Modern Jurisprudence

Vol. 3, Issue 3 | September-December 2025

ARTICLE

China's Personal Information Protection Law (PIPL) 2021: An Analysis

Zhang Yi-Chen[1]

Abstract

China's Personal Information Protection Law (PIPL, Chinese: 中华人民共和国个人信息保护法) 2021 represents one of the world's most comprehensive data-protection frameworks, introduced amid rapid digitalization, platform-economy expansion, and intensifying concerns over privacy, cybersecurity, and data sovereignty. This article provides an in-depth analysis of the PIPL's architecture, examining its core principles, legal bases for processing, data-subject rights, obligations for personal-information handlers, cross-border transfer requirements, sensitive-data protections, algorithmic-governance rules, and enforcement mechanisms. Through a structured doctrinal and comparative assessment, the paper highlights how PIPL blends GDPR-influenced privacy norms with China's unique governance model, characterized by strong state oversight, national-security imperatives, and campaign-style regulatory enforcement. The study finds that while PIPL significantly strengthens individual rights and corporate accountability, its broad state exemptions, expansive compliance burdens, data-localization rules, and regulatory opacity create substantial challenges for both domestic firms and multinational companies. Comparative insights with the GDPR, India's DPDP Act 2023, and U.S. sectoral privacy laws reveal convergences in rights and transparency requirements but marked divergences in enforcement philosophy and data-sovereignty orientation. The article concludes by identifying key policy implications and proposing reforms to enhance clarity, predictability, and long-term effectiveness within China's evolving data-governance framework.

Keywords: *Data Protection, Privacy Law, China, Cybersecurity Law, Data Sovereignty, Cross-Border Data Transfers, Algorithmic Governance, Digital Regulation, Comparative Privacy Law, Consent and Transparency, Data Localization, Enforcement Mechanisms.*

[1] The author is an Associate, Data Privacy & Cybersecurity Practice Chan & Partners Solicitors, Hong Kong SAR

Introduction

China has undergone a significant transformation in its approach to data governance, moving towards a robust regulatory framework that balances rapid economic growth with national security and personal data protection. This shift is evident in the promulgation of foundational laws such as the Cybersecurity Law, the Data Security Law, and notably, the Personal Information Protection Law of 2021 (Wang et al., 2024; Zhang, 2024). The focus has strategically broadened from mere network infrastructure development to comprehensive cybersecurity and data privacy, reflecting the state's intent to reinforce its legitimacy amidst prevalent digital abuses (Jia, 2023; Wang, 2024).

The PIPL stands as a pivotal development in the global data privacy landscape. Often drawing comparisons with the European Union's General Data Protection Regulation, PIPL shares core principles while simultaneously introducing distinct requirements (Bolatbekkyzy, 2024; Calzada, 2022; Tan & Zhang, 2021). Key distinctions include its extraterritorial reach and stringent mandates for cross-border data transfers, which necessitate data localization for significant volumes of personal information (Beccia et al., 2024, 2022). These features underscore PIPL's considerable influence on international data flows and its role in shaping the evolving global digital order (Calzada, 2022).

Despite the growing body of literature surrounding PIPL, several gaps in scholarship persist, particularly concerning its comparative analysis, enforcement mechanisms, and techno-regulatory implications. While many studies highlight the similarities and differences between PIPL and GDPR, a more coherent, theory-grounded analysis is needed to fully understand how PIPL's evolution is shaped by China's unique political, cultural, and legal environment, rather than solely by Western regulatory models (Li & Chen, 2023, 2024).

Challenges in enforcement are also a significant area requiring further investigation. Existing research points to a disconnect between technical implementation and privacy principles, insufficient collaboration between engineers and legal experts, and a general lack of understanding regarding third-party SDKs (Tao et al., 2025). The effectiveness of China's unique campaign-style enforcement, such as Special Privacy Rectification Campaigns, remains to be comprehensively evaluated, especially given the resource limitations faced by regulators (Jing et al., 2025; Tao et al., 2025). Furthermore, the ambiguity in specific PIPL provisions, like those governing separate consent and anonymization, poses practical difficulties for implementation and compliance (He et al., 2025). The techno-regulatory approach, characterized by a "twin peaks model" of enforcement via the Cyberspace Administration of China and the Ministry of Industry and Information Technology (Wang, 2024), warrants deeper exploration, particularly concerning its impact on apps' privacy practices (Kollnig et al., 2024) and the inherent tension between individual privacy rights and national security imperatives (He et al., 2025). User perceptions and online platform compliance also represent crucial, underexplored facets of PIPL's real-world impact (Zhou et al., 2024).

Against this backdrop, this paper seeks to address these scholarly lacunae by providing a comprehensive analysis of China's PIPL.

Historical and Legal Context

China's Pre-PIPL Data Governance Landscape

Before the enactment of the PIPL in 2021, China's data governance landscape was characterized by a foundational, yet fragmented, approach, primarily driven by national security and public interest concerns (Reer et al., 2023). This period saw the introduction of key legislative pieces that laid the groundwork for a more comprehensive data protection regime.

The **Cybersecurity Law of 2017** was a landmark legislation designed to protect network security, safeguard cyberspace sovereignty and national security, and regulate data collection, processing, and use by network operators (Cao & Hu, 2023; Prabu et al., 2023). It established the principle of data sovereignty, asserting state control over data acquired within mainland China (Reer et al., 2023).

Building upon the CSL, the **Data Security Law of 2021** emerged as a fundamental pillar in China's data security framework. The DSL introduced a categorized and graded protection system for data, based on its potential impact on national security, and mandated regulations for data storage and transfer (Voss & Pernot-Leplay, 2023). It also established mechanisms for data security emergency response and review systems (Voss & Pernot-Leplay, 2023). Critically, the DSL extended data localization obligations to "important data," mandating its storage within national borders (Belli, 2021). These laws together aimed to enhance the national data security protection capability and the governance of the digital economy (Cao & Hu, 2023; Prabu et al., 2023).

Prior to PIPL, **sectoral rules** also played a significant role, reflecting an earlier, U.S.-like model of data protection with specific regulations for different domains (Voss & Pernot-Leplay, 2023). An example is the Electronic Commerce Law of 2019, which included provisions requiring e-commerce operators to comply with laws and administrative regulations concerning personal information protection when collecting and using user data (Cao & Hu, 2023; Prabu et al., 2023).

The drivers behind this evolving landscape included:

- **Surveillance:** While not explicitly detailed as a direct driver for every piece of legislation, the emphasis on national security and public interest within the CSL and DSL implicitly supported the state's capacity for monitoring and control over digital information (Reer et al., 2023).
- **Digital Economy:** The rapid growth of China's digital economy necessitated robust regulatory frameworks to manage the increasing volume and complexity of data, as highlighted by the DSL's role in enhancing data governance capabilities (Cao & Hu, 2023; Prabu et al., 2023).
- **Public Trust:** The broader movement towards comprehensive personal data protection, culminating in PIPL, was also a response to a growing recognition of the need to protect citizens' rights in the digital sphere, thereby aiming to foster public trust in digital platforms and services (He & Chen, 2025).

Why PIPL Was Introduced

The introduction of the PIPL on November 1, 2021, marked a significant step in China's data governance journey, moving towards a comprehensive framework for personal data protection (Bolatbekkyzy, 2024; Tan & Zhang, 2021). Several factors converged to necessitate its promulgation:

- **Rising Domestic Privacy Concerns:** With the widespread adoption of digital technologies and the burgeoning platform economy, concerns about personal data misuse and inadequate protection grew among the Chinese populace (He & Chen, 2025). The PIPL was designed to provide individuals with extensive data protection rights, addressing these domestic privacy concerns (Tan & Zhang, 2021). The Civil Code of 2021 also created new legal rights to privacy and personal information protection, underscoring the increasing legal recognition of these rights (Belli, 2021).
- **Global Pressure:** PIPL is widely recognized as being significantly influenced by the European Union's General Data Protection Regulation (Buckley et al., 2024). It shares many core principles with the GDPR, including rights of access, correction, and deletion of personal data, as well as principles of data minimization and accountability (Weuts et al., 2025). This modeling after the GDPR reflects a broader global trend towards more stringent data protection laws and China's engagement with international data governance standards (Calzada, 2022; Tan & Zhang, 2021). However, PIPL also introduces distinct requirements, leading some to describe it as a "GDPR with Chinese characteristics" that aligns with China's unique political, cultural, and legal environment (Belli, 2021; Li & Chen, 2024).
- **Platform Economy and Big Tech Abuses:** The rapid expansion of the platform economy led to increasing instances of data security issues and personal privacy infringements by large technology companies (Chen & Liu, 2024). PIPL, alongside cyber and data security reviews following events such as Didi's IPO, aimed to curb the excessive data power of these platforms and facilitate interoperability, thereby addressing concerns about data exploitation and abuses in the big tech sector (Zhenbin, 2023).
- **State Interest in Structured Data Sovereignty:** While CSL and DSL established the principle of data sovereignty, PIPL further refined and completed China's data protection regime. The state's interest extends beyond mere control to actively structuring and "activating" data transaction, sharing, and use within a regulated environment (Zhenbin, 2023). This approach balances individual rights with broader economic and national security interests, solidifying China's approach to data sovereignty within its distinct socio-political and economic context (Li & Chen, 2024; Weuts et al., 2025).

Architecture of the PIPL

Scope, Applicability & Definitions

The PIPL establishes a comprehensive framework for safeguarding personal information within China, defining key terms and delineating its broad applicability.

- **Personal Information:** PIPL defines personal information as "all kinds of information, excluding anonymized information, recorded electronically or otherwise, relating to an identified or identifiable natural person" (Zhang & Wang, 2022). This definition is similar to that found in the European General Data Protection Regulation (Li et al., 2024). Information is considered anonymous only if it is "impossible to distinguish specific natural persons and impossible to restore" (Reer et al., 2023).
- **Sensitive Personal Information:** PIPL includes a broader scope for what constitutes "sensitive" personal information compared to the GDPR's "special category" data (Beccia et al., 2024).
- **Extraterritorial reach:** PIPL extends its applicability extraterritorially, encompassing activities such as providing products or services to individuals within China or analyzing and assessing the activities of natural persons within China. This extraterritorial scope mirrors similar provisions in Article 3 of the GDPR (Li & Chen, 2023).
- **Automated decision-making:** Article 45 of PIPL includes provisions related to the Right of Access by the Data Subject, which are comparable to GDPR's Article 15 and address aspects of automated decision-making in the context of data subjects' rights (Li et al., 2024).

Core Principles

The PIPL is built upon several core principles designed to ensure the lawful and ethical processing of personal information:

- **Legality, necessity, and transparency:** PIPL mandates that the processing of personal information must be lawful, fair, and transparent (Articles 5, 7 PIPL) (Li & Chen, 2023). This includes having a clear and reasonable purpose directly related to the processing and ensuring that the processing has the least impact on individual rights and interests (Zhao, 2023). Transparency requires disclosing the rules for processing personal information, including the purpose, manner, and scope (Zhao, 2023).
- **Purpose limitation:** Personal information can only be collected for specified, explicit, and legitimate purposes (Article 6 PIPL) (Li & Chen, 2023). If the purpose, manner, or type of personal information processed changes, renewed consent from the individual is generally required (Zhao, 2023).
- **Data minimization:** The law stipulates that only the minimum amount of data necessary to fulfill the specified purposes should be collected (Article 6 PIPL) (Li &

Chen, 2023). This principle ensures that data collection is proportionate to the processing objective.

- **Accountability:** PIPL emphasizes accountability (Article 9 PIPL), requiring those who process personal information to be responsible for the security of the data they handle (Li & Chen, 2023; Reer et al., 2023).

Roles & Responsibilities

PIPL defines various roles and assigns specific responsibilities for the handling of personal information:

- **Personal Information Handlers (equivalent of controllers):** PIPL uses the term "data handler" to encompass concepts similar to data controllers and data users found in other jurisdictions. These handlers are directly responsible for the security of the personal information they manage (Reer et al., 2023). Articles 51–59 of PIPL define their duties, while Articles 66–71 outline legal punishments for violations, including monetary penalties (Reer et al., 2023).
- **Entrusted Parties (processors):** While PIPL primarily uses the term "data handler," the law implicitly addresses scenarios where one entity processes data on behalf of another, similar to processors in other legal frameworks (Alkhamsi & Alqahtani, 2024).
- **Joint handlers:** The concept of multiple parties jointly determining the purposes and means of processing, akin to joint controllers, is implicitly covered within the PIPL's broad definition and responsibilities assigned to Personal Information Handlers.
- **Government role:** The PIPL also outlines penalties for responsible individuals within state organs who fail to adequately protect personal information, highlighting the government's role in enforcing the law and ensuring compliance (Reer et al., 2023).

Legal Bases for Processing Under PIPL

The PIPL outlines specific legal bases that must be established for the lawful processing of personal information, with consent playing a central, albeit complex, role.

Consent and Conditions for Validity

Consent is a primary legal basis for processing personal information under PIPL (Jin & Skiera, 2022). However, it comes with stringent conditions and specific requirements:

- **Explicit consent:** While PIPL requires clear consent, for certain types of data or processing activities, a higher standard of consent is mandated.
- **Separate consent:** PIPL often requires "separate consent" in situations where the GDPR might only require "explicit" consent (Li & Chen, 2023). This is particularly true for:

- **Sensitive personal information:** Processing sensitive personal information requires separate consent from the individual (Beccia et al., 2024; Jin & Skiera, 2022; Li & Chen, 2023; Yao & Fei, 2023).
- **Cross-border processing:** Transfers of personal information outside China can only occur when individuals have been properly informed and provide separate consent (2022; Voss & Pernot-Leplay, 2023). Notably, PIPL views consent as an *additional, accumulative requirement* for international data transfers, and it cannot alone legitimate such transfers (Li & Chen, 2023).

- **Revocation:** Individuals have the right to withdraw their consent (Jin & Skiera, 2022). If the purpose, manner, or type of personal information processed changes, renewed consent from the individual is generally required (Zhao, 2023).
- **Challenges in practice:** The requirement for "separate consent," especially for cross-border data transfers, can create a significant compliance burden for data handlers (Voss & Pernot-Leplay, 2023).

Exceptions to Consent

While consent is paramount, PIPL also provides other legal bases for processing personal information that do not require explicit consent (Zhao, 2023). These alternatives are typically more limited in scope compared to the broad "legitimate interest" basis often found in other data protection regimes like the GDPR (Jin & Skiera, 2022).

The recognized exceptions to requiring consent for processing include:

- **Contract necessity:** Processing is necessary for the conclusion or performance of a contract to which the individual is a party (Jin & Skiera, 2022; Zhao, 2023).
- **Legal duties/obligations:** Processing is necessary for the performance of legal duties or legal obligations (Jin & Skiera, 2022; Zhao, 2023).
- **Public interest:** Processing is for the public interest in the implementation of news reporting, public opinion monitoring, or other acts, within a reasonable range of personal information (Jin & Skiera, 2022; Zhao, 2023).
- **Emergency response:** Processing is necessary for responding to public health emergencies, or for protecting the life, health, and property of natural persons in emergency situations (Jin & Skiera, 2022; Zhao, 2023).
- **Vital interest:** Processing is necessary to protect the vital interests of the personal information subject or other individuals (Jin & Skiera, 2022).
- **Publicly disclosed information:** Processing within a reasonable range of personal information that individuals disclose themselves or other personal information that has been lawfully disclosed (Zhao, 2023).

High ambiguity vs. GDPR's clearer structure: PIPL generally provides a more prescriptive and less flexible framework for legal bases compared to the GDPR. For instance, PIPL does not explicitly recognize "legitimate interest" as a general legal basis for processing, a

significant divergence from the GDPR (Jin & Skiera, 2022). This can lead to greater ambiguity for organizations accustomed to the GDPR's broader structure and its clearer set of derogations for specific situations (Li & Chen, 2023). The "necessary" criteria for exceptions under PIPL also require further clarification (Zhao, 2023).

Rights of Individuals

The PIPL grants individuals a comprehensive set of rights concerning their personal information, largely mirroring those found in advanced data protection regimes like the GDPR. These rights aim to empower data subjects by providing them greater control and transparency over how their personal data is handled.

Right to Know

Individuals have the **right to be informed** about the processing of their personal information (Li & Chen, 2023). This fundamental right necessitates that personal information handlers adhere to principles of openness and transparency. They must clearly disclose the rules for processing, including the purpose, manner, and scope of data processing, ensuring that individuals understand how their data will be used (Zhao, 2023).

Right to Access & Data Portability

PIPL provides individuals with the **right to access** their personal information (Article 45 PIPL) and inspect it (Berzin & Mitianov, 2025; Li & Chen, 2023). They can request details about the data being processed, including purposes, recipients, retention periods, and the logic behind automated decisions (Reuben et al., 2016). Furthermore, the law includes the **right to data portability**, allowing individuals to receive their personal data in a readily usable format, facilitating its transfer to another organization (Article 45 PIPL) (Li & Chen, 2023).

Right to Correct or Delete

Individuals also possess the **right to rectification** (Article 46 PIPL), enabling them to request corrections or completion of inaccurate personal information (Aljeraisy et al., 2020; Li & Chen, 2023). Correspondingly, PIPL establishes the **right to erasure** (Article 47 PIPL), often referred to as the "right to be forgotten," which permits individuals to request the deletion of their personal data, especially if it is false, misleading, or processed in violation of the law (Berzin & Mitianov, 2025; Li & Chen, 2023).

Restrict or Refuse Processing

PIPL incorporates a right for individuals to **object to or restrict the processing** of all or part of their personal information (2024; Voss & Pernot-Leplay, 2023). This empowers data subjects to limit how their data is used, particularly if they withdraw consent or have legitimate reasons to oppose certain processing activities.

Right to Explanation for Automated Decision-Making

A significant right under PIPL is the **right to an explanation** concerning automated decision-making processes (Article 24 PIPL) (J. Lee, 2025; J. H. Lee, 2025). If an automated decision significantly impacts an individual's rights and interests, they can request an explanation. This explanation should detail the result of the decision, the types of personal information used, the major criteria involved, and the procedures by which the automated decision was made (Kim & Park, 2024). This provision aims to mitigate the opacity often associated with algorithmic decision-making (Zou & Zhang, 2022).

Vulnerable Groups (Minors' Data Protections)

While not explicitly detailed in the provided excerpts for PIPL, the law is understood to include special protections for vulnerable groups, particularly minors. PIPL's framework, drawing comparisons to the GDPR, includes provisions for **parental consent** (Article 31 PIPL), indicating specific safeguards for children's personal information processing (Li & Chen, 2023). Such provisions acknowledge that minors may be less aware of the risks and consequences of data processing and therefore require enhanced protection (Malgieri & Fuster, 2021).

Limitations and Practical Enforcement Issues

Despite the comprehensive nature of these individual rights, their practical enforcement under PIPL faces several challenges:

- **Ambiguity in Provisions:** Certain provisions within PIPL, such as the definition of "separate consent" and criteria for anonymization, remain ambiguous, creating difficulties for consistent interpretation and enforcement (He et al., 2025).
- **Balancing Act:** There is an inherent challenge in balancing individual privacy rights with broader national security interests, especially when government access to personal data is permitted under certain conditions (He et al., 2025).
- **Limited Case Law:** The nascent stage of PIPL's implementation means there is a "scant corpus of case-law," making it difficult to establish clear judicial interpretations and consistent patterns of enforcement (Li & Chen, 2023).
- **Judicial Approach:** Chinese courts may adopt a more tolerant stance when balancing individual rights against economic imperatives and business freedoms, which can lead to less stringent outcomes for data subjects (Li & Chen, 2023).
- **Fragmented Enforcement:** The absence of a single, independent data protection authority, coupled with fragmented jurisdiction among various government departments, can complicate the enforcement landscape and often places the burden of initiating legal proceedings on individuals (Deursen & Kummeling, 2019, 2020). This can be particularly challenging as Chinese courts have sometimes been described as "unwelcoming" or subject to political instructions (Deursen & Kummeling, 2019, 2020).

- **Compliance Gaps:** Studies indicate instances of non-compliance in post-PIPL privacy policies, particularly concerning inadequate risk assessments for sensitive data and challenges related to individual consent (Zhou et al., 2024).

Sensitive Personal Information

Definition and Categories

Under the PIPL, sensitive personal information is defined not just by its inherent nature, but also by a "consequentialist approach." This means that the disclosure risk and the potential damages that could arise from its misuse play a decisive role in categorizing information as sensitive (Yao & Fei, 2023). PIPL's scope for sensitive personal information is broader than the European Union's General Data Protection Regulation "special category" data (Beccia et al., 2024).

Categories of sensitive personal information explicitly mentioned or understood to be included under PIPL are:

- **Biometric characteristics** (e.g., fingerprints, facial recognition features) (Reer et al., 2023; Yao & Fei, 2023).
- **Religious beliefs** (Wawra, 2023).
- **Specific identity** (a term interpreted to cover personal attributes such as gender identity and sexual preferences) (Wawra, 2023).
- **Financial accounts** (Yao & Fei, 2023).
- **Medical health data** (Reer et al., 2023; Yao & Fei, 2023).
- **Any personal information relating to minors under 14** (Yao & Fei, 2023).

Stricter Compliance Requirements

PIPL imposes significantly stricter duties on personal information handlers when processing sensitive personal information compared to general personal information (Yao & Fei, 2023). These heightened requirements include:

- **Specific Purpose and Sufficient Necessity:** Processing of sensitive personal information must be for a specific purpose and with sufficient necessity (Reer et al., 2023; Yao & Fei, 2023).
- **Strict Protective Measures:** Handlers are required to adopt stringent protective measures to safeguard sensitive personal information (Jiang & Zheng, 2023; Reer et al., 2023; Yao & Fei, 2023).
- **Protection Impact Assessment:** A protection impact assessment is mandatory before processing sensitive personal information (Yao & Fei, 2023).

- **Separate Consent:** For certain processing activities involving sensitive personal information, obtaining "separate consent" from the individual is mandatory (Jiang & Zheng, 2023; Reer et al., 2023; Yao & Fei, 2023). This implies a higher standard of consent beyond general consent.
- **Notification Duties:** Personal information handlers must notify users of "the necessity of processing such sensitive PI" and "the influence on the individual's rights and interests" (Jiang & Zheng, 2023).

Despite these clear mandates, compliance rates for sensitive personal information protection often lag behind those for general personal information (Jiang & Zheng, 2023, 2024).

Impact on Sectors

The stringent regulations for sensitive personal information under PIPL have a notable impact across various sectors:

- **Finance:** Financial accounts are explicitly recognized as sensitive personal information (Yao & Fei, 2023). This means financial institutions and platforms handling financial data must adhere to the stricter compliance requirements, including separate consent and robust protective measures, for these data categories.
- **Health:** Real-world data related to medical and health data falls squarely within the definition of sensitive personal information (Yao & Fei, 2023). This poses significant challenges for medical research and health-related applications, as it often requires obtaining individualized "separate consent" from patients (Yao & Fei, 2023). Studies on health code apps and internet hospital apps in China have revealed that compliance with sensitive PI protection often trails behind general PI protection, particularly regarding separate consent (Jiang & Zheng, 2023, 2024).
- **Biometrics:** Biometric characteristics are explicitly listed as sensitive personal information (Reer et al., 2023; Yao & Fei, 2023). This means that entities collecting and processing biometric data, such as facial recognition for access control or payment systems, face stringent obligations under PIPL, necessitating careful adherence to the "specific purpose," "sufficient necessity," and "separate consent" principles.
- **Online Platforms:** Online platforms that collect various types of sensitive user data, including financial, health, or biometric information, are subject to the enhanced PIPL requirements. Ensuring compliance with the stricter consent mechanisms and data protection measures for these categories of data becomes a critical operational challenge, especially for platforms that operate across borders (Beccia et al., 2024). Moreover, the dynamic nature of digital technologies and the inherent context-sensitivity of personal information present ongoing obstacles to achieving comprehensive sensitive personal information protection (Li et al., 2023).

Cross-Border Data Transfers

China's PIPL establishes a stringent framework for cross-border data transfers, reflecting a cautious approach that prioritizes national security and public interest while also aiming to protect personal information (Xie et al., 2023). This framework presents unique challenges and considerations for entities operating within and outside China.

Regulatory Conditions

PIPL outlines several mechanisms for lawful cross-border data transfers, all of which require prior Personal Information Protection Impact Assessments and "separate consent" from individuals for the transfer (2022; Yao & Fei, 2023). The primary regulatory conditions include:

- **Security Assessments by CAC:** Transfers of personal information by Critical Information Infrastructure Operators and those processing large volumes of personal information (reaching certain thresholds) must undergo a **security assessment** organized by the Cyberspace Administration of China (2022; Yao & Fei, 2023). These assessments specifically evaluate the risks of data export activities on national security, public interest, and the legitimate rights and interests of individuals or organizations (Li & Chen, 2023).
- **Certification Mechanisms:** PIPL provides for **personal information protection certification** from a specialized agency recognized by the CAC as a legitimate channel for cross-border data transfers (Yao & Fei, 2023). While certification specifications exist, they are currently not well-defined enough for companies to rely confidently on them for data transfers (Voss & Pernot-Leplay, 2023). This method is generally seen as more costly than using contractual clauses (Voss & Pernot-Leplay, 2023).
- **Standard Contractual Clauses:** Personal information handlers can enter into a **standard contract** formulated by the CAC with the overseas recipient (Yao & Fei, 2023). The final version of China's Standard Contractual Provisions was published in February 2023, providing a clearer framework for when data handlers may use them (Voss & Pernot-Leplay, 2023). These clauses detail elements such as the identities of the parties, purpose of transfer, and measures to protect individuals' rights, many of which are familiar to entities accustomed to GDPR compliance (Voss & Pernot-Leplay, 2023).

Data Localization Requirements

China's data governance framework, including PIPL, imposes significant data localization requirements, particularly for specific types of entities and data:

- **Critical Information Infrastructure Operators:** CIIOs are mandated to store personal information within China (Beccia et al., 2024, 2022). If such information needs to be transferred overseas, it must undergo a security assessment by the CAC (2022). The definition of a CIIO, initially introduced in the Cybersecurity Law, is further elaborated in the Critical Information Infrastructure Security Protection Regulations from 2021 (Voss & Pernot-Leplay, 2023).

- **Large-scale Processors:** Operators processing a large amount of personal information (exceeding thresholds set by relevant government agencies) are also obliged to store this data within China (Bian, 2022, 2022). Similar to CIIOs, any overseas transfer of this data necessitates a security assessment by the CAC (2022).
- **"Important data" localization:** Beyond personal information, "important data" also faces localization requirements (Bian, 2022). While the definition of "important data" has historically been vague, it generally refers to data that, if compromised, could harm national security, economic operations, social stability, public health, or security (Voss & Pernot-Leplay, 2023). This definition does not exclude sensitive personal information from being categorized as important data, requiring a case-by-case assessment (Voss & Pernot-Leplay, 2023).

Global Implications

PIPL's provisions on cross-border data transfers have significant global implications, influencing foreign companies and contributing to an evolving data sovereignty landscape:

- **Effects on Foreign Companies:** Foreign companies operating in China or offering services to Chinese individuals face considerable compliance challenges due to PIPL's extraterritorial reach and stringent transfer requirements (2022; Zuo, 2024). Restrictions on data flows both into and out of China are expected to continue and potentially amplify, requiring economic actors to adapt to these regulations (Voss & Pernot-Leplay, 2023). This also includes stringent disclosure requirements for foreign recipients of personal data, including their identity, purpose, and method of data utilization, along with obtaining explicit consent from individuals (Zuo, 2024).
- **China–EU/US Data Transfer Tensions:** PIPL's approach to cross-border data transfers highlights a divergence from EU and US data governance models (Zhang, 2024). Unlike the GDPR, which has fewer limitations on data flow and transfer, China imposes stricter requirements driven by national security concerns (Beccia et al., 2024). While the EU emphasizes strategic autonomy and human rights, and the US focuses on economic potential, both share concerns about data storage location and its implications for data sovereignty (Zhang, 2024). The PIPL's focus on national security in its data localization requirements marks a fundamental difference compared to the GDPR's role in facilitating intra-EU/EEA data flows (Li & Chen, 2023).
- **Emergence of Data Sovereignty Framework:** China's legal framework for cross-border data flows, built upon the Cybersecurity Law, Data Security Law, and PIPL, demonstrates a strong emphasis on national security and public interests (Chen, 2024; Xie et al., 2023). This holistic approach contributes to a global competition for "discourse power in data sovereignty," with China emerging as a key player in shaping norms and regulations concerning cyberspace governance (Zhang, 2024). China's data localization measures and the broader cross-border data flow regime are central to its evolving data sovereignty framework (Tao, 2024).

Automated Decision-Making & Algorithmic Governance

The PIPL addresses automated decision-making under Article 24, which regulates processing activities that generate outputs with significant impacts on individuals' rights and interests based solely on automated means (Li & Chen, 2023; Shen & Liu, 2022). This provision mirrors GDPR Article 22 but integrates with China's broader algorithmic governance framework, emphasizing transparency, fairness, controllability, and accountability (Shen & Liu, 2022).

Transparency Obligations

PIPL imposes transparency duties on handlers using ADM, requiring them to disclose processing rules and the logic of decisions upon request (Shen & Liu, 2022). Complementing this, China's Provisions on the Administration of Algorithmic Recommendation Services (effective March 1, 2022) mandate platforms to inform users conspicuously about algorithmic services and publish the basic principles, purposes, and main operating mechanisms (Arts, 2023; Kharitonova et al., 2023). Providers must optimize the transparency and interpretability of rules for content searching, sorting, and display to mitigate undesirable effects (Kharitonova et al., 2023).

Right to Explanation

Individuals hold a statutory right to explanations for ADM outputs that significantly affect their rights, including details on decision results, data used, key criteria, and procedures (Shen & Liu, 2022). Article 48 PIPL further enables requests for explanations of processing rules (Shen & Liu, 2022). Platforms must provide mechanisms for users to query, select, or delete personal characteristic tags, enhancing contestability (Arts, 2023).

Restrictions on Profiling

PIPL restricts solely automated decisions with significant impacts, granting individuals the right to refuse such processing (Shen & Liu, 2022). The 2022 Algorithm Regulations prohibit targeting personal characteristics without consent, offering opt-out options for personalized recommendations or full deactivation (Arts, 2023; Kharitonova et al., 2023). Algorithmic bias, such as discriminatory pricing in e-commerce, is curtailed by fairness mandates under PIPL Article 21 and E-Commerce Law Article 18 (Shen & Liu, 2022).

Impact on Social Media, Fintech, E-Commerce

These regulations profoundly affect recommendation-driven sectors. Social media and internet services must manage user models, geolocation rules, and content filtering to avoid illegal recommendations while enabling manual overrides (Kharitonova et al., 2023). Fintech faces scrutiny on pricing algorithms to prevent bias against repeat users (Shen & Liu, 2022). E-commerce platforms, central to "personalized recommendation" governance, must balance algorithmic efficiency with transparency and user choice amid PIPL's ADM limits (Shen & Liu, 2022).

Alignment with China's Algorithm Regulation

PIPL's ADM rules align seamlessly with the 2022 Provisions, which build on PIPL's "automated decision-making" concept by targeting "algorithm recommendation technology" (e.g., personalized push, sorting) (Shen & Liu, 2022; "The Cambridge Handbook of Responsible Artificial Intelligence," 2022). Both emphasize principled governance—transparency via disclosures, user autonomy through opt-outs, and bias mitigation—forming a cohesive framework across PIPL, E-Commerce Law, and the Regulations (Shen & Liu, 2022). This integration supports China's normative AI systems, prioritizing public interest in digital platforms (Shen & Liu, 2022).

Compliance Obligations

The PIPL imposes a range of compliance obligations on personal information handlers (processors) to promote accountability, risk management, and the implementation of robust organizational and technical safeguards (Li & Chen, 2023; Yan, 2023). These requirements emphasize proactive measures tailored to the scale, sensitivity, and risks associated with data processing activities.

Data Protection Officer Requirements

PIPL mandates the appointment of a **personal information protection officer** (analogous to a DPO under GDPR Articles 37–39) for handlers processing personal information on a large scale, as determined by cybersecurity and informatization authorities (Li & Chen, 2023; Nan, 2023). Article 52 of PIPL specifies that this responsible person oversees the processing activities and ensures the adoption of protection measures (Jin & Skiera, 2022; Nan, 2023). The role focuses on internal supervision, compliance with processing rules, and handling individual rights requests, promoting professionalism and independence in data protection governance (Nan, 2023). Unlike smaller handlers, large-scale processors or those dealing with sensitive data must designate this position to demonstrate organizational commitment to PIPL compliance (Kaiv et al., 2023).

Regular Audits

Personal information handlers are required to establish internal management systems and operational procedures as part of their compliance framework, including **regular compliance audits** (Jin & Skiera, 2022; Yan, 2023; Zhao, 2023). Article 51 outlines measures such as formulating internal rules, conducting audits, and preventing unauthorized access or breaches (Yan, 2023). Regulators, under Article 64, may mandate audits by professional institutions for high-risk activities, with processors encouraged to perform self-audits or engage third parties routinely (Yan, 2023; Zhao, 2023). These audits evaluate processing purposes, data categories, risk impacts, and security effectiveness, ensuring ongoing adherence to PIPL standards (Yan, 2023).

Impact Assessments

Personal Information Protection Impact Assessments are mandatory under Article 55 of PIPL, particularly for processing sensitive personal information, large-scale data handling, or activities using automated decision-making that significantly affect individuals (Li & Chen, 2023; Yao & Fei, 2023). Similar to GDPR's DPIA, PIPIA involves case-by-case evaluations of legality, necessity, risks, and mitigation measures, shifting focus to ex-ante risk prevention (Yao & Fei, 2023). Handlers must retain records for at least three years and conduct assessments prior to cross-border transfers or high-risk scenarios (Jin & Skiera, 2022; Voss & Pernot-Leplay, 2023). This embeds regulatory and ethical considerations into processing, especially for real-world data in health contexts (Yao & Fei, 2023).

Incident Reporting Duties

PIPL requires prompt **notification of personal information security incidents** under Article 57, akin to GDPR Articles 33–34 (Li & Chen, 2023). Handlers must report breaches to competent authorities (e.g., Cyberspace Administration of China) without undue delay, detailing the incident's scope, impacts, and remedial actions (Li & Chen, 2023). Affected individuals must also be informed to enable rights exercise, with failures attracting penalties up to 5% of annual revenue (Jin & Skiera, 2022; Voss & Pernot-Leplay, 2023). This duty underscores the shift toward preventive compliance and rapid response.

Mandatory Measures for High-Risk Processing

For **high-risk processing**, PIPL demands enhanced safeguards, including technical protections, data minimization, separate consent for sensitive data, and security assessments (Yan, 2023; Yao & Fei, 2023). Large-scale processors or Critical Information Infrastructure Operators face localization mandates and CAC-led assessments for transfers (2022; Yao & Fei, 2023). Certification or standard contractual clauses may apply, alongside dedicated governance structures (Jin & Skiera, 2022; Yao & Fei, 2023). These measures address risks from automated decisions, biometrics, or public health data, requiring tailored impact assessments and audits (Yan, 2023; Yao & Fei, 2023).

Differences from GDPR Compliance Framework

While PIPL mirrors GDPR in procedural obligations like DPO appointment, impact assessments, breach notifications, and audits (Li & Chen, 2023), key divergences reflect China's emphasis on national security and scale-based thresholds (Beccia et al., 2024; Li & Chen, 2023). PIPL lacks GDPR's "legitimate interests" basis but imposes stricter localization and separate consent for transfers, with broader "sensitive" data scope (Beccia et al., 2024; Yao & Fei, 2023). Audits are more regulator-triggered for high risks rather than self-initiated routinely, and extraterritorial handlers must appoint China-based representatives (Jin & Skiera, 2022, 2022). Fines reach 5% of revenue (vs. GDPR's 4%), but enforcement relies on a "twin peaks" model (CAC/MIIT) without a singular independent authority (Wang, 2024). Overall, PIPL's framework is more prescriptive for large handlers, prioritizing sovereignty over GDPR's flexibility (Li & Chen, 2023; Voss & Pernot-Leplay, 2023). Furthermore, China's PIPL, unlike the GDPR, adopts a consequentialist approach to defining sensitive personal information,

focusing on the potential damages and disclosure risks rather than objective context or subjective purpose (Yao & Fei, 2023).

Enforcement and Penalties

China's PIPL establishes a robust enforcement regime characterized by a multi-agency approach and severe penalties, reflecting a campaign-style strategy that combines administrative orders, large-scale reviews, and strict sanctions to deter violations (Tao et al., 2025). This framework prioritizes national security, public interest, and rapid rectification over independent judicial oversight.

Regulatory Bodies

PIPL enforcement operates under a decentralized yet coordinated "twin peaks" model, with central and local authorities sharing responsibilities (Li & Chen, 2023; Voss & Pernot-Leplay, 2023).

- **Cyberspace Administration of China:** As the principal authority and "super-regulator," the CAC holds primary responsibility for PIPL implementation, including drafting bylaws, standards, coordination of data protection rulemaking, cross-border transfer oversight, investigations, and administrative penalties (Berzin & Mitianov, 2025; Conde et al., 2025; Li & Chen, 2023; Voss & Pernot-Leplay, 2023). It leads cybersecurity reviews and has broad powers over cyberspace offenses related to personal information (Zhao, 2023).
- **Ministry of Public Security:** The MPS collaborates on investigations, particularly for cybersecurity incidents, personnel vetting, and punitive actions against major violators, often alongside the CAC (Voss & Pernot-Leplay, 2023; Zhang, 2024; Zhao, 2023).
- **Sectoral Regulators:** Industry-specific bodies enforce PIPL alongside general rules, such as the Ministry of Industry and Information Technology for telecommunications, apps, and irregular data collection; State Administration of Market Regulation for consumer and competition issues; and others like the China Banking and Insurance Regulatory Commission (Cao & Hu, 2023; Li & Chen, 2023; Voss & Pernot-Leplay, 2023). Local Public Security Bureau branches and the National Information Security Standardization Technical Committee support standardization and practical implementation (Berzin & Mitianov, 2025; Voss & Pernot-Leplay, 2023).

Penalties

PIPL imposes graduated penalties scaled to violation severity, with maximum fines reaching 5% of annual revenue for serious breaches, alongside operational restrictions (Zeng & Kim, 2025).

- **Fines:** Up to 5% of prior-year turnover for major violations, as demonstrated in high-profile cases; even partial PIPL breaches trigger multimillion-yuan penalties on companies and executives (Conde et al., 2025; Li & Chen, 2023; Zeng & Kim, 2025).

- **Suspension of Business:** App removal from stores, operational halts, or rectification orders within short timeframes for non-compliant apps (Cao & Hu, 2023; He & Zeng, 2025; Tao et al., 2025).
- **Blacklisting:** Repeated or severe offenders face public notifications, demands for rectification, and exclusion from app stores or markets, with thousands of apps targeted in campaigns (Cao & Hu, 2023; Prabu et al., 2023; Tao et al., 2025).
- **Social Credit Implications:** While not explicitly detailed under PIPL, enforcement ties into broader data compliance pressures, potentially affecting corporate credit ratings and market access through ongoing regulatory scrutiny (Cao & Hu, 2023).

Failures to comply exacerbate punishments, emphasizing deterrence through high-pressure administration (Cao & Hu, 2023).

Early Enforcement Cases

PIPL's implementation since November 2021 has featured selective, high-impact actions, often overlapping with Cybersecurity Law violations (Creemers, 2023; Li & Chen, 2023).

- **Didi Crackdown:** In 2021, the CAC initiated a cybersecurity review against Didi Global post-NYSE IPO for illegal personal information collection, leading to app removal from stores, a joint probe with MPS and others, and the highest data protection fine to date in 2022 (exact amount undisclosed publicly), penalizing executives and underscoring opacity in processes (Conde et al., 2025; He & Zeng, 2025; Li & Chen, 2023; Zeng & Kim, 2025; Zhao, 2023).
- **Big Tech Rectifications:** MIIT issued 24 batches of notifications by June 2022, targeting apps like WeChat, Douyin, Kuaishou, and Ctrip for irregular collection and misuse, demanding rectifications or removals amid "Great Rectification" campaigns reshaping platforms (Cao & Hu, 2023; Creemers, 2023; Prabu et al., 2023).
- **Health-Code Data Misuse:** During COVID-19, health code apps prioritized public health over privacy, but post-PIPL audits revealed gaps in protection officers, audits, and consent for sensitive data; enforcement shifted to compliance mandates as zero-COVID eased (Jiang & Zheng, 2023). Special Privacy Rectification Campaigns since 2019 addressed app ecosystem violations through mass reviews (Tao et al., 2025).

Comparative Analysis

This section provides a comparative overview of China's PIPL with key global counterparts, highlighting structural alignments and divergences shaped by differing priorities such as individual rights, national security, and market dynamics (Bolatbekkyzy, 2024; Calzada, 2022).

PIPL vs. GDPR

Similarities

PIPL and the EU's General Data Protection Regulation share foundational elements, including similar definitions of personal information (excluding anonymized data), individual rights (e.g., access, rectification, erasure), legal bases for processing, and compliance mechanisms like data protection officers, impact assessments, and breach notifications (Beccia et al., 2024; Bolatbekkyzy, 2024; Calzada, 2022). Both emphasize principles of legality, necessity, transparency, purpose limitation, data minimization, and accountability (Bolatbekkyzy, 2024). Cross-border rules involve adequacy decisions, certifications, or contractual safeguards, with PIPL's certification and standard clauses echoing GDPR Article 46 (Li & Chen, 2023).

Key Differences

PIPL adopts a broader scope for sensitive personal information compared to GDPR's "special categories," incorporating a consequentialist approach based on disclosure risks and potential harm (Beccia et al., 2024). It excludes anonymous information explicitly and mandates "separate consent" for sensitive data or cross-border transfers, a tiered system lower than GDPR's "explicit consent" threshold in high-risk cases (Beccia et al., 2024; Weuts et al., 2025). Unlike GDPR's "legitimate interests" basis, PIPL prioritizes national security, allowing state access and imposing stricter data localization for Critical Information Infrastructure Operators and large-scale processors, with mandatory CAC security assessments (Beccia et al., 2024; Li & Chen, 2023). Enforcement under PIPL follows a decentralized "twin peaks" model without a single independent authority, contrasting GDPR's centralized approach; penalties reach 5% of revenue, slightly higher than GDPR's 4% cap (Li & Chen, 2023; Wang, 2024). PIPL balances rights with economic use and public interest exemptions, reflecting China's sovereignty focus over GDPR's human rights emphasis (Bolatbekkyzy, 2024; Weuts et al., 2025).

PIPL vs. India's DPDP Act 2023

Direct scholarly comparisons between PIPL and India's Digital Personal Data Protection Act 2023 remain limited, with analyses primarily benchmarking DPDP against GDPR, US, EU, Singapore, and Australia frameworks (Chacko & Mishra, 2023; Korff, 2023).

- **Consent Model:** DPDP emphasizes consent similar to PIPL and GDPR but introduces ambiguities in verification and withdrawal, potentially complicating compliance; PIPL's "separate consent" for sensitive/cross-border data adds stricter tiers absent in early DPDP drafts (Chacko & Mishra, 2023; Korff, 2023).
- **Data Fiduciaries vs. Handlers:** DPDP's "data fiduciaries" (analogous to controllers) mirror PIPL's "personal information handlers," both imposing accountability, but DPDP fiduciaries face lighter duties initially compared to PIPL's scale-based DPO mandates for large handlers (Chacko & Mishra, 2023).
- **Cross-Border Provisions:** DPDP restricts transfers to adequate jurisdictions (government-approved), akin to PIPL's CAC assessments/certifications but

without explicit localization like CIIOs; both prioritize sovereignty yet DPDP draws more from GDPR adequacy (Chacko & Mishra, 2023; Korff, 2023).

- **Enforcement Style:** DPDP establishes a Data Protection Board (appeals-focused), contrasting PIPL's campaign-style, multi-agency (CAC/MPS/sectoral) rectification; India's evolves from IT Act rules, facing constitutional challenges, while PIPL integrates national security enforcement (Chacko & Mishra, 2023; Jha, 2024; Korff, 2023).

PIPL vs. U.S. Sectoral Model

No Single Federal Law in US

The US lacks a comprehensive federal privacy law, relying on sectoral statutes (e.g., HIPAA for health, GLBA for finance) and FTC enforcement under unfair practices, unlike PIPL's holistic framework (Calzada, 2022; Wang, 2024).

State-Level Privacy (CCPA/CPRA)

California's Consumer Privacy Act provides opt-out rights, data sales disclosures, and private actions, paralleling PIPL's rights but consumer-focused without PIPL's processing bases or DPO requirements; CCPA applies to large businesses, similar to PIPL's scale thresholds, yet emphasizes sales over localization (Calzada, 2022).

Data Sovereignty vs. Data-Market Approach

PIPL conceptualizes personal data as a national security element, mandating localization and CAC oversight, diverging from the US's market-driven view treating data as a production factor with minimal flow restrictions (Calzada, 2022; Gao, 2023). US prioritizes economic innovation via self-regulation, while PIPL enforces sovereignty through ex-ante reviews, positioning China in global "discourse power" competition (Calzada, 2022; Wang, 2024).

Critiques and Challenges

While the PIPL represents a milestone in China's data governance, it has faced scholarly and practical critiques highlighting implementation hurdles, structural tensions, and broader economic repercussions (He et al., 2025; Li & Chen, 2023).

Ambiguity in Definitions

PIPL provisions suffer from interpretive ambiguities, particularly around "large-scale processing," where thresholds remain vaguely defined by government agencies without clear numerical benchmarks, complicating compliance for handlers (2022). Similar vagueness affects "separate consent," anonymization criteria, and de-identification standards, leading to enforcement difficulties due to overlapping administrative responsibilities (He et al., 2025). Courts often provide ad hoc clarifications, drawing sporadically from external precedents, exacerbating uncertainty (Li & Chen, 2023).

Expansive State Exemptions

Broad exemptions for national security, public interest, and government access undermine individual protections, allowing state actors significant leeway in data collection without robust safeguards (He et al., 2025; Qiao-Franco & Zhu, 2022). Qualifiers like "necessary measures" for data handling by authorities create loopholes, prioritizing collective imperatives over privacy and potentially neglecting ethical concerns (Qiao-Franco & Zhu, 2022).

Enforcement Unpredictability

The "twin peaks" model—split between CAC and sectoral regulators like MIIT—fosters fragmented, campaign-style enforcement, with selective high-profile actions yielding inconsistent application (Wang, 2024). Reliance on administrative discretion rather than judicial predictability, coupled with scant case law, heightens risks for businesses navigating opaque regulatory shifts (Li & Chen, 2023).

Heavy Compliance Burdens for SMEs

PIPL's scale-based obligations, including DPOs and impact assessments, disproportionately burden small and medium enterprises lacking resources for complex audits, consents, and localization, potentially stifling innovation among non-large handlers (Calzada, 2022).

Data Localization Concerns

Mandatory storage for CIIOs and large-scale processors, coupled with CAC security assessments for outflows, raises operational costs and technical challenges, with "important data" definitions remaining fluid and case-specific (2022; Voss & Pernot-Leplay, 2023).

Impact on Global Digital Economy

Stringent cross-border rules, including separate consents and equivalence mandates for foreign recipients, amplify restrictions on data flows, deterring international business and positioning China amid geopolitical data sovereignty tensions (Voss & Pernot-Leplay, 2023; Xie et al., 2023). This cautious regime, prioritizing security over fluidity, influences global norms while challenging multinationals (Calzada, 2022).

Lack of Independent Data-Protection Authority

Absence of a singular, independent supervisory body—unlike GDPR's model—relies on CAC-led coordination, risking politicization and lacking the autonomy needed for impartial oversight (Voss & Pernot-Leplay, 2023; Wang, 2024). This structural gap hinders consistent guidance and appeals, contrasting with international standards (Bolatbekkyzy, 2024).

Policy Implications

China's PIPL carries profound policy ramifications, reshaping domestic practices while influencing international norms on data flows, sovereignty, and privacy governance (Deane et al., 2023; Zhang, 2024).

Impacts on Cross-Border Business

PIPL's stringent cross-border data transfer rules—requiring CAC security assessments, certifications, or standard contractual clauses for large-scale processors and CIIOs—impose significant compliance burdens on multinational corporations (Jiang, 2024; Mbah, 2024; Zhang, 2024). Foreign firms must localize data storage, obtain separate consents, disclose overseas recipient details, and adapt IT systems, often necessitating local data centers or partnerships (Voss & Pernot-Leplay, 2023; Zhang, 2024; Zuo, 2024). This extraterritorial reach heightens costs, operational complexity, and risks of app delistings or fines up to 5% of revenue, deterring market entry and amplifying tensions for global operations (Jiang, 2024; Mbah, 2024; Xie et al., 2023). Companies like Apple and Tesla exemplify adaptations through onshore storage, underscoring PIPL's economic leverage (Voss & Pernot-Leplay, 2023).

Cyber Sovereignty Model

PIPL embodies China's "cyber sovereignty" paradigm, prioritizing national security via data localization for CIIOs and "important data," alongside state access exemptions (Li & Chen, 2023; Malikussaid & Sutiyo, 2025; Zhang, 2024). Integrated with CSL and DSL, it asserts territorial control over data flows, mandating CAC oversight and risk assessments that evaluate threats to public interests (Deane et al., 2023, 2022; Yun, 2024). This state-centric model contrasts GDPR's rights-focused approach, enabling government intervention while projecting influence through Digital Silk Road infrastructure (Borgogno & Zangrandi, 2024; Malikussaid & Sutiyo, 2025).

Fragmentation of Global Data Governance

PIPL exacerbates global data governance balkanization by diverging from GDPR and US sectoral models, with broader sensitive data scopes, no "legitimate interests" basis, and security-driven localization (Deane et al., 2023; Jiang, 2024; Mbah, 2024). It fuels "discourse power" competition, as EU/US emphasize human rights/economics while China advances sovereignty norms, complicating harmonization and MNE compliance across regimes (Borgogno & Zangrandi, 2024; Deane et al., 2023; Zhang, 2024). Emerging economies adopting localization echo this trend, hindering seamless data flows (Khasanova & Tai, 2023; Malikussaid & Sutiyo, 2025).

Future of Privacy in Authoritarian Contexts

PIPL signals authoritarian privacy's evolution: protecting citizens from private overreach while enabling state surveillance via exemptions (Jia, 2023). Unlike democratic models, it balances individual rights with party-state security, potentially inspiring hybrid regimes but risking weakened enforcement amid economic priorities (Jia, 2023; Li & Chen, 2023; Zhang, 2024). Campaign-style enforcement may evolve toward structured oversight, yet surveillance scale limits GDPR-like adequacy (Jia, 2023; Li & Chen, 2023).

Practical Industry Compliance Recommendations

Firms should appoint China-based DPOs for large-scale operations, conduct mandatory PIIAs before sensitive/high-risk processing or transfers, and implement regular audits/incident reporting (Shahlaei & Berente, 2024; Voss & Pernot-Leplay, 2023; Yao & Fei, 2023). Prioritize

data minimization, separate consents for sensitive/cross-border activities, and SCCs/certifications over assessments where feasible; SMEs may leverage codes of conduct for streamlined compliance (Beccia et al., 2024; Jiang, 2024; Shahlaei & Berente, 2024). Engage local experts, monitor CAC guidance, and build onshore infrastructure to mitigate localization risks ("The Chinese Frontiers of Data Protection: The Personal Information Protection Law (PIPL)," 2023, 2022).

Conclusion

China's PIPL marks a transformative milestone in the nation's data governance evolution, establishing a comprehensive framework that integrates individual rights with stringent national security imperatives.(Bolatbekkyzy, 2024; Calzada, 2022) This analysis reveals key findings: PIPL's broad scope, including extraterritorial applicability and a consequentialist definition of sensitive data, imposes robust obligations like separate consent, impact assessments, and data localization for critical operators, while aligning partially with GDPR principles yet diverging through the absence of "legitimate interests" and campaign-style enforcement via the CAC-led "twin peaks" model.(Calzada, 2022; Li & Chen, 2023)

PIPL's Significance in Global Privacy Architecture

PIPL positions China as a pivotal architect in the global privacy landscape, rivaling GDPR and CCPA by enforcing cyber sovereignty through localization and CAC assessments, thereby fragmenting data flows and fueling "discourse power" competitions among regimes.(Calzada, 2022; Jiang, 2024; Li & Chen, 2023) Its influence extends via the Digital Silk Road, compelling multinationals to adapt—e.g., onshore storage by firms like Apple—while inspiring non-Western jurisdictions amid balkanized governance.(2022; Zuo, 2024)

Balance Between Privacy, Security, and State Interests

PIPL adeptly balances citizen protections against private overreach—via rights to explanation, refusal of profiling, and audits—with expansive state exemptions for public interest, national security, and emergencies, embedding privacy within a sovereignty-centric paradigm.(He et al., 2025; Zhang, 2024) This "authoritarian privacy" shields individuals from platforms yet prioritizes collective security, contrasting liberal models and revealing tensions in enforcement predictability and judicial independence.(Gao, 2021; Li & Chen, 2023)

Scholars should prioritize empirical evaluations of PIPL's enforcement efficacy, including SPRCs' long-term impacts and app compliance post-2021; user perceptions of rights amid state access beliefs; techno-regulatory challenges like SDK gaps and AI intersections; and comparative studies with emerging laws (e.g., India's DPDP) to assess global harmonization potentials.(Cetin, 2024; Kollnig et al., 2024; Tao et al., 2025; Zhou et al., 2024) Addressing ambiguities in anonymization, scale thresholds, and cross-border mechanisms will further illuminate PIPL's adaptive trajectory.(Bolatbekkyzy, 2024; Wang, 2024)

References

Aljeraisy, A., Rana, O., & Perera, C. (2020). A Systematic Analysis of Privacy Laws and Privacy by Design Schemes for the Internet of Things: A Developer's Perspective. *HAL (Le Centre Pour La Communication Scientifique Directe)*. https://hal.archives-ouvertes.fr/hal-02567959

Alkhamsi, N. N., & Alqahtani, S. S. (2024). Compliance Framework for Personal Data Protection Law Standards. *International Journal of Advanced Computer Science and Applications*, *15*(7). https://doi.org/10.14569/ijacsa.2024.0150751

Arts, C. J. of L. the. (2023). Full Issue. *The Columbia Journal of Law & the Arts*, *46*(4). https://doi.org/10.52214/jla.v46i4.11775

Beccia, F., Marcantonio, M. D., Causio, F. A., Schleicher, L., Wang, L., Cadeddu, C., Ricciardi, W., & Boccia, S. (2024). Integrating China in the International Consortium for Personalised Medicine: a position paper on innovation and digitalization in Personalized Medicine. *BMC Public Health*, *24*(1). https://doi.org/10.1186/s12889-024-18009-8

Belli, L. (2021). Cybersecurity Policymaking in the BRICS Countries: From Addressing National Priorities to Seeking International Cooperation. *The African Journal of Information and Communication (AJIC)*, *28*. https://doi.org/10.23962/10539/32208

Berzin, O., & Mitianov, Z. (2025). Institutions of Personal Data in Russia and Personal Information in China: a Comparative Legal Analysis. *Legal Issues in the Digital Age*, *6*(3), 77. https://doi.org/10.17323/2713-2749.2025.3.77.98

Bian, C. (2022). Data as Assets in Foreign Direct Investment: Is China's National Data Governance Compatible with its International Investment Agreements? *Asian Journal of International Law*, *13*(2), 342. https://doi.org/10.1017/s2044251322000595

Bolatbekkyzy, G. (2024). Comparative Insights from the EU's GDPR and China's PIPL for Advancing Personal Data Protection Legislation. *Groningen Journal of International Law*, *11*(1), 129. https://doi.org/10.21827/grojil.11.1.129-146

Borgogno, O., & Zangrandi, M. S. (2024). Chinese Data Governance and Trade Policy: From Cyber Sovereignty to the Quest for Digital Hegemony? *Journal of Contemporary China*, *33*(148), 578. https://doi.org/10.1080/10670564.2023.2299961

Buckley, G., Caulfield, T., & Becker, I. (2024). How might the GDPR evolve? A question of politics, pace and punishment. *Computer Law & Security Review*, *54*, 106033. https://doi.org/10.1016/j.clsr.2024.106033

Calzada, I. (2022). Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL). *Smart Cities*, *5*(3), 1129. https://doi.org/10.3390/smartcities5030057

Cao, Y. U., & Hu, W. (2023). New IP and Standardization Practices in China's Data-centric Digital Economy. In *IntechOpen eBooks*. IntechOpen. https://doi.org/10.5772/intechopen.1001432

Cetin, M. B. (2024). Evaluating the Effects of Digital Privacy Regulations on User Trust. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2409.02614

Chacko, M., & Mishra, S. (2023). Benchmarking the Indian Digital Personal Data Protection Act 2023 against data protection frameworks in Singapore, the EU, US and Australia. *Journal of Data Protection & Privacy.*, *6*(2), 110. https://doi.org/10.69554/lxhz9342

Chen, B., & Liu, Y. (2024). Promotion and Advancement of Data Security Governance in China. *Electronics*, *13*(10), 1905. https://doi.org/10.3390/electronics13101905

Chen, M. (2024). Developing China's Approaches to Regulate Cross-border Data Transfer:Relaxation and Integration. *Computer Law & Security Review*, *54*, 105997. https://doi.org/10.1016/j.clsr.2024.105997

Conde, I. C., Li, Y., & Vyas, R. P. (2025). Global Companies and China's Data Privacy Laws: Analysing DIDI'S Case and Regulatory Compliance Implications. *Chinese Journal of Transnational Law*, *2*(1), 60. https://doi.org/10.1177/2753412x241288770

Creemers, R. (2023). The Great Rectification: A New Paradigm for China's Online Platform Economy. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4320952

Deane, F., WOOLMER, E., Cao, S., & Tranter, K. (2023). Trade in the Digital Age: Agreements to Mitigate Fragmentation. *Asian Journal of International Law*, *14*(1), 154. https://doi.org/10.1017/s204425132300036x

Deursen, S. van, & Kummeling, H. R. B. M. (2019). The New Silk Road: a bumpy ride for Sino-European collaborative research under the GDPR? *Higher Education*, *78*(5), 911. https://doi.org/10.1007/s10734-019-00377-5

Deursen, S. van, & Kummeling, H. R. B. M. (2020). A European Compass for Transporting Personal Data on the New Silk Road. In *Oxford University Press eBooks* (p. 221). Oxford University Press. https://doi.org/10.1093/oso/9780198853022.003.0012

Gao, H. (2021). Data Regulation with Chinese Characteristics. In *Cambridge University Press eBooks* (p. 245). Cambridge University Press. https://doi.org/10.1017/9781108919234.017

Gao, R. Y. (2023). A Battle of the Big Three?—Competing Conceptualizations of Personal Data Shaping Transnational Data Flows. *Chinese Journal of International Law*, *22*(4), 707. https://doi.org/10.1093/chinesejil/jmad040

He, M., & Chen, Y. (2025). Personal Data Protection in China: Progress, Challenges and Prospects In the Age of Big Data And Ai. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5187704

He, S., Zhan, X., Lei, Y., Liu, Y., Abu-Salma, R., & Such, J. M. (2025). Exploring the Privacy and Security Challenges Faced by Migrant Domestic Workers in Chinese Smart Homes. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2504.02149

He, Y., & Zeng, K. (2025). A Geopolitical Economy Analysis of China and India's Approaches to Transnational Data Governance. *Politics and Governance*, *13*. https://doi.org/10.17645/pag.10361

Jha, A. K. (2024). The Changing Face of the Data Protection Laws: From India's IT Act to Global Privacy Standards. *African Journal of Biomedical Research*, 2004. https://doi.org/10.53555/ajbr.v27i1s.1767

Jia, M. (2023). Authoritarian Privacy. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4362527

Jiang, J., & Zheng, Z. (2023). Personal Information Protection and Privacy Policy Compliance of Health Code Apps in China: Scale Development and Content Analysis [Review of *Personal Information Protection and Privacy Policy Compliance of Health Code Apps in China: Scale Development and Content Analysis*]. *JMIR Mhealth and Uhealth*, *11*. JMIR Publications. https://doi.org/10.2196/48714

Jiang, J., & Zheng, Z. (2024). Medical Information Protection in Internet Hospital Apps in China: Scale Development and Content Analysis. *JMIR Mhealth and Uhealth*, *12*. https://doi.org/10.2196/55061

Jiang, Y. (2024). Data Protection from A Global Perspective: Challenges and Strategies for Multinational Corporation Data Security Compliance. In *Advances in economics, business and management research/Advances in Economics, Business and Management Research* (p. 314). Atlantis Press. https://doi.org/10.2991/978-94-6463-542-3_39

Jin, Y., & Skiera, B. (2022). How Do Privacy Laws Impact the Value for Advertisers, Publishers and Users in the Online Advertising Market? A Comparison of the EU, US and China. *Journal of Creating Value*, *8*(2), 306. https://doi.org/10.1177/23949643221117676

Jing, T., Li, Y., Ye, J., Wang, J., & Wang, X. (2025). *Privacy Law Enforcement Under Centralized Governance: A Qualitative Analysis of Four Years' Special Privacy Rectification Campaigns*. https://doi.org/10.48550/ARXIV.2503.08568

Kaiv, E., Lewinski, D., Courto, H., Ustralia, F., Hoffmann, T., Hoffmann, S., Hünting, B., Leven, K., Lewinski, E., Saponchik, L., Vargas, M., Richthammer, M., & Widjaja, T. (2023). Data Disclosure. In *De Gruyter eBooks*. De Gruyter. https://doi.org/10.1515/9783111010601

Kharitonova, Yu., Malik, N., & Yang, T.-W. (2023). The Legal Issue of Deterrence of Algorithmic Control of Digital Platforms: The Experience of China, the European Union, Russia and India. *BRICS Law Journal*, *10*(1), 147. https://doi.org/10.21684/2412-2343-2023-10-1-147-170

Khasanova, L., & Tai, K. (2023). An Authoritarian Approach to Digital Sovereignty? Russian and Chinese Data Localisation Models. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4527052

Kim, D. H., & Park, D. H. (2024). Automated decision-making in South Korea: a critical review of the revised Personal Information Protection Act [Review of *Automated decision-making in South Korea: a critical review of the revised Personal Information Protection Act*]. *Humanities and Social Sciences Communications*, *11*(1). Palgrave Macmillan. https://doi.org/10.1057/s41599-024-03470-y

Kollnig, K., Zhang, L., Zhao, J., & Shadbolt, N. (2024). Privacy in Chinese iOS apps and impact of the personal information protection law. *Computer Law & Security Review*, *55*, 106041. https://doi.org/10.1016/j.clsr.2024.106041

Korff, D. (2023). The Indian Digital Personal Data Protection Act, 2023, viewed from a European Perspective. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4614984

Lee, J. (2025). Algorithmic bias and the New Chicago School. In *Routledge eBooks* (p. 95). Informa. https://doi.org/10.4324/9781003648024-5

Lee, J. H. (2025). Algorithmic Bias and the New Chicago School. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2502.00014

Li, Q., Jiang, T., & Fan, X. (2023). Examining Sensitive Personal Information Protection in China: Framework, Obstacles, and Solutions. *Information & Culture*, *58*(3), 247. https://doi.org/10.7560/ic58302

Li, W., & Chen, J. (2023). From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR-Inspired Personal Information Protection Law in China. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2312.08237

Li, W., & Chen, J. (2024). From brussels effect to gravity assists: Understanding the evolution of the GDPR-inspired personal information protection law in China. *Computer Law & Security Review*, *54*, 105994. https://doi.org/10.1016/j.clsr.2024.105994

Li, Z., Liang, Z., Yao, C., Hua, J., & Zhong, S. (2024). RADS-Checker: Measuring Compliance with Right of Access by the Data Subject in Android Markets. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2410.12463

Malgieri, G., & Fuster, G. G. (2021). The Vulnerable Data Subject: A Gendered Data Subject? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3913249

Malikussaid, & Sutiyo. (2025). The Impact of the Russia-Ukraine Conflict on the Cloud Computing Risk Landscape. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2506.20104

Mbah, G. O. (2024). Data privacy in the era of AI: Navigating regulatory landscapes for global businesses. *International Journal of Science and Research Archive*, *13*(2), 2040. https://doi.org/10.30574/ijsra.2024.13.2.2396

Nan, G. (2023). Protection of personal data in China: Legislation in the digital age. *Vestnik of Saint Petersburg University Law*, *14*(1), 159. https://doi.org/10.21638/spbu14.2023.110

Prabu, S. L., Prabu, L., Umamaheswari, A., Gede, I., & Kurniawan, A. (2023). Intellectual Property - Global Perspective Advances and Challenges [Working Title]. In *IntechOpen eBooks*. IntechOpen. https://doi.org/10.5772/intechopen.104193

Qiao-Franco, G., & Zhu, R. (2022). China's Artificial Intelligence Ethics: Policy Development in an Emergent Community of Practice. *Journal of Contemporary China*, *33*(146), 189. https://doi.org/10.1080/10670564.2022.2153016

Reer, A., Wiebe, A., Wang, X., & Rieger, J. W. (2023). FAIR human neuroscientific data sharing to advance AI driven research and applications: Legal frameworks and missing metadata standards [Review of *FAIR human neuroscientific data sharing to advance AI driven research and applications: Legal frameworks and missing metadata standards*]. *Frontiers in Genetics*, *14*. Frontiers Media. https://doi.org/10.3389/fgene.2023.1086802

Reuben, J., Martucci, L. A., Fischer-Hübner, S., Packer, H., Hedbom, H., & Moreau, L. (2016). *Privacy Impact Assessment Template for Provenance*. 653. https://doi.org/10.1109/ares.2016.95

Shahlaei, C. A., & Berente, N. (2024). An Analysis of European Data and AI Regulations for Automotive Organizations. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2407.11271

Shen, W., & Liu, Y. (2022). China's Normative Systems for Responsible AI. In *Cambridge University Press eBooks* (p. 150). Cambridge University Press. https://doi.org/10.1017/9781009207898.012

Tan, Z., & Zhang, C. (2021). China's PIPL and DSL: Is China following the EU's approach to data protection? *Journal of Data Protection & Privacy.*, *5*(1), 7. https://doi.org/10.69554/natu8989

Tao, H. (2024). Conflicts and Coordination in Data Localization in China and International Trade Law. In *Advances in Social Science, Education and Humanities Research/Advances in social science, education and humanities research* (p. 436). https://doi.org/10.2991/978-2-38476-277-4_49

Tao, J., Li, Y., Ye, J., Wang, J., & Wang, X. (2025). Privacy Law Enforcement Under Centralized Governance: A Qualitative Analysis of Four Years' Special Privacy Rectification Campaigns. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2503.08568

The Cambridge Handbook of Responsible Artificial Intelligence. (2022). In *Cambridge University Press eBooks*. Cambridge University Press. https://doi.org/10.1017/9781009207898

The Chinese Frontiers of Data Protection: The Personal Information Protection Law (PIPL). (2023). In *Philosophical studies series* (p. 181). Springer International Publishing. https://doi.org/10.1007/978-3-031-41566-1_11

Voss, W. G., & Pernot-Leplay, E. (2023). China Data Flows and Power in the Era of Chinese Big Tech. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4393008

Wang, A. (2024). Law and Practice of Personal Data Protection in the Digital World: A Comparison between China, the EU and the Us. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4878725

Wang, C., Liu, C., Perriam, J., & Kjær, K. M. (2024). One data state, two data logics : Unfolding China's data governance. *Research Portal Denmark*, *14*, 29. https://local.forskningsportal.dk/local/dki-cgi/ws/cris-link?src=itu&id=itu-82c33291-32eb-4204-845e-1748c1708ae6&ti=One%20data%20state%2C%20two%20data%20logics%20%3A%20Unfolding%20China's%20data%20governance

Wawra, D. (2023). Data Sensitivity and Data Protection Literacy in Cross-Cultural Comparison. In *De Gruyter eBooks* (p. 169). De Gruyter. https://doi.org/10.1515/9783111010601-010

Weuts, R., Bleher, J., Bleher, H., Flores, R., Xuanyang, G., Pujszo, P., & Almási, Z. (2025). AI Governance in Higher Education: A course design exploring regulatory, ethical and practical considerations. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2509.06176

Xie, T., Liu, J., Sengstschmid, U., & Ge, Y. (2023). Navigating Cross-Border Data Transfer Policies: The Case of China. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4408947

Yan, Y. (2023). The Risk-Based Approach to Personal Data Protection and the Response of the International Trade Law. *Beijing Law Review*, *14*(3), 1250. https://doi.org/10.4236/blr.2023.143067

Yao, Y., & Fei, Y. (2023). Overcoming personal information protection challenges involving real-world data to support public health efforts in China. *Frontiers in Public Health*, *11*. https://doi.org/10.3389/fpubh.2023.1265050

Yun, H. S. (2024). China's Data Sovereignty and Security: Implications for Global Digital Borders and Governance. *Chinese Political Science Review*, *10*(2), 178. https://doi.org/10.1007/s41111-024-00269-9

Zeng, M., & Kim, Y. (2025). Institutional reforms and regulatory shifts in China's digital platform sector: how domain-specific centralization shaped the 2020–2022 transition. *Business and Politics*, 1. https://doi.org/10.1017/bap.2025.10015

Zhang, C. (2024). China's privacy protection strategy and its geopolitical implications. *Asian Review of Political Economy*, *3*(1). https://doi.org/10.1007/s44216-024-00028-2

Zhang, C., & Wang, G. (2022). Legal Attributes of IP Attribution Information under China's PIPL: Clarification of Identifiability Terminology and Operationalisation of Identifiability Criteria. *Beijing Law Review*, *13*(3), 626. https://doi.org/10.4236/blr.2022.133040

Zhang, D. (2024). Understanding the evolution of China's approach to digital trade: interests, ideas, and institutions. *Asian Review of Political Economy*, *3*(1). https://doi.org/10.1007/s44216-024-00026-4

Zhao, J. (2023). Reflections on Criminal Compliance for Corporate Personal Information Protection. *Beijing Law Review*, *14*(2), 674. https://doi.org/10.4236/blr.2023.142036

Zhenbin, Z. (2023). *China's Data Strategies: Institutionalisation, Activation, and Layering* (p. 119). https://doi.org/10.5040/9781509973682.ch-007

Zhou, M. M., Qu, Z., Wan, J., Wen, B., Yao, Y., & Lu, Z. (2024). Understanding Chinese Internet Users' Perceptions of, and Online Platforms' Compliance with, the Personal Information Protection Law (PIPL). *Proceedings of the ACM on Human-Computer Interaction*, *8*, 1. https://doi.org/10.1145/3637415

Zou, C., & Zhang, F. (2022). Algorithm Interpretation Right—The First Step to Algorithmic Governance. *Beijing Law Review*, *13*(2), 227. https://doi.org/10.4236/blr.2022.132015

Zuo, Z. (2024). Cross-Border Data Forensics: Challenges and Strategies in the Belt and Road Initiative Digital Era. *Asian Social Science*, *20*(2), 49. https://doi.org/10.5539/ass.v20n2p49

(2022). *International Organisations Research Journal*, *17*(3). https://doi.org/10.17323/1996-7845-2022-03

(2024). *African Journal of Privacy & Data Protection.*, *1*. https://doi.org/10.29053/ajpdp.v1