Applied Artificial Intelligence Research

INNOVIAIR

A Comparative Study of the Data Ethical Foundations of the EU's GDPR and China's Personal Information Protection Law from the Perspective of Global Integration

Zhengyu Yang[a,*], Di Jiang[a], Yuyang Liu[b]

[a]Law school, Henan Normal University, Xinxiang, Henan 453000,China

[b]Nanyang No.32 Primary School, Nanyang, Henan 453000,China

ARTICLEINFO

Keywords:
Data Ethics
GDPR
PIPL
Global Integration
Rights-Based
Development-Security Balance

ABSTRACT

Data drives the development of the global economy, but at the same time, countries face the same challenge: how to protect personal information without hindering its utilization.In view of the lack of systematic ethical comparison between the two major privacy frameworks in Europe and China in the existing literature, this paper aims to examine the ethical basis of the EU's General Data Protection Regulation (GDPR) and China's Personal Information Protection Law (PIPL).This paper uses a comparative analysis method to systematically compare the similarities and differences between GDPR and PIPL in terms of ethical paradigm, system design, and governance logic. The study found that although GDPR and PIPL represent different regulatory paradigms, they are converging in global data governance.The GDPR follows a rights-based paradigm, which originates from the European tradition of emphasizing individual rights. PIPL adopts the development-security balance paradigm based on the need to balance personal protection, industry needs and national security. Although the origins are different, both laws emphasize the combination of personal data control empowerment and supervision mechanisms, and pay attention to the established system of enterprises, not just ex post punishment. By clarifying the ethical basis of the global data governance model, this study provides an analytical framework for understanding regulatory convergence in different cultural and institutional contexts.

1.Introduction

The 21st century has profoundly changed human society. The Internet, big data and artificial intelligence have elevated data from a mere record of private life to a strategic resource of great economic and social management value[1]. The generation, collection, processing and cross-border transmission of global data have gone beyond the traditional geographical boundaries and have grown exponentially. Generative artificial intelligence has changed the traditional data processing method and has a deep structural impact on the current personal information protection law.

This shift has brought huge benefits, including improved global economic efficiency, incentives for innovation, and broader service accessibility. However, it also poses new challenges: privacy issues, rising digital inequality, trust risks due to data abuse, and related sovereign and security risks[2].

Data has become a new factor of production. Cross-border data flows affect the operation of multinational enterprises and the country's innovation capabilities. The World Economic Forum's research shows that cross-border data flows currently contribute more to global economic growth than traditional trade in goods.

This has caused a consequence: data mobility brings convenience, but also introduces risks. In the development of the digital economy, the country faces the challenge of how to regulate personal information processing to balance individual rights with economic development and national security. This is a problem of national and global significance. Generative artificial intelligence further complicates this phenomenon by increasing the opacity of data processing and amplifying the risk of misuse[1].

* Corresponding author.
E-mail address: 15936586982@163.com.
https://doi.org/10.65455/a7y1rc23
Received 13 March 2026; Received in revised form 16 April 2026; Accepted 20 April 2026; Available online 19 May 2026
© The Author(s) 2026. This article is published with open access in Applied Artificial Intelligence Research under a Creative Commons Attribution 4.0 International License (CC BY 4.0). https://creativecommons.org/licenses/by/4.0/

Data governance has become an important part of global governance. According to UNCTAD statistics, as of 2021, 137 countries have implemented data protection laws, reflecting the global recognition of personal information protection. This trend originated in Europe and has now spread to Africa, Asia and the Americas, so it is necessary to strengthen the international coordination of regulatory standards.

The EU's General Data Protection Regulation (GDPR) entered into force in 2018, and China's Personal Information Protection Law (PIPL) entered into force in 2021, becoming two global data protection frameworks that cannot be ignored[3]. The EU Data Protection Regulation establishes strict standards and severe penalties, which are applied extraterritorially to entities that process European resident data. It is widely recognized as the 'gold standard' for data protection. Its regulatory impact has extended to regions including Japan, Brazil, South Korea and South Africa, a phenomenon known as the 'Brussels effect'[4], where European standards are disseminated globally through market mechanisms. This regulatory model reshapes data protection practices within Europe and the data governance strategies of multinational corporations[5].

China's PIPL combines domestic experience with international practice, selectively adopts GDPR elements, and provides tailored solutions for the world's largest digital market[6]. Its promulgation marks China's formal entry into a high-level data protection system, which has had an impact on more than 1 billion individuals and global data governance dynamics. As the world's second largest economy, China's regulatory approach reflects a path of institutional learning, while maintaining distinct cultural and policy characteristics[7].

Global integration includes not only the integration of economy and technology, but also the interaction of regulatory frameworks, standards and value systems. GDPR and PIPL are rooted in different civilizations, political and development backgrounds, reflecting different data ethics paradigms. They are defined as value systems that guide data-related activities. Although existing comparative studies mainly focus on legal technicality[8], there is insufficient attention to the ethical basis of fundamentally shaping regulatory design, which may limit the understanding of its potential policy logic[9].

A comparative analysis of these frameworks is of great benefit: it breaks through the western framework in the discourse of global data governance, provides practical guidance for the relevant norms of many countries, and is conducive to the construction of a community of shared future in cyberspace.

The core argument of this paper is that GDPR is centered on human dignity and individual autonomy, while PIPL integrates individual rights, digital economic development and national security interests, and is a 'development-security balance' paradigm[6]. These paradigms show a dynamic of both competition and convergence, which together shape global data ethics.

This paper adopts a structured analysis method: clarifying key terms and comparing the ethical characteristics of the two mechanisms. On this basis, we examine the interaction between them from the perspective of globalization and explore the research results.

The Schrims II ruling in 2020 embodies the dialectical relationship between data protection and national security interests. The European Court of Justice declared the European and American Privacy Shield null and void on the grounds that the data of European residents was not adequately protected by the US surveillance program[10]. This forces transnational entities to adopt standard contract terms and conduct rigorous transfer impact assessments. The above illustrates the legal and moral challenges in cross-border data flows.

There are different views on the ethical issues of data protection in academia. Solovy advocates that pragmatic privacy governance focuses on specific injury prevention rather than abstract rights framework. Bradford elaborated on the 'Brussels effect', showing how the GDPR standard is spread globally through market mechanisms[4]. Li and Chen describe China's regulatory model as a "gravity-assisted" model[11]. The above views emphasize different risk assessment methods. Compared with GDPR's individual-centered approach, PIPL emphasizes large-scale participation and economic security[7]. Despite these contributions, the existing literature lacks a systematic analysis of the ethical underpinnings that shape regulatory design, particularly with regard to convergence mechanisms in global data governance[9].

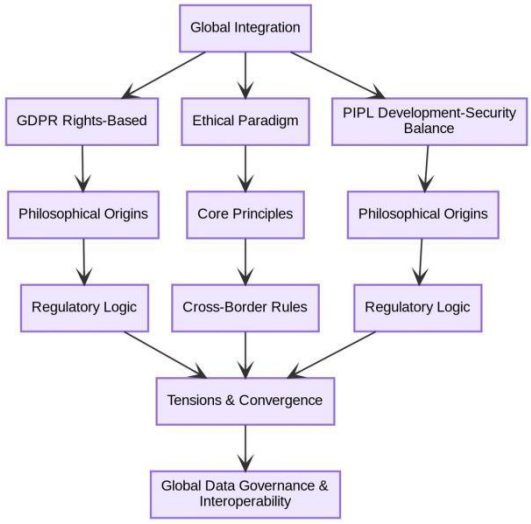


Fig 1. GDPR and PIPL in global integration: a comparative framework

2.Core concepts and how we compare

2.1.What does global integration mean here?

The global integration defined in this context refers to a digitally driven process characterized by the continuous transnational flow of data, services and platforms, accompanied by the transnational transmission of legal rules, governance concepts and moral standards. These elements adapt to the local system and potentially converge through mutual influence[12].

This analytical framework treats GDPR and PIPL as active participants in global regulatory discourse, which shape international norms while also being influenced by

competition and cooperation in global markets. Bradford's research illustrates the phenomenon that European regulation is often driven by economic rationality to achieve global standardization in cross-border business operations through market mechanisms[4].

2.2.What is a data ethical foundation?

The ethical basis of data is the basis of the regulatory framework, including the core values and beliefs that guide the governance of personal information[9]. The basic problems it solves are: the theoretical basis of data protection, the priority of value, and the resolution of value conflicts. This basic layer constitutes the normative core of the data protection system. The academic consensus emphasizes its key role in the interpretation and implementation of legal provisions[13].

2.3.The individual rights-based paradigm

The rights-based paradigm focuses on the priority of personal data rights relative to other social interests, and positions personal data as the focus of data governance[8]. Any collection or processing of personal information needs to be justified as an exception to the fundamental right of data control. This paradigm is rooted in Western liberalism and personality right theory. It conceptualizes personal data as an extension of one's identity, arguing that an individual must not be seen merely as a means to an end, but as an end in itself[14].

2.4.The development-security balance paradigm

The development-security balance paradigm is very different. It believes that personal information protection cannot be decoupled from national development and security goals. This paradigm is not an absolute priority for any single value, but to seek a dynamic balance between human dignity, industrial innovation, public welfare and national sovereignty. Data protection is not an end in itself, but a mechanism to ensure the healthy development of the digital economy and promote social interests while safeguarding security interests.

2.5.Methodological framework for comparative analysis

This study uses a four-dimensional analysis framework to compare the two regulatory systems: (1) philosophical origin, examining the ideological basis of the core principles; (2) Normative principles to identify the value orientation of embedded regulatory clauses; (3) Regulation logic, analysis of power distribution mechanism; (4) Cross-border governance approaches and evaluation of extraterritorial application strategies. These dimensions together reveal the potential value choices and determine the meeting point of different ethical foundations to produce similar practical results.

Table 1. Comparison of GDPR and PIPL data governance paradigms

Dimension	GDPR (Rights-Based Paradigm)	PIPL (Development-Security Balance Paradigm)
Philosophical Origin	Kantian human dignity, European humanistic tradition, post-WWII rights protection	Coordinated development-security concept, Chinese governance practice, digital economy pragmatism
Legislative Purpose	Protecting fundamental rights (primary); free data flow (secondary)	Balancing protection, rational use, national security (parallel)
Core Principles	Strict legal bases; individual rights; data minimization	Informed consent; classified/layered protection
Cross-Border Rule	Adequacy decision; SCCs, BCRs	Security assessment; standard contract certification; reciprocity
Regulatory Model	Independent supervisory authorities	Multi-department collaborative supervision (CAC led)
Enforcement Focus	Systemic compliance; heavy fines	Gatekeeper obligations; security-oriented

3.The GDPR's ethical characteristics: a "rights-based" paradigm with strong protection

3.1.Where the GDPR's ideas come from and what it wants to do

The ethical basis of GDPR is rooted in the European tradition of jurisprudence and has a profound humanistic influence[15]. Its ideological pedigree can be traced back to Kant's philosophy, which holds that rational beings have inherent dignity and must be regarded as 'purpose itself, not just means'. This philosophical foundation establishes individual autonomy and dignity as the supreme value in European discourse of rights.

After the Second World War, Europe began to attach importance to the protection of individual rights. Article 8 of the 1950 European Convention on Human Rights established the first legal framework of "respect for private and family life." This provision evolved into a modern data protection law, and finally in 2000, the "Charter of Fundamental Rights of the European Union" explicitly recognized "personal data protection" as an independent fundamental right, marking a critical conceptual separation from traditional privacy rights and laying a clear legal foundation for data protection[8].

GDPR's opening speech clearly established this hierarchical priority, with the primary goal of 'protecting the basic rights of natural persons, especially the right to data protection'[15].Although the regulation recognizes economic integration and free flow of data, the operation of these goals is subject to the overall requirements of ensuring 'high-level protection'. The ethical basis behind it is that strong protection of individual rights is not an obstacle to market development, but a necessary prerequisite for fostering digital trust and achieving sustainable market functions.

One of the often-neglected structural features of the GDPR is its dual structure, consisting of 173 declarations and 99 articles, which reflects Plato's theory of the duality of law as set out in his 'Laws', in which the preface serves as a persuasive element (peithao) and the legislative provisions serve as a coercive instrument (anankē). The narrative is not just a context embellishment; they include the philosophical

motivation and value judgment of the interpretation of 'article'. The doctrinal analysis emphasizes the hermeneutic significance of these rules, pointing out that they are often invoked by the judiciary to resolve ambiguities in their application, thereby underscoring their key role in understanding the ethical core of the 'regulations'[15].

3.2.Core principles and how rights are structured

GDPR operates its philosophical commitments through normative principles and a framework of individual rights, aiming to provide individuals with substantive and operational control over their personal data[16].

Legal processing framework. Article 6 establishes a strict gatekeeping mechanism and lists six permissible legal bases for data processing: consent, contract performance, legal obligations, protection of vital interests, public interest tasks, and legitimate interests[2]. Consent requires that this authorization must be free, specific, informed and revocable, so as to reconfigure the power dynamics and take the individual's independent choice as the basic basis for handling activities.

For legitimate interests, the GDPR introduces a 'reasonable expectation' standard, as described in Articles 47 to 49 of the Concert[16]. The controller must evaluate the reasonable expectations of the data subject based on the relationship between the data subjects. In the absence of such expectations, individual rights take precedence over the interests of the controller. The legitimate interests permitted include fraud prevention, cybersecurity, direct marketing, and internal group transfers, although these need to be balanced on a case-by-case basis with individual rights.

In the individual empowerment mechanism, GDPR enumerates a comprehensive set of individual rights : the right to access (to achieve data visibility), the right to correct (error correction), the right to delete (the 'right to be forgotten' for data that is outdated or withdraws consent), the right to dissent, the right to restrict processing, and the right to data portability[15]. The latter is an innovative provision that enables data migration between service providers, transforms static consent into dynamic control, promotes competition, and eases data locking. It is worth noting that the 'right to be forgotten' has a significant impact on the management of personal data history by search engines and social media platforms.

Data Subject Access Request (DSAR), as a procedural mechanism for the exercise of multiple rights under Article 15, requires the controller to confirm the processing activity and provide access within one month[17]. Studies have shown that the function of DSARs is to act as a portal right. Once an individual obtains the visibility of his / her data, he / she can subsequently exercise the right to correct, delete or object.

Restrictions on the scope of data collection. Article 5 establishes the core principles including purpose limitation. These principles, together with accuracy, storage limitations, integrity, and confidentiality requirements, form structural constraints that prevent ubiquitous, uncertain data-accumulation practices that characterize certain technology business models, thereby protecting privacy through upstream collection limitations. This framework has been characterized as the 'constitutional framework' for data protection in Europe[17].

Nuanced method for data reuse. GDPR does not completely prohibit data processing for new purposes, which will stifle useful innovation, but instead establishes a hierarchical framework of 'further processing'. The framework divides processing activities into three different levels: (1) processing that requires new legal basis; (2) The processing requires a 'compatibility' assessment of the original purpose, including an assessment of the purpose relationship, collection background, and potential personal impact; (3) Handling of exemptions from compatibility testing, including scenarios with new consent, handling of important public interests as required by EU or domestic law, and specific divisions of public interest archiving, scientific research, and statistics[16]. This flexibility recognizes the social value of data beyond the initial collection, while safeguarding individual rights in secondary use scenarios.

3.3.How the GDPR projects its power: cross-border data rules

Through the framework of 'adequacy decision' under Article 45[10], GDPR adopts a prudent mechanism to promote its standards internationally. This mechanism enables the European Commission to demonstrate that non-EU countries, regions, departments or organizations provide 'adequate protection', thereby facilitating unfettered data flows, equivalent to transfers within the EU without the need for additional authorization requirements.

The adequacy assessment criteria are comprehensive and inherently political, including an assessment of a country's data protection legislation, human rights records, the existence of an independent oversight body, and international commitments[9].This represents an overall assessment of the legal and political environment, not a list of technologies. So far, only 15 countries or regions have obtained appropriateness status, which reflects the EU's strategy of using market forces to improve global data protection standards.

In the absence of appropriateness decisions, cross-border transfers require regulatory 'appropriate safeguards', including legally binding instruments, binding corporate rules, standard contractual clauses (SCCs), approved codes of conduct and certification mechanisms. SCCs represent the most commonly used mechanisms, and the European Commission adopted revised SCCs in June 2021 to address the complexity of modern data processing.

The Meta Ireland case in 2023 reflects the 'substantial equivalence' standard. In this case, the Irish Data Protection Commission found that the US legal framework lacks equivalent protection due to insufficient supervision of EU users' data access by the US authorities. The SCC was deemed inadequate, resulting in a €1.2 billion fine and an order to suspend U.S. data transmission. The ruling resonated through the corporate sector, emphasizing that procedural compliance alone is not enough - the defacto protection standards of destination countries must meet European requirements, a fundamental principle of GDPR's cross-border transfer regulations, highlighted in authoritative commentary[10].

3.4.The GDPR in practice: what we learn from airlines

The practical implementation of these abstract principles is illustrated by four enforcement actions against European airlines analyzed in the relevant regulatory studies[18].

Transavia Airlines experienced data breaches affecting 83,000 people as a result of unauthorized third-party access, and Dutch regulatory authorities identified inadequate security measures, including weak passwords and lack of regular audits, resulting in a fine of 400,000 euros[18].

Romanian airline TAROM faced enforcement action after an internal breach, in which an employee visited and publicly shared a passenger list containing 22 people, resulting in a fine of 20,000 euros[18]. The case emphasizes that the security framework must address internal access control and employee training issues while providing technical support.

Spanish-language airline Vueling was fined 30,000 euros for non-compliant cookie practices involving insufficient user information and inappropriate consent mechanisms, enhancing transparency and the universal applicability of consent requirements[18].

British Airways suffered a shrewd attack. Users were shunted to the scene of the fraud where the payment card data was stolen. The UK Information Commissioner's Office initially proposed £183 million. This fell to £20 million, partly due to the company's representations and partly due to the impact of COVID-19 on aviation[4]. Even the number of reductions is considerable. If the security of sensitive financial data is not ensured, it will bring serious consequences.

These cases reveal the unique risk profile of civil aviation: airlines maintain a wide range of sensitive passenger data, operate through inherent cross-border networks, and rely on complex third-party partnerships-each representing a potential vulnerability. Enforcement actions consistently refer to Articles 5, 6, and 32, indicating that the focus of regulation is on basic compliance failures, not just high-profile breaches[18]. The analysis of enforcement decisions shows that more and more regulators are willing to impose major penalties for systemic violations, which is beyond the scope of catastrophic data breaches to address basic regulatory violations.

4.The PIPL's ethical characteristics: a "development-security balance" governance paradigm

4.1.Where the PIPL's ideas come from and what it wants to do

PIPL is generated in the specific socio-economic context of the rapid development of China's digital economy, exceeding 55 trillion yuan (more than 40 % of GDP) by 2023. Such exponential growth requires a regulatory framework that balances individual protection and innovation promotion while addressing evolving national security issues[2].

While incorporating international privacy norms and strengthening individual rights through constitutional protection of human dignity, 'Protected Privacy' embodies a distinct Chinese governance concept of 'coordination of development and security'. This basic principle has shaped its value balance in structure[7].

Article 1 sets three parallel goals : protecting the rights of personal information, regulating processing activities, and promoting rational data utilization. These goals are intended to be coordinated rather than prioritized[3]. "Safeguarding national security" as a basic principle runs through the entire legislation and incorporates provisions on outbound data transmission and important data categories[2]. The basic ethical framework holds that protection makes development possible, development makes protection contextualized, and security constitutes the inviolable boundary between the two.

China's cross-border data governance has undergone evolutionary development. The 2016 Cybersecurity Law implemented a restrictive framework that emphasizes domestic storage requirements and pre-transmission security assessments[2]. By 2024, regulatory adjustments have relaxed the conditions for handover, reduced the burden of compliance while maintaining safety and security, and reflected the increasing maturity of the understanding of balanced openness and regulation.

4.2.Core principles and how rights are designed

Flexible informed consent mechanism. Article 13 establishes "informed consent" as the core principle, and lists seven legal bases for handling, including clear provisions on public health emergencies[3]. The framework enables health authorities to conduct infection tracking during the COVID-19 pandemic without personal consent, giving priority to collective welfare. Article 14 provides for voluntary and explicit consent, while article 16 prohibits denial of service based on denial of consent, preventing a mandatory 'either accept or leave' consent model[3].

By requiring the form of consent to match the complexity of processing and the level of risk, PIPL introduces innovations compared to GDPR implementation, solves the 'click-to-consent' problem of providing consent without real understanding by users, and reflects the pragmatic approach of consent mechanisms in the digital market[19].

A rights framework with contextual adaptability. PIPL incorporates the rights familiar to the GDPR framework, including access, replication, correction, and deletion[3]. However, it takes a very different approach to the right to dispute: the right to erasure is expressed in restrictive language, and the right to data portability is not explicitly codified[18]. This reflects the cautious policy choices for the development of China's digital industry, where portability requirements may undermine the stability of the platform and put smaller market participants at a disadvantage.

The implementation of rights emphasizes the practical channels relative to litigation, requiring the handler to establish a convenient mechanism for individuals to exercise their rights. Article 49 allows close relatives to exercise their rights after death and maintain family privacy through a relational personality concept that is different from the GDPR individualism framework[3].

Hierarchical protection based on classification. Article 28 defines sensitive information as information including biometrics, religious beliefs, medical data, financial information, location data, and information on minors under the age of 14, which requires separate consent to be processed.

Article 31 introduces special safeguards for minors, mandatory guardian consent, which goes beyond individual protection and encompasses large-scale risk prevention[3].

In addition to sensitive data, PIPL has established a multi-level protection system: general information accepts baseline protection, sensitive information needs to be strengthened, and important data related to national security or public interest faces the strictest control. Academic analysis shows that this classification method achieves accurate allocation of regulatory resources by calibrating protection to the level of risk[7].

Severe further processing requirements. Different from the 'compatible' further treatment standard of GDPR, PIPL adopts a more stringent 'directly related' standard in Article 6. The distinction between compatibility and directness is highlighted in academic discourse[19]. Article 14 mandates new consent to changes in the purpose, method, or data type of processing to prevent task crawling and provide companies with clear compliance boundaries, while protecting individuals from unauthorized data reuse.

4.3.Regulatory logic and power structure

The Regulation on the Protection of the Right to Network Dissemination of Information establishes a distributed law enforcement framework. Article 60 gives the overall coordination power to the China Cyberspace Administration (CAC), while delegating the supervision power of specific departments to industrial and information technology, public safety and market supervision regulators. By maintaining regional compliance supervision, local authorities have created a collaborative regulatory model that is different from the independent power structure of the GDPR[19].

Enforcement provisions include severe penalties, with Article 66 authorizing fines of up to $50 million or 5% of annual income for serious violations, reflecting the size of the GDPR's penalties and indicating significant non-compliance costs.

Article 58 stipulates the special obligations of large platforms, requiring the establishment of a compliance system, the establishment of an independent monitoring body with external members, and the publication of annual social responsibility reports[3].This kind of supervision is similar to the gatekeeper supervision mechanism of GDPR, which reflects the recognition that the platform with systematic influence needs to strengthen supervision, although the implementation mechanism is different[20].

It is recommended to adopt a European regulatory model and develop a '1 + X' power system in China. The CAC will coordinate industry regulators through an information-sharing mechanism to enhance the effectiveness of law enforcement, while avoiding the fragmentation of bureaucracy[19].

4.4.Cross-border data regulation

PIPL's outbound data transmission system revolves around the four pillars of security assessment, standard contract, certification and legal exemption, and the core focuses on 'security and controllability'[2].Assess and assess potential risks to national security, public interests and individual rights, and juxtapose cross-border data flows with the protection of individual rights as a sovereign matter.

Article 38 lists the conditions [processors can pass the CAC's safety assessment, obtain special certification, use a standard contract recognized by the CAC, or meet other statutory conditions. The "Implementation Rules for Personal Information Protection Certification" in 2022 provides detailed guidance]. Article 39 requires a separate consent to overseas transfers[3], and article 40 provides for domestic storage of critical infrastructure operators and high-volume processors[11]. When the outbound transfer is indeed necessary, the safety assessment is applicable.

Article 41 is a foreign government request based on the principle of reciprocity, while article 42 restricts overseas entities from engaging in activities that are harmful to Chinese citizens or national security. PIPL and GDPR both promote data transmission through international agreements. Studies have shown that they have potential application value in the negotiation of the China-EU Passenger Name Record (PNR) agreement in China's civil aviation sector[18].

4.5.The PIPL in civil aviation

Chinese airlines face a dual compliance challenge: both to meet the requirements of GDPR for European operations and to meet the extraterritorial coverage of PIPL. Article 3 applies to the overseas processing of Chinese citizens' information[11], which reflects the targeting standard of GDPR[18].

China Eastern Airlines has provided a well-known case study, implemented a GDPR compliance project, appointed a data protection officer, and built what it calls 'six security fences'. These measures were shown to be effective in the Fang Yueming case, where the court ruled in favor of the airline after finding that the airline's data protection practices met international standards in the case of alleged improper data processing[18].

The PNR data is still a regulatory gap, because China currently relies on a limited framework of '2018 passenger information withholding measures' and requires comprehensive PNR legislation[18]. Studies have shown that while promoting multilateral cooperation, the establishment of systems consistent with international standards will enhance security and compliance. The analysis of enforcement trends shows that the lack of clear PNR rules has caused regulatory uncertainty for airlines and regulatory authorities, which highlights the need to prioritize this legislative gap.

5.Dialogue, tensions, and convergence in global integration

GDPR and PIPL are not isolated. They now exist in a world where data never stops at the border. Watching their interaction reveals a complex picture. There is competition. There is a sharp tension. But there is also convergence. Each system adjusts to the challenges posed by another system[12].

5.1.When paradigms clash

The EU's adequacy mechanism unilaterally exports its standards through a compliance assessment framework, while

China's outbound transfer system is rooted in sovereign considerations and may be regarded as protectionism from a European regulatory perspective. This divergence reflects a deeper value orientation: the supremacy of individual rights and the dynamic balance of multiple values[7].

The quantifiable economic impact has been determined. Empirical studies have shown that GDPR has reduced China's digital service exports to the EU by about 17 % compared with non-EU markets. The impact is mainly driven by compliance and operational search costs, disproportionately affecting the financial and telecommunications sectors, with the insurance industry, which is already heavily regulated, showing minimal disruption[21].

5.2.Finding common ground

Regulatory convergence is evident because PIPL incorporates elements affected by GDPR, and Chinese entities, including China Eastern Airlines and Huawei, have implemented GDPR-compliant systems and established EU-based data storage facilities[18].Both frameworks target large platforms through specific obligations: GDPR authorizes Data Protection Officers (DPOs), while PIPL requires an independent oversight mechanism[22].The convergence trend of risk-based management can be observed by using tools such as data protection impact assessment (DPIA) and data subject access request (DSAR) for full life cycle data governance[18].

China's 2022 certification system is consistent with international standards for transparency and accountability, laying the foundation for future mutual recognition with the EU[18]. Both regulatory frameworks involve algorithmic governance: GDPR Article 22 restricts automated decision-making, while PIPL requires fairness and transparency in algorithmic processing. The protection of vulnerable groups represents another convergence point. The GDPR requires parental consent for minors under 16 years of age, and the PIPL designates minors under 14 years of age to strengthen protection through guardian consent and stricter security measures[3].

Multinational enterprises promote practical integration by establishing a unified compliance system for dual-market operations, and extracting common requirements such as informed consent and notice of default while implementing local adaptation[6]. The analysis of corporate compliance reports shows that this approach is forming a defacto global norm under the formal legal framework.

5.3.The PNR puzzle

Civil aviation reflects the tension of regulation. The EU's PNR directive gives priority to public safety, while GDPR emphasizes individual rights, which leads to internal conflicts. The European Commission has resisted changes to the directive, despite the European Commission for Data Protection citing incompatibility with the European Union Court of Justice (CJEU) requirement. This debate provides valuable lessons for China's emerging PNR framework, highlighting the importance of the principles of necessity and proportionality[18].

5.4.Enforcement across borders

GDPR exercises extraterritorial jurisdiction through Article 27, which authorizes designated representatives of non-EU controllers, such as Locatefamily.com, to lead to the enforcement of fines. Article 3 of PIPL reflects this extraterritorial scope, creating a parallel regulatory basis to support potential cooperation mechanisms, including viable joint enforcement pilots within the civil aviation sector[18].

6.Conclusion

First of all, GDPR and PIPL represent different ethical paradigms and have a deep cultural foundation. GDPR enhances individual rights through a sound legal mechanism, while PIPL pursues a dynamic balance between individual, industrial and national interests. Both frameworks have made a comprehensive response to digital challenges, but neither of these methods has inherent superiority, but reflects their respective social backgrounds.

Secondly, these paradigms show compatibility through coexistence tension and convergence. Common challenges drive regulatory alliances without erasing distinct characteristics, reflecting a diversified convergence model rather than substitution. The regulatory focus has shifted from post-remediation to life-cycle governance, with prevention and systemic accountability as organizational principles.

Thirdly, ethical diversity needs to be acknowledged, because the generalization of a single model is still impractical. Future coordination should give priority to 'principle-based interoperability' - flexible mechanisms built around core principles such as transparency and accountability. In the field of civil aviation, China should learn from the experience of GDPR implementation and advocate a multilateral PNR framework.

Fourth, China's cross-border data governance needs to enhance precision, inter-agency collaboration and transparency. This requires a sound classification system, coordinated regulatory authorities, and clear review guidelines to prevent regulatory confusion and unintended trade barriers, despite good policy objectives.

The future of global data governance lies not in binary choices, but in embracing multiple paths while upholding basic values. Through multilateral dialogue, stakeholders can build an order that upholds human dignity, stimulates innovation, and maintains security. There is no single legal framework to provide universal solutions; on the contrary, cross-cultural regulatory exchanges provide mutually beneficial insights, consistent with the 'Community of Shared Future in Cyberspace' initiative.

There are some deficiencies in this study. First, the comparative analysis focuses on GDPR and PIPL, excluding other influential regulatory frameworks, such as Brazil's LGPD or India's DPDP bill. Second, empirical data on the impact of long-term compliance is still limited, especially for SMEs in developing economies. Future research should explore the trilateral comparison of emerging economies and conduct a longitudinal study on the regulatory adaptation of cross-border industries.

Author contributions Zhengyu Yang: Conceptualization, Methodology, Writing – original draft. Di Jiang: Investigation, Data curation, Visualization. Yuyang Liu: Supervision, Writing – review & editing. All authors read and approved the final manuscript.

Funding No funding was received for this work.

Data availability The data that support the findings of this study are available from the corresponding author upon reasonable request.

Declarations

Conflict of interest The authors declare no conflict of interest.

References

[1] FU X H. The Structural Impact of Generative AI on the Personal Information Protection Law and Countermeasures. Law Forum, 2025, 40(6): 102-112.
[2] YE C X, YAN W G. On the Current Situation, Problems, and Solutions of China's Cross-Border Data Regime. Journal of Beijing University of Aeronautics and Astronautics (Social Sciences Edition), 2024, 37(1): 57-71.
[3] NATIONAL PEOPLE'S CONGRESS STANDING COMMITTEE. Personal Information Protection Law of the People's Republic of China. Gazette of the Standing Committee of the National People's Congress of the People's Republic of China, 2021, (6): 1117-1125.
[4] BRADFORD A. The Brussels Effect: How the European Union Rules the World. Oxford: Oxford University Press, 2020.
[5] SCHWARTZ P M. Global data privacy: The EU way. New York University Law Review, 2019, 94(4): 771-818.
[6] GORECKA A. Competition and data protection in the digital economy: A comparative analysis of the EU and China. Tsinghua China Law Review, 2025, 18(1): 23-51.
[7] DING X D. Interpretive Reconstruction of the Sensitive Personal Information Protection System. China Legal Science, 2025, 2: 168-187.
[8] BYGRAVE L A. Data Privacy Law: An International Perspective (2nd ed.). Oxford: Oxford University Press, 2024.
[9] ZHANG C H, LI Z Z, PEI L. Multidisciplinary Intersection and Multi-Scenario Embedding: A Review of Data Ethics Research at Home and Abroad. Journal of Information Resources Management, 2025, 15(2): 91-107.
[10] YANG F. The Evolution of EU Legal Supervision of Cross-Border Data Flows in the Post-Schrems II Era and China's Response. Global Law Review, 2022, 44(1): 178-192.
[11] LI Z Z, LIU Z Y, ZHANG C H. Research on the Identification and Control of EU Cross-Border Data Risks from an Evidence-Based Perspective. Information Studies: Theory and Application, 2025, 48(4): 192-201.
[12] JIN J. The EU General Data Protection Regulation: Evolution, Key Points, and Ambiguities. Chinese Journal of European Studies, 2018, 36(4): 1-26.
[13] ZHANG J W. Legislative Intent and Systematic Structure of the Legal Bases for Personal Data Processing in the GDPR. Journal of Nanjing Normal University (Social Science Edition), 2025, 2: 127-136.
[14] KUNER C, BYGRAVE L A, DOCKSEY C, et al. The EU General Data Protection Regulation (GDPR): A Commentary. Oxford: Oxford University Press, 2020.
[15] YANG C X, QIU S T. Analysis of the Impact of EU GDPR on Cross-Border Civil Aviation Data. Journal of Beijing University of Aeronautics and Astronautics (Social Sciences Edition), 2024, 37(6): 135-150.
[16] HONG Y Q. The Fragmentation of Cross-Border Data Flow Rules and China's Response. Administrative Law Review, 2022, 4: 61-72.
[17] CHENG X. Understanding and Application of the Personal Information Protection Law. Beijing: China Legal Publishing House, 2021.
[18] ZHOU H H. Analysis of the "Gatekeeper Clause" in the Personal Information Protection Law. Science of Law (Journal of Northwest University of Political Science and Law), 2022, 40(5): 36-49.
[19] WANG D. The Institutional Construction of Security Assessment for Outbound Data Transfers. Science of Law (Journal of Northwest University of Political Science and Law), 2025, 43(5): 100-111.
[20] GAO F P. Personal Information Protection: From Individual Control to Social Control. Beijing: Law Press, 2021.
[21] MA S Z, YI Z X, PAN G J, et al. Host Country Data Privacy Protection Policies and China's Digital Services Trade Exports: Evidence from the EU's General Data Protection Regulation. Collected Essays on Finance and Economics, 2026, 42(1): 39-49.
[22] WANG L M. On the Legal Protection of the Right to Personal Information: Centered on the Distinction between the Right to Personal Information and the Right to Privacy. China Legal Science, 2013, 35(4): 62-72.