Non-final version of Wei Wang; Wayne, Chang; Sofia and Chen; Larissa. Assessing the Chinese Personal Information Protection Law (PIPL) and Beyond: The Stakeholder Architecture of Data Protection in China; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

ASSESSING THE CHINESE PERSONAL INFORMATION PROTECTION LAW (PIPL) AND BEYOND: THE STAKEHOLDER ARCHITECTURE OF DATA PROTECTION IN CHINA

Wayne Wei Wang, Sofia Chang and Larissa Chen

Abstract

This chapter provides a comprehensive evaluation of China's Personal Information Protection Law (PIPL), introduced amid escalating societal controversies related to data protection and the emerging need for a robust enforcement apparatus. With a stakeholder-centric framework, we trace the institutional impetus that led to the enactment of the PIPL and contrast it with global counterparts such as the European Union's General Data Protection Regulation (GDPR). The analysis also extends to PI-related NPC-level statutes to illuminate the PIPL's positioning within China's legislative hierarchy. We further scrutinize the core provisions of the PIPL, exploring the asymmetry of stakeholder rights and authority, the multiple enforcement agencies' landscape, punitive measures, and redress mechanisms. We argue that China's data protection framework following comparative legislative instruments is a fusion of data governance mechanisms, including the CSL, DSL, and PIPL, and their respective derivatives, which should not be directly paralleled to prevailing international systems. The PIPL, in our analysis, significantly enhances data subjects' rights while defining the responsibilities of data handlers, including those specialities in security, gatekeeping, and automated decision-making, with limited limitations upon the public sector. In conclusion, the chapter asserts the necessity of appreciating China's data protection architecture as a unique, domestically adapted system, highlighting the challenges and opportunities in aligning it with global data governance norms.

Non-final version of Wei Wang; Wayne, Chang; Sofia and Chen; Larissa. Assessing the Chinese Personal Information Protection Law (PIPL) and Beyond: The Stakeholder Architecture of Data Protection in China; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

CONTENTS

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

1. ASSESSING THE CHINESE PERSONAL INFORMATION PROTECTION LAW (PIPL) AND BEYOND: THE STAKEHOLDER ARCHITECTURE OF DATA PROTECTION IN CHINA

1.1. Introduction

China's pre-PIPL data protection regime was characterized by fragmentation, doctrinal incoherence, and a paucity of integrated statutory guidance, which rendered even expert legal interpretation a fraught exercise. The prevailing legal architecture—diffuse, underdeveloped, and internally inconsistent—left courts with limited capacity to produce principled adjudication, instead requiring them to navigate the interstices between codified norms and policy imperatives emanating from the central leadership.[1] Judicial discretion thus functioned not merely as a mechanism of legal interpretation but as an instrument for accommodating shifting policy orientations within the broader socialist legality framework.

Legislative authorities were acutely aware of the disjunction between codified norms and administrative practice. Widespread abuses of personal information—ranging from unauthorized collection to instances of fraud—had generated significant public disquiet.[2] In response, China's institutional system, premised on performance legitimacy,[3] demonstrated a capacity for policy recalibration in light of emergent social harms. This responsiveness intensified the imperative to formulate a dedicated legislative framework to regulate the collection and processing of personal data.

In the absence of a comprehensive data protection statute and an integrated enforcement infrastructure, the regulatory landscape was historically anchored in the Cybersecurity Law (CSL), promulgated in 2016. However, enforcement authority remained opaque and diffuse. The oft-cited metaphor of "nine dragons governing the waters" (九龙治水) aptly captured the institutional ambiguity: either too many agencies claimed overlapping authority or none assumed responsibility, generating a regulatory vacuum in practice.[4]

The Personal Information Protection Law (PIPL) emerged through a tripartite legislative process, comprising two rounds of public consultation (in October 2020 and April 2021) and final enactment in August 2021,[5] with over 15 years' debates of its institutional design,[6] which echoed the Brazilian and Indian experience to data protection codification. The evolution of the statutory text across these drafts offers a window into the legislature's evolving conceptualization of stakeholder rights and obligations. These revisions also reflect a growing awareness of structural asymmetries in informational power,

[1] Minhao Benjamin Chen and Zhiyu Li, 'Courts without Separation of Powers: The Case of Judicial Suggestion in China' (2023) 64 Harvard International Law Journal 203.

[2] Yue Lu, '一场信息保护的博弈 [A Game of Information Protection]' (*Xinhua Net*, 2021) <http://www.xinhuanet.com/legal/2021-10/20/c_1127974932.htm> accessed 23 April 2023.

[3] Hongxing Yang and Dingxin Zhao, 'Performance Legitimacy, State Autonomy and China's Economic Miracle' (2015) 24 Journal of Contemporary China 64.

[4] Tai Ming Cheung, 'The Rise of China as a Cybersecurity Industrial Power: Balancing National Security, Geopolitical, and Development Priorities' (2018) 3 Journal of Cyber Policy 306, 316.

[5] Fei Qiu, '个人信息保护法的立法往事 [The Legislative History of the Personal Information Protection Law]' (*法治周末 Rule of Law Weekend*, 4 November 2021) <https://finance.sina.cn/tech/2021-11-04/detail-iktzscyy3607023.d.html> accessed 3 May 2023.

[6] Yehan Huang and Mingli Shi, 'Top Scholar Zhou Hanhua Illuminates 15+ Years of History Behind China's Personal Information Protection Law' (*DigiChina - Stanford University*, 8 June 2021) <https://digichina.stanford.edu/work/top-scholar-zhou-hanhua-illuminates-15-years-of-history-behind-chinas-personal-information-protection-law/> accessed 6 December 2022.

although preliminary groundwork had already been laid by the CSL and the 2021 Data Security Law (DSL), which began to allocate substantive authority and responsibility among data processors, state actors, and individuals.

This chapter provides a thorough evaluation of the Personal Information Protection Law (PIPL), applying a stakeholder-centric framework—focused specifically on data actors—to analyze the statutory allocation of rights, obligations, and enforcement authority. The legislative choice to define "personal information" (个人信息) reflects a conceptual framework that, while superficially resembling definitions found in other jurisdictions, particularly the European Union's General Data Protection Regulation (GDPR), diverges markedly in both its scope and practical application. As such, this chapter compares the PIPL with analogous legal frameworks globally, with particular attention to its position within the BRICS bloc, to highlight areas of both alignment and divergence in legal interpretation and cultural context.

The chapter opens with a brief overview of the rule of law and institutional legal structures in the People's Republic of China, to contextualize the PIPL within its normative and administrative environment. It then traces the antecedents of the PIPL, focusing on the institutional drivers and political logic behind its enactment. Following this, it examines the PIPL in relation to cognate legislation—particularly the CSL, DSL, and the 2020 Civil Code—to clarify the PIPL's place within the NPC's legislative hierarchy. The final section engages in a doctrinal analysis of the PIPL's core provisions, with particular attention to the asymmetrical allocation of data rights and responsibilities, the pluralistic enforcement regime, and the procedural mechanisms for redress and sanction.

Ultimately, the chapter argues that China's data protection architecture represents a distinctive amalgam of normative principles and institutional imperatives. While it draws selectively from international models, its underlying logic and operational mechanisms remain embedded in China's unique administrative, political, and legal traditions.

1.2. The Chinese Legal System: Brief overview

As articulated in the Constitution of the People's Republic of China, "The People's Republic of China is a socialist state under the people's democratic dictatorship led by the working class and based on the alliance of workers and peasants."[7] This constitutional formulation, which was formally adopted at the 14th National Congress of the Communist Party of China (CPC), grounds the ideological articulation of "socialism with Chinese characteristics" and reflects the CPC's constitutional and institutional centrality in the Chinese legal and political order.[8]

Within this system, the CPC occupies the position of ruling party, entrusted with the leadership of the socialist project. Other legally recognized political parties, while nominally independent, function within a framework of what is often termed "multi-party cooperation and political consultation under the leadership of the Communist Party," and are conventionally described as participating parties.[9] These entities explicitly affirm the CPC's leadership and engage collaboratively in pursuit of shared

[7] Constitution of the People's Republic of China 1982 art 1. The standard English translation of "人民民主专政" is *People's Democratic Dictatorship*. See the latest constitution's English version at https://english.www.gov.cn/archive/lawsregulations/201911/20/content_WS5ed8856ec6d0b3f0e9499913.html. At its core, the term signifies the synthesis of democratic and authoritarian elements to preserve the people-oriented character of state power. It denotes a constitutional theory in which democratic participation is extended to the "people" as defined by the state, while coercive measures are reserved for those deemed antagonistic to the socialist order.

[8] Xiaobo Dong and Yafang Zhang, *On Contemporary Chinese Legal System* (Springer) <https://doi.org/10.1007/978-981-99-2505-6>.

[9] ibid.

socialist objectives, rather than in adversarial or oppositional roles characteristic of pluralist democracies.

The Constitution further declares that all state power belongs to the people, exercised through the National People's Congress (NPC) and local people's congresses at various levels. These bodies establish and oversee the activities of administrative, judicial, and procuratorial organs, which are constitutionally accountable to the congresses and subject to their supervision.[10] This arrangement formalizes a system of indirect democratic participation, structured within a single-party framework.

With respect to individual rights, the Constitution enumerates a range of civil and socio-economic entitlements, including rights to vote and stand for election, freedom of speech, press, assembly, association, religious belief, personal dignity, and rest, among others. However, these rights are coextensive with a set of constitutionally prescribed obligations. Articles 52 to 54 impose duties on citizens to safeguard national unity and ethnic solidarity, comply with laws and social norms, maintain public order, respect collective morality, and protect the "security, honor, and interests of the motherland."

While these obligations are formally articulated, their normative content often relies on language that is broad and indeterminate. Terms such as "national unity," "social morality," and "honor of the motherland" are open-textured and subject to evolving interpretative frameworks, which may be shaped by prevailing policy priorities and the discretion of enforcement authorities. This vagueness gives rise to a pliable legal environment, in which the balance between state interests and individual rights may shift across contexts and over time.

In the domain of cyberspace, these constitutional obligations have been operationalized through regulatory instruments that limit online anonymity and impose duties on platforms to authenticate user identities.[11] Regulations such as the "Provisions on the Administration of Internet Information Services" and accompanying enforcement guidelines mandate that service providers monitor content and implement compliance protocols. [12] Such frameworks embody the state's emphasis on public order, ideological security, and information sovereignty in digital governance.

As explored in this chapter, the Chinese legal system manifests a form of normative exceptionalism, particularly in its asymmetrical treatment of private and public power. Both Brazil's LGPD and China's PIPL exempt state security activities from general data protection requirements, but with notable differences in approach. Brazil carves out specific exceptions for "public security, national defense, state security, or criminal investigations" while still requiring these exempted activities to observe basic data protection principles.[13] China's framework demonstrates a more pronounced asymmetry, introducing significant individual data rights in the private sector while simultaneously allowing broader interpretation for state actors, for instance, allowing facial recognition under "public security" justifications. This reflects China's more expansive view of legitimate state power exemptions compared to Brazil's relatively more constrained approach.

[10] ibid

[11] The Cybersecurity Law of the People's Republic of China, enacted in 2017, includes provisions related to real-name registration. Article 24 of the Cybersecurity Law, for example, stipulates that network operators in China are required to implement measures to verify the identity of users when they sign up for online services. This real-name registration requirement aims to enhance the management of online information and improve cybersecurity.

[12] For instance, those protocols include "Regulations for Internet Content Management Administration Law Enforcement Procedures." See its English translation at https://digichina.stanford.edu/work/regulations-for-internet-content-management-administration-law-enforcement-procedures/.

[13] See Lei No 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), art 4.

Notably, the Chinese Constitution does not contain an explicit, codified right to privacy. Instead, it codifies some related rights inferring certain elements of privacy.[14] In this respect, the PIPL operates primarily as a statutory mechanism regulating the obligations of private data processors, rather than as a constitutional guarantee enforceable against public authorities. The rights framework it constructs is thus more administrative than constitutional in nature, and its protective function is circumscribed by the institutional logic of state-centered governance.

China's model of data regulation, reflecting a broader paternalistic and developmentalist orientation, should be understood within its own legal-cultural and political-ideological context. This chapter aims to offer a comprehensive examination of the PIPL, situating it within the larger architecture of China's governance model. It highlights the distinctiveness of China's rights discourse—both in its normative structure and institutional implementation—and underscores the importance of analyzing data protection not as a transposable legal category, but as a function of China's particular constitutional and administrative configuration.

1.3. The Pre-history of the PIPL: A Brief Retrospect

Prior to the release of the first draft of the Personal Information Protection Law (PIPL) of the People's Republic of China in October 2020, the regulatory framework governing personal information—or, more broadly, personal data—protection in China was characterized by fragmentation and sectoral particularism. Rather than a unified, comprehensive regime, the landscape consisted of a patchwork of sector-specific statutes, administrative regulations, judicial interpretations, and normative documents issued by an array of institutional actors, including legislative, judicial, and quasi-governmental bodies. This included, most prominently, the 2017 Cybersecurity Law, alongside a constellation of industry-specific guidelines and policy measures.[15]

1.3.1. Hard Law and Soft Law

For example, prior to the adoption of the first Civil Code of China in May 2020 and in force as of January 1, 2021,[16] the General Rules of the Civil Law of the People's Republic of China, from 2017, established that "the personal information of a natural person shall be protected by law."[17] Moreover, also published in 2017, the Personal Information Security Specification (GB/T 35273-2017 - and later updated in 2020), became the most thorough standard for personal information protection in China until the enactment of the Personal Information Protection Law.[18] The Specification included those components that are comparable to rules established in the European Union's General Data Protection Regulation (GDPR) and also transplanted in other BRICS justifications, for instance, by establishing a broad definition of personal information, including both direct and indirect personal information ("PI"),[19] setting forth principles related to personal information processing/handling,[20] and warranting personal information

[14] Wayne Wei Wang, 'Contextualizing Personal Information: Privacy's Post-Neoliberal Constitutionalism and Its Heterogeneous Imperfections in China' (2024) *55* Computer Law & Security Review 106030.

[15] Min Jiang, 'Cybersecurity Policies in China' in Luca Belli (ed), *CyberBRICS: Cybersecurity Regulations in the BRICS Countries* (Springer 2021) 186.

[16] 中华人民共和国民法典 [Civil Code of the People's Republic of China] 2020 (Order No 45 of the President) (CCC 2020).

[17] 中华人民共和国民法总则 [General Provisions of the Civil Law of the People's Republic of China] 2017 (Order No 66 of the President), art 111.

[18] Jiang (n 15) 186.

[19] Information security technology— Personal information (PI) security specification - GB/T 35273—2020 (Replacing GB/T 35273-2017) 2020 s 3.1. In the GDPR, article 4(1) defines personal data as any type of data "related to an identified or identifiable person".

[20] ibid ss 4 & 5. The GDPR establishes principles for personal data processing in Article 5.

rights/interests for PI subjects.[21] However, as a technical standard, it was regarded by academics as a type of "soft law" for reference and compliance purposes, and could not be enforced with regulatory authority by administrative bodies.[22]

1.3.2. A Legislative Fragmentation

As noted above, issues relating to the protection of personal information and the preservation of confidentiality were, prior to the enactment of a unified legal framework, addressed in a piecemeal fashion through sector-specific legislation, administrative guidelines, and supplementary regulatory provisions tailored to the particularities of discrete contexts. This regulatory pattern—marked by fragmentation, normative overlap, and inconsistent enforcement—bears notable resemblance to the experience of other BRICS jurisdictions, most notably Brazil. In both China and Brazil, the move toward the adoption of comprehensive data protection legislation was driven in significant part by the deficiencies of the prevailing regulatory architecture, particularly its inefficacy in ensuring coherent and consistent personal data governance across sectors.

For instance, the Resident Identity Card Law established the duty of confidentiality for public security organs regarding citizens' personal information gained through fabricating, issuing, assessing, or collecting identity cards from residents.[23] Moreover, the 2006 Anti-Money Laundering Statute stipulated that information correlating to clients' identities and commercial transactions, amassed for anti-money laundering objectives, must remain confidential, precluding disclosure to third parties except when legally sanctioned, exclusively utilized by authorities conducting anti-money laundering inquiries and enforcement, and solely for the purpose of scrutinizing anti-money laundering or pursuing criminal prosecutions against such activities.[24] Lastly, the Telecommunications and Internet Personal User Data Protection Regulations from 2013, applicable to "the collection and use of personal user data in the process of providing telecommunications services and Internet information services within the borders of the People's Republic of China,"[25] and the 2019 Regulations on the Protection of Children's Personal Information on the Internet, aimed at shielding the personal information of children (minors under the age of 14) on the internet.[26]

1.3.3. Agenda Enablers in the State Informatisation

In the preceding decade, China's regulatory architecture governing information governance has undergone a marked transformation—less an ad hoc assemblage of sectoral norms than an increasingly integrated legal order. This emergent coherence is evidenced by the enactment of the Data Security Law, which provides a structurally tiered framework for safeguarding data deemed critical to national and economic security, and more prominently, by the promulgation of the Personal Information Protection Law (PIPL). The PIPL—effective as of November 1, 2021—constitutes China's first comprehensive

[21] ibid s 8. Data subjects (the equivalent to what the Specification calls PI subjects) enjoy rights as defined by the GDPR's Chapter 3.

[22] Jiang (n 15) 186.

[23] 中华人民共和国居民身份证法 [Law of the People's Republic of China on Resident Identity Cards] 2003 (Order No 4 of the President) art 6.

[24] 中华人民共和国反洗钱法 [Anti-Money Laundering Law of the People's Republic of China] 2006 (Order No 56 of the President) art 5.

[25] 电信和互联网用户个人信息保护规定 [Telecommunications and Internet Personal User Data Protection Regulations] 2013 (Order No 24 of the Ministry of Industry and Information Technology) art 2.

[26] 儿童个人信息网络保护规定 [Provisions on the Protection of Children's Personal Information on the Internet] 2019 (Order No4 of the Cyberspace Administration of China) art 1.

statute on personal data protection, codifying baseline obligations for the collection, processing, and transfer of personal information. More than merely legislative innovation, the PIPL represents the terminus of over fifteen years of fragmented regulatory experimentation and sustained scholarly engagement with the normative foundations of PI in the Chinese legal system.[27]

The chronicle of PIPL originates from 2001 when China instituted the National Informatisation Leading Group as an integral phase in the nation's informatisation trajectory.[28] A pivotal aspect of this progression entailed protecting personal information; consequently, in 2003, an assemblage of scholars from the Chinese Academy of Social Sciences was commissioned to conduct comparative and contextually congruous research on PI protection.[29] This inquiry yielded the Personal Information Protection Law proposition proffered by experts in 2005, accompanied by a three-volume book series expounding additional research findings in the subsequent annum. In the same year, 2005, some drafted the "Scholars' Proposed Model Law of the People's Republic of China on the Protection of Personal Information."[30] Nevertheless, owing to administrative reconfigurations and emergent priorities, such as transitioning the informatisation endeavours from the State Council Informatisation Office to a bureau within the Ministry of Industry and Information Technology, the advancement of the Personal Information Protection Law proposal was once deferred.[31]

In this context, and in recognition of China's significant advances in its informatisation course, an emerging increase of PI-based crimes, and the escalating use of data underpinning decision-making and commercial operations nationwide, a Personal Information Protection Law legislative proposal re-emerged on the law-making agenda. The legislative process of personal information protection law was expedited by Xu Yuyu's cardiac arrest following a PI-utilized phone fraud in 2016, stimulating social reactions and debates by arousing public awareness of PI breaches.[32] In 2018, the 13th National People's Congress Standing Committee unveiled its Quintennial Legislative Blueprint for 2018 to 2023, which included the compilation of the first Chinese Civil Code, as well as proposals for the Personal Information Protection Law and the Data Security Law, in its list of prioritized initiatives.[33]

The first draft of the proposed Personal Information Protection Law during the legislative period of 2018 to 2023 was published in October 2020, the second draft in April 2021, and the final version on the 20th of August 2021, to come into force about four months later. The PIPL contains 74 articles divided into eight chapters. But to what degree does the PIPL deviate from other entities that perform comparable roles in the realm of data governance and regulation of personal information?

1.4. The Role of the PIPL: A Synthesis of National Data Legislation

In order to regulate the processing of data both within its jurisdiction and in the context of cross-border transfers, China has instituted a comprehensive data governance architecture. Central to this framework is what may be termed the "Troika of Data Protection"—comprising the *Personal Information Protection Law* (PIPL), the *Data Security Law* (DSL), and the *Cybersecurity Law* (CSL). Collectively, these statutes establish a multilayered regime governing the collection, use, storage, and transfer of data, reflecting a coordinated legislative response to the risks posed by digitalization.

[27] Huang and Shi (n 6).
[28] ibid.
[29] ibid.
[30] Lu (n 2).
[31] Huang and Shi (n 6).
[32] Lu (n 2).
[33] Changhao Wei, 'Translation: 13th NPC Standing Committee Five-Year Legislative Plan' (*NPC Observer*, 7 September 2018) <https://npcobserver.com/2018/09/07/translation-13th-npc-standing-committee-five-year-legislative-plan/> accessed 20 January 2023.

This tripartite structure invites comparative reflection with other BRICS jurisdictions, where approaches to data governance have diverged. As other chapters indicate, Brazil, for instance, has enacted sector-specific rules addressing cybersecurity but lags in the articulation of a coherent, overarching data security framework. India, while having promulgated data security obligations in various forms for over two decades, suffers from diffuse implementation and regulatory ambiguity. Russia's regulatory emphasis lies less in formulating substantive data protection norms than in asserting sovereign control over data flows—most notably through data localization mandates and content regulation. South Africa stands apart within the BRICS context in having adopted a dedicated Cybercrimes Act, which, alongside its data protection statute (POPIA), imposes explicit obligations concerning data security and cybercrime prevention.

Thus, the emergence of legislative hierarchy and intent implies that the discourse surrounding "data protection" in China had better be understood as a "data governance" system – an intricate model aiming to establish a "third way" that transcends the conventional differentiation between personal and non-personal data.[34] Furthermore, it extends beyond data protection and cybersecurity, addressing cyber/digital/data sovereignty, and technical aspects of data governance such as confidentiality, integrity, and availability – the Data CIA criteria set by the International Standard Organization (ISO).[35] It reflects China's long-lasting yearning – an imperative balance between development and security in the digital epoch. In a sense, China's data and cybersecurity governance system is evidence of a dialectic philosophy that promotes social prosperity, economic development, and the maintenance of national sovereignty,[36] as very recently advocated by its core policymakers as a "data infrastructure system," [37] – a politico-economic discourse that builds an institutional transformation from monolithic regulation to pluralistic governance, concurrently featuring deep multi-stakeholder cooperation and diverse-scenario integration during the Chinese decentralization reform of the administration.[38]

1.4.1. CSL vs. DSL vs. PIPL

Once, the Chinese legislative framework as regards personal information was sporadic and disjointed, with numerous provisions interspersed throughout assorted legislative texts. This fragmented approach persisted following the 2012 National People's Congress Decision on Strengthening Network Information Protection (NPC Decision),[39] and influenced subsequent statutes, including the Consumer

[34] Luca Belli, 'New Data Architectures in Brazil, China, and India: From Copycats to Innovators, Towards a Post-Western Model of Data Governance' (2022) 18 The Indian Journal of Law and Technology 1.

[35] See the standards of the ISO/IEC 27001 - Information security management systems.

[36] For instance, the country released, in 2015, China's strategic plan, "Made in China 2025," which plays a vital role in reducing reliance on foreign technology and achieving economic growth and political legitimacy through the development of the digital economy. See ISDP, 'Made in China 2025' (Institute for Security & Development Policy 2018) <https://isdp.eu/content/uploads/2018/06/Made-in-China-Backgrounder.pdf>.

[37] CPC Central Committee and State Council, '关于构建数据基础制度更好发挥数据要素作用的意见 [Opinions on Building a Better Data Infrastructure System to Fully Utilize the Role of Data Elements]' (2022) <http://www.gov.cn/zhengce/2022-12/19/content_5732695.htm> accessed 24 April 2023. It states "The establishment of a data infrastructure system holds significant importance in terms of both national development and security. To expedite the establishment of a data infrastructure system, it is imperative to leverage China's extensive data scale and diverse application scenarios, unlock the potential of data elements, fortify and broaden the digital economy, augment the novel impetus of economic growth, and establish a fresh national competitive edge."

[38] Ronghua Shen, '推进"放管服"改革:内涵、作用和走向 [Promoting the Reform of "Decentralization and Service": Connotation, Function and Direction]' [2019] 中国行政管理 [Chinese Public Administration] 15, 15.

[39] Standing Committee of the National People's Congress, '关于加强网络信息保护的决定 [Decision on Strengthening Network Information Protection]' (2012) <http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm> accessed 23 April 2023.

Rights and Interests Protection Law (2013 Amendment),[40] Criminal Law amendments,[41] the Cybersecurity Law,[42] and the E-commerce Law.[43] A considerable proportion of this dispersed legislative package comprised principle-oriented, declaratory provisions that exerted minimal practical influence – for instance, the 2012 NPC Decision, which lacks provisions outlining legal accountability and serves primarily as a symbolic pledge.[44]

This decentralized legislation engendered at least two propensities: firstly, a potential discord within the legal interpretative framework, evidenced by the markedly divergent definitions of personal information across multiple legislative enactments,[45] culminating in disparities in law enforcement rules and compliance system ambiguities for law-abiding entities. Secondly, the protective regime concerning personal information was increasingly characterized by administrative oversight and criminalization.[46] For instance, the Criminal Law Amendment (IX) considerably expanded the sentencing scope for the crime of infringing upon citizens' personal information – the unlawful action of obtaining, selling, or distributing someone else's personal information without their consent, elevating the maximum sentence from three to seven years.[47] Additionally, in 2017, the Ministry of Public Security publicly sought input on amending the Public Security Administrative Punishment Law, which would also introduce "detention" penalties, thereby curtailing the personal liberties of individuals who breach their user information protection obligations.[48]

China's Cybersecurity Law was formally promulgated in 2016,[49] following a structured legislative process that included public consultation and iterative drafting. The initial draft was released by the Standing Committee of the National People's Congress in June 2015,[50] with a revised version circulated

[40] 中华人民共和国消费者权益保护法 [Law of the People's Republic of China on the Protection of Consumer Rights and Interests] 2013 (Order No 7 of the President).

[41] In 2009, the Article 253 of Criminal Law Amendment (VII) made it a crime to illegally obtain and illegally provide citizens' personal information in specific circumstances, which was further improved in the Criminal Law Amendment (IX) in 2015.

[42] 中华人民共和国网络安全法 [Cybersecurity Law of the People's Republic of China] 2016 (Order No 53 of the President) (CSL 2016). An open-access English translation of the CSL for reference purposes can be found at https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/ (Stanford's Digital China Project).

[43] 中华人民共和国电子商务法 [E-Commerce Law of the People's Republic of China] 2018 (Order No 7 of the President).

[44] Rong Wang, '我国《个人信息保护法》立法前路 [China's Personal Information Protection Law Legislative Road Ahead]' (*互联网前沿 Internet Frontiers*, 2017) <https://www.tisi.org/16113> accessed 24 April 2023.

[45] See the discussions in Section 4.1.

[46] Wang (n 44).

[47] 中华人民共和国刑法(2015修正) [Criminal Law of the People's Republic of China (2015 Amendment)] 2015 (National People's Congress), art 253.1.

[48] See Article 57, proposed by Ministry of Public Security, 'Public Security Administrative Punishments Law (Draft Revisions for Solicitation of Public Comments)' (*China Law Translate*, 18 January 2017) <https://www.chinalawtranslate.com/治安管理处罚法-（修订公开征求意见稿/> accessed 24 April 2023.

[49] See the final version of the CSL at http://www.gov.cn/xinwen/2016-11/07/content_5129723.htm.

[50] NPC, '网络安全法（草案）全文 [The Full Text of the Cyber Security Law (Draft)]' (*The National People's Congress of the People's Republic of China*, 7 June 2015) <http://www.npc.gov.cn/npc/c1481/201507/82ce4cb5549c4f56be8a6744cf2b3273.shtml> accessed 23 April 2023.

in 2016 to solicit public and institutional feedback.[51] The law was subsequently adopted by the National People's Congress in November 2016 and came into force in June 2017.[52]

However, the multifaceted nature of cybersecurity in China transcends conventional notions encompassing cybercrime, cyberwar, cyber defence, and safeguarding personal data,[53] simultaneously integrating economic and societal advancement policies within its development-security discourse,[54] by shifting the ideological focus from technological issues to international geopolitical concerns (focusing on the period from 1994 to 2016),[55] and to those persistently changing concepts, such as content security and data security (from 2016 forward).[56] Indeed, the conceptualization of cybersecurity on technology, infrastructure, content, and data, upgraded to the level of national security,[57] featured the data regulatory model with Chinese characteristics.[58]

What distinguishes China's regulatory trajectory, however, is not simply the formal consolidation of its data governance regime, but the extent to which cybersecurity has been conceptualized as a multidimensional project—entwining technical regulation with ideological, economic, and geopolitical imperatives. In this regard, China's approach finds few analogues among its BRICS counterparts. Only India has articulated a similarly integrated vision of digital sovereignty and developmental transformation, as evidenced by initiatives such as India Stack and Digital India.[59] By contrast, other BRICS states have tended to adopt more compartmentalized or rhetorically driven approaches. South Africa, for instance, has made technical strides through the implementation of Zero Trust architectures and engagement in cross-border cybersecurity cooperation,[60] while Brazil—under the current Lula administration—has advanced ambitious proposals for institutional reform, including the creation of new cybersecurity bodies.[61] At the multilateral level, BRICS as a bloc has begun to exhibit modest

---

[51] NPC, '网络安全法（草案二次审议稿）全文 [Full Text of the Cybersecurity Law (Draft for Second Deliberation)]' (*The National People's Congress of the People's Republic of China*, 2016) <http://www.npc.gov.cn/zgrdw/npc/lfzt/rlyw/2016-07/05/content_1993588.htm> accessed 23 April 2023.

[52] CSL 2016.

[53] Jiang (n 15).

[54] Institute of Cybersecurity of China Academy of Cyberspace, '筑牢国家网络安全屏障——我国网络安全工作发展成就与变革 [Building a Strong National Cybersecurity Barrier - the Achievements and Changes in China's Cybersecurity Work Development]' (2022) <https://www.secrss.com/articles/50447> accessed 25 April 2023.

[55] Weishan Miao, Jian Xu and Hongjun Zhu, 'From Technological Issue to Military-Diplomatic Affairs: Analysis of China's Official Cybersecurity Discourse (1994–2016)' in Jeremy Hunsinger, Matthew M Allen and Lisbeth Klastrup (eds), *Second International Handbook of Internet Research* (Springer Netherlands 2020).

[56] Rogier Creemers, 'The Chinese Conception of Cybersecurity: A Conceptual, Institutional and Regulatory Genealogy' [2023] Journal of Contemporary China 1, 12.

[57] "Without cybersecurity, there is no national security; without informatisation, there is no modernization (没有网络安全就没有国家安全，没有信息化就没有现代化)." – President Xi Jinping, see his Speech at the first meeting of the Central Leading Group for Cyber Security and Informatisation on February 27, 2014.

[58] Henry S Gao, 'Data Regulation with Chinese Characteristics' in Mira Burri (ed), *Big Data and Global Trade Law* (Cambridge University Press 2021).

[59] Ingrid Schneider and Krishna Ravi Srinivas, 'A chance for India to shape a data governance regime' *The Hindu* (14 March 2023) https://www.thehindu.com/opinion/lead/a-chance-for-india-to-shape-a-data-governance-regime/article66615759.ece accessed 5 April 2025.

[60] BCX, 'Cybersecurity trends and adoption in Africa: a comprehensive overview for 2025' (BCX, 15 January 2025) https://www.bcx.co.za/technology-insights/cybersecurity-trends-and-adoption-in-africa-a-comprehensive-overview-for-2025/ accessed 5 April 2025.

[61] Joe Devanny and Russell Buchan, 'Brazil's Cyber Strategy Under Lula: Not a Priority, but Progress Is Possible' (Carnegie Endowment for International Peace, 8 August 2023) https://carnegieendowment.org/2023/08/08/brazil-s-cyber-strategy-under-lula-not-priority-but-progress-is-possible-pub-90339 accessed 5 April 2025

regulatory convergence in areas such as data protection, content governance, and cybercrime.[62] Ongoing discussions concerning a potential "pentalateral" cyber accord suggest a collective movement toward institutional coordination, though the depth and coherence of such efforts remain uneven.

In essence, the Data Security Law (DSL) and Personal Information Protection Law (PIPL) are perceived by policy architects as constituents of an overarching cybersecurity regulatory framework. Consequently, a degree of both synergy and discord exists amidst the trio concerning normative explication and scrutiny. As an illustration, the Cybersecurity Law (CSL) inaugurated a particular emphasis on preserving Critical Information Infrastructure (CII) [63] – subject to the Multi-Level Protection System[64] – encompassing public communicative and informational utilities possessing the capacity to considerably imperil national security and interests. [65] This culminates in the Data Grading and Classification System under the DSL.[66] Pertaining to personal data, the CSL prescribes the principle of data localization for personal information and important data amassed and produced by CII operators, necessitating storage within China's borders, save for instances where security assessments by the Cyberspace Administration of China (CAC) and additional State Council departments permit otherwise.[67]

Such regulatory stringency—especially the integration of cybersecurity considerations into the treatment of both infrastructural and personal data—has no close analogue among other BRICS jurisdictions. While Russia and South Africa have prioritized cybersecurity within their respective national strategies, they have not articulated a comparably comprehensive or securitized framework for data governance. In this respect, the Chinese model stands apart in its synthesis of cyber, data, and national security regulation within a single, coherent legislative architecture.

Moreover, the Data Security Law, ratified in June 2021 during the 29th session of the Standing Thirteenth National People's Congress,[68] a brief interval after the promulgation of the PIPL, further fortifies China's data governance paradigm, encompassing provisions for transnational data transfer and delineating regulations that interconnect with both the PIPL and the Cybersecurity Law of China. The DSL accentuates the protection of national security by augmenting the stipulations of the CSL and expanding China's extraterritorial jurisdiction over specific data categories.[69] Concurrently, it advocates

---

[62] Luca Belli, 'Cybersecurity Convergence in the BRICS Countries' *CyberBRICS* (20 September 2021) https://cyberbrics.info/cybersecurity-convergence-in-the-brics-countries/ accessed 4 April 2025.

[63] The Critical Information Infrastructure Security Protection Regulations were enacted on September 1, 2021, subsequent to their approval at the 13th Standing Committee meeting of the State Council on April 27, 2021. The objective is to safeguard the security of critical infrastructure and defend against cyber threats, in accordance with the Cybersecurity Law. Critical information infrastructure is defined by regulations as comprising of significant network infrastructure and information systems in crucial industries, including but not limited to telecommunications, energy, transportation, finance, and e-government. The destruction, loss of functionality, or data leakage of critical infrastructure could have a substantial impact on national security, the economy, public interest, and people's livelihood. See 关键信息基础设施安全保护条例 [Critical Information Infrastructure Security Protection Regulations] 2021 (Order No 745 of the State Council) art 2.

[64] CSL 2016, art 21.

[65] ibid art 31.

[66] 中华人民共和国数据安全法 [Data Security Law of the People's Republic of China] 2021 (Order No 84 of the President) (DSL 2021) art 21. An open-access English translation of the DSL for reference purposes can be found at https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/ (Stanford Digital China Project).

[67] CSL 2016, art 37.

[68] DSL 2021.

[69] CAC, '专家解读｜《数据安全法》为全球数据安全治理贡献中国智慧和中国方案 [Expert Interpretation | "Data Security Law" Contributes Chinese Wisdom and Chinese Solutions to Global Data Security Governance]' (*Cyberspace Administration of China*, 2021) <http://www.cac.gov.cn/2021-06/15/c_1625341228851523.htm> accessed 25 April 2023.

for open data endeavours,[70] as well as incentives for "soft law" – inclusive of enhancing societal cognizance of data security,[71] fostering self-regulatory measures,[72] devising ancillary technological standards,[73] and endorsing security certification.[74] In pursuit of this objective, the DSL inaugurates a data grading and classification system that categorizes data predicated on various factors, including significance to economic and social development, potential detriment to national security, public interests, lawful rights and interests of individuals or organizations, and the likelihood of alteration, destruction, disclosure, or illicit procurement or utilization of information.[75] Notably, the DSL introduces a novel classification of "core national data" that subsumes domains such as national security, vital components of the national economy, significant facets of citizens' lives, and major public interests.[76]

The DSL distinctly bolsters institutional mechanisms for national data security by allocating the National Security Council,[77] in collaboration with vertical departments under the Ministry of Public Security, Ministry of State Security, and the Cyberspace Administration of China,[78] the responsibility of supervising its implementation. Furthermore, the DSL stipulates that each administrative region and department is accountable for data acquisition and security within their respective domains.[79] As the DSL emphasizes national security, it enforces more rigorous regulations on data localization and transfer,[80] as well as imposes stringent penalties for failure to comply.[81] For example, it elucidates the prerequisites for accessing data to preserve national security or probe criminal activities,[82] as well as mandates prior authorization for foreign judicial or law enforcement agencies' data requisitions.[83] In addition, any transference of China-originated important data overseas imposes a security assessment in accordance with the Cyberspace Administration of China's guidelines.[84]

The interrelation between the Cybersecurity Law (CSL), Data Security Law (DSL), and Personal Information Protection Law (PIPL) was further underscored by the 2022 amendments to the CSL. In September 2022, the Cyberspace Administration of China (CAC) resolved to modify the CSL, with the aim of harmonizing its provisions with recently enacted legislation, such as the Administrative Punishment Law, Data Security Law, and Personal Information Protection Law.[85] For instance, the revised draft of the CSL refined the legal liability provisions concerning violations of personal information rights and interests by invoking the application of the PIPL. The monetary penalty has also been escalated from "1 million" to "50 million" or "5%" of the previous year's turnover.[86] The

[70] DSL 2021, ch V.
[71] ibid art 9.
[72] ibid art 10.
[73] ibid art 17.
[74] ibid art 18.
[75] ibid art 21.
[76] ibid.
[77] ibid art 5.
[78] ibid art 6.
[79] ibid.
[80] ibid ch IV.
[81] ibid ch VI.
[82] ibid art 35.
[83] ibid art 36.
[84] ibid art 31.
[85] CAC, '关于公开征求《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》意见的通知 [Notice on Public Solicitation of Opinions on the "Decision on Amending the Cybersecurity Law of the People's Republic of China (Draft for Comments)]' (*GOV.CN*, 2022) <http://www.gov.cn/xinwen/2022-09/14/content_5709805.htm> accessed 2 May 2023.
[86] ibid.

amendment inaugurates more stringent penalties for breaches of the Cybersecurity Law,[87] endowing authorities with grander legal authority to address violations and safeguard users' rights.[88]

1.4.2. The Conflicting Role? The PIPL vs. The Chinese Civil Code (CCC)

China's data protection regime beyond the PIPL exhibits institutional coherence through the troika of the data governance framework. This framework enhances the stickiness of China's PI protection under its administrative law or public law system. However, the explanatory mainlines of the individual rights protection established in the Chinese civil code (CCC) represent another significant aspect of comprehending the PIPL.

China attempted to formulate civil laws on four separate occasions since 1949, but external circumstances impeded success until the Fourth Plenary Session of the 18th Central Committee of the Communist Party of China that marked the beginning of the codification.[89] In 2014, the Fourth Plenary Session of the Eighteenth Central Committee of the Communist Party of China decided to codify the Civil Code.[90] A "two-step process" was later established to elaborate on the General Provisions followed by the compilation of sub-sections of the Civil Code, ultimately leading to a unified Civil Code.[91] The compilation began in 2015, with the General Provisions passed in 2017 and subsequent sub-sections integrated in December 2019.[92] After further refinement by the Standing Committee, the Civil Code was deliberated upon during the Third Session of the 13th National People's Congress in 2020,[93] and ultimately took effect in January 2021.[94]

Once perceived as the foundational legislation governing the market economy, the Civil Code emerged in part as a redressal mechanism for reputation and privacy infringements amidst the digital revolution characterized by pervasive information dissemination.[95] Central to this notion is the distinct delineation of personality rights, encapsulated within Chapter 6 of Book IV, which concurrently establishes personal information protection and the civil right to privacy.[96] In this context of juxtaposed enumeration,

---

[87] This was highlighted in the Didi Chuxing case, in which the ride-hailing company that received a record fine of US$1.2 billion for contravening China's cybersecurity, data security, and personal information protection regulations including the CSL. 'China Ride-Hailing Giant Didi Fined $1.2bn after Probe - BBC News' *BBC News* (21 July 2022) <https://www.bbc.com/news/business-62248513> accessed 23 April 2023.

[88] Arendse Huld, 'China Cybersecurity Law: CAC Solicits Opinions on Amendment' (*China Briefing News*, 20 September 2022) <https://www.china-briefing.com/news/china-cybersecurity-law-cac-solicits-opinions-on-amendment/> accessed 23 April 2023.

[89] Xinhua News Agency, 'China Drafting Civil Code: Spokeswoman' (*The State Council of the People's Republic of China*, 2 April 2016) <http://english.www.gov.cn/news/top_news/2016/03/04/content_281475301143367.htm> accessed 23 April 2023.

[90] Xinhua News Agency, '新时代的人民法典——《中华人民共和国民法典》诞生记 [The People's Code of the New Era——The Birth of the "Civil Code of the People's Republic of China"]' (*Central's People Government of the People's Republic of China*, 2020) <http://www.gov.cn/xinwen/2020-05/28/content_5515766.htm> accessed 25 April 2023.

[91] ibid.

[92] ibid.

[93] ibid.

[94] CCC 2020.

[95] People's Daily, '人民美好生活的法治保障——写在《中华人民共和国民法典》诞生之际 [Guarantee of the Rule of Law for a Better Life for the People— Written on the Occasion of the Birth of the "Civil Code of the People's Republic of China"]' (*Central's People Government of the People's Republic of China*, 28 May 2020) <http://www.gov.cn/xinwen/2020-05/31/content_5516270.htm> accessed 25 April 2023.

[96] Article 1032 of the CCC defined Privacy as "the tranquility of the private life of a natural person, and the private space, private activities, and private information that he is unwilling to be known to others." In contrast, Article 1034 defined Personal Information as "various information recorded electronically or in other forms that can identify a specific natural person separately or in combination with other information, including a natural person's

personal information is construed as a legal interest rather than an aspect of personality rights.[97] This metamorphosis from a singular privacy paradigm in the pre-Civil Code era to a dualistic framework inclusive of both privacy and personal information protection has engendered a more inconsistent judicial implementation of privacy-vs-personal-information terminology.[98] Despite Article 1034, which elucidates the distinction between personal information and the right to privacy by employing the phrase "personal information of privacy nature," these discrepancies persist.[99]

1.5. The Characteristics of the PIPL: A Multidimensional Perspective

The Chinese PIPL legislative intent, as stated in the official public statement made by its legislator in October 2020,[100] precisely prior to the publication of the first draft, is to remedy the lack of regulation of the widespread collection and use of personal information by different parties, as well as institutionally reaching an interest-coordinating trade-off between frequent infringements of personal information and the development of the digital economy. Although some claim a considerable degree of comparability between the PIPL and the GDPR,[101] a significant portion of the PIPL rules features their normative heterogeneity from the established ones.

1.5.1. What is (Sensitive) Personal Information?

The PIPL featured an intentional normative trade-off between regulation and growth. On the one hand, the Article 4 of the PIPL initiated and expanded the scope of personal information, as well as excluding anonymization from the PI definitive scope, notably from a compliance perspective. Prior to the PIPL, personal information was defined in the then-existing laws for practitioners' reference, such as the Cybersecurity Law,[102] and the Chinese Civil Code.[103] In both contexts, there was a narrow interpretation of PI in the context of identifiability, in which the term "identifiability" implied only the requirement of "identification" but not the requirement of "relating-to". The National Standard GB/T 35273 in between, short for Information Security Technology - Personal Information Security Specification, for the first time, broadened the concept of "personal information" to include "any type of information recorded electronically or by other means that, by itself or in combination with other information, can identify a specific natural person or reflect the activities of a specific natural person".[104] In Annex A (GB/T 35273-

name, date of birth, identity card number, biological recognition information, address, telephone number, e-mail address, health information, and whereabouts information, among others."

[97] Personal Information defined in the CCC is classified as encompassing "other personality interests arising from personal freedom and personal dignity". See CCC 2020, art 990.

[98] Lu Zhang, '"Personal Information of Privacy Nature" under Chinese Civil Code' (2021) 43 Computer Law & Security Review 105637, 2–3.

[99] ibid 5.

[100] Junchen Liu, '关于《中华人民共和国个人信息保护法（草案）》的说明 [Explanation on the Personal Information Protection Law of the People's Republic of China (Draft)]' (*National People's Congress*, 2020) <http://www.npc.gov.cn/npc/c30834/202108/fbc9ba044c2449c9bc6b6317b94694be.shtml> accessed 26 January 2023.

[101] Xu Ke and others, 'Analyzing China's PIPL and How It Compares to the EU's GDPR' (2021) <https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/> accessed 11 January 2023.

[102] As Article 76(5) of the Cybersecurity Law says, "Personal information means all kinds of information recorded in electronic or other forms, which can be used, independently or in combination with other information, to identify a natural person's personal identity, including but not limited to the natural person's name, date of birth, identity certificate number, biometric information, address, and telephone number."

[103] CCC 2020, art 1034. It says "Personal information is information recorded electronically or in other ways that can be used, by itself or in combination with other information, to identify a natural person, including the name, date of birth, identification number, and biometric information, residential address, telephone number, email address, health information, whereabouts, and the like, of the person."

[104] Information security technology— Personal information (PI) security specification - GB/T 35273—2020 (Replacing GB/T 35273-2017) (n 10), s 3.1.

2020), it indicated the two criteria for determining PI, namely "identification" + " relating-to."[105] The former focuses on the inherent attributes of an individual that are identifiable. In contrast, the latter focuses on the information generated by a particular natural person in the course of his or her activities (e.g., location data, phone call history, web browsing history, etc.).

On the other hand, the PIPL diverges from the GDPR in its approach to sensitive personal information (PI). Article 28 of the PIPL provides a flexible "generalization + enumeration" definition of sensitive PI, likely offering room for interpretation and compliance in emerging technologies. Categories of sensitive PI in the PIPL include biometrics, religious beliefs, specific identity, medical and health, financial accounts, trajectory/location data, and information of minors under 14 years old.[106] Meanwhile, the PIPL imposes more stringent handling prerequisites for sensitive PI, with extra procedural obligations to PI handlers. Sensitive PI handling is influenced by factors such as purpose specificity, data handling necessity, and security measure stringency.[107] The PIPL requires separate consent mechanisms for sensitive PI handling,[108] disallowing general consent, authorization, or bundling tactics. Additionally, the PIPL mandates not only informing the individual but also notifying them of the necessity and impact of handling sensitive PI on their rights and interests.[109]

Among the BRIC countries, China's PIPL defines sensitive personal information broadly as data that, if misused, could endanger individual dignity or security. Brazil's LGPD enumerates specific sensitive data categories—such as race, religion, political views, health, sex life, and biometric or genetic identifiers—requiring explicit consent for processing, subject to narrow exceptions.[110] India's DPDPA (2023) does not define sensitive data per se but adopts a risk-based model, imposing heightened obligations on Significant Data Fiduciaries based on factors like data volume, sensitivity, and potential national impact.[111] Russia's Federal Law No. 152-FZ similarly designates special categories, including biometric, health, and criminal data, which are strictly regulated and generally require explicit consent, with safeguards commensurate to data sensitivity.[112]

The final conceptual expansion is on the PI of the deceased. Article 49 of the PIPL provides a comprehensive approach to addressing the issue of posthumous management of personal information in the era of big data. It is institutionally rooted in the provisions of Article 994 of the Civil Code regarding the protection of the personality rights of the deceased.[113] It offers a framework for the inheritance of personal data, enabling individuals to exercise their autonomy and testamentary freedom. Thus, the PIPL, to some extent, allows for priority to be given to the deceased's own arrangements for their personal information.[114]

---

[105] ibid Annex A.

[106] 中华人民共和国个人信息保护法 [Personal Information Protection Law of the People's Republic of China] 2021 (Order No. 91 of the President) (PIPL 2021) art 28. An open-access English translation of the PIPL for reference purposes can be found at https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (Stanford's Digital China Project).

[107] ibid.

[108] ibid art 29.

[109] ibid art 30.

[110] See Lei No 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais) arts 5(II), 11.

[111] See Digital Personal Data Protection Act 2023 (India) s 10.

[112] See Federal Law No 152-FZ on Personal Data (27 July 2006, Russia) arts 6, 10, 19, 22.

[113] As Article 994 of the Chinese Civil Code says, "Where the name, likeness, reputation, honor, privacy, or body of a deceased person is infringed upon, his spouse, children, and parents have the right to request the actor to assume the civil liability according to the law…"

[114] As Article 49 of the PIPL says, "…except as otherwise arranged by the deceased before his or her death."

1.5.2. Rights Bundle of Data Subjects: Intensifying Individual Control over Data

In essence, the PIPL's conceptual basis, rooted in the self-determination of personal information, seeks to supplement the bundle of rights (权利束), as prescribed by the civil code and viewed as an expandable normative concept concerning the positive rights formulation for personal information – namely, instrumental rights granted to individuals by the State through institutional safeguards in order to fulfil its obligation to protect personal information.[115] To address the exorbitant power asymmetry between individuals and information handlers, characterized by disparities in technical, economic, and information prowess, the PIPL confers rights upon individuals and imposes obligations upon information handlers, like most data protection legislation, to rectify this imbalance, entailing, for example, judicious access to and control of data.

The architecture of data control is initially manifested through Article 44, establishing the right to know, the right to decide, and the right to restrict/refuse – Individuals possess an overarching privilege to dictate the management of their PI. Nevertheless, this provision, as a more eminent stratum of jurisprudence, omits the delineation of the scope and demarcations pertaining to an individual's right to know. Concurrently, Article 44 stipulates, as an "exception clause," that exclusions apply "unless otherwise dictated by legislation and administrative regulations." This suggests that under exceptional circumstances—such as when personal data is processed in pursuit of demonstrable public interest objectives or for the prevention and investigation of unlawful or criminal conduct—the data subject's rights above may be lawfully limited or derogated from, subject to proportionality and necessity constraints as recognized in statutory and administrative practice.

The PIPL also serves to enhance individuals' control over their personal data by delineating rights to access, duplication, rectification, and deletion, as likewise but abstractly stipulated in the Civil Code.[116] Article 45 of the PIPL strengthens an individual's right to know and decide the treatment of their personal data, in tandem with its Article 44, while Article 107 of the CCC safeguards access and duplication rights, and grants the right to contest and rectify inaccuracies. Furthermore, Articles 46 and 47 elucidate rights to rectify, supplement, and delete personal information, building upon the Civil Code and Cybersecurity Law.[117] The PIPL broadens the circumstances for deletion requests,[118] integrates exemptions to Article 1037 of the Civil Code, and necessitates the creation of mechanisms for receiving and processing applications to exercise individual rights. Lastly, the PIPL final draft commendably incorporates specificity into Article 47(1)(a) by clarifying the conditions for deletion applicability, although further clarification on "deletion of personal information that is technically unattainable" remains necessary.

The intensification of individual data control, as manifested through Article 45 of the Personal Information Protection Law (PIPL), aims to dismantle data silos and monopolies by instituting the right to data portability, aligning with policy trajectories that emphasize internet governance, anti-competitive practices, and antitrust constraints, while fostering data interoperability and common prosperity.[119] However, the actualization of data portability necessitates further clarification on legitimate grounds for personal information transfer, technical milieu, and third-party rights and interests balancing, like those

---

[115] Wang Xixin, '重思个人信息权利束的保障机制：行政监管还是民事诉讼 [Reflecting upon the protection mechanism of personal information rights bundle: administrative supervision or civil litigation]' (2022) 44 法学研究 Chinese Journal of Law 3.
[116] CCC 2020, art 1037.
[117] ibid; CSL 2016, art 43.
[118] PIPL 2021, art 47.
[119] Nathaniel Taplin and Jacky Wong, 'Common Prosperity: Decoding China's New Populism' *Wall Street Journal* (28 August 2021) <https://www.wsj.com/articles/common-prosperity-decoding-chinas-new-populism-11630159381> accessed 4 May 2023.

in Article 20 of the GDPR and Article 18 of the LGPD, lest enterprises face augmented compliance burdens and unbridled competition. Article 48 of the PIPL also endows users with a claimable right to request clarification in accordance with standard clause contracting rules of the CCC,[120] compelling private entities to solicit informed consent upon initial application engagement.[121]

Despite these provisions, the PIPL's scope remains indeterminate, encompassing limitations and ambiguities surrounding binary choices, data collection indispensability, and the distinction between fundamental and augmented commercial functions,[122] rendering the efficacy of discourse between individual users and personal information handlers in a transitional phase, as will be discussed in the following.

1.5.3. General and Special Obligations of Data Handlers

While endowing data subjects with enhanced autonomy over their personal information, the PIPL concurrently delineates fundamental tenets, encompassing "Explicit Purpose + Minimal Scope" and "Informed-Consent" processing rules, alongside provisions for security breach disclosure and rectification, as well as distinct responsibilities for prominent, platform-based personal information handlers. Nevertheless, these imposed duties exhibit a pronounced emphasis on security discourses and reactive strategies in response to societal and public perceptions, such as debates surrounding automated decision-making and facial recognition technology.

1.5.3.1. The Principle of "Explicit Purpose + Minimal Scope" (Purposefulness + Necessity) (Article 6)

The principle of purposiveness, articulated in Article 6 of the Personal Information Protection Law (PIPL), requires that the processing of personal data be directed toward a specific, legitimate, and reasonably ascertainable purpose. It further demands a demonstrable nexus between that purpose and the functional offerings of the data-handling entity. Closely related is the principle of necessity, which operates as a foundational constraint on data collection practices. Under this standard, only data strictly relevant and proportionate to the fulfillment of an organization's operational objectives may be lawfully collected, thereby precluding the accumulation of superfluous or tangential information.

The application of these principles is neither formalistic nor uniform; rather, it is contingent upon the structure and logic of divergent business models and must be interpreted in conjunction with pre-existing regulatory instruments that anticipate and inform the PIPL's normative framework. For instance, mobile application operators are required to assess whether the scope of personal information they collect exceeds what is deemed "necessary" under the *Provisions on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications*,[123] which delineates baseline requirements across 39 app categories. This regulatory apparatus thus operationalizes the necessity principle through sector-specific guidance, introducing a functionalist calibration between legal standards and industry practice.

1.5.3.2. The Principle of "Informed Consent" (Articles 13, 14, 15,16 &17)

The PIPL marks a significant departure from the CSL's unitary legislative foundation, which is principally anchored in the monolithic "informed consent" paradigm. It carefully refines and amplifies

[120] CCC 2020, art 496(2).

[121] Konrad Kollnig and others, 'Before and after China's New Data Laws: Privacy in Apps' (arXiv, 2 March 2023) 5–6 <http://arxiv.org/abs/2302.13585> accessed 11 April 2023.

[122] ibid 5.

[123] 常见类型移动互联网应用程序必要个人信息范围规定 [Provisions on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications] 2021 (No. 14 of the Secretary Bureau of Cyberspace Administration of China).

the scope of the exception "otherwise mandated by law or administrative regulations," as articulated in Article 1035 of the Civil Code. To explicate with greater doctrinal precision, this clause—prior to the PIPL's enactment—had broader applicability under Article 42, Paragraph 1 of the CSL, wherein consent functioned as the central normative basis for personal information processing, subject only to limited exceptions such as anonymization.

For instance, the *Personal Information Security Specification* enumerates eleven exemptions from the consent requirement, notwithstanding the fact that not all are undergirded by formal legal authority.[124] Concurrently, Article 1036 of the Civil Code delineates three specific circumstances under which personal information may be processed without the data subject's consent. Against this background, the seven lawful bases for processing personal information set forth in Article 13 of the PIPL represent a more comprehensive and normatively robust articulation of the "informed consent" principle, one that is marked by heightened legal determinacy. This evolution may, in turn, contribute to greater efficiency in the circulation and handling of personal information.

Fundamentally, the "Informed Consent" doctrine, extrapolated from the 13th, 14th, 15th, 16th, and 17th provisions of the PIPL, can be construed as follows: the acts of "informing" and "consenting" form the bedrock tenets in the domain of PI handling. Acquiescence should be elicited premised upon the provision of exhaustive prior disclosure, eschewing deceptive, duplicitous, or intimidatory stratagems.[125] Providers must not, under any circumstance, withhold products or services contingent upon a person's dissent to consent.[126] Entities involved in data management ought to offer an expedient mechanism for the retraction of consent.[127] Contrasting with the preliminary draft, the ratified version incorporates an ancillary stipulation in the legitimate reasons for the PI handling, specifically the "imperative administration of human resources."[128] This provision functions as an equipoise to redress the predicament wherein the breadth of employee personal data garnered on the foundation of an employment contract is markedly circumscribed, and its application is confined.[129]

Notably, within the parameters of Article 14 in the PIPL, the notions of "separate consent" and "written consent" are expounded, and ensuing clauses lay down the mandate for separate consent in particular circumstances pertaining to the PI handling: 1) the relay of processed PI to a third-party entity;[130] 2) the public exhibition of processed PI;[131] 3) the deployment of personal visual and identity data (e.g. facial recognition) accrued in public domains for objectives transcending the preservation of public safety;[132] 4) the handling of sensitive PI;[133] 5) the outbound PI transfer.[134]

1.5.3.3. Security Obligations: Measures, Audits and Assessments

The PIPL, meanwhile, outlines the security obligations of entities handling personal information in safeguarding the confidentiality and integrity of such data. The law integrates provisions from the Cybersecurity Law,[135] mandating the maturity of a comprehensive executive framework for the stratified

[124] Information security technology— Personal information (PI) security specification - GB/T 35273—2020 (Replacing GB/T 35273-2017) (n 10).
[125] PIPL 2021, art 14.
[126] ibid art 16.
[127] ibid art 15.
[128] ibid art 13(2).
[129] "The employment contract shall contain the basic information of the worker, including the worker's name, address, and resident ID card or other valid ID card numbers, etc." See 中华人民共和国劳动合同法(2012修正) [Labor Contract Law of the People's Republic of China (2012 Amendment)] 2012 (Order No. 73 of the President) art 17.
[130] PIPL 2021, art 23.
[131] ibid art 25.
[132] ibid art 26.
[133] ibid art 29.
[134] ibid art 39.
[135] CSL 2016, arts 25, 26, 39 and 40.

stewardship of personal information. Handlers must employ sophisticated technical measures, including encryption and de-identification for instance, to ensure the security, autonomy, and controllability of personal information.[136] Furthermore, the integration of instructional mechanisms for training practitioners and devising emergency plans into routine operations is required.[137] The PIPL also obliges the designation of a personal information protection officer (PIPO) contingent upon reaching a predetermined threshold for personal information handling.[138] That's said, Brazil's LGPD broadly requires "technical and administrative measures" without prescribing specific implementations;[139] and India's DPDP Act similarly employs a principles-based approach with "reasonable security measures,"[140] giving organizations flexibility in implementation while being less prescriptive than China's regulation, reflecting different regulatory philosophies that balance compliance clarity against implementation flexibility.

The PIPL evidently addresses the regulatory gap for foreign organizations by stipulating that foreign personal information handlers subject to the legislation must institute specialized domestic entities or designate domestic representatives.[141] These handlers are obliged to submit their commitments to the department overseeing personal information protection (e.g. CAC and its subordinate agencies).[142] This provision parallels the extraterritorial jurisdiction expansion of the PIPL, aligning it with resembled mechanisms in the European Union's General Data Protection Regulation (GDPR),[143] as well as other extraterritorial counterparts globally. Consequently, foreign personal information handlers potentially subjected to the PIPL are required to establish institutions within China or appoint representatives for submission.

The PIPL mandates that personal information handlers undertake a personal information protection impact assessment (PIPA) prior to engaging in specific handling activities.[144] This evaluation is consistent with the "personal information security impact assessment" notion portrayed in the Chinese national standard, GB/T 39335-2020.[145] The European Union's GDPR encompasses a comparable legal framework, the Data Protection Impact Assessment (DPIA), which data controllers must fulfil when processing activities pose a heightened risk to the rights and freedoms of personal data subjects.[146] India's 2023 DPDP Act adopts a targeted approach where only government-designated "significant data fiduciaries" (based on data volume, sensitivity, and risk) must conduct periodic impact assessments;[147] while Brazil's LGPD employs the most flexible framework, allowing its data protection authority discretionary power to request assessments rather than mandating them for specific processing activities, giving organizations greater implementation flexibility at the cost of less prescriptive guidance.[148] By elevating DPIA prerequisites to obligatory legal responsibilities, the PIPL may thus impose more rigorous stipulations on corporate internal compliance system development, streamlining compliance and execution for handlers while diminishing internal decision-making intricacy and uncertainty risk.

---

[136] PIPL 2021, art 51.
[137] ibid.
[138] ibid art 52.
[139] See Lei No 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais) art 46.
[140] See Digital Personal Data Protection Act 2023 (India) s 8(5).
[141] ibid art 53.
[142] ibid.
[143] General Data Protection Regulation (GDPR) 2016 (2016/679) art 3.
[144] PIPL 2021, art 55.
[145] Information security technology—Guidance for personal information security impact assessment - GB/T 39335-2020 2020.
[146] GDPR 2016, art 35.
[147] See Digital Personal Data Protection Act 2023 (India) ss 10(1), 10(2)(c)(i). See also Anirudh Burman, 'Understanding India's New Data Protection Law' (Carnegie Endowment for International Peace, 3 October 2023) https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en accessed 4 April 2025.
[148] Lei No 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais) art 38.

1.5.3.4. "Taming" Platforms: Gatekeeping and Automated Decision-Making

Substantial internet platforms, characterized by vast user populations and complex business structures,[149] wield significant power over transactions and personal data processing within their purview, thereby incurring heightened legal responsibilities for personal information (PI) protection. The PIPL defines a "gatekeeper" based on three criteria: providing essential internet platform services, having a substantial user base, and operating a complex business model, all of which are required. Regulations further specify that a "substantial user base" means over 50 million registered users or more than 10 million monthly active users, while "essential internet platform services" involve data processing with significant effects on national security, economic operations, or international livelihood.[150] However, there is no specific explanation for what constitutes a "complex business model." Therefore, an entity qualifies as a "gatekeeper" if it is a "personal information handler" with over 50 million registered users or 10 million monthly active users, operates a complex business, and has activities that exert significant influence.

In accordance with Article 58, enhanced oversight of "gatekeeper" corporations can be achieved by implementing four measures regarding these prominent digital platforms: establishing autonomous organizations comprising external members for PI protection supervision, formulating platform obligatory rules for PI handling and security, managing non-compliant behaviour within the platform, and disseminating social responsibility reports for public scrutiny.[151] Conversely, the PIPL recognizes that smaller PI handlers do not pose systemic risks and, as stated in Article 62(2), prescribes tailored PI protection protocols and standards to be separately introduced for these entities, as well as for emerging technologies like facial recognition and artificial intelligence.[152]

Pursuant to Article 24 of the PIPL, PI handlers employing automated decision-making instruments are mandated to ascertain transparency in the decision-making process and maintain equitable and impartial outcomes.[153] Differential treatment in aspects such as pricing or other transactional terms that lack reasonable justification, exemplified by the prevalent phenomenon of "Big Data Shashu" – a business tactic of using behavioural data to manipulate price discrimination – is prohibited,[154] which is analogous to Article 22 of the GDPR.[155] Furthermore, congruent provisions are present in the Personal Information Security Specification and the E-Commerce Law.[156] In instances where automated decision-making mechanisms are utilized for disseminating information or engaging in commercial promotion towards individuals, PI handlers ought to furnish alternative choices devoid of personalized targeting or facilitate convenient refusal methods for the recipients.[157] In circumstances where automated decision-making significantly impinges on an individual's rights and interests, the individual reserves the right to solicit elucidation and to reject decisions derived solely from automated processes.[158]

---

[149] PIPL 2021, art 58.

[150] 网络数据安全管理条例 [Online Data Security Management Regulations] 2024 (Order No. 790 of the State Council) (ODSMR 2024) art 62(8).

[151] ibid.

[152] ibid art 62(2).

[153] ibid art 24.

[154] Yaling Jiang, 'China's Personal Information Protection Law Is Here. What's Changing?' (*SixthTone*, 2021) <https://www.sixthtone.com/news/1008846> accessed 8 May 2023.

[155] GDPR 2016, art 22.

[156] See Information security technology— Personal information (PI) security specification - GB/T 35273—2020 (Replacing GB/T 35273-2017) (n 10), s 7.5(b); E-Commerce Law of the People's Republic of China 2018, art 18.

[157] PIPL 2021, art 24.

[158] ibid.

1.5.4. Limited Limitations upon the Public Sector

Indeed, the PIPL imposes regulatory constraints on the public sector, albeit to a limited extent in Section 3 of Chapter 2. The legislature necessitates conformity to the aforesaid section regarding its legitimate enactment while abiding by both general and specific stipulations pertaining to the PI handling, including the inform/notice obligations.[159] Exceptions exist wherein legal and administrative regulations necessitate confidentiality or exempt the need for disclosure under specific circumstances, as well as instances where notifying state organs would impede the execution of statutory obligations.[160] Moreover, the statute obliges data localization for public institutions, and when transferring data across borders is indispensable, a security assessment must be undertaken.[161]

Further elucidated within Section 3 are discrete guidelines for public institutions handling PI. Article 33 unambiguously asserts that, concomitant with the exclusive guidelines of this section, the endeavours of public institutions in relation to PI handling are additionally subject to other provisions delineated within the PIPL.[162] Simultaneously, Article 37 incorporates "bodies authorized by legal statutes and regulations to oversee public affairs" within the horizon of provisions applicable to public institutions handling PI while performing their legislatively mandated responsibilities.[163] It substantively broadens the ambit of applicability for this section, establishing a benchmark for "public affairs functions" that extends beyond the narrowly circumscribed purview of state organs.

1.5.5. Cross-Border Personal Information Flow with Chinese Characteristics

The PIPL introduces an intricate regulatory framework for data localization and transference, which ought to be, however, in part concretized through legal interoperability.[164] Central to this framework is the stipulation that handlers of personal information adhere to protection criteria delineated by the law, in addition to relevant international treaties and conventions China has concluded or acceded to,[165] serving as bilateral and multilateral approaches to reaching adequacy across jurisdictions. That said, the statute espouses the unobstructed flow of personal information across borders, concomitantly ensuring the deployment of rigorous security measures to achieve offshore recipients' jurisdictional protective adequacy.[166]

In general, the definitive draft amalgamates and systematizes the indispensable prerequisites for cross-border PI transfers by embracing obtaining the explicit consent of the individuals concerned and notifying them of the imminent transference.[167] Article 38 of the PIPL elucidates the stipulations for the provision of personal information to global recipients, which entail ascertaining that the activities of foreign recipients are congruent with the protection standards mandated by the legislation. This universal obligation establishes an overarching mechanism for transnational data transfer, attainable via three primary modalities: a Personal Information Security Assessment supervised by the cyberspace departments (PISA), Personal Information Protection Certification conferred by specialized institutions (PIPC), or the enactment of Standard Contractual Clauses (SCCs).[168] This multifarious approach to PI

[159] ibid art 35.
[160] ibid.
[161] ibid art 36.
[162] ibid art 33.
[163] ibid art 37.
[164] Luca Belli and Danilo Doneda, 'Data Protection in the BRICS Countries: Legal Interoperability through Innovative Practices and Convergence' (2023) 13 International Data Privacy Law 1.
[165] PIPL 2021, art 38.
[166] ibid.
[167] ibid art 39.
[168] ibid art 38.

protection exemplifies China's unwavering dedication to upholding protection and security amidst an increasingly interconnected global setting.

Comparatively, BRICS countries exhibit divergent approaches to transnational data transfers: China implements the most prescriptive framework with three government-overseen pathways (Security Assessment, Certification, or Standard Contractual Clauses); Brazil recently aligned closer to the EU model with its August 2024 ANPD Resolution establishing adequacy decisions, SCCs, and binding corporate rules;[169] Russia employs a notification-and-approval system requiring companies to inform Roskomnadzor before transfers and obtain approval for non-adequate countries;[170] India takes a unique "negative list" approach allowing transfers to all countries except those specifically restricted by the government;[171] while South Africa permits transfers when recipients are subject to adequate protective laws or binding agreements,[172] with each framework reflecting varying degrees of government intervention versus business flexibility and different underlying philosophies about data sovereignty versus free data flows.

Specifically, the tripartite avenues for the transference of personal information (PI) beyond national boundaries adhere to a hierarchical order of applicability, in accordance with the Chinese paradigm for data security: 1) Primarily, the Personal Information Security Assessment (PISA) criteria serve as a fundamental consideration for data exportation;[173] 2) Subsequent to ascertaining the inapplicability of security assessment classification, the selection between Personal Information Protection Certification (PIPC),[174] and Standard Contractual Clauses (SCCs),[175] may be exercised.

For instance, Article 40 of the PIPL decrees that operators of critical information infrastructure and PI handlers who process personal information up to the threshold specified by the Cyberspace Administration of China (CAC) and its subordinate agencies, must store domestically collected data within the borders of China in order to address concerns regarding data localization.[176] In circumstances mandating the provision of data beyond national borders, the exclusive prerequisite of security assessment (PISA) is applicable,[177] in lieu of the stipulations delineated in Article 38 pertaining to the PIPC and SCCs.[178] This post-security-assessment exception supplements and details the constraints

[169] Fernando Bousso and Matheus Botsman Kasputis, 'Brazil's New Regulation on International Data Transfers' (IAPP, 4 September 2024) https://iapp.org/news/a/brazil-s-new-regulation-on-international-data-transfers accessed 4 April 2025.
[170] DLA Piper, 'Transfer in Russia - Data Protection Laws of the World' https://www.dlapiperdataprotection.com/index.html?t=transfer&c=RU&c2= accessed 4 April 2025.
[171] See *DPDPA 2023, s 17*.
[172] See *POPIA, s 72*.
[173] In 2022, the China Administration of Cybersecurity (CAC) introduced the "Measures for the Security Assessment of Outbound Data Transfer," which provided comprehensive guidelines for the transfer of important data and data managed by Critical Information Infrastructure Operators (CIIOs), or data exceeding the threshold established by the CAC. See 数据出境安全评估办法 [Measures for the Security Assessment of Outbound Data Transfer] 2022 (Order No. 11 of the Cyberspace Administration of China).
[174] In 2022, the TC260, short for National Information Security Standardization Technical Committee released the Version 2.0 of the standard documentation, namely Cybersecurity Standards Practice Guide—Security Certification Specifications for Cross-Border Processing Activities of Personal Information. See 网络安全标准实践指南—个人信息跨境处理活动安全认证规范V2.0 [Cybersecurity Standards Practice Guide—Security Certification Specifications for Cross-Border Processing Activities of Personal Information V2.0] 2022 (TC260-PG-20222A).
[175] In 2023, the CAC eventually released the "Measures for the Standard Contract for the Outbound Transfer of Personal Information." See 个人信息出境标准合同办法 [Measures for the Standard Contract for the Outbound Transfer of Personal Information] 2023 (Order No. 13 of the Cyberspace Administration of China).
[176] PIPL 2021, art 40.
[177] ibid.
[178] ibid art 38.

imposed by the Cybersecurity Law.[179] This methodology is intended to ensure uniform adherence to data protection measures while expediting reasonable PI cross-border flow within a fortified infrastructure.

Meanwhile, on March 22, 2024, nearly six months after the release of the "Draft Regulations on Regulating and Promoting Cross-Border Data Flows," the Cyberspace Administration of China (CAC) officially promulgated the "Regulations on Promoting and Regulating Cross-Border Data Flows" (hereinafter referred to as the "New Cross-Border Data Regulations"), which took effect immediately upon publication.[180] This marked the establishment of a uniquely Chinese "dynamic adjustment mechanism for cross-border data regulation." The "New Cross-Border Data Regulations" provide regulatory exemptions for data transfers abroad by enumerating specific scenarios and aligning with practical needs, thereby reducing compliance burdens for businesses in common business contexts. However, while the regulations relax requirements for certain data transfers, they impose stricter oversight on the export of sensitive personal information. Compared to the more rigid, prohibitive measures adopted in other jurisdictions, these regulations offer a more flexible and clear compliance framework, supporting safe and orderly cross-border data flows in diverse business scenarios. Additionally, the regulations reference the negative list mechanism within free trade zones, which facilitates cross-border data flows by specifying restricted or prohibited data types, thereby allowing data not on the list to move more freely and simplifying the compliance process for businesses.[181]

1.6. The Enforcement of the PIPL: The Cyberspace Administration of China and Others

Diverging from certain legal frameworks, such as that of the European Union, China has yet to institute a singular data protection authority. Instead, a multifaceted enforcement climate persists, with the Cyberspace Administration of China (CAC) assuming a supervisory and coordinating capacity, and specialized agencies shouldering discrete responsibilities. The PIPL stipulates that the national cyberspace departments shall orchestrate and harmonize PI protection efforts, as well as the relevant supervision and administration tasks.[182] Furthermore, the legislation allocates the obligations of various State Council departments (including public security, market supervision, industrial information & technology, and sectoral regulatory bodies) within their respective purviews, collectively referred to as “departments responsible for PI protection.”[183] As for the grassroots enforcement, the PIPL also delegates responsibility for its execution to pertinent departments at the county level or above, under the authority of local people's governments.[184] Concurrently, the inception of the National Data Administration (NDA) transpired in the early months of 2023, tasked with the mandate of synchronizing the progression of Digital China, the digital economy, and the digital societal landscape, among other pertinent areas. The NDA is poised to operate as a central-level entity under the auspices of the National Development and Reform Commission, while simultaneously sharing designated functions with the Cyberspace Administration of China (CAC).[185]

Actually, the BRICS countries exhibit distinct approaches to data protection authorities: China uniquely employs a multi-agency regulatory framework with the Cyberspace Administration of China (CAC)

[179] CSL 2016, art 37.

[180] 促进和规范数据跨境流动规定 [Provisions on Promoting and Regulating Cross-border Data Flow] 2024 (Order No. 16 of the Cyberspace Administration of China).

[181] ibid art 6.

[182] PIPL 2021, art 60.

[183] ibid.

[184] ibid.

[185] Yan Luo and others, ‘China Reveals Plan to Establish a National Data Bureau’ (*Global Policy Watch*, 8 March 2023) <https://www.globalpolicywatch.com/2023/03/china-reveals-plan-to-establish-a-national-data-bureau/> accessed 23 April 2023.

coordinating among specialized agencies, while the other BRICS nations have adopted more centralized models similar to the EU's approach – Brazil with its National Data Protection Authority (ANPD), India with the Data Protection Authority of India (DPAI), Russia with Roskomnadzor (Federal Service for Supervision of Communications, Information Technology and Mass Media), and South Africa with its Information Regulator established under POPIA; this divergence highlights China's preference for distributed regulatory authority versus the single-authority approach adopted by other BRICS members, creating different enforcement dynamics where China gains flexibility but potentially sacrifices consistency, while other BRICS countries benefit from unified oversight but may lack China's regulatory specialization across different sectors and technological domains.

Essentially, the PIPL delineates the distribution of authority and responsibility within a complex regulatory framework, incorporating supervisory bodies endowed with extensive interpretive discretion and robust safeguards. Consequently, in relation to the PIPL, their status transcends that of a basic regulator, establishing those bodies as co-governance adjudicators. This role involves not only the traditional regulatory sphere but also spearheads initiatives in consciousness-raising, education, and guidance;[186] it is additionally entrusted with the evaluation of PI protection in mobile apps,[187] as well as the refinement of supplementary regulations and benchmarks,[188] the advancement of identity verification technologies,[189] and the facilitation of PI protection assessment and accreditation services for entities concerned.[190]

Chapter 7 of the PIPL addresses the legal liability of enterprises neglecting their responsibilities – three classifications: administrative, civil, and criminal, in conjunction with public interest litigation. Initially, the legislation substantially augments the penalty standard for administrative liability. Beyond the million-penalty standard established by the preceding Cybersecurity Law,[191] the statute introduces a novel penalty criterion for "grave circumstances," escalating the unit fine.[192] The new penalty threshold for "grave circumstances" has been elevated to no more than 50 million yuan or up to 5% of the prior year's turnover, potentially resulting in business suspension or even revocation of pertinent business permits or licenses.[193] Fines imposed on those directly accountable and other responsible parties have increased to at least 100,000 yuan and up to one million yuan.[194] Furthermore, the newly designated department responsible for PI protection at the provincial level or higher may elect to prohibit them from serving as directors, supervisors, senior managers, and PI protection officers within relevant enterprises for a specified duration.[195] In instances where PI handling does not yet constitute a severe violation defined as "grave circumstances" above-mentioned, mobile apps can still be instructed to suspend or terminate service.[196] Meanwhile, Article 69 of the PIPL stipulates the principle of presumed fault in cases of PI infringement, signifying that PI handlers must present exculpatory evidence in pertinent lawsuits.[197] Lastly, the PIPL reemphasizes the circumstances of PI-related crimes,[198] and links to the system of breach-of-credit files.[199]

[186] PIPL 2021, art 61(1).
[187] ibid art 61(3).
[188] ibid art 62(1).
[189] ibid art 62(3).
[190] ibid art 62(4).
[191] CSL 2016, art 64.
[192] PIPL 2021, art 66.
[193] ibid.
[194] ibid.
[195] ibid.
[196] ibid.
[197] ibid art 69.
[198] ibid art 71.
[199] ibid art 67.

One of the most innovative approaches in the PIPL is to lay out grounds for public interest litigation. Three types of organizations—people's procuratorates, consumer organizations as established by law, and entities recognized by the CAC—can initiate public interest litigation pertaining to personal information violations.[200] Another Notice by the Supreme People's Procuratorate clarifies that procuratorial organs at all levels should prioritize the following aspects when executing their duties in public interest litigation: strict protection of sensitive PI; specialized protection of vulnerable groups' PI; focused protection of PI managed in key sectors (such as education, healthcare, employment, social security, consumption), and large-scale personal information involving over one million people; and precise protection of personal information of specific subjects formed by temporal, spatial, and other connections.[201]

1.7. Conclusion

The evolution of China's personal data protection legislation has been a progressive gaming process, particularly with regard to how the Chinese institution intervenes and responds to the public's concerns. Concurrently, the intellectual participation of the academic community in structuring China's data protection system via, for instance, Expert Legislative Proposal Drafts, manifests prominently an endeavour forged through studying multiple jurisdictions, including the EU, from a comparative perspective, all while adapting them in consonance with domestic socio-political and economic institutional considerations.

China's data protection framework, thus, ought to be comprehended along two distinct trajectories. Initially, the primary impetus for its data protection legislation was geared towards mitigating personal information-associated illicit activities and fortifying the cybersecurity — both at a system and infrastructure echelon — of state informatisation. Although these original drivers embraced some rights protection provisions, it was not until the enactment of the PIPL that the fundamental rights/interests framework for data protection was carved out in a relatively complete, clear, and predictable manner. Secondly, it is imperative to recognize that China's data protection architecture extends beyond the Personal Information Protection Law (PIPL) and is more accurately depicted as a fusion of data governance mechanisms. This incorporates, at a minimum, data governance troika — Cybersecurity Law (CSL), Data Security Law (DSL), and PIPL, in addition to their respective derivatives. This interconnected mixture/fusion has also materialized in the recent Online Data Security Management Regulations.

In this context, the Chinese data protection framework should not be regarded as an absolute parallel to the prevailing international system; it cannot be directly "aligned, or right-sizing" demanding a substantial delineation of key legal transposition terms — such as the characterization of personal information or the definition of a handler/processor, which requires a considerable degree of differentiation.

After delineating and advocating for the principal dichotomies, this chapter discerns that, analogously to the previously mentioned comparative legal legislative procedure, the Personal Information Protection Law (PIPL) indeed advances in a significant leap, empowering data subjects with rights while simultaneously crystallizing the responsibilities of data handlers. Furthermore, it inaugurates a poly-sectorial and inter-departmental collaborative regulatory system, with the CAC presiding as the chief agency.

---

[200] ibid art 70.

[201] Jingjing Yan, '最高检下发通知 明确个人信息保护公益诉讼办案重点 [The Supreme People's Procuratorate Issued a Notice to Clarify the Key Points of Handling Public Interest Litigation Cases for Personal Information Protection]' (*Supreme People's Procuratorate*, 2021) <https://www.spp.gov.cn/spp/zdgz/202108/t20210822_527281.shtml> accessed 9 May 2023.

Notably, it deploys anonymization as a pivotal stipulation to stimulate the circulation of personal information. It has designed a comprehensive rights framework for data subjects, which is largely commensurate with the General Data Protection Regulation (GDPR), albeit with constraints imposed on the right to data portability, as well as the asymmetrical decisive power among different stakeholders due to the normative uncertainty between general principles and exceptional measures. In terms of obligations incumbent upon data handlers, the PIPL underscores overarching principles and orchestrates a specialized system of security responsibilities. This framework includes creating a gatekeeper role for large-scale platforms, along with mechanisms to deny automated decision-making. Finally, China's transnational PI transfer paradigm is strikingly multifaceted, endeavouring to harmonize security concerns with the free flow of PI through a stratified data classification mechanism. The practical implications and repercussions of the "data sovereignty" clauses within the PIPL,[202] which makes a complex element of cross-jurisdictional data protection adequacy, are yet to be fully discerned and understood.

2. APPENDIX A – PERSONAL INFORMATION PROTECTION LAW OF THE PEOPLE'S REPUBLIC OF CHINA

Adopted at the 30th Meeting of the Standing Committee of the Thirteenth National People's Congress on August 20, 2021.

CHAPTER I
GENERAL PROVISIONS

Article 1 This Law is enacted in accordance with the Constitution for the purposes of protecting the rights and interests on personal information, regulating personal information processing activities, and promoting reasonable use of personal information.

Article 2 The personal information of natural persons shall be protected by law. No organization or individual may infringe upon natural persons' rights and interests on their personal information.

Article 3 This Law shall apply to the processing of personal information of natural persons within the territory of the People's Republic of China.

This Law shall also apply to the processing outside the territory of the People's Republic of China of the personal information of natural persons within the territory of the People's Republic of China, under any of the following circumstances:

(1) for the purpose of providing products or services for natural persons inside the People's Republic of China;

(2) analyzing or evaluating the behaviors of natural persons within the territory of the People's Republic of China; and

(3) any other circumstance as provided by any law or administrative regulation.

[202] PIPL 2021, arts 42 and 43.

Article 4 "Personal information" refers to various information related to an identified or identifiable natural person recorded electronically or by other means, but does not include anonymized information.

Personal information processing includes personal information collection, storage, use, processing, transmission, provision, disclosure and deletion, among others.

Article 5 Personal information shall be processed according to law when it is necessary, with justified reason, and in good faith, and the processing may not involve misguidance, fraud, coercion, and the like.

Article 6 Personal information processing shall be based on explicit and reasonable purposes and directly related to those purposes, and shall exert the minimum impacts on the rights and interests of individuals.

The collection of personal information shall be limited to the minimum scope required by the purpose of processing, and personal information may not be collected excessively.

Article 7 The principles of openness and transparency shall be observed in the processing of personal information, the rules for processing personal information shall be disclosed, and the purposes, means, and scope of processing shall be explicitly indicated.

Article 8 The quality of personal information shall be guaranteed in personal information processing, to avoid adverse impacts on the rights and interests of individuals caused by inaccurate and incomplete personal information.

Article 9 Personal information processors shall be responsible for their personal information processing activities and take necessary measures to ensure the security of the personal information they process.

Article 10 No organization or individual shall illegally collect, use, process, or transmit the personal information of other persons, or illegally trade, provide or disclose the personal information of other persons, or engage in personal information processing activities that endanger national security or harm public interests.

Article 11 The state shall establish and improve the personal information protection system to prevent and punish infringements upon the rights and interests on personal information, strengthen publicity and education on personal information protection, and promote a favorable environment for the government, enterprises, relevant industry organizations, and the public to jointly participate in personal information protection.

Article 12 The state will actively engage in the development of international rules on personal information protection, promote the international exchanges and cooperation in personal information protection, and encourage the mutual recognition of personal information protection rules and standards, among others, with other countries, regions, and international organizations.

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

CHAPTER II
PERSONAL INFORMATION PROCESSING RULES

Section 1
General Rules

Article 13 A personal information processor can process personal information of an individual only if one of the following circumstances exists:

(1) the individual's consent has been obtained;

(2) the processing is necessary for the conclusion or performance of a contract in which the individual is a party, or necessary for human resources management in accordance with the labor rules and regulations established in accordance with the law and the collective contracts signed in accordance with the law;

(3) the processing is necessary for the performance of statutory duties or obligations;

(4) the processing is necessary for the response to public health emergencies, or for the protection of life, health, and property safety of natural persons in emergencies;

(5) the personal information is reasonably processed for news reporting, media supervision, and other activities conducted in the public interest;

(6) the personal information disclosed by the individual himself or other legally disclosed personal information of the individual is reasonably processed in accordance with this Law; and

(7) other circumstances as provided by laws or administrative regulations.

Individual consent shall be obtained for processing personal information if any other relevant provisions of this Law so provide, except under the circumstances specified in Subparagraphs (2) to (7) of the preceding paragraph.

Article 14 Where personal information processing is based on individual consent, the individual consent shall be voluntary, explicit, and fully informed. Where any other law or administrative regulation provides that an individual's separate consent or written consent must be obtained for processing personal information, such provisions shall apply.

In the case of any change of the purposes or means of personal information processing, or the category of processed personal information, a new consent shall be obtained from the individual.

Article 15 Where personal information processing is based on individual consent, an individual shall have the right to withdraw his consent. Personal information processors shall provide convenient ways for individuals to withdraw their consents.

The withdrawal of consent shall not affect the validity of the processing activities conducted based on consent before it is withdrawn.

Article 16 A personal information processor shall not refuse to provide products or services for an individual on the grounds that the individual withholds his consent for the processing of his personal information or has withdrawn his consent for the processing of personal information, except where the processing of personal information is necessary for the provision of products or services.

Article 17 A personal information processor shall, before processing personal information, truthfully, accurately and fully inform an individual of the following matters in a easy-to-notice manner and in clear and easy-to-understand language:

(1) the name and contact information of the personal information processor;

(2) the purposes and means of personal information processing, and the categories and storage periods of the personal information to be processed;

(3) the methods and procedures for the individual to exercise his rights as provided in this Law; and

(4) other matters that the individual should be notified of as provided by laws and administrative regulations.

Where any matter as set forth in the preceding paragraph changes, the individual shall be informed of the change.

Where the personal information processor informs an individual of the matters specified in the first paragraph by formulating personal information processing rules, the processing rules shall be made public and be easy to consult and save.

Article 18 When processing personal information, personal information processors are permitted not to inform individuals of the matters specified in the first paragraph of the preceding article where laws or administrative regulations require confidentiality or provide no requirement for such notification.

Where it is impossible to notify individuals in a timely manner in a bid to protect natural persons' life, health and property safety in case of emergency, the personal information processors shall notify them without delay after the emergency is removed.

Article 19 Except as otherwise provided by laws and administrative regulations, the storage period of personal information shall be the minimum time necessary to achieve the purpose of processing.

Article 20 Where two or more personal information processors jointly determine the purposes and means of processing certain personal information, they shall reach an agreement on their respective rights and obligations in processing the personal information. However, this agreement shall not affect an individual's request to any one of them to exercise his rights as provided in this Law.

Where, in jointly processing certain personal information, a processor infringes the rights and interests on personal information and causes damages, other personal information processors shall bear joint and several liability in accordance with law.

Article 21 A personal information processor entrusting the processing of certain personal information to a party shall reach an agreement with the entrusted party on the purposes, period and means of processing, the categories of personal information to be processed and the protection measures, as well as the rights and obligations of both parties, among others, and shall supervise the personal information processing activities of the entrusted party.

The entrusted party shall process personal information in accordance with the agreement and may not process personal information beyond the purposes, means and other conditions as agreed upon. Where the entrustment contract has not taken effect, or is invalid, or is revoked or terminated, the entrusted party shall return the personal information in question to the personal information processor or delete it and shall not retain the personal information.

Without the consent of the personal information processor, the entrusted party may not sub-contract the processing of personal information to any other party.

Article 22 Where a personal information processor needs to transfer personal information due to a merger, division, dissolution, or bankruptcy or for other reasons, the processor shall inform the individuals of the name and contact information of the recipient of the transferred personal information. The recipient shall continue to perform the obligations of the said personal information processor. Any change of the original purposes or means of processing by the recipient shall be subject to individual consent in accordance with this Law.

Article 23 To provide personal information for any other processor, a personal information processor shall inform the individuals of the recipient's name and contact information, the purposes and means of processing and the categories of personal information to be processed, and shall obtain the individuals' separate consent. The recipient shall process personal information within the scope of the purposes, means, and categories of personal information mentioned above. Any change of the purposes or means of processing by the recipient shall be subject to individual consent in accordance with this Law.

Article 24 Personal information processors using personal information for automated decision making shall ensure the transparency of the decision making and the fairness and impartiality of the results, and may not apply unreasonable differential treatment to individuals in terms of transaction prices and other transaction conditions.

Information push and commercial marketing to individuals based on automated decision making shall be simultaneously accompanied by options not specific to their personal characteristics or with convenient means for individuals to refuse.

Where a decision that may have a significant impact on an individual's rights and interests is made through automated decision making, the individual shall have the right to request clarification from the personal information processor and the right to refuse the processor for making the decision only through automated decision making.

Article 25 Personal information processors shall not disclose the personal information they process, except where separate consents has been obtained from the individuals.

Article 26 Image collection and personal identification equipment in public places shall be installed only when it is necessary for the purpose of maintaining public security, and shall be installed in compliance with the relevant provisions of the state and with prominent reminders. The personal images and identification information collected can only be used for the purpose of maintaining public security and, unless the individuals' separate consents are obtained, shall not be used for any other purpose.

Article 27 A personal information processor may reasonably process the personal information disclosed by an individual himself or other legally disclosed personal information, except where the individual expressly refuses. Where the processing of disclosed personal information may have a significant impact on an individual's rights and interests, the personal information processors shall first obtain the individual's consent in accordance with the provisions of this Law.

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

Section 2
Rules on Processing Sensitive Personal Information

Article 28 "Sensitive personal information" is personal information that once leaked or illegally used, may easily lead to the infringement of the personal dignity of a natural person or may endanger his personal safety or property, including information such as biometrics, religious belief, specific identity, medical health status, financial accounts, and the person's whereabouts, as well as the personal information of a minor under the age of 14 years.

Personal information processors can process sensitive personal information only when there is a specific purpose and when it is of necessity, under the circumstance where strict protective measures are taken.

Article 29 For the processing of sensitive personal information, individual's separate consent shall be obtained. Where other laws or administrative regulations provide that written consent shall be obtained for the processing of sensitive personal information, such provisions shall prevail.

Article 30 In addition to the matters specified in the first paragraph of Article 17 of this Law, a processor processing sensitive personal information shall notify an individual of the necessity of processing his sensitive personal information and the impact it has on his rights and interests, except where such notification is not required in accordance with the provisions of this Law.

Article 31 To process the personal information of minors under the age of 14, personal information processors shall obtain the consent of the parents or other guardians of the minors.

Personal information processors processing the personal information of minors under the age of 14 shall develop special rules for processing such personal information.

Article 32 Where other laws or administrative regulations provide that relevant administrative permit shall be obtained for the processing of sensitive personal information or impose other restrictions, such provisions shall prevail.

Section 3
Special Provisions on the Processing of Personal Information by State Organs

Article 33 This Law shall apply to the processing of personal information by state organs; where there are special provisions in this Section, the provisions of this Section shall prevail.

Article 34 When state organs process personal information in order to perform their statutory duties, they shall act in accordance with the authority and procedures prescribed by laws and administrative regulations, and shall not exceed the scope and limits necessary to perform their statutory duties.

Article 35 When state organs process personal information in order to perform their statutory duties, they shall fulfill the obligation of notification in accordance with the provisions of this Law, except under the circumstances specified in the first paragraph of Article 18 of this Law or where notification will hinder the state organs from performing their statutory duties.

Article 36 Personal information processed by state organs shall be stored within the territory of the People's Republic of China. A security assessment shall be conducted where it is truly necessary to provide such information for any party outside of the territory of the People's Republic of China. In the security assessment the relevant departments shall provide support and assistance if so requested.

Article 37 Where organizations authorized by laws or regulations with the function of administering public affairs process personal information in order to fulfill their statutory duties, the provisions herein on the processing of personal information by state organs shall apply.

CHAPTER III
RULES ON PROVISION OF PERSONAL INFORMATION ACROSS BORDER

Article 38 A personal information processor that truly needs to provide personal information for a party outside the territory of the People's Republic of China for business sake or other reasons, shall meet one of the following requirements:

(1) passing the security assessment organized by the national cyberspace department in accordance with Article 40 of this Law;

(2) obtaining personal information protection certification from the relevant specialized institution according to the provisions issued by the national cyberspace department;

(3) concluding a contract stipulating both parties' rights and obligations with the overseas recipient in accordance with the standard contract formulated by the national cyberspace department; and

(4) meeting other conditions set forth by laws and administrative regulations and by the national cyberspace department.

Where an international treaty or agreement that the People's Republic of China has concluded or acceded to stipulates conditions for providing personal information for a party outside the territory of the People's Republic of China, such stipulations may be followed.

The personal information processor shall take necessary measures to ensure that the personal information processing activities of the overseas recipient meet the personal information protection standards set forth in this Law.

Article 39 Where a personal information processor provides personal information for any party outside the territory of the People's Republic of China, the processor shall inform the individuals of the overseas recipient's name and contact information, the purposes and means of processing, the categories of personal information to be processed, as well as the methods and procedures for the individuals to exercise their rights as provided in this Law over the overseas recipient, etc., and shall obtain individual's separate consent.

Article 40 Critical information infrastructure operators and the personal information processors that process personal information up to the amount prescribed by the national cyberspace department shall store domestically the personal information collected and generated within the territory of the People's Republic of China. Where it is truly necessary to provide the information for a party outside the territory of the People's Republic of China, the matter shall be subjected to security assessment organized by the national cyberspace department. Where laws, administrative regulations, or the provisions issued by the national cyberspace department provide that security assessment is not necessary, such provisions shall prevail.

Article 41 The competent authorities of the People's Republic of China shall handle foreign judicial or law enforcement authorities' requests for personal information stored within China in accordance with relevant laws and the international treaties and agreements concluded or acceded to by the People's Republic of China, or under the principle of equality and reciprocity. Without the approval of the

competent authorities of the People's Republic of China, no organization or individual shall provide data stored in the territory of the People's Republic of China for any foreign judicial or law enforcement authority.

Article 42 Where overseas organizations or individuals engage in personal information processing activities, which infringe upon the rights and interests of citizens of the People's Republic of China on personal information or endanger the national security or public interests of the People's Republic of China, the national cyberspace department may include them in a list of restricted or prohibited recipients of personal information, publicize the list, and take measures such as restricting or prohibiting the provision of personal information for such organizations and individuals.

Article 43 Where any country or region adopts any prohibitive, restrictive or other similar discriminatory measures against the People's Republic of China in terms of personal information protection, the People's Republic of China may take countermeasures against the aforesaid country or region based on actual situations.

CHAPTER IV
INDIVIDUALS' RIGHTS IN PERSONAL INFORMATION PROCESSING ACTIVITIES

Article 44 Individuals shall have the right to be informed, the right to make decisions on the processing of their personal information, and the right to restrict or refuse the processing of their personal information by others, except as otherwise provided by laws or administrative regulations.

Article 45 Individuals shall have the right to consult and duplicate their personal information from personal information processors, except under circumstances as set out in the first paragraph of Article 18 and Article 35 of this Law.

Where an individual requests the consultation or duplication of his personal information, the requested personal information processor shall provide such information in a timely manner.

Where an individual requests the transfer of his personal information to a designated personal information processor, which meets the requirements of national cyberspace department for transferring personal information , the requested personal information processor shall provide means for the transfer.

Article 46 Where an individual discovers that his personal information is incorrect or incomplete, he shall have the right to request the personal information processors to rectify or supplement relevant information.

Where an individual requests the rectification or supplementation of his personal information, the personal information processors shall verify the information in question, and make rectification or supplementation in a timely manner.

Article 47 In any of the following circumstances, a personal information processor shall take the initiative to erase personal information, and an individual has the right to request the deletion of his personal information if the personal information processor fails to erase the information:

(1) the purposes of processing have been achieved or cannot be achieved, or such information is no longer necessary for achieving the purposes of processing;

(2) the personal information processor ceases to provide products or services, or the storage period has expired;

(3) the individual withdraws his consent;

(4) the personal information processor processes personal information in violation of laws, administrative regulations, or agreements; or

(5) other circumstances as provided by laws and administrative regulations.

Where the storage period provided by any law or administrative regulation has not expired, or it is difficult to erase personal information technically, the personal information processor shall cease the processing of personal information other than storing and taking necessary security protection measures for such information.

Article 48 An individuals has the right to request a personal information processor to interpret the personal information processing rules developed by the latter.

Article 49 The close relatives of a deceased natural person may, for their own legal and legitimate interests, exercise the rights to handle the personal information of the deceased, such as consultation, duplication, rectification, and deletion, as provided in this Chapter, except as otherwise arranged by the deceased before death.

Article 50 A personal information processor shall establish the mechanism for receiving and handling individuals' requests for exercising their rights. Where an individual's request is rejected, the reasons therefor shall be given.

Where an individual's request to exercise his rights is rejected by a personal information processor, the individual may file a lawsuit with the people's court in accordance with the law.

CHAPTER V
OBLIGATIONS OF PERSONAL INFORMATION PROCESSORS

Article 51 Personal information processors shall take the following measures to ensure that their personal information processing activities are in compliance with laws and administrative regulations based on the purpose and means of processing, the categories of personal information to be processed, the impact on personal rights and interests, and the potential security risks, among others, and shall prevent unauthorized access to, as well as breach, tampering or loss of any personal information:

(1) formulating internal management system and operational procedures;

(2) implementing classified management of personal information;

(3) adopting corresponding security technical measures such as encryption and de-identification;

(4) reasonably determining the operational authority of personal information processing, and regularly conducting safety education and training for practitioners;

(5) formulating contingent plans for personal information security emergencies and organizing the implementation of such plans; and

(6) other measures as provided by laws and administrative regulations.

Article 52 A personal information processor that processes personal information up to the amount prescribed by the national cyberspace department shall designate a person in charge of personal information protection, who shall supervise the personal information processing activities of the processor as well as the protective measures taken thereby, among others.

The personal information processor shall disclose the contact information of the person in charge of personal information protection, and submit the said person's name, contact information, and other information to the departments with personal information protection duties.

Article 53 Personal information processors outside the territory of the People's Republic of China as specified in the second paragraph of Article 3 of this Law shall set up specialized agencies or designate representatives within the territory of the People's Republic of China to be responsible for handling personal information protection related matters, and shall submit the names, contact information, and other information of the agencies and representatives to the departments with personal information protection duties.

Article 54 Personal information processors shall regularly conduct compliance audits of their personal information processing activities with laws and administrative regulations.

Article 55 In any of the following circumstances, a personal information processor shall assess in advance the impact on personal information protection and keep a record of the course of the processing:

(1) processing sensitive personal information;

(2) using personal information to conduct automated decision making;

(3) entrusting personal information processing to another party, providing personal information for another party, or publicizing personal information;

(4) providing personal information for any party outside the territory of the People's Republic of China; or

(5) conducting other personal information processing activities which may have significant impacts on individuals.

Article 56 The assessment of impact on personal information protection shall include the following contents:

(1) whether the purposes and means of personal information processing, are legitimate, justified and necessary;

(2) the impact on individuals' rights and interests, and security risks; and

(3) whether the protection measures taken are legitimate, effective, and compatible with the degree of risks.

The report of the impact assessment on personal information protection and the processing record shall be retained for at least three years.

Article 57 Where the breach, tampering, or loss of personal information occurs or may occur, a personal information processor shall immediately take remedial measures and notify the departments with personal information protection duties and the relevant individuals. The notice shall include the following items:

(1) the categories of personal information that has been or may be breached, tampered with or lost, and the reasons and possible harm of the breach, tampering and loss;

(2) the remedial measures adopted by the personal information processor and the measures the individuals may take to mitigate the harm; and

(3) the contact information of the personal information processor.

Where the measures taken by the personal information processor can effectively avoid the harm caused by breach, tampering, or loss of personal information, the personal information processor is not required to notify individuals; where the departments with personal information protection duties consider that harm may be caused, they have the authority to request the personal information processor to notify individuals.

Article 58 A personal information processor that provides important internet platform services involving a huge number of users and complicated business types shall perform the following obligations:

(1) establishing and improving the personal information protection compliance system in accordance with the provisions of the state and establishing an independent organization mainly composed of external members to supervise the protection of personal information;

(2) following the principles of openness, fairness, and justice, formulating platform rules, and clarifying the norms and obligations that product or service providers within the platform should meet when processing personal information;

(3) stopping providing services for product or service providers within the platforms that process personal information in serious violation of laws and administrative regulations; and

(4) regularly publishing social responsibility reports on personal information protection for public supervision.

Article 59 The party entrusted with the processing of personal information shall, in accordance with this Law and relevant laws and administrative regulations, take the necessary measures to ensure the security of the personal information entrusted for processing, and assist the entrusting personal information processor in fulfilling the obligations provided by this Law.

CHAPTER VI
DEPARTMENTS WITH PERSONAL INFORMATION PROTECTION DUTIES

Article 60 The national cyberspace department shall be responsible for the overall planning and coordination of personal information protection and related supervision and administration. The relevant departments of the State Council shall, in accordance with this Law and other relevant laws and administrative regulations, be responsible for personal information protection and related supervision and administration within the scope of their respective duties.

The duties of personal information protection and related supervision and administration of the relevant departments of the local people's governments at or above the county level shall be determined in accordance with the relevant provisions of the state.

The departments provided in the preceding two paragraphs are collectively referred to as the departments with personal information protection duties.

Article 61 Departments with personal information protection duties shall perform the following personal information protection duties:

(1) conducting publicity and education on personal information protection, and guiding and supervising personal information processors in their protection of personal information;

(2) receiving and handling complaints and reports related to personal information protection;

(3) organizing evaluations on applications, etc. in terms of personal information protection and publish the results of such evaluations;

(4) investigating and handling illegal personal information processing activities; and

(5) other duties as provided by laws and administrative regulations.

Article 62 The national cyberspace department shall coordinate relevant departments to promote personal information protection through the following efforts in accordance with this Law:

(1) formulating specific rules and standards for personal information protection;

(2) developing special personal information protection rules and standards for small personal information processors, the processing of sensitive personal information, and new technologies and applications such as face recognition and artificial intelligence;

(3) supporting the research and development, and promoting the application of secure and convenient electronic identity authentication technology, and advancing the public services for network identity authentication;

(4) promoting the development of a personal information protection service system with the participation of various social sectors, and supporting relevant institutions in providing personal information protection assessment and certification services; and

(5) improving the complaint and reporting mechanism related to personal information protection .

Article 63 A department with personal information protection duties when fulfilling related duties may take the following measures:

(1) questioning relevant parties, and investigating circumstances related to personal information processing activities;

(2) consulting and duplicating the parties' contracts, records, account books and other relevant materials related to personal information processing activities;

(3) conducting on-site inspections, and investigating suspected illegal personal information processing activities; and

(4) inspecting equipment and articles related to personal information processing activities; and sealing up or seizing equipment and articles related to illegal personal information processing activities as proved by evidence after submitting written reports to and obtaining approval from the principal person in charge of the departments with personal information protection duties.

When departments with personal information protection duties carry out their duties in accordance with the law, the parties concerned shall cooperate and provide assistance, and shall not reject or obstruct them.

Non-final version of Belli; Luca. Understanding the BRICS countries, their digital cooperation, and their emerging data protection architectures; in Luca Belli & Walter B. Gaspar (Eds) Personal Data Architectures in the BRICS Countries. Oxford University Press. (2025)

Article 64 Where a department with personal information protection duties finds, when performing its duties, relatively high risks in personal information processing activities or the occurrence of personal information security incidents, the department may hold an interview with the legal representative or the principal person in charge of the personal information processor according to the provided authority and procedures, or request the processor to entrust a professional institution to conduct compliance audits of the personal information processing activities. The personal information processor shall adopt measures to make rectification and eliminate potential risks as required.

Where a department with personal information protection duties, in performing its duties, finds an illegal personal information processing activity that may involve a crime, the department shall transfer the case to the public security organ in a timely manner in accordance with the law.

Article 65 Any organization or individual has the right to complain and report to a department with personal information protection duties about illegal personal information processing. The department that receives such a complaint or report shall handle it in a timely manner in accordance with the law, and notify the complainant or informant of the results.

Departments with personal information protection duties shall publish their contact information for receiving complaints and reports.

CHAPTER VII
LEGAL LIABILITY

Article 66 Where personal information is processed in violation of the provisions of this Law or without fulfilling the personal information protection obligations provided in this Law, the departments with personal information protection duties shall order the violator to make corrections, give a warning, confiscate the illegal gains, and order the suspension or termination of provision of services by the applications that illegally process personal information; where the violator refuses to make corrections, a fine of not more than RMB one million yuan shall be imposed thereupon; and the directly liable persons in charge and other directly liable persons shall each be fined not less than RMB 10,000 yuan nor more than RMB 100,000 yuan.

In case of an illegal act as prescribed in the preceding paragraph and the circumstances are serious, the departments with personal information protection duties at or above the provincial level shall order the violator to make corrections, confiscate the illegal gains, impose a fine of not more than RMB 50 million yuan or not more than five percent of the previous year's turnover; may also order the suspension of relevant businesses, or order the suspension of all the business operations for an overhaul, and notify the competent authorities to revoke relevant business permits or license; shall impose a fine of not less than RMB 100,000 yuan but not more than RMB 1 million yuan upon each of the directly liable persons in charge and other directly liable persons, and may decide to prohibit the abovementioned persons from serving as directors, supervisors, senior managers, or the persons in charge of relevant companies within a specific period of time.

Article 67 Any violation of the provisions of this Law shall be entered in the relevant credit record and be published in accordance with the provisions of the relevant laws and administrative regulations.

Article 68 Where any state organ fails to fulfill the personal information protection obligations as provided in this Law, the organ at the higher level or the departments with personal information

protection duties shall order it to make corrections, and discipline the directly liable person in charge and other directly liable persons in accordance with the law.

Where a staff member of a department with personal information protection duties neglects duties, abuses power, or practices favoritism, which does not constitute a crime, the staff member shall be subject to sanction in accordance with the law.

Article 69 Where a personal information processor infringes the rights or interests on personal information due to any personal information processing activity and cannot prove that the processor is not at fault, the processor shall assume the liability for damages and other tort liability.

The liability for damages prescribed in the preceding paragraph shall be determined based on the losses of individuals incurred thereby and the benefits acquired by the infringing personal information processor; and where it is difficult to determine the aforementioned losses or the benefits, the amount of damages shall be determined based on the actual circumstances.

Article 70 Where a personal information processor processes personal information in violation of the provisions of this Law and infringes the rights and interests of many individuals, the people's procuratorate, the consumer organizations specified by law, and the organization designated by the national cyberspace department may file a lawsuit with the people's court in accordance with the law.

Article 71 Any violation of this Law which constitutes a violation of public security administration shall be subject to public security administration penalty in accordance with the law. If the violation constitutes a crime, the violator shall be held criminally liable in accordance with the law.

CHAPTER VIII
SUPPLEMENTARY PROVISIONS

Article 72 This Law is not applicable where a natural person processes personal information for personal or household affairs.

Where other laws provide personal information processing in statistical or archives management activities organized and conducted by the people's governments at all levels and their relevant departments, the provisions of such laws shall prevail.

Article 73 For purposes of this Law, the following terms shall have the following meanings:

(1) "A personal information processor" refers to an organization or individual that autonomously determines the purposes and means of personal information processing.

(2) "automated decision making" refers to the activities of automatically analyzing and evaluating personal behaviors, hobbies, or economic, health, and credit status, among others, through computer programs, and making decisions.

(3) "de-identification" refers to processing personal information to make it impossible to identify specific natural persons in the absence of the support of additional information.

(4) "anonymization" refers to the process of processing personal information to make it impossible to identify specific natural persons and impossible to restore.

Article 74 This Law shall come into force as of November 1st , 2021.