Current Research in Law & Practice

Journal Homepage: www. brilliance-pub.com/crlp

The Application of Personal Information Self-Determination on E-Commerce Platforms: A Legal Analysis Based on the Personal Information Protection Law

Chengyu Han[1]

[1] *Southwest University of Political Science and Law, China*

Correspondence: Chengyu Han, Southwest University of Political Science and Law, China.

ABSTRACT

The rise of digital commerce has intensified concerns over consumer privacy and data security, particularly on e-commerce platforms that process vast amounts of personal information. The Personal Information Protection Law enacted in China in 2021, strengthens personal information self-determination, granting individuals greater control over their data while imposing strict regulations on businesses. This paper analyzes the legal foundations of self-determination under the PIPL, focusing on consent mechanisms, data subject rights, algorithmic transparency, and cross-border data restrictions. Despite these safeguards, enforcement remains challenging due to opaque data collection, excessive profiling, and regulatory gaps. To enhance compliance, this study proposes policy reforms emphasizing transparency, user control, algorithmic accountability, and stronger enforcement mechanisms. By addressing these challenges, China can better balance technological innovation with consumer privacy rights, fostering a more sustainable and ethical digital economy.

KEYWORDS

PIPL, personal information self-determination, e-commerce platforms, data privacy, digital economy

1. Introduction

In the era of digital commerce, personal information has become one of the most valuable assets for businesses, especially for e-commerce platforms that rely heavily on consumer data to enhance user experience, optimize sales strategies, and drive targeted advertising. The rapid expansion of China's e-commerce industry, led by platforms such as Alibaba, JD.com, and Pinduoduo, has resulted in extensive data collection practices, ranging from browsing history and transaction records to biometric information and behavioral patterns. While data-driven strategies benefit both businesses and consumers by enabling personalized recommendations, fraud prevention, and efficient services, they also raise significant concerns regarding privacy, data security, and user autonomy.

Against this backdrop, the concept of personal information self-determination—which refers to an individual's ability to control the collection, processing, and dissemination of their personal data—has gained prominence. Rooted in the fundamental principles of data protection and digital rights, this concept has been widely recognized in global legal frameworks such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). In China, the enactment of the Personal Information Protection Law (PIPL) in 2021 marked a critical step toward strengthening user rights and regulating the handling of personal data by enterprises, particularly e-commerce platforms.

The PIPL establishes strict guidelines for data collection, processing, sharing, and cross-border transfers, requiring businesses to obtain explicit and informed consent from users before processing their personal data. It grants individuals the right to access, correct, delete, and transfer their data, reflecting the legal recognition of personal information self-determination. However, despite these legal safeguards, challenges remain in enforcing compliance and ensuring that users can effectively exercise their rights. Many e-commerce platforms continue to engage in opaque data collection practices, excessive user profiling, and algorithmic decision-making that undermine consumer autonomy.

This paper aims to critically examine the application of personal information self-determination on Chinese e-commerce platforms through the lens of the PIPL. It will analyze the legal foundations that underpin this right, discuss the challenges in its implementation within the e-commerce ecosystem, and explore policy recommendations to enhance user control over their data. By addressing these issues, this study seeks to contribute to the ongoing discourse on balancing data-driven innovation with consumer privacy protection in China's rapidly evolving digital economy.

2. Legal Basis of Personal Information Self-Determination under the PIPL

Personal information self-determination is a cornerstone of digital privacy rights, granting individuals the ability to control how their personal data is collected, processed, stored, and shared. In China, the Personal Information Protection Law (PIPL) establishes a comprehensive legal framework to safeguard personal data and reinforce consumer autonomy, particularly in the e-commerce sector where vast amounts of personal data are collected daily. The PIPL is built upon fundamental principles of legality, necessity, transparency, and proportionality, ensuring that personal information processing remains within defined limits and under the control of data subjects. These principles align closely with international data protection standards, such as the General Data Protection Regulation (GDPR) of the European Union, but reflect the unique regulatory priorities of China, which balances individual rights with national security concerns and industrial digitalization.

One of the core legal foundations of personal information self-determination under the PIPL is the requirement of lawful, fair, and necessary processing, meaning that e-commerce platforms must collect and use personal data only within legal boundaries, ensuring that the extent of data collection does not exceed what is required for providing a given service. Purpose limitation further mandates that data collection should be restricted to explicitly stated purposes, preventing companies from using personal data beyond the scope initially agreed upon by the user. Data minimization reinforces this by stipulating that companies should collect only the minimum amount of data necessary to achieve the stated purpose, limiting unnecessary and excessive data accumulation.

At the heart of personal information self-determination is the requirement for informed and voluntary consent. The PIPL sets a high bar for valid consent, requiring that it be explicit and specific rather than implied or generalized. This ensures that consumers retain agency over their data, making an active decision about whether to allow their personal information to be processed. Data subjects have the right to withdraw consent at any time, compelling companies to provide a simple and accessible mechanism for revoking prior approvals. The withdrawal of consent must not result in discriminatory treatment, meaning that platforms cannot penalize users for exercising their right to control their data.

Beyond consent, the PIPL grants a broad range of data subject rights that reinforce personal information self-determination. Individuals have the right to object to or restrict data processing, which is particularly relevant in cases of automated decision-making, such as algorithmic profiling used by e-commerce platforms for targeted advertising or price discrimination. Consumers also have the right to access and obtain a copy of their personal information, allowing them to verify what data has been collected and whether it is being used in accordance with the original consent agreement. Users can request corrections or deletions of inaccurate or unnecessary data, ensuring that outdated or irrelevant personal information does not remain in a company’s possession indefinitely.

Another critical aspect of the legal framework is the right to data portability, which enables individuals to transfer their personal information from one service provider to another. This provision is especially relevant in the e-commerce sector, where customers may wish to switch platforms without losing their transaction history, saved preferences, or other data crucial to their shopping experience. Data portability fosters consumer choice and market competition, preventing large platforms from monopolizing user data and thereby locking consumers into a single ecosystem.

In the context of automated decision-making and algorithmic governance, which are widely employed by Chinese e-commerce platforms, the PIPL imposes additional obligations to protect consumer rights. Companies that rely on automated decision-making for marketing, pricing, or personalized recommendations must provide clear explanations about how these algorithms affect users. Consumers have the right to opt out of automated profiling and demand human intervention in cases where automated decisions significantly impact their rights and interests. This is particularly relevant in cases of dynamic pricing, where users may unknowingly be charged different prices based on algorithmic assessments of their shopping behavior.

Despite these robust legal protections, enforcement remains a challenge. The PIPL requires companies to establish mechanisms for handling consumer requests related to data access, correction, deletion, and portability, but many e-commerce platforms fail to provide seamless and user-friendly avenues for individuals to exercise these rights. To enhance compliance, the Cyberspace Administration of China (CAC) and other regulatory bodies have been given the authority to conduct audits, impose fines, and even suspend business operations in cases of serious violations. Notably, companies that engage in illegal data processing face fines of up to 5% of their annual revenue or 50 million RMB (approximately 7.8 million USD), underscoring the serious legal consequences of non-compliance.

In addition to domestic enforcement, the PIPL places strict restrictions on cross-border data transfers, which is critical given that many Chinese e-commerce platforms operate internationally. Companies conducting cross-border transfers must undergo security assessments and obtain user consent before sharing personal data outside China. These regulations are designed to prevent foreign entities from exploiting Chinese consumer data while maintaining national data sovereignty. Companies that violate these provisions may face regulatory scrutiny, leading to data localization requirements or restrictions on cross-border partnerships.

The PIPL provides a strong legal foundation for personal information self-determination in China's e-commerce landscape. By enshrining data subject rights, informed consent requirements, algorithmic transparency, and cross-border data transfer regulations, the law seeks to balance digital innovation with consumer protection. However, the effectiveness of these legal provisions ultimately depends on strict enforcement, corporate compliance, and increased public awareness of digital privacy rights. The next section will examine the practical challenges that hinder the full realization of personal information self-determination in the e-commerce sector and explore potential policy solutions.

3. Challenges in Implementing Personal Information Self-Determination on E-Commerce Platforms

Despite the legal framework established by the Personal Information Protection Law (PIPL), the effective implementation of personal information self-determination on Chinese e-commerce platforms remains challenging due to a combination of business practices, technological constraints, consumer awareness gaps, and regulatory enforcement difficulties. The vast and dynamic nature of the e-commerce industry in China, where platforms process enormous amounts of user data to enhance personalized marketing and optimize sales strategies, creates a conflict between commercial interests and privacy protection. As a result, several barriers hinder the ability of consumers to fully exercise their rights over personal data.

One of the most pressing challenges is the lack of transparency in data collection practices. Many e-commerce platforms adopt overly complex and ambiguous privacy policies, making it difficult for users to fully understand the scope and extent of data collection. Legal requirements mandate that consent must be informed and explicit, yet in practice, most privacy policies are long, technical, and filled with legal jargon, discouraging users from thoroughly reading them. Furthermore, platforms often use bundled consent mechanisms, where users are forced to agree to an all-encompassing data processing policy to access basic services, rather than being given granular control over different aspects of their personal data. This not only weakens the principle of personal information self-determination but also contradicts the data minimization and purpose limitation requirements outlined in the PIPL.

Another major challenge stems from excessive data processing and algorithmic profiling, which are deeply embedded in the operational models of Chinese e-commerce platforms. Companies collect vast amounts of personal data, including purchase history, browsing behavior, biometric data, and even facial recognition information, to optimize advertising strategies and consumer engagement. Many platforms employ automated decision-making systems to determine product recommendations, pricing strategies, and targeted promotions, often without clear user consent. While these algorithms are designed to enhance customer experiences, they also create significant risks of discrimination, price manipulation, and loss of user control over how their data is used. Many consumers are unaware that their data is being processed in such an extensive manner, and even when they do understand, they often lack effective opt-out mechanisms to limit algorithmic tracking. The PIPL requires platforms to provide users with explanations of automated decision-making processes, yet in practice, companies offer minimal or vague justifications, leaving consumers with little recourse.

The difficulty in exercising data subject rights presents another substantial barrier to personal information self-determination. Although the PIPL grants users rights such as data access, correction, deletion, and portability, enforcing these rights remains highly problematic. Many e-commerce platforms do not provide clear or easily accessible interfaces for users to modify or delete their personal data. Even when these options are available, lengthy bureaucratic procedures, repeated verification requests, and intentional delays discourage users from pursuing data-related requests. Some platforms employ dark patterns, such as misleading user interface designs, to make it difficult for individuals to withdraw consent or disable certain data tracking settings. For instance, opting out of targeted advertising or algorithmic recommendations often requires multiple steps buried deep within privacy settings, deterring users from fully exercising their rights.

Another critical challenge lies in cross-border data transfers and data security risks. Chinese e-commerce platforms, particularly those with international operations, routinely engage in cross-border data exchanges, raising concerns over data sovereignty and security. The PIPL imposes strict conditions for transferring data outside of China, requiring companies to conduct security assessments, obtain regulatory approvals, and inform consumers about potential risks. However, enforcing these requirements remains difficult, especially given the global nature of digital commerce and cloud-based data storage. Many multinational e-commerce platforms process Chinese consumer data through offshore servers or third-party service providers, making it harder for Chinese regulators to monitor compliance effectively. Concerns over data leaks, cyber threats, and unauthorized access further complicate the enforcement landscape. Cases of data breaches and illegal data sales have highlighted the vulnerabilities in cross-border data management, reinforcing the need for stricter enforcement mechanisms.

Regulatory enforcement itself presents a major implementation challenge. While the Cyberspace Administration of China (CAC) and other government agencies have the authority to investigate and penalize non-compliant platforms, enforcement actions remain inconsistent and reactive rather than proactive. Many e-commerce companies, particularly small and medium-sized enterprises (SMEs), lack the technical expertise or financial resources to fully comply with PIPL requirements, leading to widespread non-compliance or partial implementation of data protection measures. The interpretation of legal obligations varies across different platforms, creating loopholes that companies exploit to minimize compliance costs. For example, some platforms claim that certain types of data do not qualify as "personal information" under the law, thereby avoiding the need for explicit consent. The enforcement gap is further widened by the relatively low level of digital literacy among consumers, who may not be fully aware of their rights or how to seek legal recourse when their privacy is violated.

The evolving nature of technology and business models complicates regulatory oversight. With the rapid adoption of artificial intelligence, blockchain, and big data analytics, new methods of data processing are constantly emerging, often outpacing the legal framework designed to regulate them. For instance, the integration of biometric authentication, voice recognition, and Internet of Things (IoT) devices into e-commerce ecosystems introduces new privacy risks that the current PIPL provisions may not adequately address. The metaverse and virtual shopping experiences further blur the lines between personal and behavioral data, raising concerns over increased surveillance and reduced user autonomy. As a result, regulators face an ongoing challenge in keeping up with technological advancements while ensuring that personal information self-determination remains a meaningful and enforceable right.

In summary, while the PIPL provides a strong legal foundation for personal information self-determination, its implementation on e-commerce platforms faces significant hurdles, including opaque data collection practices, excessive profiling, difficulties in exercising data subject rights, cross-border data transfer risks, weak enforcement mechanisms, and rapid technological developments. Overcoming these challenges requires a multi-faceted approach, including stricter regulatory oversight, improved consumer awareness, enhanced corporate compliance measures, and adaptive legal frameworks that evolve alongside emerging technologies. Without these measures, the balance between digital commerce growth and consumer privacy protection will remain difficult to achieve in China's e-commerce ecosystem.

4. Legal and Policy Recommendations for Strengthening Personal Information Self-Determination

Addressing the challenges in implementing personal information self-determination on Chinese e-commerce platforms requires a multi-dimensional approach that includes regulatory intervention, corporate compliance improvements, technological safeguards, and consumer empowerment. While the Personal Information Protection Law (PIPL) provides a strong legal foundation, its enforcement must be bolstered through greater transparency, stronger user control mechanisms, algorithmic accountability, and robust legal remedies. The following recommendations outline key strategies to strengthen personal information self-determination in China's e-commerce landscape.

4.1 Enhancing Transparency and User Awareness

One of the primary obstacles to personal information self-determination is the lack of transparency in data collection and processing. Many e-commerce platforms use complex and technical privacy policies that discourage users from fully understanding how their data is handled. To ensure that consumers can make informed choices about their personal information, regulatory authorities should mandate standardized, plain-language privacy policies that clearly explain the types of data collected, the purposes of processing, and the specific rights available to consumers.

Platforms should implement real-time data collection notifications that inform users when their data is being gathered and provide just-in-time consent options rather than relying on broad, pre-approved agreements. Companies should also be required to provide annual transparency reports detailing their data processing activities, security measures, and compliance with user requests for data access, deletion, or modification.

Furthermore, increasing public awareness of digital rights is critical. Government agencies and non-governmental organizations (NGOs) should launch consumer education campaigns to help individuals better understand their privacy rights under the PIPL. These initiatives could include online courses, workshops, and educational materials that explain how to navigate privacy settings, withdraw consent, and file complaints in case of violations. Strengthening digital literacy programs in schools and universities can also empower younger generations to take an active role in protecting their personal information.

4.2 Strengthening User Control Mechanisms

For personal information self-determination to be meaningful, users must have practical and accessible tools to manage their data. Many e-commerce platforms currently make it difficult for users to modify privacy settings, opt out of tracking, or delete their accounts, creating unnecessary barriers to self-determination. Regulators should require platforms to implement user-friendly privacy dashboards that allow individuals to easily view, modify, and delete their personal data without bureaucratic hurdles.

E-commerce platforms should also be mandated to provide granular consent options, enabling users to selectively approve different types of data processing instead of being forced to accept all-or-nothing privacy policies. Users should have the ability to opt out of personalized advertising, algorithmic recommendations, and third-party data sharing through clear and intuitive settings. Platforms should standardize the process for withdrawing consent so that users can revoke permissions as easily as they granted them.

To further enhance user control, China could consider adopting a centralized privacy preference management system, similar to the Global Privacy Control (GPC) standard used in some jurisdictions. This would allow consumers to set their privacy preferences at the browser or device level, ensuring that their choices are automatically applied across multiple platforms without requiring them to manually configure settings for each service.

4.3 Algorithmic Accountability and Fair Data Processing

The widespread use of algorithmic decision-making in e-commerce, particularly for personalized recommendations, dynamic pricing, and targeted advertising, raises concerns about excessive data profiling, discrimination, and user manipulation. The PIPL (Article 24) already requires companies to provide explanations for automated decisions that have a significant impact on individuals. However, in practice, these explanations are often vague and insufficient, failing to provide meaningful insight into how algorithms process user data.

To enhance algorithmic transparency, regulators should impose strict disclosure requirements that compel companies to provide detailed explanations of how their algorithms function, including the data points used, the decision-making criteria, and the potential consequences for users. Independent audits of algorithmic systems should be conducted to ensure fairness, non-discrimination, and compliance with data protection regulations.

Platforms should also be required to offer manual override options, allowing users to opt out of automated profiling and request human intervention in cases where algorithmic decisions negatively impact their rights or interests. This is particularly crucial in dynamic pricing models, where consumers may unknowingly be charged different prices based on their shopping behavior. To prevent unfair practices, regulators should prohibit price discrimination based on personal data unless there is a clear, justifiable reason.

Furthermore, China could introduce an Algorithmic Transparency Labeling System, where e-commerce platforms are required to disclose the level of personalization and automation used in their services. Similar to nutrition labels on food products, this system would enable consumers to quickly understand the extent to which their data is being analyzed and how it affects their shopping experience.

4.4 Strengthening Enforcement and Legal Remedies

Despite the strong provisions of the PIPL, enforcement remains one of the biggest challenges in ensuring personal information self-determination. Many e-commerce platforms fail to comply fully with data protection requirements, and regulatory actions have often been reactive rather than proactive. To address this, Chinese authorities should increase regulatory oversight through routine compliance inspections, randomized audits, and unannounced platform reviews to ensure that e-commerce companies are adhering to the law.

The Cyberspace Administration of China (CAC) and the State Administration for Market Regulation (SAMR) should establish a dedicated enforcement unit focused on investigating consumer data protection violations within the e-commerce industry. This unit should have the authority to impose significant fines, temporary suspensions, and even platform shutdowns for repeat offenders. A whistleblower program should be introduced to encourage employees and consumers to report privacy violations, offering incentives for disclosures that lead to enforcement actions.

Consumers must also have effective legal remedies when their data rights are violated. The PIPL provides users with the ability to file complaints and seek redress, but many consumers lack access to legal assistance or are unaware of how to take action. Establishing a centralized digital rights protection agency could provide individuals with free legal support, dispute resolution services, and direct reporting channels for privacy violations. Class-action lawsuits should be encouraged in cases where multiple consumers are affected by the same data protection breaches, allowing for collective enforcement of digital rights.

To further deter non-compliance, the financial penalties for data privacy violations should be significantly increased for large e-commerce platforms that repeatedly fail to protect consumer rights. In addition to fines, companies should be required to provide compensation to affected users, reinforcing accountability and ensuring that privacy violations carry tangible consequences.

4.5 Adapting Regulatory Frameworks to Emerging Technologies

As technology evolves, new challenges to personal information self-determination continue to emerge. The rise of biometric data collection, blockchain-based transactions, and metaverse commerce introduces novel privacy risks that existing regulations may not fully address. To stay ahead of technological developments, regulators should adopt a flexible, adaptive regulatory framework that evolves alongside emerging innovations.

This could be achieved by establishing a regulatory sandbox where e-commerce companies can test new data processing technologies under close supervision, allowing regulators to evaluate risks before these technologies become widely adopted. Additionally, China should strengthen cross-border cooperation with international data protection authorities to develop harmonized global privacy standards, ensuring that Chinese consumers are protected even when engaging with foreign e-commerce platforms.

Strengthening personal information self-determination on e-commerce platforms requires a comprehensive approach that prioritizes transparency, user control, algorithmic accountability, enforcement, and regulatory adaptability. While the PIPL has laid a strong legal foundation, its effectiveness depends on strict enforcement, increased consumer awareness, and corporate compliance. By implementing these recommendations, China can ensure that its digital economy continues to thrive while upholding the fundamental rights of individuals to control their personal data in an increasingly data-driven world.

5. Conclusion

The right to personal information self-determination is fundamental in safeguarding individual privacy and ensuring that consumers retain control over their digital identities. As China's e-commerce industry continues to expand, personal data has become an invaluable asset for platforms, fueling algorithm-driven marketing strategies, personalized recommendations, and dynamic pricing models. However, the extensive collection and processing of personal information have heightened privacy risks, making it crucial to ensure that individuals can exercise meaningful control over their data. The Personal Information Protection Law (PIPL) has established a robust legal foundation for protecting consumer rights, emphasizing informed consent, purpose limitation, data minimization, and algorithmic transparency. While these principles align with global data protection standards, the actual enforcement and implementation of these rights remain challenging in practice, particularly within the fast-moving and highly competitive e-commerce ecosystem.

Despite the legal framework in place, many platforms continue to engage in opaque data practices, making it difficult for users to fully understand or control how their personal information is used. The prevalence of bundled consent, excessive data profiling, and automated decision-making without adequate user oversight undermines the principle of personal information self-determination. The complexity of privacy policies, the use of dark patterns to discourage opt-out choices, and the limited accessibility of data deletion or portability mechanisms further weaken consumer autonomy. The challenges surrounding cross-border data transfers and compliance with strict regulatory requirements for international data flows further complicate the enforcement landscape, requiring a more coordinated and adaptive approach from regulatory bodies.

Ensuring the full realization of personal information self-determination requires a multi-faceted approach that balances technological innovation, business interests, and consumer protection. E-commerce platforms must take greater responsibility in implementing transparent, user-friendly privacy mechanisms that empower consumers to make informed decisions about their data. Regulatory authorities, particularly the Cyberspace Administration of China (CAC) and State Administration for Market Regulation (SAMR), must intensify enforcement efforts, conducting proactive audits, issuing stringent penalties for non-compliance, and ensuring that businesses are held accountable for data protection violations. Consumer education initiatives are necessary to raise awareness about digital privacy rights and equip individuals with the knowledge needed to navigate privacy settings and legal recourse mechanisms effectively.

Technological solutions such as privacy-enhancing technologies (PETs), blockchain-based consent management systems, and AI-driven privacy assistants could play a crucial role in strengthening user control over personal data. These innovations could allow individuals to automate privacy preferences, track how their data is being used in real-time, and revoke consent seamlessly without relying on cumbersome manual processes. To further enhance algorithmic accountability, platforms must ensure that their automated decision-making systems are auditable, explainable, and fair, reducing the risk of data-driven discrimination and manipulation.

Achieving a fair and transparent digital environment requires continuous legal adaptation and cross-industry collaboration to ensure that data governance frameworks remain effective in addressing emerging privacy challenges. China's digital economy will continue evolving with advancements in big data analytics, artificial intelligence, and the metaverse, presenting new risks that current data protection laws may not fully anticipate. Regulatory flexibility, international cooperation, and industry best practices must be integrated into China's privacy governance strategy to ensure that personal information self-determination remains a protected and enforceable right in the long term. If these measures are effectively implemented, China can strike a balance between technological progress and individual privacy protection, fostering a more ethical, sustainable, and consumer-centric digital economy.

6. References

[1] H. Chen, "A comparative analysis of personal data protection regulations between China and the EU," Electronic Commerce Research, 21, pp. 1-22, 2021.

[2] National People's Congress of China, Cybersecurity Law of the People's Republic of China, 2016.

[3] National People's Congress of China, Data Security Law of the People's Republic of China, 2021

[4] National People's Congress of China, Personal Information Protection Law of the People's Republic of China, 2021.

[5] X. Zhang, L. Li, and M. Wang, "China's emerging data protection framework," Journal of Cybersecurity, 8 (1), pp. 1-21, 2022.