Demystifying data law in China: a unified regime of tomorrow

Peiru Cai* and Li Chen**

Key Points

- Over the past 10 years, China's data law regime has gradually come into shape to fulfil the dual purposes of data protection and utilization. Chinese data law is undergirded by three pillars, namely, 'Cybersecurity Law', 'Data Security Law', and 'Personal Information Protection Law'.
- These laws employ a horizontal data classification schema and a vertical grading mechanism. The law mainly uses the classification method to analyse the narrowly defined data and the hierarchical vertical grading mechanism to manage personal information.
- The overall purpose of Chinese data law is to maintain and advance the physical security and juridical security of data. However, the interests underlying each legislation are quite different; the specific legal goals and normative values of each legislation also reveal structural differences.
- Although the internal structure of each data legislation is clear, there is controversy over whether, in practice, each legislation should be applied sequentially in each given situation instead of applying the different legislations simultaneously.
- Overall, while the basic framework of China's data law has been established, it is worth observing that as it is still a relatively independent new legal field in China, improvements can be made to streamline its concepts, guiding philosophy, policy goals, and application.

Introduction

The development of big data, cloud computing, and artificial intelligence technology drives not only the transformation of the Chinese economy but also a new way of life that is seamlessly integrated with technology. The troves of data generated by users and processed by various business operators fuel the remarkable growth of businesses. Data are therefore widely regarded as a fundamental strategic resource and a crucial factor of production in China. Data can be used to identify individuals, revealing their political views, habits, hobbies, consumption preferences, physical movements, and other traits. Data might also be regarded as a commercial secret of Internet products providers due to the competitive advantage it might offer. Data are also critical to upholding public and national interests.[1]

The newly enacted government regulations aim to aggressively regulate China's mobile applications, e-commerce, and 'smart' products. The Chinese government's much-touted '*The Outline of the Fourteenth Five-Year Plan for National Economic and Social Development of the People's Republic of China and Vision 2035*' proposes to 'strengthen the protection of data involving national interests, commercial secrets, and personal privacy, and accelerate the promotion of fundamental legislation in the fields of data security and personal information protection, and strengthen the security protection of data resources throughout their life cycle'. Recognizing the diverse interests underlying data, this document reflects plans to create an independent and distinctive field of 'data law' in China's legal landscape, and strike a balance between national interests, economic development, technological innovation, and personal privacy.

*Peiru Cai, Law School, Fudan University, Shanghai, China
**Li Chen, Law School, Fudan University, Shanghai, China
Email: lichen@wustl.edu.

[1] Regarding the importance of data, the following two important documents are crucial to gain insights: State Council of China, 'Notice of the State Council on Issuing the Action Outline for Promoting the Development of Big Data', no 50 (2015) of the State Council. 'Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, A European Strategy for Data', COM/2020/66 final.

China's data regulation began with the *Decision on Strengthening Network Information Protection promulgated by the Standing Committee of the National People's Congress* ('NPCSC') in 2012. The Cybersecurity Law ('CSL') was thereafter introduced in 2015 before the Data Security Law ('DSL') and Personal Information Protection Law ('PIPL') were promulgated in quick succession in 2021. At the time of this article, administrative regulations, departmental rules, normative documents, and national standards are being rapidly published to provide guidance in implementing those laws.[2] With the concomitant development of the rule of law, the basic framework of China's data legislation has now come to shape with the PIPL's enactment. The legislative agenda in the following years will now shift towards developing rules to supplement the existing framework in accordance with the articulated logic of China's data law.[3] The *Administrative Regulation on Network Data Security (Draft for Comments)* ('NDS Regulation'), for example, published by the Cyberspace Administration of China ('CAC') in November 2021, contains detailed guidelines for implementing the CSL, DSL, and PIPL.

A brief survey of the existing academic literature reveals a piecemeal approach that either focuses on a single piece of legislation or a specific regulatory regime.[4] Strikingly, there is no comprehensive study that examines the entire data regulatory regime.[5] For example, around the time when the Chinese Civil Code and PIPL were enacted, a few notable Chinese scholars have focused on whether there is an absolute right to personal information independent of the right to privacy.[6] Event-driven research is also prevalent in China. Several significant legal developments in foreign jurisdictions have attracted the attention of Chinese scholars. Such developments included the European Court of Justice's invalidation of the Safe Harbour[7] and Privacy Shield[8] agreements on cross-border transfer of personal data between Europe and the USA. Another example would be the US' attempt to gain access to banking data stored in China which alarmed Chinese regulators.[9] These events have ignited a plethora of research on data export issues in China, paving the way for the advent of a crucial area of data law in recent years.[10] Significantly, it is our observation that some high-impact homegrown research findings have persuaded Chinese lawmakers to adopt recommendations that were implemented through the enactment of the DSL and PIPL.[11]

While previous research has served to aid the law in its progress, stability, and operability, it is now crucial to expound on the basic framework of data law, which has been concretized. Several issues will be explored,

[2] From January to December 2021, Chinese government at the central and local levels had released as many as 18 laws, regulations, rules, and other normative documents related to the regulation of personal information and data protection.

[3] Fang Xinping (from the CAC): the development of supporting laws and regulations for the DSL and PIPL is underway (21 December 2021) <https://www.sohu.com/a/510514206_161795?g=0> accessed 28 December 2021.

[4] Of note, some studies have focused on what constitutes Cyber Law (or 'Internet Law'), treating it as a separate domain of law. However, Cyber Law is a broader concept that encompasses the regulation of network infrastructure and network content and the study of cyber torts and cybercrimes. See Zhou Hanhua, 'On Internet Law' (2015) 3 China Legal Science 20 (in Chinese). Lai Xiaopeng, 'On the Independent Legal Branch of Cyber Law' (2019) 11 Law Science Magazine 65 (in Chinese). Zhou Qingshan, 'On the Overall Construction of Cyberlaw System' (2014) 8 Hebei Law Science 9 (in Chinese). This article will not discuss whether there is a hierarchy of Cyber Law and Data Law as this is beyond the scope of the article.

[5] Some studies have attempted to unify the legal notion of rights in data law from the dichotomy of public data and private data. Some studies attempt to distinguish between data and information to map out the taxonomy in data law. This article takes the legal text of data law as the primary basis for investigation and discussion. It focuses on how data law, as a new legal field, came into being. See Xu Ke, 'Data Rights: Regulatory Integration and Differentiation of Regulations' (2021) 4 Tribune of Political Science and Law 92 (in Chinese). Mei Xiaying, 'The Legal Significance of the Distinction between Information and Data' (2020) 6 Journal of Comparative Law 155 (in Chinese).

[6] Wang Liming, 'Legal Protection of Personal Information: Centered on the Line Between Personal Information and Privacy' (2013) 4 Modern Law Science 64 (in Chinese). Wang Liming, 'Harmony and Difference: Delineation and Application of Rules on Right to Privacy and Personal Information' (2021) 2 Law Review 17 (in Chinese). Cheng Xiao, 'Protection of Personal Information in the Perspective of Civil Code Codification' (2019) 4 China Legal Science 34 (in Chinese). Wang Cheng, 'Selection of a Model for Civil Law Protection of Personal Information' (2019) 6 Social Sciences in China 140 (in Chinese).

[7] *Maximillian Schrems v Data Protection Commissioner*, Judgment of the Court (Grand Chamber) of 6 October 2015, Case C-362/14.

[8] *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*, Judgment of the Court (Grand Chamber) of 16 July 2020, Case C-311/18.

[9] Kadhim Shubber, 'Court Bolsters US Power to Grab Chinese Bank Records' *Financial Times* (London, 7 August 2019) <https://www.ft.com/content/d60497f6-b875-11e9-96bd-8e884d3ea203> accessed 28 December 2021.

[10] See Zhang Jinping, 'International Rules for Cross-border Data Transfer and China's Regulatory Reactions–Comments on the Restriction Rules of Cross-border Data Transfer in China's "Cyber Security Law"' (2016) 2 Politics and Law 136 (in Chinese). Hong Yanqing, '"Lawfare" Maelstrom in the Enforcement of Cross-border Data Retrieval: Taking the United States, the European Union and China as Examples' (2021) 1 Global Law Review (in Chinese); Wu Xuan, 'Construction of Personal Information Cross-border Rules from the Perspective of Data Sovereignty' (2021) 3 Tsinghua University Law Journal 74 (in Chinese); Ye Kairu, '"Long-arm Jurisdiction" in the Rules of Data Cross-border Flow: An Originalism Probe of EU GDPR' (2021) 1 Law Review 106 (in Chinese).

[11] A typical example is that in the formulation of the PIPL, the first and second review drafts did not specify the enabling law of the said legislation. Later, some scholars proposed that the protection of the fundamental rights of China's Constitution should be the legislative basis. In the third review draft, the drafters added the expression 'in accordance with the Constitution' in art 1 of the said legislation. See Wang Xixin, 'The State's Obligation to Protect Personal Information and its Elaboration' (2021) 1 China Legal Science 145 (in Chinese); Wang Xixin and Peng Chen: 'Constitutional Basis of Personal Information Protection Legal Regime' (2021) 3 Tsinghua University Law Journal 6 (in Chinese).

and questions include: Is there a clear thread that joins the three core pillars (the CSL, DSL, and PIPL) and a considerable number of normative documents into a coherent and well-structured regulatory framework? What are the common goals and values underlying Chinese data law? How do they co-exist and interact in their application? What reflections and improvements can we draw from the above? This article explores and answers these crucial questions from the premise that the data regulatory regime in China is a unified body of law.

The constitution of data law

Basic elements of data law

Chinese data law has extended its scope: from regulating the management of the basic network facilities and equipment, it now regulates the management of the data and information generated, processed, and stored in those networks. The legislative purpose of the CSL, which was first tabled in 2015, was to establish China's sovereignty in cyberspace. This approach recognized that national security and national interests transcend geographical boundaries and are also engaged in cyberspace.[12] According to the NPCSC's *Notes on the (Draft) Cybersecurity Law of the People's Republic of China*, the law contains six sections: (i) securing network products and services; (ii) network operations; (iii) network data; (iv) network information; (v) monitoring, early warning, and emergency response; and (vi) the network security supervision and management system.[13] Chinese scholar Zhou Hanhua, who participated in the drafting of the CSL, opined of the relationship between the six sections: 'It is the fundamental law of national information legislation, which is based on the operation security of the network, proposing "Operation Security of Critical Information Infrastructure", and then taking into account the protection of personal information, network information content management, and how to promote and facilitate the development of the network security industry.'[14] Evidently, the main purpose of the CSL concerns the physical security of networks; its focus lies in ensuring the security of facilities, equipment, and network systems for data storage and operation—only part of the CSL concerns data regulation.[15] This is of fundamental and guiding significance to the subsequent legislative developments that sought to regulate the different aspects of cyber law.

With the CSL as the starting point, the DSL and PIPL were enacted with the aim of providing protection for data and information, including those generated, processed, and stored on network devices. In other words, the DSL and PIPL policed content stored within networks. On this account, it is important to clarify the relationship between 'data' (*shuju*), 'information' (*xinxi*), and 'personal information' (*geren xinxi*).[16]

The similarities and differences between 'data' and 'information' were hot topics in early academic discourse on Chinese internet governance and data law.[17] One prominent study distinguished between three modes of data and information usage in the Chinese regulatory framework, judicial decisions, and academic research: information meshed with data, information embedded data, and data embedded information.[18] However, the legislature has chosen to distinguish the concept of 'data' from the concept of 'information'. Article 3(1) of DSL provides that data 'refers to any recording of information by electronic or other means'.

[12] National People's Congress, 'China Intends to Enact a Network Security Law' <http://www.npc.gov.cn/zgrdw/npc/xinwen/lfgz/2015-06/25/content_1939381.htm> accessed 28 December 2021.

[13] National People's Congress, 'On the "Cybersecurity Law of the People's Republic of China (Draft)"' <http://www.npc.gov.cn/zgrdw/npc/lfzt/rlyw/2015-07/08/content_1941286.htm> accessed 28 December 2021.

[14] National People's Congress, 'Interpretation of the Cybersecurity Law: Launching the Legislation on Information Networks in China' <http://www.npc.gov.cn/zgrdw/npc/lfzt/rlyw/2016-11/10/content_2002309.htm> accessed 28 December 2021.

[15] For example, art 21 of CSL states that 'Network operators shall, according to the requirements of the rules for graded protection of cybersecurity, fulfill the following security protection obligations, so as to ensure that the network is free from interference, damage or unauthorized access, and prevent network data from being divulged, stolen or falsified.'

[16] Apart from the CSL, DSL, and PIPL, the concepts of data and personal information are not consistent in several laws and the relationship between them lacks clarity. For example, the NPCSC's *Notes on the (Draft) Cybersecurity Law of the People's Republic of China* aim, among other things, articulate the goal of strengthening the protection of 'electronic information that can identify citizens and relate to their personal privacy'—is this synonymous with personal information within the meaning of the PIPL? Also, the *Civil Code* both recognizes the personality rights over personal information and provides property law protection for 'data' in art 127; therefore, the debate on giving proprietary right to personal information must be traced back to the relationship between data and personal information. Typically, eg Shen Weixing, 'On Data Usufruct' (2020) 11 Social Sciences in China 111 (in Chinese); Ma Yufei, 'Conflicts and Coordination between Enterprise Data Rights and User Information Right: Under the Background of Data Security Protection' (2021) 7 Law Science Magazine 160 (in Chinese).

[17] Due to the mixed-use of data and information by relevant regulation in the previous data law in China, as well as the use of the term 'personal data' in the European Union and 'information privacy' and 'personally identified information' in the USA; the relationship between data and information had presented a formidable challenge for Chinese researchers in their choice of expression. Chinese researchers often have to define the meaning of data or information at the beginning of the article to clarify the research object to avoid confusion. For example, Mei Xiaying, 'The Legal Attributes of Data and Its Civil Law Orientation' (2016) 9 Social Sciences in China 167 (in Chinese). Zheng Guan, 'Personal Information Consideration and Its Basic Institutional Design' (2019) 2 Peking University Law Journal 480 (in Chinese).

[18] Han Xuzhi, 'The Ambiguous Use of the Scope of Information Rights and its Consequences' (2020) 1 East China University of Political Science and Law Journal 86 (in Chinese).

Based on this definition, the relationship between the three laws can be examined in terms of their regulated objects: first, the DSL and CSL intersect insofar as both regulate 'network data' (*wangluo shuju*) or 'electronic data' (*dianzi shuju*); they differ insofar as data recorded in a non-electronic manner is regulated by DSL but not by the CSL. Secondly, 'data' regulated by DSL follows the conversion rule of 'data-information-knowledge-intelligence', which considers data as the carrier of information, and information as referring to the knowledge contained in the data.[19] In other words, the relationship between data and information is akin to that between 'form' and 'content'.[20] Similarly, this distinction also encapsulates the relationship between the 'data' under the DSL and 'personal information' under the PIPL.[21] Electronic data in itself does not contain personal information, but if the data can be used to identify and associate itself with a specific natural person, then the data can be said to be converted into personal information and be subject to regulation under the PIPL.[22]

The Chinese legislature opted to use the terminology of 'personal information', rather than directly import the term 'personal data' as found in the EU General Data Protection Regulation (GDPR), because it considered that personal data mainly referred to binary codes of 0 and 1, which it saw as distinct from the expression of content characterized by information. However, both terms essentially refer to the same object. This explains why the *Shenzhen Special Economic Zone Data Regulation* issued in 2021 expressed that: 'personal data means data containing information that can identify a specific natural person, excluding the anonymised ones'.[23] Therefore, in Chinese data law, personal data and personal information are synonymous. However, this does not mean that both the DSL and PIPL apply to personal data protection issues, which will be expounded on in the following section.

The constitutive logic of data law

Chinese data law is a heterogeneous system of law combining multi-level and multi-sectoral legislation. At its core, the CSL, DSL, and PIPL apply to all data processing activities and provide unified and centralized processing rules. There are systematic rules governing data processing procedures, the rights and obligations of participants, and regulatory duties. At the peripheries, nearly 100 laws and regulations also provide for data processing or personal information protection. For instance, the *Law on Protection of Consumer Rights and Interests* and the *E-Commerce Law* prescribes in detail rules for the protection of personal information belonging to vulnerable parties; it regulated the bulk of data processing activities before the DSL and PIPL were enacted. Other laws regulate specific fields and professions, such as the *Audit Law*, the *Military Service Law*, the *Oversight Officials Law*. These laws provide for personal information protection in the course of carrying out professional activities or performing administrative duties.[24] As such laws mainly focus on the protection of rights in the context of data processing, provisions are typically brief and declaratory. They do not provide an effective guide for compliance. Therefore, Chinese data law can be characterized as having the CSL, DSL, and PIPIL at its core, providing for norms universal to Chinese data law. From that core diffuses systematic legal norms as well as special or declaratory provisions that are scattered throughout various laws.

There are also numerous regulatory documents that supplement Chinese data legislation. These include a wide range of regimes designed to protect critical information infrastructure (*guanjian xinxi jichusheshi*), assess data export security, and review network security. They also regulate various situations wherein data are used, such as in Internet-connected vehicles, facial recognition technology, and epidemic prevention and control.

The number and complexity of these norms pose a challenge to the understanding of this burgeoning area of law. How does one understand the interaction between the three pillars of Chinese data law (ie the CSL, DSL, and PIPL)? How are they organized internally? How do the subordinate norms develop and link together? After putting forward the essential features of Chinese data law, this part critically examines the specific contents of the CSL, DSL, and PIPL. It posits that Chinese data law is joined by the common thread of classifying data and according data different hierarchies

[19] 'What is the Data, Information, Knowledge, Wisdom (DIKW) Pyramid?' *Ontotext* <https://www.ontotext.com/knowledgehub/fundamentals/dikw-pyramid/> accessed 28 December 2021.

[20] ibid 93–94.

[21] In China, two criteria govern the legal characterization of personal information. The first is identifiability, which refers to information identifying a specific natural person (from information to a person). The second is relevance, which refers to information that arises from the activities of a specific natural person when that person is known (from a person to information). See *Huang v Tencent Technology (Shenzhen) Co Ltd* and others on 'Network Tort Liability Disputes over Privacy and Personal Information Rights' (2019) Jing 0491 Min Chu no 16142 (in Chinese).

[22] Han (n 18) 94.

[23] Shenzhen Special Economic Zone Data Regulation, art 2.1.2.

[24] For example, art 16 of the Audit Law (amended in 2021) states that 'audit institutions and auditors shall maintain the confidentiality of State secrets, work secrets, commercial secrets, personal privacy and personal information which have come to their knowledge in the course of performing their duties and shall not divulge or illegally provide them to others.'

of protection, and is thus a harmonized legal field with a constitutive logic.[25]

The data protection system in China comprises two aspects: a horizontal aspect ('data classification protection') and a vertical aspect ('data hierarchy protection').[26] Horizontal data classification categorizes and manages data according to common attributes, such as the 'producer', the 'possessor', the 'concerned area', and the 'industry'. Vertical data hierarchical protection grades data according to the degree of harm to national security, social order, public interest, and the legitimate rights and interests of individuals that would follow from any harmful interference and destruction of the data.[27] The idea is to classify data into different categories and then adopt different intensities of protection for varying 'hierarchies' of data. Thereafter, compliance obligations of varying severity will be imposed on the data processing process (which includes collection, transmission, storage, access, sharing, circulation, destruction, etc). The twin methods of data classification protection and data hierarchical protection are the thread that unifies and organizes many aspects of Chinese data law. Each of the two methods will be elaborated upon in turn.

Data classification

The main role of data classification is to identify the applicable data laws. For instance, as aforementioned, separate categories for personal information/personal data and network data have been created. Personal information is subject to the provisions of the PIPL; but when such information is generated, processed, and stored on network facilities and equipment, the relevant provisions of the CSL would also apply. Conversely, data excluding personal information (hereinafter referred to as 'narrowly defined data') is subject only to the provisions of the DSL—but where such data are associated with a network, especially one belonging to the critical information infrastructures that the CSL protects, the CSL also applies. In other words, in Chinese data law, 'data' is a 'primary category', and 'narrowly defined data' and 'personal information' are 'secondary categories' that are subsumed under this primary category.

Moreover, since data in different fields have varying characteristics and need different approaches in its protection and utilization, data regulations are mainly targeted at certain industries and/or subject matters. These sub-categories are not tertiary categories that are subsumed under personal data and narrowly defined data but exist as a secondary category alongside 'narrowly defined data' and 'personal information'. These regulations are selectively applied together with the CSL, DSL, and PIPL to the extent that these laws are engaged. It is worth noting, however, that such regulations are not accorded the same status as legislation, and do not override the provisions of the CSL, DSL, and PIPL.

First, examples of legislation/regulations targeting specific industries include those governing scientific data,[28] medical data,[29] and automobile network data,[30] among others. Such special legislation/regulations supplement the general rules of the CSL, DSL, and PIPL and exist principally in the form of departmental rules. For instance, in August 2021, the CAC, the National Development and Reform Commission ('NDRC'), the Ministry of Industry and Information Technology ('MIIT'), the Ministry of Public Security ('MPS'), and the Ministry of Transport ('MOT') jointly issued a document entitled *Several Provisions on the Management of Automobile Data Security (for Trial Implementation)*.[31] This document laid down overarching principles tailored to automobile data processing, which include the 'principle of processing

[25] It is the fundamental system in the field of rule of law for data in China. 'Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035.' This document specifically stated, 'We will improve differentiated and hierarchical data protection systems applicable to the big data environment.'

[26] It is worth noting that the notion of data classification and grading used in this article is different from the data classification and grading protection system in art 21 of DSL, which required the government to establish. The former refers to the macro ideas of data law design, and the latter refers to the specific implementing regime.

[27] See China's Zhejiang Province has released 'Guidelines for Classification and Grading of Public Data in Digital Reform' (DB33/T 2351—2021). See art. 3.2, 3.3. Different data classification and grading standards apply to different fields.

[28] 'Notice of the General Office of the State Council on Issuing the Measures for the Management of Scientific Data', no 17 (2018) of the General Office of the State Council.

[29] 'Guiding Opinions of the General Office of the State Council on Promoting and Regulating the Application and Development of Big Data in Health and Medical Care', no 47 (2016) of the General Office of the State Council.

[30] Cyberspace Administration of China, National Development and Reform Commission, Ministry of Industry and Information Technology, Ministry of Public Security, Ministry of Transport, *Several Provisions on the Management of Automobile Data Security (for Trial Implementation)* (16 August 2021).

[31] The event that drove the provisions was that in April 2021, after a Tesla car was involved in an accident and the car owner asked Tesla to disclose the driving data half an hour before the crash, but was declined, after which the issue of how the automobile data should be stored and accessed came under the spotlight <https://baijiahao.baidu.com/s?id=1698081822750290828&wfr=spider&for=pc> accessed 28 December 2021. Related documents also include the MIIT's *Notice on Strengthening the Cybersecurity and Data Security of Internet of Vehicles* (MIIT Wang An [2021] no 134, 15 September 2021); and the MIIT Division of Science and Technology's *Guidelines on the Construction of a Cybersecurity Standard System for Internet of Vehicles* (Intelligent Networked Vehicles) (Draft for Comments) (21 June 2021).

data inside vehicles', the 'principle of non-collection by default', and the 'principle of accuracy range application'. It also modified the informed consent rule for collecting data inside and outside the vehicle.[32]

Secondly, examples of specific subject matters that are regulated include personal data, enterprise data, and government data. However, such categories are not mutually exclusive, as enterprise data that can identify individuals would also be considered personal data, and government data may also be classified under enterprise data or personal data in some cases.

Among these categories, 'government data', also known as 'public data',[33] is likely to be at the forefront of future legislative development. This category was first articulated in a separate chapter of the DSL, and therefore followed in *Opinions of the CPC Central Committee and the State Council on Improving the Systems and Mechanisms for Market-based Allocation of Factors of Production* of 2020. The rules governing government data largely involve data sharing across government departments and the disclosure of government data.

The former is now governed and facilitated by departmental rules such as the MOT's *Measures for the Management of Government Data Sharing in Transport*, released in April 2021.[34] The latter, also known as the 'opening of public data', in which 'public management and service agencies disclose data produced or acquired in the course of performing their duties and providing public services by law' to society at large,[35] is now mainly governed by local regulations.[36] These regulations include the *Measures of Guangdong Province for the Management of Public Data*, *Interim Measures of Zhejiang Province for the Opening and Security Management of Public Data*, and *Interim Measures of Shanghai Municipality for the Opening of Public Data*. Evidently, the protection and use of personal data and government data are fairly established and is developing.

The other category of data subject to extensive rules is personal data, which is governed by the specific rules of the PIPL. In contrast, enterprise data are not governed by specific regulations. This is because enterprises already possess the incentive to fully exploit data; data privacy and public interest issues involved therein are then delegated to tort or administrative rules.[37]

In sum, data law developed by way of classifying different types of data and this approach sets the overall framework. At the most general level, the CSL, DSL, and PIPL were enacted to govern different broad categories of data. Following which, specialized laws were created to meet the particularities of certain sectors and domains. However, data classification offers little guidance on how those specific laws should function internally. To this end, data grading is employed.

Data grading

Data grading (under data hierarchy protection) has become the main axis of the internal structure of Chinese data law; the hierarchization of data ensures a delicate balance between the costs and benefits of data protection and utilization. The CSL distinguishes between data generated by critical information infrastructure and other general data, and the difference lies in the importance of the data operation facilities in question. The CSL also requires personal information and key data (*zhongyao shuju*) that is collected and generated by critical information infrastructure to be stored locally. If cross-border transfer is needed, a security assessment shall be conducted (Article 37).

[32] Special legislation is launched for data of specific areas, mainly because these data processing activities, due to their particularities in terms of subjects, implementing scenarios, risks, etc. These demand rules differ from the general ones. For example, here, as one of the particularities of Internet of Vehicles data, the processing of personal information of people inside and outside the car is necessary for the car's operation. For the people inside the vehicle, all activity information will be comprehensively collected and analysed, and then used for commercial promotion and insurance pricing. Those outside the car cannot be informed and give their consent. Therefore, the general rules of personal information processing need to be supplemented and modified. See Li Shuo, 'Research on the Legislation of Self-driving Cars' (2019) 2 Administrative Law Review 112 (in Chinese); Jiang Su, 'The Challenges of Self-driving Cars to the Law' (2018) 2 China Law Review 186 (in Chinese).

[33] Public data refer to the data resources collected and generated by public institutions in the legal performance of their duties—see *Interim Measures of Shanghai Municipality for the Opening of Public Data*, art 3—an equivalent to 'public sector information' under the EU open data regime.

[34] Ministry of Transport, Measures for the Management of Government Data Sharing in Transport (no 33 [2021] of the Ministry of Transport, issued on 6 April 2021, effective on 15 April 2021).

[35] Definition of public data quoted from art 3, s 1, Item 1 of the *Measures of Guangdong Province for the Management of Public Data.*

[36] Government data (public data) opening-up is different from government information disclosure. The former aims to achieve the best use of data, while the latter seeks to promote government transparency and satisfy the public's right to know, for which the corresponding principles, rules, and remedies are different. See Song Shuo, 'Government shall Choose a Legislation Paths of Opening Data which is Different from the Path of Information Disclosure' (2021) 1 Law Science 91 (in Chinese).

[37] The disputes over data rights and interests between enterprises can be very complex. In Chinese law, they are mainly resolved through the Anti-Unfair Competition Law, Copyright Law, and other relevant laws. See *Beijing Weimeng Chuangke Network Technology Co Ltd v Beijing Taoyou Tianxia Technology Co Ltd* (Dispute over Unfair Competition) Beijing Intellectual Property Court (2016) Jing Min Zhong no 588 Civil Judgment (in Chinese); *Tencent Technology (Shenzhen) Co Ltd v Zhejiang Soudao Network Technology Co Ltd* et al. (Dispute over Unfair Competition), Zhejiang Hangzhou Intermediate People's Court (2019) Zhe 8601 Min Chu no 1987 Civil Judgment (in Chinese); *Anhui Meijing Information Technology Co Ltd v Taobao (China) Software Co Ltd* (Dispute over Unfair Competition) Zhejiang Hangzhou Intermediate People's Court (2018) Zhe 01 Min Zhong no 7312 Civil Judgment (in Chinese).

The DSL further specifies that data shall be assessed according to the importance of the data and any potential harm that transfer might cause. For data identified as important, a heightened level of protection is required (comprising data administrators, risk assessments, and export security assessment). The DSL's criteria for determining key data (and consequently requiring enhanced control) constitute its distinct value in comparison with the CSL.[38] Further, data concerning national security, lifelines of the national economy, the livelihoods of important people, and major public interests are classified as 'core data' (*hexin shuju*) and subject to the strictest control because it is more highly valued than 'key data'.[39] Core data are in effect data of utmost importance, and it can be distinguished from key data by the aforementioned criteria.

The identification of key data involves two issues: who defines what is 'key data', and how should 'key data' be defined. On the first issue, the DSL establishes that while the central government is responsible for developing a catalogue of key data, it is incumbent upon different regions and governmental departments to flesh out the details. The power to define is vested in the government because of the public and national interest in according a higher standard of protection to 'key data'. Even where individual interests are engaged, it would nevertheless concern the government in situations where the information concerned is aggregated in such density to affect the interests of the majority. Data enterprises are not in a position to define what is 'key data' because they are oriented towards their own economic interests and do not have an incentive to defend public, national, and individual interests.

On the second issue, the current practice is to clarify what is meant by 'key data' through a piecemeal, non-exhaustive enumeration of individual categories of key data. For example, Article 73(1)(3) of the *NDS Regulation* identifies seven categories of key data, to name a few for illustration: undisclosed government data, job secrets, intelligence data, law enforcement, and judicial data, 'data relating to the construction, operation, and security of national infrastructure and critical information infrastructure', and 'data on the geographical location and security of vitally sensitive regions where national defence facilities, military administration areas, and defence scientific research and production units reside'. In another example, five important categories of automobile data are listed in the *Several Provisions on the Management of Automobile Data Security (for Trial Implementation)* (Article 3, paragraph 6).

Upcoming developments are underway and there are plans to publish a national guide to serve as a standard of reference for identifying key data. This guide is already in its consultation stage and will be termed the *Information Security Technology – Identification Guide of Key Data* ('Guide'). It starts by identifying seven key sectors and thereafter specifies which types of data are of crucial importance within these sectors, including those related to economic operations, population and health, natural resources and environment, science and technology, and security and protection.

Personal information enjoys independent protection in Chinese data law and is divided into two categories—'general personal information' and 'sensitive personal information' (*mingan geren xinxi*)—according to its proximity to personal interests. The latter is subject to more stringent requirements in rules governing the purpose of processing, the content of the notification, and consent.[40] Here, it is important to discern the nexus between 'sensitive personal information' and 'private information' (*simi xinxi*). The concept of 'private information' is contained in a provision of the *Civil Code* in the part governing personality rights. According to Article 1034, section 3 of the *Civil Code*, personal information with private characteristics, that is information that an individual would not want others to know, would be considered personal information that engages the right to privacy and the rules on the right to privacy would apply exclusively.[41] In contrast, sensitive personal information is information that might potentially

[38] The identification of key data is an important task in the implementation of DSL. Liu Jinrui proposes that 'specialized data security legislation should aim to regulate key data on the grounds that it may seriously endanger national security or public safety'. See Liu Jinrui, 'Innovation in Data Security Paradigm and its Legislative Elaboration' (2021) 1 Global Law Review 17 (in Chinese). Xu Ke took the view that key data should be those 'once tampered with, destroyed, leaked or illegally used, would seriously endanger state power, sovereignty, unity and territorial integrity, the well-being of the people, the sustainable economic and social development and other vital interests of the state'. See Xu Ke, 'Freedom and Security: A Chinese Solution for Cross-Border Data Flows' (2021) 1 Global Law Review 34 (in Chinese). Apart from these academic discussions, at the practice level, China has initiated the development of a national security standard. Namely, 'Identification Guide of Key Data'.

[39] DSL, art 21(2).

[40] For example, for the general personal information, only a general consent is needed, but for the sensitive personal information, a separate consent is obligatory. Again, according to the *Data Export Security Assessment Measures (Draft for Comments)* issues by the CAC in October 2021, where the personal information of more than 100,000 people or sensitive personal information of more than 10,000 people are transferred overseas accumulatively, a security assessment of outbound data is mandatory.

[41] Some studies have put forward the categorization of the subjective and objective elements of private information. The subjective element is the 'unwillingness to be known to others', and the objective element is that the information has secrecy attributes and is in a secret state. See Xu Ke and Sun Mingxi, 'Re-clarification of Personal Private Information–From the Relationship between Privacy and Personal Information' (2021) 1 China Applied Jurisprudence 12 (in Chinese).

cause harm to the person and property of a natural person if the information were to be leaked or used illegally.[42]

This illustrates that the distinction between 'private information' and other personal information is a horizontal distinction dependent upon whether the personal information is of a private nature. Correspondingly, the distinction between 'sensitive personal information' and 'general personal information' is a vertical distinction dependent upon the importance of personal information.[43] This distinction also explains why the rules on the right to privacy apply in some situations and the rules on personal information protection apply in other situations.[44]

However, it is still debatable if either distinction provides greater protection than the other.[45] It may well be that the result of the two different dividing approaches may in many cases be similar, ie private information is likely to be sensitive personal information and thus be subject to greater protection in any case.[46] Nonetheless, there will be cases where private information will not be regarded as sensitive personal information and vice versa. For example, while a user may regard her web browsing history as private information (since it might reveal her political preferences and psychological state), the personal information used in this marketing modus operandi is typically not deemed sensitive absent the crystallization of serious harms[47] because this information would be critical for companies in putting together efficient and cost-effective advertising recommendations.

To summarize, in Chinese data law, data classification and grading reveal the guiding philosophy underlying the organization and structure of data law. The horizontal approach of data classification is adopted within several pertinent legislations and is pitched at a broader level of abstraction. When it comes to the internal design and implementation of these laws, a hierarchical approach is the main means of managing narrowly defined data and personal information so to effectively balance the interest in protecting information and data resources against the interest in its usage.

The unification of values in data law

As already argued, while data law is a field characterized by a well-defined core of legal norms, yet it has a patchy system of associated provisions and supporting rules. Data classification and grading knit together a multitude of legal norms into a unifying whole. This, however, merely reflects a formal unity. For these data rules to normatively take shape as an independent area of law, they must share certain core values. This article identifies two values: physical security and juridical security. Although both values permeate the field of data law, structural differences arise when these values are applied to the protection of narrowly defined data and personal information.

Unified overall goal of data law

Although the CSL and DSL both include 'security' in the title of the law, whereas PIPL adopts the word 'protection', all three legislations share the same underlying philosophy of promoting the circulation and use of data and information but preventing leakage or misuse. The dual goals of data security/protection and utilization can be unified under a general notion of 'security'.

[42] There is no more precise standard on how sensitive personal information should be defined at the legislative level. Some studies have drawn on multi-factors proposed by Paul Ohm for determining sensitive personal information and concluded that China should combine three factors. Namely, (i) 'whether the disclosure of the information will lead to significant harm', (ii) 'the chance of causing harm to the information subject', (iii) and 'the sensitivity of the social majority to a certain type of information' to determine whether a certain type of personal information is sensitive. Based on these criteria, the study further identified by questionnaire the health information, sex life and sexual orientation, ID number, financial information, political views, correspondence information, genetic information, biometric information, and precise geographical location as sensitive personal information in China. See Hu Wentao, 'Conception on the Definition of Personal Sensitive Information in China' (2018) 5 China Legal Science 247 (in Chinese). Also see Paul Ohm, 'Sensitive Information' (2015) 88 Southern California Law Review 1149.

[43] It is worth noting that sensitive personal information can again apply different levels of protection by internal classification and grading.

[44] The application of personal information protection and the right to privacy is still under debate so far. See Zhou Hanhua, 'Parallel or Overlap: Relationships between Personal Information Protection and Privacy Protection' (2021) 5 Peking University Law Journal 1167 (in Chinese).

[45] Among the interpretations of the Civil Code promulgated by the legislature and some theoretical studies, many argue that the intensity of protection is the highest for private information, followed by sensitive personal information, and the weakest for general personal information. See Huang Wei (ed), *People's Republic of China Civil Code Interpretation* (Law Press 2020) 193–95 (in Chinese); Wang Liming, 'Legislative Highlights, Characteristics and Applications for the Chapter of Personality Rights in the Civil Code' (2020) 17 Journal of Law Application 14 (in Chinese); Zhang Yong, 'The Public-Private Law Integrated Protection of Sensitive Personal Information' (2022) 1 Oriental Law 73 (in Chinese).

[46] One prominent scholar argues that the difference between private personal information and sensitive personal information is that the former is a civil right, therefore must be determined in the context of a specific natural person's personal dignity, personal freedom and private peace. While the latter is created by PIPL to regulate the processing of information, which is specified, objective, and not individualized. See Cheng Xiao, 'Sensitive and Private Information in the Protection of Personal Information' *People's Court Daily* (Beijing, 19 November 2020) 005 (in Chinese).

[47] The personal data breach scandal relating to the Facebook and Cambridge Analytica is a classic counterexample. See Kevin Granville, 'Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens' *New York Times* (New York, 19 March 2018).

Scholars have proffered different taxonomies of data security. Chinese scholar Liu Jinrui divides data security into two notions. First, the security of data itself, which requires 'ensuring the confidentiality, integrity and availability of data in the intensive flow of data'. Secondly, the security of data use, which requires 'preventing the security risks arising from large-scale aggregation and analysis of data' so that the use of data can be controllable and legitimate.[48] Chinese scholar Xu Ke proposes that data security can be categorized into 'independent security' (confidentiality, integrity, and availability of data), an 'autonomous and controllable' nature (state's control over key data), and 'macro security' (prevention, control, and management of threats to national sovereignty, public interest, and community security arising from data processing and use).[49]

These studies answer the three crucial questions of 'what objects are secure', 'for whom are they secure', and 'how are they secure'; they identify explicit or potential objects to be protected and the adverse effects that follow if such objects are not protected. Yet, the positive nature of utilization-oriented data remains neglected in academic literature. Considering previous studies, this article proposes a novel approach, arguing that the objectives of the data law should fall into two dimensions: physical security and juridical security.

Physical security, also known as 'network data security'[50] in the CSL, is 'the ability to safeguard the integrity, confidentiality and usability of data'. This directly corresponds to the three internationally accepted elements of data security[51]: that data legally collected by data processors[52] should not be subject to illegal access, processing, and disclosure. The targets of sanction are illegal intruders (outsiders) and illegal leakers (insiders). The goal is to maintain data storage systems and equipment in a physically and statically secure status. This is mainly achieved by setting requirements for data retention methods, technologies, and management schemes. These requirements include taking security-related technical measures such as encryption and de-identification, determining the operation privileges relating to personal information processing, and providing security education and training for employees on a regular basis (PIPL, Article 51).

Juridical security is no longer an issue arising solely from the conflict between data processors and data controllers on the one hand and trespassers and leakers on the other. Instead, it reflects a delicate balancing of interests between data processors and the abstract interests of the state, society, and individuals. This concept encompasses the concepts of 'security of data use' proposed by Liu Jinrui and 'macro security' proposed by Xu Ke. Under DSL's legal framework, 'data security refers to the adoption of necessary measures to ensure the *effective protection* and *legal use* of data, and the capability to guarantee the continuous security of data'.[53] The former component, 'effective protection', is the equivalent of physical security. 'Legal use' under the DSL means that the use and circulation of data must comply with legal requirements, underpinning which is the value defined herein as juridical security. Juridical security comprises three specific elements:

First, personal security. Personal security in the context of juridical security aims to ensure that the lawful data processing does not adversely affect the privacy, free development of personality, personal dignity and,

[48] See Liu (n 38) 8.

[49] See Xu Ke, 'Data Security Law: Positioning, Legislation and Institutional Design' (2019) 3 UIBE Law Review 54 (in Chinese).

[50] The difference between 'cyber data security' and 'cyber information security' is that the former is concerned with preventing electronic data from being stolen, tampered with, and illegally collected and processed, including all data that can or cannot identify a person. The latter is about the legality and controllability of information dissemination activities. For example, suppose a network operator finds any information that is prohibited by laws and administrative regulations from release or transmission. In that case, it shall immediately cease the transmission of such information and take measures such as deletion to prevent disseminating such information (art 47 of CSL). Therefore, cyber information security in the sense of intelligence and communication science does not fall within the scope of this article <http://www.npc.gov.cn/zgrdw/npc/lfzt/rlyw/2015-07/08/content_1941286.htm> accessed 28 December 2021.

[51] This is also in conformity with China's national standard on information security technology glossary (GB/T 25069-2010). See <http://www.gb688.cn/bzgk/gb/newGbInfo?hcno=474F1252FDA038A894A4E54EF47D4E59> accessed 28 December 2021. Confidentiality (2.1.1), Availability (2.1.20), Integrity (2.1.42).

[52] In Chinese data law, data processor and information processor are only different in what they process, and they share the same defining criteria and differ from the EU's definitional approach. According to GDPR, a data controller is who determines the purposes and means of the processing. A data processor is independent of the controller and processes personal data on behalf of the controller. The primary purpose of the distinction is that the data controller assumes most of the personal information protection obligations. In China, the subject under regulation is mainly the personal information processor. The concept of personal information controller has not appeared in the PIPL. According to art 73(1)(1), 'Personal information processor' refers to an organization or individual that independently determines the purpose and method of the processing in the processing of personal information', which is the same as the definition of data controller in GDPR. According to some studies, since the PIPL has collectively referred to various processing activities as 'the processing of personal information', the concept of 'personal information processor' is just corresponding to it. Moreover, the distinction between controller and processor is only for the internal legal relationship, which does not matter to the information subject. Furthermore, in case multiple people are involved in the processing of personal information, the issue of responsibility and liability in personal information protection can be clearly resolved by distinguishing the processor and the trustee, as provided for in art 59 of the PIPL. See Cheng Xiao, 'On Liability of Processors in the Joint Processing of Personal Information' (2016) 6 The Jurist 20 (in Chinese).

[53] DSL, art 3(2).

in particular, the fundamental rights of individuals.[54] For example, the rule of notice and consent, one cardinal rule in personal data protection, does not permit messaging and social apps to read or tap into private communications indefinitely because this infringes the right of freedom and confidentiality of communication under Article 40 of the *Chinese Constitution.*[55]

Secondly, security, freedom, and social values in public life. In the information age, data processing permeates all aspects of public life, both online and offline. While digital tracking and monitoring technologies are remarkably effective in maintaining security and order within the public sphere, the use of such technologies in state surveillance (including Internet platform surveillance) may threaten democratic and liberal values.[56] Juridical security dictates that any infringement of these values be kept to a minimum and only to the extent that it is necessary.[57] For example, Article 26 of the PIPL imposes strict limits on the purposes for which image collection or personal identification equipment can be installed in public places and on the use of data collected by such equipment. Community values, or network civilization,[58] are also engaged where data processing activities may affect community ties. For instance, it is prohibited to accord unreasonable differential treatment to individuals through automated decision-making even where there is voluntary consent (PIPL, Article 24).

Thirdly, national security. Given that analysing aggregate data may expose critical national intelligence, a perennial theme of data law is to mitigate the national security risks involved in data processing. According to the *Guide*, key data refers to data that has the potential to reveal vital information that might affect national security, including information about the country's military, economy, and population. The enhanced measures to managing key data and mass personal information is also geared towards protecting national security, and this theme is prominently reflected in the *NDS Regulation* and the *Data Export Security Assessment Measures (Draft for Comments)* ('Export Measures').[59]

The preceding analysis has argued that physical security concerns the technical requirements for data management and preservation. In contrast, juridical security involves making a value judgment on whether certain values should be prioritized, upheld, or discarded, and this value judgment guides what the rules of data law should be.[60] By taking personal, social, and national interests into account, juridical security sheds light on what data management regimes should be in place to keep profit-oriented data processing activities and the aggrandizement of state power in check, so as to strike the proper balance between different interests. This balancing process is chiefly carried out by the data classification and grading approach outlined above, which applies varying standards of protection for the use and protection of different categories of data.

Divergent structure of interests in data law

Although the overall objectives of PIPL and DSL are the same, they differ in their focus. The PIPL focuses more on the juridical protection of personal information and this is reflected in the balancing exercise that weighs the purpose, manner, and depth of personal information processing. For example, upon the release of the PIPL, the Chinese legislature was keen to emphasize that its restrictions on automated personal information processing activities would ensure fair and equitable results and that personal information processors 'shall not impose unreasonable discriminatory treatment on

[54] Despite a growing consensus on the ultimate value of personal information protection for information subjects in Chinese academic circles, there is wide controversy over the exact object of protection. For example, Yang Lixin believes that it is the individual's right to control personal information that is protected. Cheng Xiao contends that personal information itself is not an interest to be protected by law, and that the protection of personal information is intended for other interests attached to personal information that requires legal protection. Lu Qing opines that the protection of personal information is to ensure the proper and full recognition of an individual's identity by others, as a protection of the identity production process. Yang Lixin, 'Personal Information: Legal Interest or Civil Rights——An Interpretation of "Personal Information" in Article 111 of the General Provisions of Civil Law' (2018) 1 Legal Forum 40 (in Chinese); Cheng (n 6) 37; Lu Qing, 'Identity Construction and Its Legal Protection in the Digital Era: Consideration Centered on the Protection of Personal Information' (2021) 5 Chinese Journal of Law 10 (in Chinese).

[55] Zhang Xinbao, 'Collection of Personal Information: Restricting the Application of the Principle of Informed Consent' (2019) 6 Journal of Comparative Law 3 (in Chinese).

[56] See Li Yanshun, 'Research on Citizen's Privacy Protection in Public Video Surveillance' (2019) 3 Science of Law 56 (in Chinese).

[57] See Liu Yanhong, 'The Legal Logic and Limitation of Mass Surveillance in the Use of Public Space' (2020) 2 Legal Forum 13 (in Chinese).

[58] The concept of 'online civilisation' derives from the *Opinions on Strengthening the Construction of Network Civilization* issued by the General Office of the Central Committee of the Communist Party of China and the General Office of the State Council on 14 September 2021, which intends to boost the Internet ecosystem and regulate online behaviour with community-approved values, morals, and laws. This is also reflected in art 8 of the DSL, 'show respect for social morality and ethics, observe business ethics and professional ethics' and art 5 of the PIPL, 'principle of good faith'.

[59] Omer Tene, an expert on data privacy, said in a press interview, 'If European data protection laws are grounded in fundamental rights and US privacy laws are grounded in consumer protection, Chinese privacy law is closely aligned with, and I would even say grounded in, national security.' Ignore China's New Data Privacy Law at Your Peril, 5 November 2021 <https://www.wired.com/story/china-personal-data-law-pipl/> accessed 28 December 2021.

[60] Physical security and juridical security are not completely separate and independent from each other. Some studies have pointed out that the emphasis on cybersecurity may affect privacy protection in both positive and negative ways. See Christopher Kuner and others, 'The Rise of Cybersecurity and its Impact on Data Protection' (2017) 7 International Data Privacy Law 74.

individuals in respect of the transaction price and transaction conditions'.[61] This is a rule that emerges from the careful balancing of multiple values, which include market efficiency, fairness, and human dignity.[62] Another example is that the PIPL neither proscribes the application of automated decision-making nor invokes the 'opt-in' mode but ensures the consumer's right to fair trade by limiting differential pricing or 'big data stabbing'.[63]

While the rules of the PIPL reflect a value-based decision, value-based rules are relatively few in the DSL. In contrast, DSL attaches more importance to physical security. For example, the state is required to establish data security risk assessment, reporting, information sharing, monitoring, and early warning mechanisms; data processors should establish a sound data security management system throughout the whole process. In a symposium comprising key Internet companies held by MIIT in July 2021, the ministry requested Internet companies to implement the DSL given the importance of data security in safeguarding state sovereignty, security, and development interests.[64] Yet, in relation to physical security, it must be acknowledged that the aim 'is not to eliminate all data risks, but to reduce and keep losses below acceptable levels through a continuous process of crisis identification and risk management'.[65]

The differing weights accorded to physical security and juridical security in the PIPL and DSL reflect the distinct stakeholders engaged by the two laws. The principal stakeholders regulated by the DSL are state and data processors because the technical costs of data protection are mainly borne by the state and data processors. Correspondingly, when the confidentiality, integrity, and availability of data are compromised, harm is primarily caused to state interests, public interests, and the interests of data controllers—chief of which is the state interest. Individuals are typically not affected by such events.

The DSL imposes a series of positive obligations on the state (and not individuals); these include the implementation of a big data strategy, support for research on data development and use, the development of a standards system, and the establishment of a data trading system.[66] In particular, the DSL promotes data utilization through the implementation of the 'government data opening-up system' that was initiated by the State Council in 2016.[67] The direct beneficiaries of public data disclosures are enterprises, rather than individuals, for two reasons. First, enterprises have strong capabilities and technology for mining and analysing public data, whereas individuals do not typically have such resources. Secondly, while Shanghai, as a vanguard of public data disclosure, has developed an operation model whereby authorized entities may exploit public data and supply data products and services,[68] it is almost impossible for individuals to be authorized due to the lack of capacity and funding.

In contrast, the stakeholders engaged by the PIPL include information subjects, processors, and the state, and these parties interact within a sophisticated interest relationship. This may be illustrated by using information subjects as a starting point.

For information subjects, the use of personal information comes with both benefits and costs. On one hand, the information subject trades information for free access to Internet products, such as free messaging apps like WeChat and Facebook, whose revenues derive mainly from advertising. Advertisement recommendations are made through sophisticated personal profiling that draws on the user's personal information.[69] On the other hand, this means that individuals can no longer hide behind a proverbial screen. There is now a possibility of being tracked, monitored, and spied on by information processors. This might trigger a 'chilling effect'

[61] Legislative Affairs Commission of the NPCSC, 'Six Major Changes to the Personal Information Protection Law (Third Review Draft)' <https://www.thepaper.cn/newsDetail_forward_14068281> accessed 28 December 2021.

[62] Five days after the PIPL was promulgated, on 27 August 2021, the Cyberspace Administration of China immediately unveiled the 'Internet Information Service Algorithm Recommendation Management Regulations (Draft for Comment)', which was finally passed on 16 November 2021. Moreover, this provision of the PIPI was included in art 21 of the said document.

[63] See Cai Peiru, 'The Distinction of Personal Information Protection Principles: Protection by Process and Protection as a Result' (2021) 5 Administrative Law Review 99 (in Chinese). Ge Jiangqiu and Chen Li, 'The Obligation to Provide "Non-Personalised" Search Results Under the Chinese E-Commerce Law, (2021) 41 Computer Law & Security Review 1.

[64] The Cybersecurity Bureau under MIIT has invited 12 major Chinese technology companies, including Alibaba Group Holding, Tencent Holdings, and ByteDance, to attend a major meeting to discuss various issues concerning improvements in their operations to comply with the China's Data Security Law. See Che Pan, 'Beijing Summons Alibaba, Tencent, ByteDance, 9 Other Tech Firms over Data Security Concerns' *South China Morning Post* (Hong Kong, 30 July 2021). See Chinese government's official announcement <https://wap.miit.gov.cn/xwdt/gxdt/sjdt/art/2021/art_7049a30c7bcc43c0b611028def52e726.html> accessed 28 December 2021.

[65] Xu (n 49) 60.

[66] DSL, arts 14–17, 19.

[67] State Council of China, 'Notice of the State Council on Issuing the Interim Measures for the Administration of Sharing of Government Information Resources' no 51 [2016] of the State Council.

[68] Shanghai Data Regulation, ch 3 s III.

[69] See Ge Jiangqiu, 'Regulatory Purpose and Restricted Application of the Customized Search Results Clause of the E-Commerce Law from an Interpretive Perspective' (2021) 3 Science of Law (Journal of Northwest University of Political Science and Law) 98 (in Chinese).

that suppresses and distorts the opportunity for the free development of personality.[70]

We turn to information processors. Information processors have a considerable financial incentive to produce personal information, and this applies especially to information processors that rely on cutting-edge software and well-trained algorithms to aggregate and dissect data.[71] Some of the information gathered is quite unlike inherent personal information such as names and I.D. numbers; examples include web browsing history generated from a user's interaction with a computer, browser, or search engine.[72] Therefore, there is a justifiable need for information processors to analyse, utilize, and even circulate such elementary personal information.[73]

Lastly, the state has an interest in using personal information for social management and scientific research. During this epidemic, one example is the identification of potentially infected persons through the personal health code, which uses location data.[74] Significantly, at a time when the development of big data has taken on the status of a state's competitive strength, the exploitation of data is crucial to enhancing a state's global competitiveness and to maintaining its security.[75] This is why China has elevated data to the status of a production factor. However, given the glaring mismatch of power between the state and information subjects, it is argued that the state should espouse and practice pro-protection bias in favour of information subjects.[76] This would go towards respecting personal autonomy and ensuring that its citizens retain the spirit of democracy and self-determination at a constitutional level.[77]

The interests in personal information processing activities are multi-faceted and complex, and those interests of different stakeholders can converge or conflict with one another.[78] The same stakeholder would also have to contend with its own conflicting interests. What makes the situation even more complicated is that it involves multiple value preferences: personality interests versus economic interests, and individual autonomy pitted against compulsory state protection.[79] To reach a more sophisticated balance of interests would demand more refined rules; the definition and scope of interests would need to be clarified, especially in relation to the 'notice-consent rule'. This is something that, at present, cannot be accommodated within the policy-oriented nature of the CSL and DSL.

In essence, the differences between the DSL and the PIPL are caused by the differing interests underlying data security and personal information protection in China. This difference has led the two laws to adopt different regulatory paradigms: the former focuses on the compliance obligations of data processors under administrative supervisory agencies, while the latter shifts to the 'notice-consent rule' that is independently determined by information processors and data subjects (although the latitude that this rule provides is still in many ways subject to mandatory constraints and

[70] Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (Vintage Books 2001).

[71] See Hu Ling, 'The Commonality of Personal Information and Its Realization from the Perspective of Social Function' (2019) 6 Law and Social Development 179 (in Chinese).

[72] In a judgment handed down by the Hangzhou Internet Court, the court clarified how to define the data rights of enterprises and users. The data controlled by network operators are divided into raw data and derivative data. For a single data entity, the data control subject can only enjoy limited use rights in accordance with its agreement with the user. For the integrated data resource aggregated from a single original data, the data control subject enjoys benefits in the field of competition. Zhejiang Hangzhou Intermediate People's Court (2019) Zhe 01 Min Chu no 1987 Civil Judgment (in Chinese).

[73] In the 'Taobao Meijing Case' case, Meijing Company solicited, organized, and helped others to obtain derivative data at a low price from Taobao Company through the analysis of various personal information on the latter's company's site. The court held that the derivative data 'can confer considerable commercial benefits and competitive advantages on developers or operators, and the property rights thereof arising should also belong to the said developers or operators'. Thus, Taobao prevailed in the fight to exclude others to exploit these data. See *Anhui Meijing Information Technology Co Ltd v Taobao (China) Software Co Ltd* (Dispute over Unfair Competition) Zhejiang Hangzhou Intermediate People's Court (2018) Zhe 01 Min Zhong no 7312 Civil Judgment (in Chinese).

[74] Paul Mozur, Raymond Zhong and Aaron Krolik, 'In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags' *New York Times* (New York, 1 March 2020); Hu Ling, 'The Rise of Health Codes, Digital Identities and Authentication Infrastructure' (2021) 2 China Law Review 102 (in Chinese).

[75] Central Committee of the Communist Party of China, 'State Council of China, Opinions of the CPC Central Committee and the State Council on Improving the Systems and Mechanisms for Market-based Allocation of Factors of Production' (30 March 2020).

[76] See Wang (n 11) 146.

[77] See Fred H Cate and Robert Litan, 'Constitutional Issues in Information Privacy' (2002) 9 *Michigan Telecommunications and Technology Law Review* 35.

[78] See Zhang Xinbao, 'On the Structure of Rights and Interests Relating to Personal Information' (2021) 5 Peking University Law Journal 1155 (in Chinese).

[79] Zhang Xinbao proposed that the protection of personal information should weigh multiple groups of interests. The theory of 'two-sided strengthening, three-party balancing' should be adopted for the following objectives. First, to strengthen the protection of personal sensitive private information. Secondly, to strengthen the use of personal generic information. Thirdly, to balance the interests of individuals in the protection of personal information (personal autonomy and human dignity interests) and the commercial use interests of information companies, and the public interests of the state to manage the society. This theory has a substantial influence on the academic research and legislative development of China's personal information protection theory. See Zhang Xinbao, 'From Privacy to Personal Information: Theory of Interests Rebalancing and its Institutional Arrangement' (2015) 3 China Legal Science 49 (in Chinese). This article is the most highly cited one in China's top law journal 'China Legal Science' in the past 10 years. This view has also palpably influenced China's judicial decision-making. See '*Huang v Tencent Technology (Shenzhen) Co Ltd* and others on Network Tort Liability Disputes over Privacy and Personal Information Rights' (2019) Jing 0491 Min Chu no 16142 (in Chinese).

limitations by the state).[80] However, the overarching goal of both legislation is identical in essence, that is to strengthen the physical and juridical security of data, and in so doing, achieve a balance between data protection and use that would facilitate development.

Critical thoughts on the application of data law in China

As pointed out above, while the relationship between data and information is that of form and content, the term 'personal information' is interchangeably used with 'personal data' in practice. Furthermore, although data includes electronic and non-electronic forms under Chinese legislation, the reality is that data are mostly stored and processed in computers and Internet systems which means that the terms 'network data' and 'data' have much overlap in practice. These conceptually distinct but practically highly unified objects pose considerable challenges for the application of law.[81] This section analyses the application of three pillars of data law from both theoretical and practical perspectives and hopes to unite norms with reality; at the same time, it hopes to provide clarity on the practical characteristics shaping the application of Chinese data law.

Theoretical approach to the application of data law

First, the CSL is fundamental to the regulation of the Internet sphere and its coverage extends to several aspects: from macro issues like sovereignty and the determination of national strategy, to the physical protection of critical information infrastructure, and the regulation of content. With the small exception of data not located in cyberspace, the CSL is relevant to virtually all issues of data law and this general scope of applicability renders the CSL as being fundamentally important to the field of data law.

Another issue is that 'narrowly defined data' and 'personal information' are secondary classifications under the concept of data to which the DSL and the PIPL apply respectively. So, a critical question worthy of examination is: Is it possible for the same data processing activity to simultaneously contravene both the DSL and the PIPL? Undoubtedly, the processing of data that is not personally identifiable will not trigger the PIPL. Therefore, the question that remains is, can the processing act of personal information breach the DSL? Since the standards imposed by the PIPL on data processing are conspicuously higher than those in the DSL, there is normally no room for the DSL to operate. The most likely controversy is whether 'personal information' that engages the PIPL may also constitute 'key data' or 'core data' under the DSL and thus be subject to more regulatory restraints under the DSL. If the answer is in the affirmative, both laws will be triggered. Some scholars have suggested that since the legal characterization of key data is related to the value of the data at stake, personal data or enterprise data can amount to "key data" if they are of importance.[82]

However, this interpretation finds neither support from legal norms nor from the letter of the law. There are at least three reasons why the PIPL and the DSL should not apply concurrently.

First, while the DSL's enhanced protection of key data is reflected in three aspects: (i) specification of the person(s) responsible for data security and the requirement of a management body; (ii) requirements for periodic risk assessment; (iii) and a special regime for the management of data export, the PIPL addresses the same three aspects with rules that are more detailed and specific.

Secondly, the concurrent application of both will render the relevant liability provisions under the two legislations ambiguous and uncertain. For example, if there is an illegal export of key data, the maximum fine specified in the DSL is 10 million RMB, while a violation of the PIPL can result in a fine of up to 50 million RMB or 5 per cent of the previous year's turnover. This presents a marked conflict between the DSL and the PIPL.

Thirdly, as a matter of conceptual expression, the *NDS Regulation* that was published on 14 November 2021 treats 'key data' and 'personal data' as distinct concepts that do not overlap. For example, it stipulated that the same data security emergency response mechanism shall apply if key data or personal information of more than 100,000 people are leaked, destroyed, or lost (Article 11(2)). Article 26 also expressly states that 'data processors handling the personal information of more than one million people shall also comply with the provisions of Chapter IV hereof on processors of key data.' However, it is precisely because 'a large amount of personal information' is not legally synonymous with 'key data' that specific clauses are needed to clarify that the same regime applies to both. Therefore, there is no overlap between the PIPL and DSL in its regulated objects.

[80] Cai (n 63) 98 (in Chinese).

[81] See Mei (n 5) 151.

[82] See Hong Yanqing, 'Building A Framework for Security Review of the Cross-border Data Flow' (2017) 2 Information Security and Communication Privacy 59 (in Chinese).

To treat the DSL and PIPL as legislations that do not apply concurrently would better fit the respective features of each legislation. This is because some tensions within the PIPL do not concern the DSL. For instance, there is tension over whether the PIPL should apply to all activities involving personal information, and the basic consensus that PIPL should exempt those information processing activities that are necessary for social interaction.[83] The rationale is that individuals cannot be completely isolated from the rest of the world and proper disclosure of personal information is necessary for social life; blocking the flow of personal information would increase the costs of social interactions and transactions.[84] Moreover, it is costly to comply with the obligations of personal information processors under the PIPL, which include the informed consent requirement, category-based management, technical security measures, and risk assessment. Therefore, it would be neither necessary nor reasonable to regulate individual and scattered information processing activities that are negligible.[85]

In contrast, the DSL does not contain such conditions because there is no individuality in narrowly defined data and, therefore, no need to mandate the circulation of data to facilitate social interactions. On the contrary, mandating the circulation of data would go against China's efforts to develop a data trading market. Data, if forced to circulate, will lose its scarcity, and decrease in commercial value. This would not be conducive to the robust development of the data market.

To conclude, personal information is a species of data, which may also be referred to as personal data, and which is regulated by the PIPL. In contrast, the DSL governs narrowly defined data and not personal data. These distinctions suggest that the theoretical concepts in data law follow a logic that is clear and hierarchical. However, as explained below, how data law is applied in practice is more complex.

Practical characteristics in the application of data law

Chinese data law has progressed at a relatively slow pace as the DSL and the PIL has only taken effect around September 2021. At a time when guidance for law enforcement is scarce, a glimpse into a recent high-profile enforcement case is undoubtedly the prime illustration of how China's regulators apply data law in practice.[86] The ongoing cybersecurity review of the 'Didi' taxi-hailing app by Chinese regulators, which has received intense attention both at home and abroad, will be discussed.[87]

On the evening of 30 June 2021, Beijing time, China's leading taxi app 'Didi' made its low-profile debut on the New York Stock Exchange. Merely two days later, on 2 July, the Office of Cybersecurity Review led by the CAC launched a cybersecurity review of the 'Didi' app and suspended its user registration. The stated purpose for these actions was to 'prevent national data security risks, safeguard national security and protect the public interest'. [88] This unprecedented move marked the first cybersecurity review since the establishment of the cybersecurity review system. On 4 July, the CAC issued a statement admonishing 'Didi' for collecting personal information in serious violation of the law and removed it from online application stores. The CAC imposed more severe measures on 9 July and abruptly pulled 25 apps associated with Didi from those stores. At the same time, Chinese companies newly listed in the USA, such as 'Full Truck Alliance' and 'Kanzhun', also came under cybersecurity review.[89] The main reason for the Chinese government's launch of such a rapid and sweeping review of network security, data security, and personal information protection for applications such as 'Didi' was because the company was rumoured to have provided many types of corporate-owned data, including users' personal information, travel data, and road information to foreign

[83] See Ding Xiaodong, 'Reflection and Reconstruction of Personal Information Rights on the Applicable Premise and Legal Interest Basis of Personal Information Protection Law' (2020) 2 Peking University Law Journal 341 (in Chinese); Wang Yuan, 'Restatement of Personal Information Protection in Civil Law' (2021) 2 East China University of Political Science and Law Journal 68 (in Chinese).

[84] See Richard A Posner, 'The Economics of Privacy' (1981) 71 The American Economic Review 405.

[85] Ding (n 83); Wang (n 83).

[86] In terms of users' data, for the 12 months ending on 31 March 2021, Didi had 493 million annual active users globally and 15 million annual active drivers globally. Out of these numbers, China boasted 377 million annual active users and 13 million annual active drivers respectively. See Jane Li, 'The Highlights of Chinese Ride-hailing Giant Didi's IPO Filing, in Five Numbers' *Quartz* (New York, 11 June 2021).

[87] ibid.

[88] CAC, 'Announcement of the Office of Cybersecurity Review on the Launch of Cybersecurity Review of "Didi"' <http://www.cac.gov.cn/2021-07/02/c_1626811521011934.htm> accessed 28 December 2021. See Liyan Qi and Trefor Moss, 'Chinese Regulators Target Ride-Hailing Company Didi Just Days after IPO' *Wall Street Journal* (New York, 2 July 2021).

[89] CAC, 'Announcement of the Office of Cybersecurity Review on the Launch of Cybersecurity Review of the "Full Truck", "Truck Gang", "Kanzhun"' <http://www.cac.gov.cn/2021-07/05/c_1627071328950274.htm> accessed 28 December 2021. See Jacky Wong, 'Didi and the Big Chill on China's Big Data' *Wall Street Journal* (New York, 5 July 2021); Chong Koh Ping and Serena Ng, 'China Widens Data-Security Probe of U.S.-Listed Tech Companies' *Wall Street Journal* (New York, 6 July 2021).

countries during their listing process. There was, therefore a risk that the company had seriously infringed on users' personal information, privacy, and security, as well as national security. The event culminated in the planned delisting of Didi from the US stock exchange.[90] In the aftermath of this incident, the *NDS Regulation* and the *Cybersecurity Review Measures* stipulated that greater scrutiny will be placed on the listing of data processors abroad or in Hong Kong. In particular, processors that handle the personal information of more than one million people must undergo a cybersecurity review before they are allowed to list abroad.

The measures by the CAC highlighted the legal distinction between narrowly defined data and personal information. The announcement issued by the CAC on 2 July only suggested the possibility of *data security risks* during the listing of Didi in the USA, which was sufficient to trigger the administrative coercive measures of 'stopping new user registration' to prevent the spread of harm. In contrast, the take-down measures on 4 and 9 July were administrative penalties levied to protect *personal information.*

These enforcement actions further reveal two prominent features in the application of data law.

The first feature is that the provider of a network service tends to simultaneously process narrowly defined data and personal information. This is for two reasons. First, because personal information is the scarcest and most valuable data resource that fuels the business growth of Internet companies, those companies would harvest and exploit it to the greatest extent possible.[91] Secondly, personal information can be revealed after narrowly defined data are aggregated and processed. After personal information is anonymized, it becomes narrowly defined data. This shows that even though, theoretically, the processing of narrowly defined data and the processing of personal information are independent of each other and are subject to different laws, data processing is likely to contravene both legal regimes because the interconversion of narrowly defined data and personal information occurs frequently.

The second feature is that it is often easier and quicker to take law enforcement if data processors violate laws governing the processing of personal information. For instance, in the 'Didi' case, it was appropriate and expedient for the CAC to justify its measures on the violation of personal information processing requirements. Chinese laws have consistently required that personal information processing activities be subject to the 'Minimum Necessary Principle', whereby personal information processors may only collect and use personal information that is necessary to fulfil their services, ie only information without which the purpose of processing will fail.[92] This principle permeates through the DSL, *Civil Code*, PIPL, and the recommended national security standard in the *Information Security Technology–Personal Information Security Specification.*

It is also apposite to observe that the scope of the minimum necessary data for each type of product and service is quite controversial. This vagueness has, to some extent, granted latitude to data processors and law enforcement authorities.[93] Furthermore, the restrictions on the scope and depth of personal information processing in China are incredibly rigid, which substantially fetters the ability of data processors to acquire and exploit data. Insistence upon strict adherence to these restrictions may reduce the accuracy of personal profiling and personalized advertising recommendations, thereby undermining the business model of free Internet services. While it must be recognized that the legal norms governing information processing activities are in a 'buffer period' of refinement and development, the transformed regulatory paradigm is not entirely certain and clear. To clarify the law will pave the way for ascertaining and punishing violations.

The irresistible prospect of enormous illegal profits has resulted in widespread violations by information processors. Regulators could also be more adept at policing excesses and irregularities in personal information

[90] Didi announces de-listing from US stock market, marking 'the end of a barbaric growing period for Chinese internet companies', *BBC News Chinese* (3 December 2021) <https://www.bbc.com/zhongwen/simp/chinese-news-59517945> accessed 28 December 2021.

[91] Hu Ling, 'Two Types of Property Right in the Digital Economy from Digital Resources to Digital Architecture' (2021) 6 Peking University Law Journal 1585 (in Chinese).

[92] See Liu Quan, 'On the Principle of Legality, Legitimacy and Necessity of Personal Information Processing' (2021) 5 The Jurist 8 (in Chinese).

[93] In 2019, several regulators in China carried out a joint enforcement action to probe the following topics: 'undisclosed collection and use rules', 'unclear purpose, method and scope of collection and use of personal information', 'collection and use of personal information without the user's consent', 'the principle of illegal necessity, collection of personal information that has nothing to do with the service provided', 'providing personal information to others without the user's consent', 'failing to provide options for deleting or correcting personal information as required by law, or failing to publish information such as complaints, reporting methods, etc'. The regulators evaluated more than 1000 apps and found numerous violations of laws and regulations. There were 6,976 flagged questions about the use of personal information. See Cyberspace Administration of China, Ministry of Industry and Information, Ministry of Public Security, State Administration for Market Regulation, Special Report on APPs' Illegal Collection, and Misuse of Personal Information (2019).

processing activities. While both the CSL and DSL demand compliance with security regulations concerning the export of key data, yet even by the time of the 'Didi' case, no data export security assessment system had been established,[94] neither was any cybersecurity review ever initiated. Moreover, both regimes focus on the impact of data processing on national security, which is a concept too inherently vague and for which sound evidence and careful judgment is required. This means that lengthy investigations and political entanglements are inevitable, thus precluding a timely response to possible violations.

Conclusion: toward the systematization of data law

Legislative developments should be in sync with the significance, urgency, and ripeness of the issues it seeks to address. Yet, the DSL was only enacted 5 years after the enactment of the CSL, and it took 10 years for the PIPL be enacted after the expert proposal draft was published in 2003. Only now has the flurry of legal development in this field arrived, influenced in no small part by national political priorities and setbacks owing to the irreconcilable competing interests of stakeholders. It is also necessary to observe that because the Chinese legal system has developed by way of gradual, discrete legislative evolution, this has inevitably led to disagreements and misunderstandings surrounding the data law regime.

First, under the basic framework of data law, the objects of regulation overlap to a large extent. Most importantly, concepts of data, network data, information, and personal information overlap considerably in substance. They co-exist in the same domain of law, posing challenges to both the theoretical conceptualization of data law and its application for two reasons.

One reason is that big data and fast-evolving algorithmic technology may now render personalized decisions about a particular individual without the need to convert data into information. Failure to regulate such data as personal information will have the adverse effect of eroding the concept of personal information. Another reason is that the widespread use of computer technology and cloud-based data storage has caused substantial overlap within the regulatory regime of data law. For instance, both narrowly defined data under the DSL and personal information under the PIPL are now generally collected, processed, and stored via computer networks. This high degree of overlap causes the CSL to almost always be triggered simultaneously with the DSL or PIPL when it comes to data issues, resulting in confusion and repetition in the application of the law.

The *NDS Regulation* published by the CAC addresses this issue and functions as a common supporting rule so to minimize overlap in the application of the CSL, DSL, and PIPL. It provides that not more than one data regime would apply in respect of certain issues such as data-sharing rules, the response mechanism in a data security emergency, and data export security assessment.

Secondly, although data classification and grading elucidate how data law can be constructed, it does not account for the practical aspects of data processing and raises questions of legal application. While it starts off by categorizing data into different sectors, fields, and stakeholders, this presupposes that the classes and grades of data can be identified even before such data are created and processed. However, the information produced by data analytics is often beyond prediction, and the importance of data changes as it increases in volume, interacts with other data sets, and as data analytical capabilities evolve.

Furthermore, the objective of data classification and grading is to set out legal requirements of varying severity so to balance data protection with the interests involved in the analysis and flow of data. Effectively, it situates a piece of data in horizontal and vertical coordinates and ascertains the applicable law, but the coordination between the two dimensions often raises questions. As mentioned above, the PIPL distinguishes between 'general personal information' and 'sensitive personal information'. The *Civil Code* distinguishes between 'private information' and 'other personal information' and provides in Article 1034, paragraph 2, that 'private information in personal information shall be governed by the provisions on privacy right; where there are no provisions, the provisions on the protection of personal information shall apply.'

At this point, a dilemma arises as to how the rules protecting private information under the right to privacy relate to the rules protecting sensitive personal information under the personal information protection regime.[95] (i) The protection of private information under the right to privacy is not necessarily more robust than that of sensitive personal information under the rules for personal information protection.[96] The right to process private information lies either in the legal provisions or the

[94] In 2017, the CAC published the *Measures for the Security Assessment of Personal Information and Key data to be Transmitted Abroad (Exposure Draft)*, but no further progress was made. It was not until October 2021 that the CAC published the Export Measures.

[95] See Wang Liming, 'Basic Issues in the Protection of Sensitive Personal Information——Based on the Interpretation of the Civil Code and Personal Information Protection Law' (2022) 1 Contemporary Law Review 6 (in Chinese).

[96] On special protection for sensitive personal information, see Sun Qingbai, 'The Special Institutional Logics of Sensitive Personal Information Protection and Its Regulation Strategy' (2022) 1 Administrative Law Review 119 (in Chinese).

express consent of the right holder (Article 1033 of the *Civil Code*). The processing of sensitive personal information also requires the individual's consent (PIPL, Article 29). Moreover, while the right to process sensitive personal information is limited to what is necessary to satisfy a specific purpose, there is no such limitation on the right to process private information. (ii) Under the personal information protection regime, individuals enjoy the right to, among other things, consult, copy, transfer, and delete personal information. In contrast, these positive rights are not available under the right to privacy. (iii) The relationship between the *Civil Code* and PIPL is also subject to heated debate.[97] It is doubtful whether the civil law provisions can decide the sequence in which the *Civil Code* and PIPL should apply.

Thirdly, the relationship between the laws governing data security and those governing national security is unclear. As mentioned above, the overall goal of data law is to ensure the physical and juridical security of data, which are collectively referred to as 'data security'. The CSL and DSL both explicitly prescribe the maintenance of national sovereignty and security as their legislative purposes; similarly, the personal information protection system under the PIPL also involves data security. In that case, are these three laws subordinate to the National Security Law ('NSL'), the fundamental law for the maintenance of national security?[98] Some scholars argue that 'cybersecurity should not be considered merely as the security of the cyber domain or information system – cybersecurity should be the national security in the cyber era'.[99] Similarly, some scholars advocate that 'in the context of the future co-existence of DSL and PIPL, DSL should be grounded in the protection function of public security and national security. The protection of personal security will fall upon PIPL.'[100] Other scholars, however, hold the opposite view that while NSL mainly safeguards sovereignty and political security, the DSL is concerned with protecting the legitimate rights and interests of citizens and organizations and promoting the development of the data industry.[101] The unclear relationship between data law and the NSL affects the status of data law in the Chinese legal system. Furthermore, if the CSL and DSL, two laws explicitly concerned with security, are subordinate to the NSL in the field of national security, it raises the question of whether the PIPL could still be regarded as part of a synergistic whole with the DSL and CSL. The relationship between data laws and national security laws in the Chinese legal system will also affect the formulation of legal rules, that is whether national security should be an interest that is prioritized in data processing.

Fourthly, the redundancy of some rules is also worthy of examination. While the CSL charts out a broad legislative framework governing cyberspace, its broad coverage also belies inadequate rules that fail to provide comprehensive regulation of data processing behaviour and offer very little special protection for network data and network personal information. The existing rules of data regulation under the CSL have been mostly made redundant by subsequent legislation like the DSL and PIPL. As mentioned above, the CSL mainly governs the protection of critical infrastructure, and it relates to data protection insofar it requires enhanced protection of personal information and key data generated by critical information infrastructures (Article 37). However, the DSL and PIPL have similar provisions which are even broader in scope than Article 37 of the CSL. This empties the regulatory role of the CSL insofar as data regulation is concerned, and this outcome falls short of the legislature's goal of using the CSL as a means of providing special protection for network data.

In addition, seemingly separate data security assessment systems for the protection of personal information and key data in fact converge into the same 'Cybersecurity Review System' that is led by the CAC.[102] Furthermore, there is an overlap between the

[97] See Wang Xixin, 'The Three-level Frame and Protection Mechanism of Personal Information Rights and Interests' (2021) 5 Modern Law Science 119 (in Chinese); Shi Jiayou, 'The Private Law Dimension of Personal Information Protection: On the Relationship between Civil Code and Personal Information Protection Law' (2021) 5 Journal of Comparative Law 14 (in Chinese); Long Weiqiu, 'The Basic Law Position and Protection Function of Personal Information Protection Law' (2021) 5 Modern Law Science 84 (in Chinese).

[98] Standing Committee of the National People's Congress, 'National Security Law of the People's Republic of China' (2015). See art 25—'The State shall develop network and information security assurance system, enhance network and information security assurance capabilities, strengthen innovative research and development, and application of network and information technologies and realize the security and controllability of network and information core technologies, critical infrastructure, and information systems and data in key areas; the State shall also enhance network management, prevent, deter and punish network criminal acts such as cyber-attacks, network intrusion, network theft and illegal spread of harmful information in order to safeguard the sovereignty, security and development interests of the state cyberspace.'

[99] See Yang Rong, 'From Information Security, Data Security to Algorithm Security - Legal Governance of the Cyberspace from the Perspective of Overall National Security Concept' (2021) 1 Law Review 132 (in Chinese).

[100] Huang Daoli and Hu Wenhua, 'Situation, Dilemma and Countermeasures of China's Data Security Legislation: Comment on the Data Security Law of the People's Republic of China (Draft)' (2020) 6 Journal of Beijing University of Aeronautics and Astronautics (Social Sciences Edition) 15 (in Chinese).

[101] See Zhai Zhiyong, 'The System Orientation of Data Security Law' (2021) 1 Soochow University Philosophy & Social Science Edition 75 (in Chinese).

[102] See CAC, Cybersecurity Review Measures, revised on 16 November 2021.

Cybersecurity Review System and the Data Export Security Assessment System. The former focuses on 'national security risks that may be brought about by data processing activities and overseas listing', and such risks include 'theft, disclosure, damage, illegal use or cross-border transfer of core data, key data or large amounts of personal information' and 'risks of influence, control or malicious use of critical information infrastructure, core data, key data or large amounts of personal information by foreign governments after overseas listing'.[103] Similarly, the latter also addresses the impact of exporting data on national security by taking into account the above considerations.[104] The overlap between these regimes not only reflects the redundancy of legal norms but also blurs the legal concepts of cybersecurity, data security, and personal information security. This raises pressing questions about whether the respective legislative regimes have achieved their intended goals.

Finally, insofar as legal compliance is concerned, the analysis of the 'Didi' case reveals that it can be difficult for a data processor to pin down which rules are applicable to its practices—whether it is the CSL, DSL, PIPL, or the other accompanying rules. In most cases, a large-scale data processor simultaneously handles a large amount of personal information and narrowly defined data. Personal information may also be converted into key data after anonymization. It could well be the case that more than one legislation is applicable, such as in the 'Didi' case, where the CAC's complaints concurrently involved the CSL, DSL, and PIPL. The latest normative documents issued (of which some are still early drafts) suggest that a prudent strategy for legal compliance would be to first follow the trail of the data processing activities—from collection, sharing, transfer, to cross-border transfer, etc. With this as a starting point, data processors can thereafter establish concrete data protection measures by identifying activities are governed by the applicable legislative regimes.

In conclusion, the awaited advent of the PIPL heralded the establishment of a robust body of Chinese data law. With this development, this article attempts three objectives. First, it has attempted to find the unifying element across the CSL, DSL, and PIPL. Secondly, it has attempted to explore the normative rationale for unifying data law. Thirdly, it has attempted to articulate how each legislation is conceptually distinct and yet are so inextricably linked; these links serve to shape a legal field that is externally uniform and internally coherent. Despite the theoretical possibility of assembling the myriad of data law norms into a coherent system, admittedly, there are bound to be logical inconsistencies, overlaps, redundancies, and uncertainties in the application of these norms. While it must be acknowledged that the contours of data law are obscure and its content still defective for the time being, this ultimately presents itself as an opportunity to tweak and enhance existing rules, paving the way for a more unified data law of tomorrow.

Acknowledgement

The authors wish to thank Chong Fu Shan and Li Ruoqing.

Funding

This research is funded by the Program for Professors of Special Appointment (Eastern Scholar) at Shanghai Institutions of Higher Learning (TP2019001), 'Research on the Rule of Law of Outdated Information in Data Governance', Shanghai Municipal Foundation for Philosophy and Social Science (2021ZFX004), Postdoctoral Project No. 69: 'Interpretation of Public Law Principles on the Processing of Personal Information by State Agencies' (2021M690651).

https://doi.org/10.1093/idpl/ipac004
Advance Access Publication 25 February 2022

[103] Cybersecurity Review Measures, revised on 16 November 2021, art 10.

[104] Export Measures, arts 4, 8.