Computers and Artificial Intelligence；Vol.3, No.1; 2026
E-ISSN: 3006 -3728 P-ISSN：3006-371X
DOI: https://doi.org/10.70267/cai.26v3n1.3540
Published by: Zeus Press

Ethical Issues of Data Rights in the Big Data Era

Kuangzhi Qin*

University of California, Irvine, CA92697, USA

**Corresponding author: Kuangzhi Qin*

Abstract

The ethical issues of data rights have presented unprecedented complexity in the era of big data, and traditional rights frameworks are difficult to effectively respond to the inherent conflict between data liquidity and ownership certainty. The essence of data rights is not simply a matter of legal recognition, but rather involves the dynamic balance between individual dignity, social equity, and technological power. The informed consent during the data collection stage often becomes a formality, and the data processing process leads to a gradual dilution of ownership. The distribution of benefits in the data trading process is clearly tilted towards the platform, and these ethical dilemmas collectively point to the failure of the data subject rights protection mechanism. Starting from the perspective of the data lifecycle, this study analyzes the generation logic of ethical conflicts in each stage, proposes a governance path for constructing a full cycle ethical review mechanism and platform responsibility list, in order to promote the transformation of data rights from formal rights confirmation to substantive protection.

Keywords

big data era, data rights, ethical issues, data lifecycle

1. Introduction

The definition and protection of data rights are becoming an unavoidable ethical hurdle in the process of digital civilization. When the collection of personal information extends from specific scenarios to non influential and all-weather situations, the traditional rights protection model based on individual consent appears inadequate in the face of technological architecture. The value added and ambiguity of ownership brought by data processing severely tilt the balance of income distribution, and the contributions of data subjects are often obscured by abstract digital labor. These ethical challenges not only concern individual dignity, but also involve the foundation of social justice.

2. Core Concepts and Theoretical Foundations of Data Rights Ethics

2.1 The Essence and Types of Data Rights

Data rights are the legitimate collection of rights and interests between natural persons and data platforms in the digital age, centered around clarifying the reasonable boundaries of each party in data generation, holding, and use. The names, consumption preferences, and travel trajectories generated by natural persons'

daily shopping, travel, and social interactions are all specific carriers of data rights. As the original generator of data, natural persons have basic control over their own data and can decide whether to open location information or consumption records to the platform. This control is simply a manifestation of personal will. After legally obtaining data, data platforms have the right to process and use it, but they cannot override the right of natural persons to control it. E-commerce platforms can use consumer data to optimize recommendations but cannot disclose privacy. Therefore, they can be divided into the right of natural persons to control and the right of platform processing and use, which are interconnected and have their own boundaries, in line with reality and easy for ordinary readers to understand.

2.2 Primary Analytical Frameworks for Data Rights Ethics

The main analytical framework of data rights ethics revolves around the rights and responsibilities of data subjects, data platforms, and regulatory authorities. It is based on the concept of "separation of three rights" proposed in the "Twenty Articles on Data" and conforms to the actual scenarios of data usage to construct logic. The ethical demands of data subjects focus on preventing their own data from being abused and leaked, such as not wanting personal chat records or consumption habits to be leaked arbitrarily when using apps on a daily basis. This demand constitutes the basic premise of the framework. The ethical obligation of data platforms is reflected in the legitimate acquisition and use of data, and they cannot illegally capture other people's platform data or excessively collect user information based on their technological and resource advantages. This is a key link in the framework that connects the demands of the subjects with regulatory requirements. The regulatory authorities are responsible for clarifying the ethical boundaries of all parties involved, regulating the platform's illegal use of data, and enabling the framework to adapt to various daily data ethical scenarios, avoiding abstract expressions. Ordinary readers can also clearly understand the practical role of the framework [1].

3. Ethical Conflicts in Data Rights Generation and Circulation

3.1 Informed Consent Dilemmas in Data Collection

The core of the informed consent dilemma in the data collection stage is the power imbalance between the collecting party and the collected party. When homeowners live in the community, they often encounter property management companies requiring facial information to be entered in order to pass through. Property management companies often do not clearly inform the retention period and scope of facial information, nor do they provide alternative methods such as card swiping. Homeowners are forced to agree in order to enter and exit normally. App operators also use a similar approach when users register, hiding informed consent terms in lengthy privacy policies with small fonts and obscure language. Most users are forced to check their consent without carefully reading them. Owners and ordinary users may appear to have given their consent, but in reality, they do not truly understand the specific purpose of their data being collected. This superficial consent has no substantive meaning and makes informed consent a form of evasion of responsibility by the collection party, forming an unbreakable ethical conflict.

3.2 Security Responsibility Attribution in Data Storage

As the core responsible party for data storage, enterprises often choose to outsource their data storage business to third-party trustees in order to reduce operating expenses. This model itself is reasonable, but the core problem is that many companies neglect management after outsourcing, neither conducting on-site verification of the completeness of the entrusted party's security protection facilities, nor regularly supervising the standardization of their data processing processes, relying only on a formal confidentiality agreement as the basis for performance. Some entrusted parties lack a basic sense of responsibility, and without authorization from the entrusted enterprise, they transfer the data they undertake to other small institutions for additional benefits. The relevant regulations issued by regulatory authorities are often vague and lack specific and actionable supervision rules, making it difficult to detect such violations in a timely manner. Once a data breach occurs, the enterprise and the entrusted party tend to shift responsibility to each other. The enterprise evades its obligations by outsourcing its business, while the entrusted party claims to have fulfilled its basic responsibilities according to the agreement. Ultimately, the interests of ordinary

people are still damaged. After the personal data breach, it is often difficult to determine the specific responsible party, and the process of safeguarding rights faces many obstacles.

3.3 Ownership Dilution Issues in Data Processing

Most ordinary users lack a clear understanding of their own data ownership. In scenarios such as using mobile applications, browsing web pages, and online shopping, the original ownership of personal information voluntarily filled in and usage traces passively generated should belong to the users themselves. But in the actual data flow process, these data will be quietly collected and summarized by the platform, and then transferred to professional data processing enterprises for processing. Data processing enterprises invest manpower and technology costs to integrate and analyze scattered raw data, forming commercially valuable derivative data, and then arbitrarily attribute it to themselves, ignoring the core position of users as the source of raw data. The platform leverages its own advantages in data collection and storage to jointly enjoy the right to use and benefit from derivative data with processing enterprises [2]. Even if users accidentally become aware of the processing and utilization of their own data, they have a vague understanding of their own rights boundaries and lack convenient channels for safeguarding their legitimate rights and interests, gradually losing control over the original data. This passive state is a direct manifestation of the dilution of data ownership.

3.4 Unequal Benefit Distribution in Data Transactions

The unfair distribution of profits in the data trading process is essentially the result of unequal status among the three parties involved in the transaction. This unfairness is not an isolated phenomenon, but widely exists in daily data trading activities. The data providers are mostly ordinary enterprises or individuals who hold the core raw or processed data, but due to the lack of trading channels and discourse power, they can only passively accept the unreasonable allocation rules formulated by the trading platform. Only a small amount of fixed income can be obtained from each transaction, and the value-added dividends generated by the subsequent commercial utilization of data cannot be enjoyed. The data demander, relying on the purchased data for commercial operations and obtaining substantial profits, did not provide any additional compensation to the supplier; As an intermediary data trading platform, it not only extracts a relatively high proportion of transaction commissions, but may also take advantage of loopholes in the rules to disclose the data information of the supplier to other demanders without authorization in order to seek dual benefits. Even if the supplier is aware of the obvious unfairness in the distribution of profits, they can only passively bear this result due to the lack of clear distribution standards and effective ways to protect their rights.

3.5 Algorithmic Bias and Discrimination in Data Utilization

Algorithmic bias and discrimination are widely present in daily life scenarios, but most users fail to notice them. This bias is not due to the subjective malice of algorithms themselves, but rather stems from the subjective cognition and potential preferences of algorithm designers. During the process of model development, algorithm designers may unconsciously integrate their own values and preferences into algorithm rules, and these hidden preferences will be directly applied to various service scenarios by data using enterprises. For example, some short video platforms' recommendation algorithms prioritize pushing high-quality content to users of specific age groups and regions based on the designer's potential preferences, while other users who meet the same interests and needs can only obtain ordinary or even low-quality pushed content. Ordinary users find it difficult to perceive the biases behind algorithms and often attribute unreasonable push notifications to their own luck. Even if they vaguely perceive unfair treatment, they cannot identify the root cause of the problem and lack effective direction for safeguarding their rights. Data using enterprises, on the other hand, overly focus on their own operational efficiency and profits and fail to actively carry out verification and correction of algorithm biases [3].

4. Governance Pathways for Data Rights Ethics

4.1 Establishing Fundamental Rules for Data Rights Certification

Data ownership rights should be established based on current legal practices and market conditions, following the tripartite division of rights proposed in the "Twenty Data Regulations." This framework clarifies the core responsibilities of three parties: data subjects, data processors, and registration authorities, avoiding overlapping or gaps in authority. As the originators of personal and raw data, data subjects have the right to define the scope and methods of their data usage, without being forced to accept unreasonable authorization terms. In cases of unauthorized data ownership claims, they may file an objection review with the registration authority using their identity information. Data processors must truthfully report legally collected and processed data, prohibiting the inclusion of others' raw or already registered data into their own ownership scope. Processed data products must be separately reported with clear source attribution, ensuring traceability of the processing process. Registration authorities should streamline the ownership registration process by eliminating complex technical review requirements, adopting user-friendly reporting forms, and implementing categorized management for personal and commercial data. They must avoid a one-size-fits-all registration standard while retaining records for at least five years to facilitate future rights disputes. This approach ensures that ownership rules are effectively implemented in every aspect of daily data processing, remaining practical while resolving ethical conflicts in the registration process.

4.2 Building Ethical Review Mechanisms Across the Data Lifecycle

The Ethics Review Committee shall establish a simple and operable review process in accordance with the "Interim Measures for Scientific and Technological Ethics Review," without setting complex technical thresholds. It shall involve ethics experts and legal practitioners, implement a conflict-of-interest system, and conduct dynamic reviews of the entire process of data collection, processing, usage, and destruction. Routine inspections shall be conducted biannually, and the review process shall be restarted if any changes occur in the data processing procedures. Data processing entities must submit complete operational plans to the Ethics Review Committee before engaging in data-related activities, clearly defining the scope and methods of data collection. They must not conceal data sources or evade review. Once approved, the plans must be strictly followed. In case of non-compliant operations, a corrective report must be submitted immediately and subject to re-examination. Data subjects have the right to inquire with the Ethics Review Committee about the review records of their related data. If violations such as unauthorized data collection or misuse are identified during the review process, they may apply for the committee's intervention with relevant supporting documents. The Ethics Review Committee must provide feedback on the verification results within a reasonable timeframe and urge the data processing entity to rectify the issues, ensuring the review mechanism is genuinely integrated into daily data processing scenarios and avoiding formalistic reviews [4].

4.3 Enhancing Data Subject Rights Exercise Mechanisms

Data subjects often face difficulties when exercising their data rights, such as uncertainty about how to proceed or lack of avenues for feedback. Personal information processors can set up clear and straightforward access points for rights exercise in prominent locations of their apps or platforms, avoiding lengthy and obscure procedures. They should explicitly inform data subjects of the specific steps for reviewing, copying, correcting, or deleting personal information, as well as the feedback timelines. The access points must not be hidden within complex settings pages or privacy terms. Upon receiving a rights exercise request from a data subject, the processor must provide a clear response within a reasonable timeframe, with detailed legal explanations for any unmet requests to prevent the application from being ignored. Additionally, dedicated consultation channels should be established to address various questions data subjects encounter during the rights exercise process. Regulatory authorities can conduct regular inspections of personal information processors' implementation of rights exercise mechanisms, urging corrective actions against entities that fail to comply with requirements, delay feedback, or unjustifiably reject legitimate requests. This ensures that data subjects' rights are genuinely realized rather than remaining confined to legal provisions and platform commitments, effectively resolving the practical challenges individuals face when exercising their data rights in daily life.

4.4 Creating Ethical Responsibility Lists for Data Platforms

The data platform needs to develop an exclusive ethical responsibility list based on its own business scenarios. The list should abandon abstract expressions and focus on specific behavioral norms for the entire process of data collection, storage, use, and sharing. The list should be tailored to daily operational reality and can be adjusted and improved at any time. For example, in the data collection process, it is necessary to clearly indicate that the collection scope is limited to necessary business content and sensitive information such as user biometric and family economic status should not be collected without authorization. Before collection, users should be informed of the purpose and usage boundaries of the data in easy to understand language to avoid using professional terminology that may make it difficult for users to understand clearly. Regulatory authorities need to provide guidance on the development of lists for data platforms in various industries, define responsibility bottom lines in accordance with relevant laws and regulations, require platforms not to evade core ethical obligations, conduct interviews and rectification for platforms that fail to develop lists as required or have lists that are merely formalities, and urge platforms to implement ethical responsibility lists in every position and specific operational link. Third party organizations can be commissioned by regulatory authorities to conduct regular checks on the implementation of data platforms' lists, with a focus on ensuring consistency between the lists and actual operations. Any violations discovered during the checks should be truthfully reported to regulatory authorities, while assisting the platform in optimizing the list content to ensure that the lists truly regulate the platform's data processing behavior, meet the actual needs of the general public for data rights protection, and make ethical responsibility no longer a requirement on paper [5].

4.5 Promoting Universal Education in Data Ethics Literacy

The education department can take the lead in integrating various popular science resources and work with relevant units to develop popular data ethics textbooks that are suitable for daily life. The content of the textbooks avoids complex theories and professional terminology, and focuses on explaining the ethical boundaries and self-protection methods that users should pay attention to in common scenarios such as mobile app authorization, personal information filling, and network data sharing. It can also work with media platforms to launch short videos, graphic and textual popular science popularization, and other forms of communication that are easily accepted by the public, so that people of different ages can easily understand them. Colleges and universities can combine their disciplinary advantages to offer general data ethics courses for all students. The courses are not limited to classroom lectures, but can also introduce common cases of data breaches, privacy violations, etc. in reality for analysis, guide students to establish correct data ethics concepts, and encourage students to participate in community data ethics popularization volunteer activities. Communities can rely on the New Era Civilization Practice Station to regularly invite university teachers and practitioners in related fields to conduct free lectures. During the lectures, they can answer questions based on the practical problems encountered by residents in their daily lives, such as how to identify excessive collection of personal information by apps and how to refuse data requests from unfamiliar platforms. This will enable data ethics knowledge to truly enter people's lives and integrate into daily behavior, effectively improving the data ethics literacy and self-protection ability of ordinary people.

5. Conclusion

Examining the ethical issues of data rights essentially involves questioning how to place the subjectivity of individuals in the tide of technology. The rights conflicts exposed at various stages of the data lifecycle are not isolated technical flaws, but rather a concentrated manifestation of the existing regulatory system lagging behind digital practices. The exploration of governance paths needs to go beyond simple compliance thinking and shift towards value reconstruction centered on human dignity. Through the embedding of ethical review mechanisms and the clarification of responsibility lists, the allocation of data rights can truly respond to users' reasonable expectations. Only in this way can technological progress and comprehensive human development move from binary opposition to coordinated coexistence.

References

[1] Lee Myung Suk.(2016).A Study on the Ethical Issues and Sharing Behavior of User's Information in the Era of Big Data.Journal of the Korea Society of Computer and Information,21(10),43-48.

[2] Wen Liangming, Zhang Lili, & Li Jianhui. (2019). A Study on Ethical Issues in Scientific Data Sharing in the Big Data Era. Information and Documentation, 40(02), 38–44.

[3] Myung-Suk Lee.(2016).Study on the Ethical Issues and Sharing Behavior of User’s Information in the Era of Big Data.Journal of the Korea Society of Computer and Information,21(10),43-48.

[4] Wang Huashu & Liu Shijie. (2022). Research on Translation Data Ethics in the Big Data Era: Concepts, Issues, and Recommendations. Shanghai Translation, (02), 12–17.

[5] Wu Jinqing & Chen Jie. (2022). Challenges and Reflections on Information Ethics in the Big Data Era: A Perspective from the Marxist Concept of Rights. Journal of Hohai University (Philosophy and Social Sciences Edition), 24(02), 22–29+109–110.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgment

This paper is an output of the science project.

Copyrights