on confessions alone to infer an individual's mental state. Instead, a comprehensive evaluation should consider multiple dimensions: the specific circumstances surrounding the act (including AI application scenarios, operational command logs, purpose of use, technological proficiency, post-action attitudes, and actual consequences). Based on this holistic analysis, it becomes possible to determine whether the relevant parties acted intentionally or negligently. Furthermore, clear criteria should be defined for presuming intentional misconduct—specifically, when individuals exploit AI's concealment, anonymity, and traceless features to commit illegal acts on a large scale, or when they knowingly use AI despite awareness of its potential for unlawful output and continue doing so while allowing harmful consequences to unfold. In such cases, subjective intent may be directly presumed. This approach effectively resolves the difficulty of establishing subjective fault and provides essential judicial support for scientifically appropriate sentencing.

4.4. Improve the regulatory framework and streamline the administrative-criminal connection mechanism

To meet the demands of modernizing intelligent social governance, a legal regulatory mechanism for generative AI should be established based on integrating administrative oversight and criminal justice rules—characterized by “administrative supervision as a front measure, criminal liability as a fallback, tiered regulation, and seamless coordination.” This approach aims to overcome current shortcomings in the existing regulatory system, such as regulatory delays, inadequate administrative-criminal linkage, and inconsistent judicial standards.

First, AI compliance oversight and criminal liability criteria should be unified and structured in a graduated manner. The specific statutory compliance obligations of generative AI service providers must be clearly defined, and the threshold distinguishing illegal administrative acts from criminal offenses involving AI should be clarified. Standards for categorizing violations into minor infractions, general violations, and serious crimes should be established. For minor violations with limited harm, appropriate administrative penalties—including orders to rectify and credit-based sanctions—should be applied. In contrast, when violations are severe and result in personal injury, significant property damage, disruption of public order, or threats to social security, criminal liability mechanisms should be triggered to pursue corresponding criminal charges. This ensures effective coordination between administrative and criminal penalties, enabling a tiered and proportionate response.

Second, nationwide consistency in judicial rulings for various intelligent crime cases should be achieved. The highest judicial authorities may issue guiding cases and judicial opinions based on typical AI-related criminal cases to standardize criteria regarding specific criminal charges, liability allocation, and sentencing for emerging AI-related offenses. This will effectively resolve the problem of inconsistent judgments in similar cases and ensure uniformity in judicial outcomes. Ultimately, this will foster a rule-of-law governance model that integrates functional innovation, risk control, and precise accountability. It will rigorously punish all forms of intelligent crime while maintaining a bottom-line mindset that preserves sufficient room for AI technological advancement and industrial development, ensuring dynamic balance and coordinated progress between technological innovation and societal safety.

5. Conclusion

The explosive development of generative AI technology is an inevitable requirement of the digital era. The new forms of intelligent crime it has generated are not entirely novel categories of offenses, but rather a series of legal application challenges arising from traditional crimes taking on distorted forms through intelligent technologies. At its core, this reflects a mismatch between the traditional criminal law framework and the rapid pace of technological advancement, as well as an incompatibility between conventional judicial standards and the evolving patterns of intelligent criminal conduct. To address these emerging legal challenges in the age of intelligence, there is no need to reconstruct the entire criminal law system or judicial structure; instead, officials should improve regulatory approaches by focusing on specific problems, guided by technical characteristics and judicial practice. This includes clarifying the criteria for applying traditional criminal charges, establishing a tiered liability mechanism, refining relevant judicial regulations, and building a comprehensive system for administrative-criminal coordination to precisely resolve issues related to the conviction, attribution, and adjudication of new intelligent crimes. This will enable precise governance and appropriate oversight of AI-related offenses. By strictly punishing intelligent criminal acts and safeguarding cybersecurity and social stability, while adhering to the principle of inclusive and cautious regulation, officials can balance technological innovation with legal security, ensure the healthy, orderly, and high-quality development of the generative AI industry, and advance the modernization of legal systems and capabilities in intelligent societies.

Disclosure statement

The author declares no conflict of interest.

References

- [1] Chen XB, Yin JH, 2026, Risk Classification and Hierarchical Governance of Criminal Offenses Involving False Information from Generative Artificial Intelligence. *Journal of Kunming University of Science and Technology (Social Sciences Edition)*, 26(1): 1–11.
- [2] Li YT, Guo HX, 2025, Prevention and Governance of Criminal Risks in Generative Artificial Intelligence. *People's Procuratorate*, 2025(24): 105.
- [3] Zhang HR, 2024, Exploring New Types of Fraud Crimes Caused by Generative Artificial Intelligence. *Legal Forum*, 2024(3): 143–157.
- [4] Shi HT, 2025, Research on the Mechanism and Countermeasures of New Types of Crime Driven by Artificial Intelligence. *Proceedings of the 2025 Academic Exchange Conference on Social Development and Innovation*. China Association for Intelligent Engineering, China Association for Intelligent Engineering, 2025: 3.
- [5] Li SJ, 2024, Study on Criminal Law Regulation of Crimes Involving Weak Artificial Intelligence, thesis, People's Public Security University of China.
- [6] Sun DX, 2023, Knowledge Deconstruction and Criminal Law Responses to Artificial Intelligence Crime. *Youth Crime Issues*, 2023(2): 4–19.

Publisher's note

Bio-Byword Scientific Publishing remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.