Academic Journal of Management and Social Sciences
ISSN: 2958-4396 | Vol. 14, No. 3, 2026

Legal Boundaries and Institutional Reconstruction of Data Rights Allocation in the Context of the Platform Economy

Xiaoya Shang

Dalian Ocean University, Dalian, Liaoning, China

Abstract: In the context of the platform economy, data as a new factor of production is characterized by ambiguous entitlement and imbalanced use, giving rise to conflicts of interest among multiple actors. Taking the allocation of data rights within platform ecosystems as the main thread, this paper first sorts out the structure of data entitlements, and summarizes the main dilemmas in practice, including the formalization of user consent, unclear boundaries between personal information protection and data re-use, concentration of data on dominant platforms that squeezes competition, and weak remedies for data-related rights. On this basis, it explores potential paths for reshaping the legal boundaries and reconstructing the institutional framework of data rights allocation in the platform economy, focusing on restructuring data collection and use procedures, coordinating personal information protection with data-driven innovation, improving competition rules and data openness arrangements, and strengthening remedies and liability allocation for data rights. The aim is to provide normative reference for the market-oriented allocation of data as a production factor.

Keywords: Platform Economy; Data Rights Distribution; Legal Boundaries; Institutional Reconstruction; Personal Information Protection Introduction.

1. Introduction

With the rising prominence of the platform economy, data has evolved from a by-product of business processes into a key element in value creation [1]. While platforms aggregate, analyse and trade data, they not only foster business model innovation, but also amplify risks such as excessive data collection, abusive processing and weak rights remedies [2]. Existing legal frameworks built around personality rights, property rights and intellectual property often fail to adequately address the needs of multi-actor data rights allocation in platform scenarios, leading to increasingly salient problems of blurred legal boundaries and insufficient institutional supply. Against this backdrop, this paper focuses on data rights allocation in the context of the platform economy and, from the perspectives of theoretical foundations, practical dilemmas and institutional reconstruction, seeks feasible paths to reshape the legal boundaries of data rights.

2. Theoretical Foundations of Data Rights Allocation and Its Legal Boundaries in the Platform Economy

2.1. Constituent Elements and Entitlement Structure of Data Rights in the Platform Economy

In platform-based settings, the constituent elements of data rights mainly include data types, entitled parties and the content of rights. In terms of data types, they cover not only personal information that can identify natural persons, but also de-identified user behaviour data, platform operation data and derivative data generated through algorithmic analysis.

The entitled parties are interwoven among users, platform operators and third-party partners, and no longer correspond to a single, centralized ownership structure. As for the content of rights, on the one hand it manifests as control rights over personal information, such as the rights to be informed, to consent, to access, to rectify and to erase; on the other hand, it manifests as utilisation rights of platforms and business users in relation to data collection, processing, sharing and benefit distribution. The coexistence of diverse data types and multiple actors renders data rights a composite entitlement structure where personality interests, proprietary interests and public interests are intertwined, laying the analytical groundwork for defining lawful boundaries and allocation rules.

2.2. Value Orientation and Institutional Basis of the Legal Boundaries of Data Rights Allocation

The value orientation of the legal boundaries of data rights allocation is reflected in the balancing of multiple objectives. On one side lies the emphasis on respecting natural persons' dignity, privacy and informational self-determination, and preventing individuals from being excessively "datafied" or reduced to mere instruments; on the other side lies the need to ensure that data, as a new factor of production, can effectively contribute to innovation and efficiency, while maintaining an open and orderly competitive environment and safeguarding overall public interests. At the institutional level, relevant boundaries are typically constructed at the intersection of general civil law rules and specialised data governance regimes, including theories of personality rights and property rights, the principle of contractual autonomy, and regulatory logics concerning personal data protection, cyberspace governance, competition law and fair trading. Through the combined application of principles such as lawfulness and legitimacy, data minimisation, purpose limitation and fair and

reasonable use, different jurisdictions jointly sketch out the basic normative framework for data rights allocation in the platform economy, thus providing institutional support for further adjustment and reshaping of legal boundaries[3].

3. Practical Dilemmas of the Legal Boundaries of Data Rights Allocation in the Platform Economy

3.1. Imbalances in Data Collection and Use under the Formalization of User Consent

In the operation of platform-based businesses, user consent to data processing is often obtained via tick-box mechanisms and bundled privacy policies, with the authorisation process highly standardised and formalised. Platforms tend to design lengthy and complex terms, default opt-ins and function bundling to cover a variety of data collection and secondary use scenarios in a single stroke, leaving users with little real opportunity to read, understand or choose. The gap between ostensibly "voluntary consent" and the practical lack of informed and substantive choice weakens users' control over the scope of data flows, retention periods and purposes of use. As a result, data collection and utilisation are more closely aligned with platform business interests and technological logic, leading to a marked imbalance in power and benefits.

3.2. Boundary Conflicts between Personal Information Protection Rules and Data Re-Use

In the platform economy, personal information protection rules emphasise specific purposes, data minimisation and purpose limitation, whereas data re-use relies on cross-context aggregation and correlation analysis, creating inherent tensions between the two. When platforms seek to re-purpose data originally collected for basic services—such as for targeted marketing or algorithm training—it is often unclear whether such use qualifies as "compatible purposes" or whether renewed consent is required, and there is a lack of unified standards in this respect. At the same time, the technical boundaries between de-identification and anonymisation remain blurred, and different actors may diverge significantly in their assessments of re-identification risks. Consequently, data re-use in practice faces both regulatory uncertainty and latent risks of infringement and regulatory disputes.

3.3. Squeezing of Competitive Order and Business Users' Data Rights by Platform Data Concentration

In the platform economy, leading platforms accumulate massive user bases and behavioural data over time, and, aided by algorithmic recommendation and network effects, achieve a high degree of control over data resources. Data tends to be locked within platforms and sedimented as "private assets", while smaller business users can only access platforms as attached participants, relying on platform-generated traffic and profiling services, and lacking independent control and stable access to data relevant to their own business. Data generated in the same transaction process is more often treated as platform-owned resources, while business users' rights to access and port transaction data, by-product data and review data remain weak, making it difficult for them to transfer and utilise such data across platforms. This undermines their bargaining power and innovation space. Data concentration strengthens platform control over market entry and information, resulting in a "winner-takes-most" competitive structure and further marginalising and instrumentalising the data rights of business users[4].

3.4. Weak Data Rights Remedies and Obstacles to Rights Realisation

In platform scenarios, infringements of data rights often occur in concealed forms, and rights-holders face substantial difficulties in discovering and evidencing such infringements. Internal complaint and appeal mechanisms on platforms are frequently operated via online forms and automated responses, with opaque procedures and long response times, making it difficult for users to understand the standards applied and the progress of handling. Cross-platform and multi-party data flows further complicate the identification of responsible actors, and rights-holders often struggle to determine whether to direct their claims against the platform, third-party business users or other participants. Limited regulatory resources, high professional thresholds for judicial procedures and relatively high costs of legal action together mean that individuals facing data misuse or processing beyond the agreed scope often end up passively accepting or giving up pursuing remedies, resulting in pronounced structural barriers to the realisation of data rights.

4. Institutional Reconstruction Paths for the Legal Boundaries of Data Rights Allocation in the Platform Economy

4.1. Reshaping Data Collection and Use Procedures and User Consent Rules

Reshaping data collection and use procedures requires transforming user consent from a "one-off formality" into a dynamic mechanism that is understandable, subject to genuine choice, and sustainable over time. When designing consent flows, platforms should present different data types and usage scenarios in a layered manner, clearly distinguishing between data that is strictly necessary for basic services and data used for value-added services, targeted recommendations, algorithm training and other purposes, and provide separate notices and granular consent options for each. The wording of consent notices should keep length and technical jargon under control, and highlight data types, purposes, sharing partners and retention periods through icons, short summaries and emphasis markers, while also providing easily accessible entry points for users to review and withdraw consent at any time. For secondary uses of data, platforms may introduce mechanisms such as periodic consent reconfirmation or prominent notices in the event of material changes, requiring users to make fresh choices at key points. At the same time, platforms should establish internal systems for recording and auditing data processing activities, incorporating information on "which consent was relied upon and for what purpose the data was used" into log management, so as to support subsequent liability tracing and compliance assessment.

For example, on the account management page of a ride-hailing platform, a dedicated "Data and Privacy Center" module can be created, breaking down data collection and use procedures into a series of visual switches. Trip location data

and order records, which are necessary to provide the core service, can be accompanied by concise explanations of their purposes and retention periods in the terms, and be marked as "required" in the interface. By contrast, personalised recommendations, behavioural profiling and data sharing with third-party partners can each be assigned an independent toggle, leaving it to users to decide whether to activate them. When granting consent, users can expand a "more details" panel with one click to view the corresponding data categories, purposes of use and potential sharing scope, and they may withdraw consent or restrict certain uses at any time on the same page. On the back end, the platform automatically records every change to these switches together with the associated scope of data processing, and can provide such records to regulators or dispute resolution bodies in the event of data access requests or controversies, thereby strengthening the substantive and verifiable nature of user consent at the procedural level.

4.2. Coordinating Personal Information Protection Requirements and the Boundaries of Data Re-Use

Coordinating personal information protection requirements with the boundaries of data re-use calls for data classification and compatibility assessment as core tools. Platforms can, based on risk levels, distinguish between sensitive personal information, ordinary personal information and de-identified data, and set differentiated conditions for re-use: sensitive personal information is restricted to core services and a limited range of legally permitted scenarios; ordinary personal information may be reused within a defined scope on the basis of adequate notice and user choice; and de-identified data may be used for algorithm training and service optimisation, provided that re-identification risks are effectively controlled.

On this basis, internal rules combining "purpose catalogues + compatibility assessments" may be established. Proposed new uses of data should be subject to ex ante review, assessing factors such as data source, extent of change in purposes and potential impacts on individual rights, and the assessment conclusions and grounds for use should be recorded in ledgers and logs so that re-use activities remain on a verifiable compliance track.

For example, an online education platform may construct a "data type–purpose–consent method" matrix, marking identifiers such as ID numbers and contact details as sensitive data, to be used solely for account management and security checks; categorising course browsing histories and assignment completion records as ordinary personal information, to be used for teaching analytics and personalised recommendations; and treating aggregated and de-identified learning behaviour data as the basis for course optimisation and system iteration. When business units propose new data uses, a compliance team reviews them against the matrix and pre-set compatibility criteria to decide whether the data may be used directly, requires additional consent, or must first be de-identified. The review process and conclusions are briefly documented. Through this operational mechanism, the coordination between personal information protection requirements and the boundaries of data re-use can be progressively solidified in concrete scenarios.

4.3. Regulating Competition Governance and Data Openness under Platform Data Concentration

Against the backdrop of highly concentrated platform data, competition governance and data openness should form a mutually reinforcing institutional configuration. From the perspective of competition rules, data control capacity can be incorporated into assessments of market power, with merger control and behavioural regulation paying particular attention to dominant platforms' exclusive control over key data sets[5]. For operators with significant platform power, obligations of non-discrimination in algorithmic ranking, traffic allocation and interface access should be imposed, and the use of data advantages for self-preferencing or the exclusion of trading partners should be prohibited. In terms of data openness, differentiated arrangements can be made for different layers of data: statistical and aggregated industry data may be made available to the public via open interfaces or periodic reports, while data directly relating to the transactions of business users can be covered by "reasonable, transparent and predictable" data access rules. Standardised APIs, data portability and related arrangements can help ensure that business users maintain continuous access to and reasonable use of data about their own operations.

For example, a comprehensive e-commerce platform, in designing its compliance scheme, may mandate an independent department to draft "Platform Data Access and Use Guidelines", which specify lists and access methods for categories such as publicly available industry statistics, analytical reports accessible to partner institutions, and order and review data retrievable by merchants. The guidelines may provide a general description of the data dimensions and basic logic used in search rankings and recommendation slots, and explicitly state that the purchase of value-added services cannot be used as a hidden ranking factor. Merchants are provided with standard interfaces through which to export their own transaction data. When regulators assess platform conduct, these guidelines and their implementation status can serve as important reference points. Combined with complaint channels and spot checks, they enable targeted enforcement against data-related differential treatment, refusals to deal or the imposition of unreasonable conditions, thereby fostering a more open and equitable competitive environment under conditions of data concentration.

4.4. Improving Data Rights Remedies and Liability Allocation Mechanisms

Improving data rights remedies and liability allocation mechanisms requires both the diversification of redress channels and the refinement of responsibility rules. On the remedial side, platforms should establish a unified and prominent "Data Rights Request" interface and adopt standardised procedures to categorise and handle requests for access, rectification, erasure, withdrawal of consent and objection. Clear conditions for acceptance, response time limits and evidentiary requirements should be set, and the outcomes and reasons for decisions should be recorded automatically for ex post review. At the same time, institutional arrangements should link internal platform complaint procedures with third-party mediation bodies, industry dispute resolution platforms and regulatory complaint channels, thereby offering a graduated range of options—from internal platform remedies, industry self-

regulation to administrative supervision and judicial remedies—that lower the cost and threshold of asserting data-related rights. On the responsibility side, liability can be allocated by reference to the degree of control and benefit realised by platforms, business users and technical service providers at different stages of data collection, storage, sharing and re-use. For typical scenarios, rules such as presumptions of fault or joint and several liability may be established, while limited liability relief or "compliance safe harbours" can be offered to actors who have followed established compliance standards and taken prompt remedial measures, thereby enhancing incentives for proactive compliance.

For example, a large integrated platform may integrate all data-related request channels into a single "Account – Data and Rights" section. After a user submits a request, the system automatically indicates the types of data involved, the actors potentially responsible and the expected handling time, and displays the platform's internal review, communications with third parties and the final outcome step by step. When cross-actor data disputes arise, the platform can apply pre-published liability allocation guidelines to distinguish between its own data control decisions and independent processing by business users. Where unlawful processing falls within the platform's decision-making and management remit, it assumes primary responsibility; where conduct is clearly attributable to third parties, the platform assists rights-holders in preserving evidence and guides them towards industry mediation or regulatory complaint channels. Through this operational framework, data rights remedies become more accessible and transparent, and responsibility boundaries are progressively consolidated and rendered more predictable in practice.

5. Conclusion

The platform economy has reshaped the ways in which data is generated and utilised, and has also challenged existing entitlement structures and legal boundaries. This paper has mapped the structure of data entitlements in platform settings, identified practical situations such as formalised user consent, tensions between protection and re-use, data concentration and weak remedies, and advanced corresponding ideas for reconstructing authorisation procedures, coordinating protection and utilisation, regulating competition and data openness, and improving remedies and liability allocation. Overall, establishing clear and enforceable legal boundaries for data rights allocation is a crucial precondition for the sound operation of the platform economy, and relevant rules still need to be continuously tested and refined in practice.

References

[1] Liu H , Liu X , Sun B ,et al.On the Determinants of Platform Boundary: A Study from the Perspective of Transaction Cost Theory[J].International Journal of Crowd Science, 2025, 9(3): 175-180.DOI:10.26599/IJCS.2025.9100005.

[2] Culiberg B , Abosag I , Ater B .Psychological contract breach and opportunism in the sharing economy: Examining the platform-provider relationship[J].Industrial Marketing Management, 2023, 111(000):13.DOI: 10.1016/j. indmarman. 2023. 04.007.

[3] Li X .Response Strategies to Legal Risks of Big Data-Enabled Digital Economy[J].Transactions on Economics, Business and Management Research, 2024, 6:74-84.DOI: 10. 62051/ evm 7fp76.

[4] Piasna A .Precariousness in the Platform Economy[J].Faces of Precarity, 2022: 130-145.DOI:10. 51952/97815292200 94. Ch 009.

[5] Eugénie Coche, Kolk A ,Václav Ocelík. Unravelling cross-country regulatory intricacies of data governance: the relevance of legal insights for digitalization and international business[J]. Journal of International Business Policy, 2024, 7.DOI: 10. 1057/s42214-023-00172-1.