Analysis of the Impact of Legal Liability Allocation on Privacy Protection in Artificial Intelligence Technology in the Digital Era

Yanling Song*

Jilin Judicial Police Vocational College, Changchun, 130062, China
**Corresponding author:rebecca1981-11@163.com*

Abstract: *In today's era, the rapid development of digital technologies such as artificial intelligence (AI), big data, cloud computing, and the Internet of Things has brought unprecedented opportunities for growth, while also inevitably raising a series of severe challenges. Among these, the issue of privacy protection has become a particularly prominent and pressing concern in the digitalization process.This paper analyzes the problems and causes of privacy risks in the age of artificial intelligence, with the aim of exploring the intrinsic relationship and interaction mechanisms between legal liability allocation and privacy protection in AI technologies under the digital context. It seeks to enrich the theoretical research system concerning legal responsibility in the digital era and to provide strong support for the scientific formulation of relevant legal policies at the practical level. Ultimately, this research aims to promote the healthy development of artificial intelligence and the effective protection of citizens' privacy rights, contributing to the coordinated and balanced development of technology and the rule of law amid the digital wave.*

Keywords: *Digital era; Artificial intelligence; Privacy protection; Legal liability*

Introduction

At present, with the continued advancement of digital transformation, artificial intelligence, as a new type of technology, has profoundly and extensively reshaped human production and lifestyle. In light of the new challenges posed to privacy protection in the AI era, an in-depth exploration of the legal liability allocation in this domain is of great significance. Currently, China's legislation on privacy protection remains relatively underdeveloped. Most existing laws and regulations are general and principle-based, lacking sufficient effectiveness and operability in practical implementation. Therefore, it is essential to thoroughly examine the legal issues surrounding privacy protection in the context of artificial intelligence and to further improve the related legal framework. This is not only necessary to safeguard citizens' legitimate rights and interests but also serves as a critical foundation for ensuring the healthy and orderly development of AI.

1. Challenges to Privacy Rights Posed by Artificial Intelligence Technology

Artificial intelligence (AI) technology, while bringing tremendous convenience to human life, also presents new challenges to the protection of individual privacy rights. With the widespread adoption of AI products and the increasing prevalence of smart devices equipped with processors and sensors, the ability to monitor individuals' physical spaces has been significantly enhanced as these devices continuously collect personal data during service delivery [1].

1.1 Causes of Privacy Risks in Artificial Intelligence Technology

1.1.1 Limitations of AI Technology

In the development of AI technology, algorithmic models often lack transparency and may exhibit data bias. Deep learning algorithms, for example, function as "black box" systems whose internal decision-making logic is difficult to interpret. Data bias not only affects the accuracy and performance of AI models but may also exacerbate existing societal biases. AI systems often fail to explain their decisions, which restricts their application in critical fields. Moreover, erroneous decisions are difficult

to detect and correct due to the opaque nature of these processes.

1.1.2 Uncertainty in AI

Algorithmic predictions are prone to errors and biases, and reverse-engineering AI models is highly challenging, making their inner workings hard to access or understand. In decision-making processes, AI algorithms typically lack transparency and explainability. Data biases in machine learning models may result in hidden discrimination or flawed decisions that compromise privacy rights and social justice. As environments grow increasingly complex, uncertainty heightens the risk of algorithmic discrimination. The traditional “informed consent” principle becomes inadequate in the intelligent era, necessitating the development of new privacy protection paradigms. It is essential to strengthen privacy protection throughout the entire data lifecycle—from data collection, storage, processing, and transmission to destruction—by establishing robust safeguards at every stage [2].

1.1.3 Profit-Driven Behavior

In data-driven business models, companies often prioritize profit maximization. When faced with the trade-off between data utilization and privacy protection, many companies excessively collect and misuse user data to expand their businesses and extract commercial value. In some cases, data is sold to third parties without obtaining full user authorization, severely increasing the risk of privacy breaches.

1.1.4 Risk Awareness

The boundaries of privacy rights remain vague, and users often lack sufficient awareness of how to protect their personal data. Enticed by online services, users may hastily disclose personal information and agree to privacy policies without proper scrutiny, indirectly encouraging companies to over-collect data. Public understanding of AI varies widely, with both blind trust and undue fear being common. Meanwhile, the current legal framework struggles to keep pace with the rapid development of AI, leaving many emerging applications unregulated. The lack of clear legal definitions and guidelines has become a significant factor contributing to privacy risks [3].

1.2 Privacy Risks Posed by Artificial Intelligence Technology

1.2.1 Infringement of Privacy Rights

Personal data is frequently leaked, and AI algorithms can deeply mine sensitive information such as personal routines and social interactions to generate detailed user profiles. When exploited by malicious actors, such information poses threats to individuals’ personal and financial safety. Although biometric technologies (e.g., facial and fingerprint recognition) are widely used, the lack of adequate supervision during data collection and usage has led to frequent misuse.

1.2.2 Data Breaches

Data security faces serious threats, including constant hacking and cyberattacks. AI systems themselves are vulnerable and often suffer from disorganized data management, creating conditions conducive to data leaks. The opaque nature of AI algorithm operations increases the risk of data misuse. In some cases, organizations collect and exploit personal data without user consent, turning protected information into a profit-making tool [4].

1.2.3 Involuntary Privacy Infringement

Smart devices and applications often collect sensitive information—such as location data and browsing history—without users' awareness. Privacy policies on internet platforms are frequently complex and difficult to understand, misleading users into granting data access without fully realizing the implications.

1.3 Current Status of Privacy Risks in AI Technology

Existing privacy protection laws are largely based on models of "consumer choice" or "notice and consent." However, in the AI era, individuals find it difficult to truly understand or control where their information goes. As problems like data misuse and algorithmic discrimination emerge, it is essential to include information privacy, spatial privacy, and decisional privacy within the scope of legal protection. Additionally, the “black box” nature of AI systems complicates the assignment of legal responsibility, necessitating the clarification of legal liabilities among different stakeholders and the improvement of regulatory frameworks for AI [5].

2. Exploration of Responsibility Allocation Theories

2.1 Principles of Legal Responsibility Allocation

Artificial intelligence (AI), as an independent technological entity, should be regarded as a special "legal person" within the legal responsibility allocation framework. This "legal person" status primarily serves to incorporate AI into the scope of legal supervision and regulation, providing a procedural foundation for the formulation of specific future rules. From a legal perspective, AI cannot be considered a "subject" in the legal sense but rather an "object" of legal structures and control. Consequently, any "rights" arising from AI are, in fact, attributed to the stakeholders closely associated with it, as these stakeholders are the entities that truly possess legal subject status. Therefore, establishing AI's legal personality as an artificial technological entity and strengthening its supervision and effective control play a crucial role [6].

When allocating legal responsibility, it is essential to balance innovation incentives with risk prevention measures appropriately. If the threshold for assigning responsibility is too stringent, it may hinder AI development; conversely, if the responsibility is too lenient, public interests may not be adequately protected. In AI scenarios, algorithms become key decision-makers, but the lack of a clear legal subject identity poses significant challenges in defining responsibility.

From the perspective of responsibility allocation principles, the primary responsibility should be borne by the main stakeholders. Data controllers must handle personal privacy data with caution and bear corresponding compensation responsibilities in the event of infringement. If it is challenging to determine specific responsible parties, relevant stakeholders should assume joint liability. In the AI domain, negative phenomena such as algorithmic discrimination and privacy violations occur frequently, necessitating a clear delineation of responsibilities among stakeholders. Not only should algorithm developers be accountable for their development outcomes, but users must also consider whether they can foresee risks and take reasonable measures to prevent harm. Additionally, platforms must fulfill their responsibilities in reviewing various applications and preventing improper use. Other stakeholders, such as data providers, hardware manufacturers, and network service providers, may also bear joint fault [7].

2.2 Models of AI Responsibility Allocation

When AI systems cause harm to others' interests, determining how to allocate legal responsibility becomes a significant challenge. Currently, courts often apply product liability standards when handling AI-related cases, which largely resemble traditional rules applied to non-corporate owners with unlimited liability. In most cases, if a company designs, manufactures, or sells a defective product, it bears strict liability for any damage caused by that product. The "strict" aspect of strict liability implies that even if the company is not negligent, it can still be held accountable. That is, when introducing a product to the market, the company should be aware of potential consequences if the product is used as intended.

However, existing responsibility allocation models may face challenges when dealing with complex, advanced AI systems. If AI needs to bear responsibility for its actions, it requires legal personality to assess such responsibility, and this responsibility must be governed by established legal principles. Both AI itself and its developers can benefit from a clear legal framework. Current responsibility allocation models struggle to define the legal subject status of AI systems. If the harm caused by AI originates from its development and application stages rather than the fault of specific users, the process of pursuing responsibility may regress indefinitely, ultimately making it impossible to identify a human entity that can bear legal responsibility. This ambiguity in responsibility attribution poses a severe challenge to the effectiveness and fairness of the entire legal responsibility system [8].

Granting AI legal personality, thereby making it an independent legal responsibility subject, is a potential solution to this issue. In this scenario, legal responsibility would be attributed to this special AI entity, encompassing other natural or legal persons involved in AI development and application processes. This approach helps to clearly delineate the legal responsibilities that AI itself should bear and the moral responsibilities of related human actors. Companies, as artificial entities with legal personality, coexist with natural persons within the legal system, providing procedural guidance for distinguishing the legal rights and responsibilities of different subjects. Nevertheless, practical implementation of granting AI legal personality and achieving a balance between innovation incentives and responsibility constraints requires further in-depth exploration and research. Evidently, the AI responsibility allocation model urgently needs innovative changes at the legal system level to establish a reasonable, fair, and era-appropriate AI legal responsibility framework [9].

3. Case Studies

The issue of data privacy in autonomous vehicles highlights the inadequacy of current legal systems in effectively addressing the challenges of responsibility attribution posed by AI. According to existing tort law theories, when an autonomous vehicle accident occurs, potential responsible parties may include the vehicle user, automobile manufacturer, autonomous driving technology provider, and algorithm developer. In cases of data breaches or privacy violations, it is necessary to determine the degree and scope of responsibility for each party based on specific circumstances: automobile manufacturers must ensure the legality and compliance of data collection and initial processing; autonomous driving technology providers must guarantee data security during algorithm training and system operation to prevent privacy issues caused by technical vulnerabilities or poor management; algorithm developers must also ensure data security during storage and transmission to prevent unauthorized access or tampering. In response to autonomous vehicle accidents, some scholars have proposed granting AI entities legal personality, making them independent responsibility subjects, which could help clarify complex legal relationships. While this viewpoint has certain merits, it still faces numerous theoretical and practical obstacles. Theoretically, although AI can process data and make decisions based on algorithms, whether this decision-making process is equivalent to human behavior remains highly controversial. Practically, AI lacks independent property and entity identity, making it difficult to bear actual responsibilities such as compensating for losses like natural or legal persons. This presents significant challenges in assigning legal personality to AI and holding it independently accountable [10].

In the field of data privacy, AI technology poses severe challenges to the traditional "notice-and-consent" model. The 2018 "Alipay Annual Statement" incident vividly illustrates that algorithmic discrimination and data misuse risks have become pressing issues. In this case, users' data were analyzed and displayed for specific purposes without their knowledge, potentially infringing on their privacy. This situation calls for legislators to carefully balance data-driven innovation with personal privacy, not only promoting the reasonable flow of data but also enhancing user authorization mechanisms to ensure users have sufficient rights to be informed and to choose during data usage.

Numerous AI cases clearly demonstrate that cross-disciplinary comprehensive governance has become an urgent necessity. Even within the realm of privacy protection, the legal fields involved are extensive, closely related to constitutional provisions on citizens' fundamental rights, as well as laws such as consumer rights protection and antitrust regulations. Therefore, policymakers must adopt a systematic perspective to address the paradigm shifts brought about by AI, actively coordinate rules across different fields, and comprehensively improve and optimize the legal system. This approach aims to create a stable and predictable legal environment for AI innovation. Achieving this goal requires collaborative efforts from legislative bodies, law enforcement agencies, industry, academia, and other stakeholders to find the optimal balance between innovation and regulation through continuous exploration, ensuring that AI develops steadily along a healthy and orderly path, bringing significant benefits to society while minimizing potential negative impacts.

Conclusion

In the era of big data, the rapid development of artificial intelligence (AI) technology has posed numerous challenges to the protection of privacy rights. The vast and diverse range of personal data has rendered the traditional legal framework for privacy protection increasingly inadequate. Based on the theory of legal responsibility allocation and through case studies, this paper conducts an in-depth analysis of how responsibility allocation affects privacy protection within AI technologies. The study reveals that, in the digital age, clearly defining the scope of legal subjects' responsibilities and reasonably dividing the rights and obligations of all parties are key to regulating AI technologies and safeguarding personal privacy rights.

The responsibility allocation model proposed in this paper adopts a multidisciplinary perspective, incorporating tort law, consumer protection law, and other legal domains. It effectively addresses typical privacy infringements such as algorithmic discrimination and data misuse. By clarifying the layered responsibilities of AI system developers, operators, and users, this model enhances both the precision and deterrence of privacy protection mechanisms. In conclusion, this study enriches AI governance research both theoretically and practically, refines the theory of legal responsibility allocation, and lays a more solid legal foundation for privacy protection. It also opens up new paths for optimizing privacy protection mechanisms in the digital age.

Fund Project

This paper is a phased achievement of the 2024 legal research project of the Jilin Law Society titled "Research on the Privacy Protection Mechanism of Legal Responsibility and Artificial Intelligence Technology in the Digital Era."

References

[1] "The Algorithm Did It": Legal Responsibility and the Regulation of Artificial Intelligence [D]. Salve Regina University, 2021.
[2] Yang Changyu. Technological Challenges Faced by Law in the Digital Era and Legal Responses [J]. Qiushi Journal, 2022:12.
[3] Petro S. Korniienko, Oleh V. Plakhotnik, Hanna O. Blinova. Contemporary Challenges and the Rule of Law in the Digital Age [J]. International Journal for the Semiotics of Law - Revue internationale de Sémiotique juridique, 2023.
[4] Huang Ying. Research on Privacy Protection in the Era of Artificial Intelligence [J]. Comparative Study on Cultural Innovation, 2020:2.
[5] Legal Protection of Personal Information Rights [D]. Jiangxi University of Finance and Economics, 2018.
[6] Fang Hui. Exploring the Criminal Law Path for Privacy Protection in the Era of Big Data [J]. Legal System and Society, 2023:3.
[7] R. Alkabbj, A.Z. Alrazim, R. Binsaddig. The Impact of Using Artificial Intelligence on Preparing General Budget and Government Decision-Making in Jordan [D], 2024.
[8] T. Ma, Z. Zhang. Research on the Key Technologies of Big Data Security and Privacy Protection in the Field Based on Artificial Intelligence [D], 2023.
[9] Wang Yuanzhi, Xi Bin. Challenges and Prospects of the Civil Rights System in the Digital Era [J]. Southeast Jurisprudence, 2021.
[10] Zhang Pengran. Application Strategies of Artificial Intelligence Technology in Cyber Information Security [J]. Computer Applications Abstracts, 2023.