WEP Warwick Evans Publishing

Transactions on Social Science, Education and Humanities Research
ISSN: 2960-1770, eISSN: 2960-2262 | Volume 14
LHPPR 2025

The Impact of Generative Artificial Intelligence on the Protection of Data Legal Interests in Criminal Law: A Case Study of ChatGPT

Yuanhao Xu *

School of law, Jiangsu University, Zhenjiang 212000, China

* Corresponding Author Email: 3220806048@stmail.ujs.edu.cn

Abstract. The rapid advancement of generative artificial intelligence (GAI) poses significant challenges to the current framework of data legal interest protection under Chinese criminal law. Represented by models such as ChatGPT, GAI systems possess powerful capabilities in data extraction, analysis, and generation. Even when data is obtained legally, the use of deep mining, correlation analysis, and multimodal outputs may give rise to new forms of data-related criminal risks. However, China's current criminal law framework, which centers on "data control" and emphasizes the protection of data at the source, lacks adequate regulation over behaviors characterized by "lawful acquisition + unlawful analysis." In addition, existing issues such as the outdated classification of criminal offenses, ambiguity in identifying responsible actors, and disproportionately lenient sentencing standards have further endangered the effective protection of data-related legal interests. To address these emerging challenges, criminal law should evolve by expanding the scope of liability, improving legislative frameworks, enhancing regulatory coordination, and restructuring penal models. These efforts would facilitate a paradigm shift in governance from "data control" to "data utilization", aiming to reconcile the tension between technological innovation and the protection of legal interests.

Keywords: Generative Artificial Intelligence; Data Legal Interests in Criminal Law; Lag of Criminal Law; Responsible Entities; Sentencing Models.

1. Introduction

The Fourth Technological Revolution is advancing with irresistible force, rendering artificial intelligence (AI) an integral component of contemporary human life. With the continuous evolution of data acquisition capabilities and technological innovation, AI has assumed a novel form. In contrast to traditional AI, which primarily performs data processing and analysis, generative AI possesses the ability to internalize and replicate underlying patterns of reality, enabling it to autonomously generate logically consistent and semantically coherent content in response to user input [1]. Undeniably, the benefits that AI has conferred upon society are unprecedented: whether in terms of enhanced accessibility to information or the increased efficiency of service provision, AI continues to profoundly improve human experiences and interactions in various domains.

Nevertheless, like any transformative technology, artificial intelligence entails a duality that cannot be overlooked. ChatGPT, as a representative application of generative AI, has elicited growing concerns regarding employment displacement, infringement of personal privacy, and challenges to data protection. In this context, the legal system is called upon to perform its normative and regulatory functions. Legislative authorities in China have promulgated a series of legal instruments—such as the Cybersecurity Law, Data Security Law, and Personal Information Protection Law—with the aim of strengthening ex ante data safeguards and constructing a robust legal and institutional framework for data security governance [2]. Within the realm of criminal law, not only have existing statutory provisions encompassed data-related offenses since the inception of the Criminal Code, but subsequent amendments have also expanded and refined the scope of such offenses. At present, system of data crimes in China includes both computer-related offenses under traditional data-use scenarios (e.g., the crime of sabotaging computer information systems, the crime of illegally acquiring data from computer systems), and information-content-based offenses classified by the nature of the data's semantic content (e.g., infringement of personal information, misappropriation of trade secrets,

and illegal acquisition of state or military secrets) [3]. However, the inherent lag of legislative processes raises critical doubts as to whether the current criminal law framework is sufficiently equipped to address the novel legal dilemmas introduced by generative AI. Contemporary generative AI exhibits characteristics such as potent content generation capabilities, multimodal outputs, architectural diversity, and expansive applicability. Yet, existing legal regulation continues to concentrate on illegal data acquisition and control at the source level. Given that the datasets employed by generative AI are often publicly accessible and legally obtained, most of its outputs currently escape the scope of criminal liability under existing law. Against this backdrop, this paper seeks to examine the legal tensions between generative AI and criminal law, identify normative blind spots and regulatory deficiencies, and propose constructive recommendations to enhance the capacity of criminal law to respond to data-driven technological transformations—thereby reinforcing its subsidiary and residual regulatory function.

2. The Operational Logic of Generative Artificial Intelligence

Taking ChatGPT as a representative example, its core functionality is underpinned by natural language processing (NLP) technologies, with its technical foundation rooted in the application of deep learning neural networks to train a large-scale language model known as GPT (Generative Pre-trained Transformer). Through the ingestion and analysis of vast corpora of textual data, this model acquires the capacity to comprehend and generate human-like natural language expressions [4]. The entire process can be conceptually divided into three main stages: data preparation, computational processing, and content generation.

In the data preparation stage, generative AI systems rely on massive, heterogeneous datasets as the foundation for deep learning-based imitation. These datasets are not only voluminous but also diverse in content, encompassing textual, audio, and visual modalities. Moreover, their sources span a broad range of channels, including manually labeled datasets, sensor-acquired data, observational data, and analytically derived metrics. The resulting data chain is highly complex, enabling deep learning algorithms to acquire what is referred to as transferable knowledge representation capacity, or the "ability to generalize insights into the nature of knowledge" [5]. Following data collection, generative AI systems apply machine learning techniques to translate raw data into machine-interpretable representations. This transformation is critical for training generative models, as it enables the identification of latent structures and patterns within the data through statistical analysis and learning algorithms, thereby producing meaningful input for subsequent model training [6].

The computational processing stage involves key operations such as user feedback incorporation, data preprocessing, feature extraction, and model training. These elements collectively form the technical backbone of model learning and content generation. The central objective of this phase is to convert the massive volumes of raw data into structured formats interpretable by machines, extracting salient features that allow generative models to better process and internalize information. Consequently, these models can generate diverse, novel, and contextually appropriate outputs [6].

Finally, in the content generation stage, generative AI systems utilize the representations and patterns learned during the previous stages to derive a generalized operational mechanism. Based on user inputs, the system encodes prompts or initial data into vector representations understandable by the model. These vectors are further processed through contextual encoders to capture semantic meaning, structural logic, and implicit relationships. The output is then generated progressively through a token-by-token decoding process, often involving techniques such as reverse diffusion to synthesize the final output.

These three stages together form the core generative loop of systems like ChatGPT. As the analysis above demonstrates, data constitutes the very foundation of ChatGPT's operational mechanism. However, within the current legal framework, ChatGPT's extensive data acquisition activities—whether involving massive pre-collected foundational datasets, user-generated data during interactions, or self-derived data generated through autonomous learning algorithms—may

unavoidably result in the infringement of legally protected data interests associated with each of these categories. Yet,existing legal infrastructure in China appears insufficient to adequately address such risks. The following section will provide a detailed analysis of the current shortcomings in legal regulation and explore potential pathways for more effective governance.

3. Legal Issues Arising from Generative Artificial Intelligence

3.1. Autonomous Data Infringement by Generative Artificial Intelligence

3.1.1. Autonomous and Unauthorized Data Acquisition.

In the current digital era, data proliferation has reached an explosive scale, with diverse types of data emerging incessantly. As generative AI evolves through continuous learning, it absorbs and integrates ever-increasing volumes of information. However, vast amounts of data circulating on the Internet include personal information disclosed without the consent of data subjects, and even illicit data of questionable legality. In the course of periodic database updates, generative AI systems leverage their powerful data scraping capabilities to incorporate this content into their training corpora. At present, AI systems lack the capacity for normative judgment regarding the legality of data sources. ChatGPT, for instance, extracts data solely based on algorithmic access protocols, without the ability to discern whether the data was lawfully obtained. This raises substantial risk of infringing upon the data rights of individuals and entities. Furthermore, ChatGPT currently lacks real-time correction mechanisms capable of addressing post hoc changes in data legality. Content that may have been lawfully published at the time of acquisition could, through subsequent developments, become privacy- or rights-infringing; yet, ChatGPT is unable to autonomously rectify such retroactive violations. Accordingly, generative AI systems are prone to the unauthorized acquisition of sensitive or protected data.

3.1.2. Autonomous and Unauthorized Data Disclosure.

Massive datasets are foundational to the development of generative AI. ChatGPT, in particular, relies heavily on large-scale datasets to improve its performance. Among the data analyzed during training, a significant portion may contain inadequately anonymized personal information. Although OpenAI has claimed that data has been anonymized, large language models can, through mechanisms of "memorization and reconstruction," reproduce fragments of training data containing private details [7]. There have been documented cases where system vulnerabilities led to the accidental disclosure of users' personal data to other users, including names, chat histories, and even sensitive information such as credit card numbers [8]. In 2023, the Italian Data Protection Authority fined OpenAI €15 million for suspected violations of the EU General Data Protection Regulation (GDPR). Moreover, publicly available data is inherently limited in scope and cannot ensure the comprehensiveness of AI-generated responses. To enhance output quality, generative AI may resort to deep data mining, which involves the storage, analysis, and secondary use of user interactions. Such practices significantly increase the likelihood of disclosing trade secrets or personal data. These developments underscore the profound impact that ChatGPT may exert on data protection interests.

3.1.3. Autonomous and Unauthorized Data Usage.

As the computational power of generative AI continues to grow, so does its ability to generate context-specific responses based on user input. However, AI systems fundamentally lack human-level cognition, and rely solely on their internal datasets when generating replies. When confronted with queries, generative AI does not make decisions based on intent or ethical reasoning, but rather retrieves and assembles content according to internal algorithmic patterns. This process introduces risks of unauthorized or infringing responses, especially in cases where the dataset includes multiple conflicting answers. The algorithm may, without developer oversight, select and reproduce data in a manner that constitutes infringement. For instance, in 2024, a company released an editing software that, when given prompts related to the television series Joy of Life, could automatically generate 37-second video clips—without authorization from the rights holder, who subsequently filed a lawsuit

[9]. In such cases, the AI system, acting autonomously based on its learned data usage patterns, illegally used data in a way that violated intellectual property rights. If the AI's output arises not from any direct human instruction but from autonomous learning mechanisms, then there exists a non-trivial legal risk of "spontaneous" unauthorized data use by the AI [10].

3.2. Illegal Exploitation of Generative AI by Malicious Actors

3.2.1. Malicious Use of Generative AI to Infringe Data Rights.

While ChatGPT has undoubtedly enhanced academic productivity and daily convenience, it has also, inadvertently, created new vectors for criminal misuse. For instance, ChatGPT can generate high volumes of highly realistic fake videos and text, which may be exploited by malicious actors to destabilize public trust and societal order. As the model becomes increasingly powerful, it may facilitate the automation, industrialization, and scaling of criminal activities. One concern lies in ChatGPT's code-generation capabilities: while useful for legitimate development, they can also lower the technical barrier for cybercrime. If the model is exploited to automate the creation of malicious software or web crawlers for data theft, the resulting damage—especially to entities with weak cybersecurity defenses—could be severe. Moreover, black and grey markets are already integrating ChatGPT into automated fraud operations, such as generating phishing emails that mimic familiar speech patterns, or fabricating identity information for use in fake reviews and money laundering. These developments present a substantial threat to data security and legal order.

3.2.2. Malicious Use of Generative AI to Illegally Acquire Data.

In the contemporary information economy, data equates to competitive advantage. Exploiting current deficiencies in ChatGPT's data protection mechanisms, malicious actors have devised methods to coax sensitive information from the model. In 2022, researchers demonstrated that GPT-3.5 could be prompted to output fragments of its training data containing real telephone numbers , exposing significant vulnerabilities. Given ChatGPT's powerful data retrieval abilities, bad actors have also begun to apply these tools in financial markets, where the ability to process information quickly directly impacts investment outcomes [11]. As a result, developers or users of generative AI may leverage proprietary datasets to manipulate or monopolize market behavior, thereby amplifying information asymmetries. Furthermore, ChatGPT's strong inferential capabilities make it susceptible to abuse in crime facilitation. If a user queries ChatGPT for advice on committing illegal acts and receives a detailed response, this may fall under the offense of "teaching criminal methods" as defined in Article 295 of China's Criminal Law. Such interactions threaten not only economic security but also broader social and institutional stability. Consequently, the improper use of generative AI by malicious actors poses serious challenges to the integrity of economic systems, public order, and the rule of law.

4. The Current Legal Status in China

4.1. The Present State of China's Criminal Law

Following the enactment of the Amendments (VII), Amendments (IX), and Amendments (XI) to the Criminal Law of the People's Republic of China, and in conjunction with existing provisions under the original Criminal Code, a relatively comprehensive legal framework for the regulation of data-related offenses has emerged, reflecting clear regulatory priorities. From a structural perspective, the offenses that protect data-related legal interests may be categorized into two groups: those that directly address data-related violations and those that do so indirectly.

Direct regulation includes offenses such as the infringement of citizens' personal information and the illegal acquisition of computer system data at the data acquisition stage; the offense of sabotaging computer systems and copyright infringement at the data processing and generation stage; and the failure to fulfill cybersecurity management obligations or the facilitation of cybercrime at the data dissemination stage. These offenses, especially those stemming from Amendment (VII), demonstrate

China's emphasis on protecting data interests at the source. This reveals a regulatory logic centered on "data control," which seeks to prevent unauthorized access, dissemination, or interference with data, thereby reinforcing the exclusivity of the data subject's control over their own data [12].

Indirect regulation refers to situations in which the act of data infringement is not explicitly criminalized, but falls within broader statutory categories. For instance, if a perpetrator facilitates data theft by others via information networks, this may constitute the offense of facilitating cybercrime. The theft, disclosure, or misuse of trade secrets in electronic form may fall under the offense of infringing trade secrets. The acquisition of state secrets by means of purchase or theft may amount to the offense of illegally obtaining state secrets. Similarly, using data to commit traditional offenses could constitute fraud or theft. Unlike direct regulation, these offenses are not premised on the data abuse itself but on the broader consequences or context of the act. As such, China's criminal law does not yet reflect a "data use–oriented" regulatory model, which would refrain from prohibiting all acts of access and use, and instead focus on curbing harmful or abusive use, in an attempt to balance data subjects' rights with the social value of data utilization [12].

In sum, both the number of statutory provisions and the nature of offenses illustrate that lawmakers in China continue to prioritize the suppression of unauthorized data control, reflecting a predominantly "data control–oriented" approach [13]. However, in the face of rapid technological progress and the exponential growth of AI capabilities, this model is increasingly inadequate. The following sections analyze how generative AI challenges the protective scope of criminal law regarding data interests.

4.2. The Impact of Generative Artificial Intelligence on Criminal Protection of Data Interests

4.2.1. The Lag in China's Criminal Legal System.

When ChatGPT engages in the unlawful acquisition of data at the source, it may still fall under offenses such as infringement of personal information. However, in cases where ChatGPT lawfully collects publicly available data and subsequently engages in illegitimate or harmful analysis, such as the extraction and use of deepfake biometric data, the existing criminal legal framework appears insufficient [14]. For instance, under Article 282 of the Criminal Code, the offense of illegally obtaining state secrets requires the subjective element of intent—namely, that the actor knowingly obtains classified state information. Yet, the powerful inferential and data aggregation capabilities of generative AI make it possible to extrapolate sensitive information such as military deployments or infrastructure details without the user possessing the requisite mens rea for criminal liability.

Moreover, data that seems benign in isolation can, through AI-enabled synthesis, be transformed into high-risk or sensitive information [15]. The lack of criminal regulation over such illegitimate data analysis behavior may encourage malicious actors to pursue "legal acquisition + illegal inference" schemes, circumventing legal liability while still harming protected data interests. As generative AI becomes more adept at mining and analyzing datasets, the challenges of safeguarding data rights under criminal law will increase exponentially.

Regrettably, China's criminal law does not provide adequate protection against the misuse of lawfully obtained data. While current legislation focuses on ensuring the data subject's control rights, it neglects the legal regulation of downstream processing and analysis. When actors legally obtain data but later misuse it, criminal sanctions are lacking. Since the collection is lawful, such actions do not satisfy the elements of Article 253-1 (infringement of personal information) and may, at most, incur civil or administrative liability under Article 66 of the Personal Information Protection Law.

Similarly, the criminal law lacks provisions addressing the misuse of API access. For instance, in a 2024 case adjudicated by the Guangdong High Court, the company Jian Yixun illegally accessed the Weibo server through unauthorized API calls, scraping massive backend data and selling it via the iDataAPI platform. The extracted data included personal information, comment history, and multimedia content, with over 2.179 billion API calls and profits exceeding ¥21.79 million [16]. Yet,

the final judgment imposed only a civil fine of ¥20 million. When egregious misuse of personal data is not subject to criminal penalties, the credibility of legal data protection is undermined. While this legislative gap may be understandable given the historical context, it is now imperative that the criminal legal framework be updated to address the threats posed by generative AI. Establishing more robust offense categories and revising statutory protections is no longer optional—it is essential.

4.2.2. Ambiguities in Attributing Criminal Responsibility.

Under current Chinese criminal law, criminal responsibility is limited to natural persons and legal persons. If the developer of ChatGPT were to intentionally engage in illegal conduct that infringes data-related interests, they would clearly bear liability. However, where ChatGPT lawfully collects data and autonomously engages in harmful analysis or dissemination, and the developer neither directs nor intends such outcomes, the legal framework provides no clear basis for attributing criminal responsibility [17].

Presently, there is no statutory provision in Chinese criminal law that allows for the attribution of criminal liability to generative AI systems themselves. Nonetheless, when illegal harm occurs, it cannot be ignored simply because it lacks a human actor. Whether developers can invoke the defense of "technological neutrality" to avoid liability remains a contentious issue and will require further legislative clarification.

Moreover, when users provide vague or seemingly benign prompts—such as “write a phishing email” or “simulate a family member asking for money”—questions arise as to whether the developer has instigated the crime, or whether algorithmic bias (rather than malice) triggered the result. These situations challenge the traditional requirement of “knowledge or foreseeability” under criminal law, and cast doubt on whether such conduct constitutes criminal facilitation. Hence, clarifying the scope and attribution of criminal responsibility in the age of AI is vital for effectively regulating the misuse of generative technologies.

4.2.3. Disproportionate Sentencing Relative to Harm.

The current sentencing framework for data-related crimes involving generative AI fails to reflect the scale and severity of potential harms. Consider the offense of infringing on personal information: according to judicial interpretations by the Supreme People’s Court and the Supreme People’s Procuratorate, the offense is considered “serious” if it involves more than 50 records of sensitive information or more than 5,000 general data records. Yet, GPT-4–based web crawlers can retrieve over 100,000 records per second, a scale not contemplated by existing law. Despite this technological leap, automated data extraction has not been listed as an aggravating factor.

This mismatch extends beyond privacy crimes. For example, in defamation cases, a message is deemed “serious” if it garners over 5,000 views or 500 reposts. These thresholds are wholly incompatible with the data generation and amplification capacity of large language models. Thus, updating sentencing standards and incorporating AI-specific aggravating factors is crucial to preserving the deterrent function of criminal law.

5. Regulatory Approaches

As technology and society continue to evolve, the computing power and data acquisition capabilities of generative artificial intelligence (AI) are expected to grow exponentially. In the data-driven era, the coupling between generative AI and data will deepen, giving rise to an increasing number of novel behaviors that infringe upon data-related legal interests [17]. To enhance the protection of such interests under criminal law and to establish viable governance pathways for regulating data-related offenses, this paper proposes three key approaches: expanding the scope of criminal liability subjects, refining existing offense categories, and correcting the disproportionate sentencing standards currently in place.

5.1. Expanding the Scope of Criminal Liability Through Legislation

According to the current provisions of China's Criminal Law, only two categories of entities qualify as subjects of criminal liability: legal entities explicitly stipulated by law, and natural persons possessing the capacity to bear criminal responsibility. Articles 17 and 18 of the Criminal Law state that age and mental condition are determining factors for the criminal responsibility of natural persons, while Article 30 requires that a legal entity can only bear criminal liability if it meets specific statutory conditions [18].

Under the traditional concept of criminal law, the capacity to commit a crime refers to an individual's ability to recognize and control their own behavior, which is understood as a combination of cognitive and volitional capabilities [19]. From this perspective, generative artificial intelligence (GAI) is, at present, merely a crystallization of human intelligence. Although its computational and output capabilities have demonstrated a potential comparable to that of the human brain, it remains an object that functions according to predefined data and algorithms. Consequently, it is generally held that GAI cannot, under any circumstances, be recognized as a subject of criminal responsibility.

However, with the continuous evolution of criminal behavior, and particularly following the emergence of GPT-4, generative AI has exhibited capabilities in logical reasoning and expressing intent. It can also be programmed to reflect the value preferences of its developers through algorithmic configurations [20]. Meanwhile, certain jurisdictions around the world have gradually begun to acknowledge the legal significance of GAI's conduct. If generative AI is deemed to bear no criminal liability under any circumstances, this could profoundly undermine the public's intuitive sense of justice in the realm of criminal law.

As previously explained, if the developers of generative AI act lawfully during its creation, it would be inappropriate to hold them criminally liable under current legal doctrine. At the same time, both a laissez-faire approach—simply turning a blind eye—and arbitrarily placing all responsibility on the developers are inadequate responses. If left unregulated, the legal interests in data protection, as safeguarded by criminal law, would become meaningless; victims' rights would be rendered illusory, and previous efforts to protect data rights would be completely negated. Conversely, if all liability is attributed to the developers, the uncertainty in AI-generated outputs would likely hinder further innovation. In the present era, where "science and technology constitute the primary productive force" [21], the development of generative AI technologies would inevitably suffer severe setbacks.

Therefore, the author believes it is indeed necessary to expand the recognition of subjects who may bear criminal responsibility. However, it should also be acknowledged that, within criminal law academia, a long-standing view maintains that AI should not be deemed qualified to commit criminal acts, holding that "no matter how advanced AI becomes, it can never possess human free will." Thus, an unrestricted recognition of AI as a criminal subject is also unacceptable. In light of this, the author proposes that legislators should, through legislation, grant generative AI a limited and conditional status as a subject of criminal liability—for example, by introducing a new provision following Article 18 of the Criminal Law, specifically addressing GAI's potential criminal subjectivity. This would enable the legal system to regulate GAI when it engages in criminal behavior outside the scope of its original programming [22].

The author indeed holds that the definition of criminally liable subjects should be expanded through legislation. However, this does not imply that all forms of artificial intelligence should be classified as such. Criminal law, as the ultimate safeguard for assigning responsibility, must still uphold the principle of restraint. Thus, the author argues that generative AI, by virtue of its capacity for analysis and reasoning, should be recognized as a subject of criminal liability, whereas weaker forms of AI—those lacking such analytical functions—need not fall within the scope of criminal liability. Weak AI is more akin to a tool created by humans to facilitate daily life; in such cases, it is unnecessary to impose excessive blame on the AI system itself. Instead, a limited criminal subject status should be granted specifically to generative AI.

In conclusion, China's Criminal Law should broaden its definition of criminally liable subjects. The current restriction to natural persons and legal entities is insufficient in addressing emerging legal realities. By granting generative AI the status of a criminal subject, the law can better reflect the public's intuitive sense of justice, and effectively avoid the awkward dilemma where unlawful acts committed by AI result in no legal accountability. This reform carries strong and immediate real-world significance.

5.2. Enriching the Current Criminal Law System

The existing criminal law framework in China exhibits certain deficiencies, particularly in its failure to incorporate a regulatory perspective on data utilization. As a result, when individuals engage in conduct that infringes upon the lawful rights and interests of others, criminal law often lacks the tools or mechanisms to respond effectively. Although new laws have been introduced in succession, China's regulatory system has not yet kept pace with the rapid development of generative artificial intelligence. In light of this, the author proposes several recommendations aimed at enhancing the current criminal law system and regulatory mechanisms, so as to provide more robust protection for data-related legal interests.

5.2.1. Establishing the Crime of Illicit Data Analysis.

The author defines illicit data analysis as the use of generative artificial intelligence (GAI) to conduct algorithmic analysis of data for the purpose of committing unlawful or criminal acts. As previously discussed, China's current criminal law framework contains significant regulatory gaps in addressing acts of data analysis. Data analysis constitutes a critical and indispensable link in the data processing chain of generative AI. Without this analytical component, GAI's ability to generate outputs from massive datasets would be severely curtailed. Some may argue that data analysis is merely a preparatory phase of data usage. However, this view is fundamentally flawed. Modern generative AI can perform deep mining and feature extraction on seemingly trivial data, revealing additional layers of sensitive information. For instance, even if an insurance company obtains users' pharmaceutical purchase data through lawful means, using GAI to infer the user's health status and deliver targeted insurance marketing would constitute an evident violation of individual privacy. Such conduct not only renders privacy protection ineffective but also paves the way for monopolistic practices in a data-driven ecosystem. Even if one could debate the degree of harm in such privacy infringements, more serious consequences arise when GAI is used to analyze vast amounts of raw data to extract information involving military deployments, scientific research, or other sensitive data concerning national security. This would pose a grave threat to social order and national interests. If such behavior is not subject to criminal regulation, then individuals may legally obtain large volumes of publicly accessible data and subsequently conduct illicit algorithmic analysis to derive sensitive or restricted information [23], thereby circumventing criminal sanctions altogether—an outcome clearly incompatible with the foundational principles of criminal justice.

In summary, illicit data analysis severely undermines the legal interests in data that criminal law is designed to protect. If left unregulated, continued advances in GAI may ultimately render the concept of "privacy" meaningless. Therefore, it is imperative to introduce the crime of illicit data analysis into the Criminal Law. This offense would help fill the existing legal vacuum by protecting individuals' rights to data autonomy, derivative data interests, and the orderly flow of data, while providing legal grounds for punishing conduct that disrupts data governance through unauthorized data analysis.

To ensure the deterrent and regulatory functions of this new crime, its statutory formulation must be clear and precise. Criminal law must articulate the scope and content of prohibited conduct with sufficient specificity so that individuals can reliably distinguish criminal from non-criminal behavior, and thereby ensure that no conduct is punished unless clearly proscribed by law [24]. The author will now elaborate on the constitutive elements of this proposed offense: First, the subject of this offense should be broadly defined to include both natural persons and legal entities. In the current era, access

to GAI is widely available, and both individuals and organizations are capable of engaging in the conduct in question. For individual offenders, both the direct actor and the technical decision-maker should fall within the scope of liability. For organizational offenders, both data controllers and technical service providers should be included. However, such a broad definition introduces a dilemma: excessively expanding the range of liable subjects may inadvertently stifle GAI development by inducing caution and hesitation in research and innovation. To mitigate this, it is necessary to introduce an exemption mechanism for specific subjects. For example, research institutions that meet certain legal or ethical standards could be exempted from liability. This would ensure that illegal behavior is curbed without unduly hindering scientific advancement.

Nevertheless, differentiated liability standards must be applied to different types of actors to avoid arbitrary or disordered accountability. For direct actors, liability should attach if they operate the analysis system in a manner that foreseeably causes harm. For technical decision-makers, liability should arise where they possess authority over the analysis process and are aware of its illegality. Data providers should be held liable if they intentionally supply datasets for the purpose of illegal analysis. Technical service providers should be liable if they fail to exercise due diligence, particularly in monitoring the purposes of user-conducted data analysis on their platforms. Second, the mental element (mens rea) of this offense requires that the actor be subjectively aware of the illegality of their actions. This awareness must be substantial and well-defined, consisting of two components: (1) the foreseeability of technical risks, and (2) knowledge of the data's legal status. Regarding the foreseeability of technical risks, actors must understand that their analytical methods may result in privacy breaches. For instance, employing GAN models to reverse-engineer training data could disclose the original dataset and expose sensitive information. Or, the actor may knowingly use GAI to draw inferences beyond the authorized scope of data use—such as when a user authorizes login data for online shopping, but the actor extrapolates health conditions from the same data.

As for knowledge of data illegality, extensive elaboration is unnecessary. Current criminal law already prohibits the illegal acquisition of personal information, trade secrets, and state secrets [23]. What must be emphasized here is that data may contain legally protected elements such as biometric information or personal trajectories, which are explicitly off-limits for analysis. If an individual is aware of such content within a dataset yet proceeds with analysis, the mental requirement of this offense is satisfied. It is worth noting, however, that when GAI systems autonomously engage in such conduct, they should be treated as a special case that does not require this mental element to be satisfied. Furthermore, in accordance with the principle of restraint in criminal law, the offense must be limited to intentional acts. Including negligent or grossly negligent conduct within the scope of criminal liability would produce a chilling effect on GAI research and development, thereby impeding technological progress.

Because the actus reus (objective element) of this offense is relatively clear—namely, the unauthorized analysis of data—it is necessary to clarify the specific legal interests protected by this offense. The author proposes a three-tiered model of protected data interests: 1. Basic data rights, including data integrity and interpretability; 2. Derivative data interests, such as rights associated with data products and relational data networks; 3. Systemic data ecology, encompassing the sustainability and renewability of data resources. By constructing the offense of illicit data analysis around these protected interests, criminal law can provide a comprehensive legal shield against the disruptive force of generative artificial intelligence.

5.2.2. Establishing the Crime of Illicit Data Manipulation.

Since the advent of generative artificial intelligence, its ability to manipulate data has increased significantly. As generative AI continues to develop, data manipulation may come to affect every stage and aspect of social life. This not only escalates risks to public safety but also increases systemic threats to the economic order and erodes the foundations of technological trust. It is therefore evident that the social harm of data manipulation has substantially intensified. However, China’s current

criminal law does not yet include provisions regulating such conduct. Accordingly, the author argues that, in order to fill this legislative gap, it is necessary to establish the crime of illicit data manipulation.

The author considers that the subject and object of the crime of illicit data manipulation are similar to those of the previously discussed crime of illicit data analysis and will not elaborate further here. As for the constitutive elements of this crime, the author believes that three aspects require particular clarification. The first concerns the objective element, which must be clearly categorized. If only general or abstract wording is used, the definiteness requirement of criminal law cannot be satisfied. In future data-related incidents, the proposed provision may be misapplied as a catch-all offense. This would not only contradict the legislative purpose of the offense but also significantly hinder the development of generative AI technologies. The author believes that the objective element of this crime can be primarily divided into three types: the first is data tampering, referring to the systematic falsification or destruction of structured data through technical means; the second is algorithm poisoning, referring to the deliberate input of misleading training data that leads generative AI models to produce harmful outputs; the third is data concealment, referring to the distortion of facts through data cleansing or selective disclosure techniques.

The second aspect is the subjective element. The mental state required for the crime of illicit data manipulation must be intent, either direct or indirect. That is, the actor must be aware that their conduct will affect the authenticity of the data system and either actively pursue or deliberately allow the occurrence of data pollution. Any mental state below intent should not be included. Cases where the authenticity of the data system is compromised due to negligence during scientific research or normal business operations should not fall within the scope of this offense.

The third aspect concerns the harmful consequences. Only when the consequences of the act reach a serious degree should it constitute this crime, so as to prevent overly broad application. The author proposes that the harmful consequences be divided into three categories: direct economic loss, disruption of social order, and threats to national security. Different threshold standards can be set according to the category of harm. For direct economic loss, the threshold can be defined as causing economic damage of over 10,000 yuan. This is not an arbitrary figure; according to the Interpretation by the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Law in Handling Criminal Cases Involving the Security of Computer Information Systems, economic loss exceeding 10,000 yuan constitutes a "serious circumstance." For disruption of social order, the threshold can be defined as triggering mass incidents or public opinion crises. For threats to national security, it can be defined as compromising the functionality of critical infrastructure or threatening key facilities.

In conclusion, the author believes that establishing the crime of illicit data manipulation is an appropriate measure to improve the current structure of China's criminal law. It would not only fill the legal void in regulating data manipulation behaviors but also help delineate the boundaries of safe technological application, thereby safeguarding both the realization of data value and the prevention of social risks.

5.3. Establishing a Comprehensive Regulatory Framework

5.3.1. Building a Robust Dynamic Compliance System.

In the current social context, constructing a robust and dynamic compliance system is essential. The State Council or other relevant regulatory bodies should promote the establishment of a full-process criminal compliance mechanism by generative AI developers—covering the entire chain from data collection to algorithm design to content generation. This would transform the administrative obligations stipulated in the Cybersecurity Law and Data Security Law into criteria for assessing "reasonable foreseeability" under criminal law.

As for institutional design, the first step is to review the legitimacy of data sources used by generative AI creators, ensuring compliance with legal requirements regarding data ownership and personal

information rights. Simultaneously, a traceability system should be established for data collection activities, enabling efficient investigation in the event of disputes or violations.

Second, algorithm design should be subject to appropriate regulation. Article 8 of the Provisions on the Administration of Algorithmic Recommendation Services mandates that algorithm service providers regularly audit and assess the logic, models, data, and outcomes of their algorithms and prohibits the deployment of models that induce addiction or excessive consumption, or that otherwise violate laws or ethics. This obligation should be partially transferred to public authorities. A mandatory algorithm registration system for generative AI should be established, particularly for high-risk models, requiring developers to disclose technical details such as dataset composition and bias correction mechanisms.

Third, a risk control system should be developed for the content generation phase. Standards for filtering generated content must be formulated. Developers should embed sensitive keyword libraries into generative models, such that if user inputs involve prohibited terms, content generation is automatically halted. Furthermore, real-time monitoring mechanisms and post-incident tracing systems should be implemented to detect abnormal outputs, restrict use by high-risk users, and prevent the dissemination of harmful content.

5.3.2. Transforming Administrative Obligations into Criteria for Criminal Law Foreseeability.

The author argues that where a company has fulfilled the obligations outlined in Article 21 of the Cybersecurity Law—which establishes a graded cybersecurity protection system requiring network operators to ensure protection against interference, damage, unauthorized access, and data leakage, theft, or alteration—as well as Article 27 of the Data Security Law, which mandates the development of a full-process data security management system, employee training, technical safeguards, and risk mitigation in internet-based data processing—then the developers of generative AI may be deemed to have fulfilled their duties and exercised substantive due care. As such, criminal liability should be excluded.

Conversely, if a company has failed to meet these obligations, a tiered legal consequence framework can be established to evaluate non-compliance. Enterprises that have taken partial compliance measures but failed to meet all requirements could be granted a grace period for corrective action, along with partial liability mitigation, thereby balancing legal deterrence with the encouragement of active remediation.

5.4. Rectifying the Unduly Lenient Criminal Sentencing Framework

As previously discussed regarding the mismatch between the sentencing standards for crimes involving the infringement of citizens' personal information in China, the current criminal punishment system remains insufficiently aligned with the threats that generative artificial intelligence poses to data-related legal interests. As a result, the benefits that offenders may gain from such conduct far exceed the legal costs they may bear. This significantly weakens the deterrent function of criminal law and encourages further misuse of generative AI to infringe upon citizens’ personal information, thereby undermining the very legal interests that criminal law is designed to protect. Consequently, restructuring the existing sentencing system and strengthening the punitive force of criminal law in the field of data protection is an urgent imperative. The author offers the following recommendations.

5.4.1. Introducing Aggravating Circumstances.

First, it is necessary to introduce aggravating circumstances, by designating the use of automated tools to obtain information as a statutory aggravating factor. For data-related crimes committed through AIGC, the sentencing range should be increased on the basis of traditional offenses of the same kind. In general, the upward adjustment should expand to the next statutory sentencing range, but must not exceed the maximum sentence for the specific offense. For instance, according to Article 253 (1) of the Criminal Law, which concerns the crime of infringing citizens’ personal information,

the basic sentence is fixed-term imprisonment of not more than three years, while serious cases are punishable by three to seven years. However, when automated tools are involved, the resulting harm increases exponentially, and thus the sentence for serious cases should be elevated from the original three to seven years to seven to fifteen years. Another example is the crime of infringing trade secrets under Article 219 of the Criminal Law, where the standard sentence is fixed-term imprisonment of not more than three years, and serious cases are punishable by three to ten years. If automated tools are used to reverse-engineer and extract information, the risk of leaking core trade secrets increases sharply. In this case, the original sentence of three to ten years should be elevated to ten to fifteen years.

However, this upward adjustment must not be arbitrary but should be based on a standardized model. The author believes that introducing a data-equivalent sentencing model is a suitable approach. This model is composed of a base sentence, magnitude factor, sensitivity level, harm coefficient, and an upper limit. The base sentence is set according to the lower bound of the aggravated sentencing range. The magnitude factor is calculated based on the quantity of personal data infringed, with each additional 10,000 records constituting a magnitude unit, and each unit adding 0.5 years to the sentence. The sensitivity level of the data is determined by the type of information infringed: the first level corresponds to general personal information, the second level to private personal information, and the third level to sensitive personal data. The sentence is increased by 0.5 years for the first level, and for each additional level, an additional 0.5 years is added, with the maximum sensitivity level being three. The harmful consequences caused by the offender are also integral to sentencing, including reputational harm, financial loss, or threats to personal safety. These consequences should be assessed using a coefficient system, with five points as the maximum, and the coefficient multiplied by 0.5 to calculate the additional sentence. The total sentence after adjustment must not exceed fifteen years. The author deems it necessary to explain the rationale behind choosing an increment of 0.5 years: from a technical perspective, the expansion of data volume may cause a multiplicative increase in harm, and the relationship between volume and harm is not necessarily linear. Therefore, a stepwise approach based on rounded thresholds is more appropriate. In the proposed model, when the amount of data infringed exceeds 10,000, one additional unit is added, and the sentence increases by 0.5 years. From the perspective of balancing deterrence with the principle of proportionality, increasing the sentence by a full year per unit may lead to excessive punishment. Thus, 0.5-year increments both reflect the principle that greater data infringement should result in heavier penalties, and avoid overly severe sentencing, thereby aligning with the restrained nature of criminal law.

Data-Equivalent Sentencing Calculation Model

```
def sentence_calculation(base, data_volume, sensitivity, harm_effect): # Base sentence (in years), determined by the lower bound of the aggravated penalty range

base = x # Base sentence (in years), determined by the lower bound of the aggravated penalty range

volume_factor = math.floor(data_volume / 10000) * 0.5 # Add 0.5 years for each additional 10,000 records of data

sensitivity_factor = sensitivity * 0.5 # Sensitivity level (scale: 1 to 5)

harm_factor = harm_effect * 0.5 # Degree of harm caused (scale: 0 to 5)

total = base + volume_factor + sensitivity_factor + harm_factor

return min(total, 15) # Cap the total sentence at a maximum of 15 years
```

5.4.2. Restructuring the System of Property-Based Penalties.

At present, China's criminal sentencing framework contains only general provisions regarding fines for data-related offenses. For enterprises, profit remains the primary objective; if unlawful behavior is not met with corresponding financial restrictions, the deterrent effect of criminal law will inevitably diminish. Therefore, it is necessary to introduce new standards for property-based penalties. The author will offer several suggestions in the following discussion.

The author believes that the imposition of fines should be determined based on the specific circumstances of each offense. First, in cases where the value of the data is clear and the data assets can be quantitatively assessed, the fine imposed on the offender should be calculated by multiplying the market value of the data assets by an appropriate ratio. Second, in cases where the value of the data is unclear but the technical gains obtained by the offender—namely, the commercial benefits derived through the use of generative AI—can be clearly identified, the fine should be based on the offender's illegal proceeds, multiplied by a corresponding proportion. Finally, in circumstances where neither the market value of the data nor the technical gains are readily measurable, the fine may be calculated based on the number of data entries infringed, by assigning a standard monetary amount per entry and multiplying this by the total number of infringements. The author does not attempt to establish concrete numerical standards for fines at this stage, but rather provides a conceptual framework for penalty design. The precise benchmarks should be defined through future judicial interpretations in practical contexts. As this is a legislative discussion, the author refrains from overstepping the boundaries of legislative recommendations.

It should also be noted that, following the imposition of a fine, if the offender still possesses technical assets that may facilitate further infringements of data-related legal interests—such as model parameters, training logs, or computational infrastructure—then such assets should be subjected to transparent seizure or mandatory destruction in order to eliminate the risk of recidivism.

5.4.3. Introducing Disqualification Penalties in the Form of Technological Bans.

In addition to imposing basic criminal penalties and fines, the author proposes that crimes involving the use of generative AI to infringe upon data-related legal interests should be supplemented with a final layer of protection: the introduction of a disqualification penalty in the form of a technological ban. Where individuals engage in such conduct, a time-limited revocation of professional qualifications may be applied. Specific measures could include prohibitions on engaging in technological research and development, restrictions on the offender's participation in generative AI model development, data collection, or data analysis, as well as placing offenders on a national data blacklist, thereby prohibiting access to public data platforms and isolating them from data networks, alongside restrictions on their use of computing power.

With respect to enterprises, the state could mandate the structural division of data-related business units and the separation of departments involved in the offense. For entities engaged in industries requiring licensing, relevant service qualifications may be revoked, and re-approval through national security review procedures may be required. However, such penalties should not be applied excessively. Instead, a standard of "serious circumstances" should be clearly defined, and only when this threshold is met should such disqualification measures be considered appropriate. Both the principle of restraint in criminal law and the practical necessity of encouraging technological development dictate that these penalties should not be imposed in minor cases. Overuse of such penalties may not only constitute an abuse of criminal law but also hinder the advancement of generative AI technologies and obstruct scientific innovation.

In the era of unprecedented growth in generative artificial intelligence, the author has, in this section, discussed three dimensions of reform: introducing statutory aggravating circumstances, reconstructing the property-based penalty system, and establishing disqualification penalties in the form of technological bans. The author believes that these proposals may contribute to an initial framework whereby the destructive potential of technology is proportionately matched by the strength of criminal sanctions. However, given the author's limited scope of knowledge and lack of practical experience, the discussion remains confined to legislative analysis, without proposing specific standards. The author acknowledges that articulating such standards without empirical grounding may be insufficiently persuasive, and thus believes that future refinement through judicial practice would be a more prudent course.

6. Conclusion

The rise of generative artificial intelligence marks a new chapter in the data era within the broader context of the Fourth Industrial Revolution. While technological iterations have disrupted traditional modes of criminal behavior, they have also compelled the legal system to respond. When confronted with the automated and large-scale infringement of data-related legal interests by generative AI, the traditional paths of criminal law regulation prove increasingly inadequate. The lag of criminal law is no longer a theoretical concern but a pressing challenge that threatens to leave data-related legal interests unprotected. Criminal law alone is far from sufficient to address the regulatory dilemmas posed by generative AI. In the future, we must consider embedding technological ethics into the genetic fabric of the law. Through multidimensional governance, including sector-specific norms and code-based standards, we can preserve necessary margins for technological fault tolerance and experimentation. The interaction between the rule of law and technological advancement is an ongoing process with no fixed end. The governance of generative artificial intelligence is not only a matter of legal reform but also a profound inquiry into the relationship between human rationality and technological civilization. As criminal law evolves from a "guardian of data" to a "check on algorithms," we are poised to establish a new paradigm for the protection of legal interests in the digital age—one that emerges from the dialectic between order and innovation.

References

[1] Liao, Lingmei, Liu, Zhou, Luo, Shu, et al. (2025). A Study on the Path of Empowering Basic Theories of Traditional Chinese Medicine with AI Technology. Journal of Nanjing University of Chinese Medicine (Social Science Edition), 26 (02), 138 – 142.

[2] Fang, Huiying. (2023). A Systematic Assessment and Multi-Dimensional Construction of the Criminal Law Regulation Model for Data Crimes. Theory and Reform, (6), 78 – 79.

[3] Liu, Xianquan. (2024). New Approaches to Criminal Law Regulation of Data Crimes Involving Generative Artificial Intelligence. Contemporary Law, 38 (06), 3 – 15.

[4] Meng, Tianguang. (2023). Intelligent Governance: Governance Propositions in the Era of Artificial General Intelligence. Xuehai, (2), 42.

[5] Jin, Zixin. (2024). Operating Mechanism, Potential Risks, and Legal Responses of Generative Artificial Intelligence from a Data Perspective. Journal of Chengdu Administrative College, (06), 59 – 70+119.

[6] Yang, Jianwu, Luo, Feiyan. (2024). Operating Mechanism, Legal Risks, and Regulatory Paths of ChatGPT-like Generative AI. Administration and Law, (04), 101 – 115.

[7] The Paper. (n.d.). Disaster from GPT-2's Mouth: Chatting with AI and Extracting Others' Privacy. Retrieved from https://www.thepaper.cn/newsDetail_forward_10468395.

[8] Fan, Xuehan, Lü, Qian. (2023, April 7). Italy's Ban Sparks Waves: ChatGPT Faces Data Security Challenges. China Business News, A01.

[9] Information retrieved from: https://baijiahao.baidu.com/s?id=1827015640159974536&wfr=spider&for=pc.

[10] Liu, Xianquan. (2023). The Impact of Generative AI on the Criminal Law Protection System for Data Interests. Journal of Chinese Criminal Law, (04), 20 – 34.

[11] Liu, Xianquan, Yu, Yueyang. (2024). Criminal Law Improvement for Securities and Futures Crimes Involving Generative AI. Journal of Zhejiang Gongshang University, (03), 47 – 57.

[12] Yu, Gaizhi. (2022). From Control to Utilization: A Paradigm Shift in Criminal Law Data Governance. Social Sciences in China, (07), 56 – 74+205.

[13] Liu, Xianquan. (2024). New Approaches to Criminal Law Regulation of Data Crimes Involving Generative Artificial Intelligence. Contemporary Law, 38 (06), 3 – 15.

[14] Sheng, Hao. (2023). Criminal Risks of Generative Artificial Intelligence and Legal Regulation. Journal of Southwest University of Political Science & Law, 25 (04), 122 – 136.

[15] Li, Zhenlin, Pan, Xinyuan. (2023). Dilemmas and Responses in Criminal Law Protection of Data Security under Generative AI: A Perspective Based on ChatGPT. Criminal Research, (02), 25 – 33.

[16] Information retrieved from: http://www.gdcourts.gov.cn/xwzx/fayuanxinmeiti/content/mpost_1733943.html

[17] Liu, Xianquan. (2023). The Impact of Generative AI on the Criminal Law Protection System for Data Interests. Journal of Chinese Criminal Law, (04), 20 – 34.

[18] Zhang, Xiaoyan. (2021). On the Criminal Subject Status of Strong Artificial Intelligence (Master's thesis). Qingdao University.

[19] Chen, Wei, Xiang, Minxi. (2024). Rethinking the Criminal Subject Qualification of Generative AI such as ChatGPT from the Perspective of "Cultivation Theory". Journal of Anhui Normal University (Social Science Edition), 52 (05), 96 – 106.

[20] Yuan, Zeng. (2023). A Study on the Responsibility Capacity of Generative Artificial Intelligence. Oriental Law, (03), 18 – 33.

[21] Xi Jinping. (2023). Selected Readings from Xi Jinping's Works, Vol. 1. Beijing: People's Publishing House, pp. 27 – 28.

[22] Zhang, Xiaoyan. (2021). On the Criminal Subject Status of Strong Artificial Intelligence (Master's thesis). Qingdao University, p. 31.

[23] Liu, Xianquan. (2022). A Study on the Improvement of Criminal Law Regulation of Data Crimes. Journal of Chinese Criminal Law, (05), 20 – 35.

[24] Zhang, Jianjun. (2005). Challenges and Development of the Principle of Legality in Criminal Law. Gansu Agriculture, (10), 146 – 147.