JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2022, 1–12
https://doi.org/10.1093/cybsec/tyac011
Research paper

Research paper

China's emerging data protection framework

Rogier Creemers *

Leiden Institute for Area Studies, Leiden University, Matthias De Vrieshof 3, Leiden, Zuid Holland, The Netherlands

*Correspondence address. Leiden Institute for Area Studies, Leiden University, 2311 BZ Leiden, The Netherlands.
Tel: +31 71 527 2850; E-mail: r.j.e.h.creemers@hum.leidenuniv.nl

Received 5 November 2021; revised 23 May 2022; accepted 5 July 2022

Abstract

Over the past 5 years, the People's Republic of China has accelerated efforts to establish a legal architecture for data protection. With the promulgation of the Personal Information Protection Law (PIPL) and the Data Security Law (DSL) in the summer of 2021, the first phase of these efforts have been concluded. These will have a significant impact on data flows within China, but also merit foreign attention. They provide a new approach to data protection to be subjected to comparative analysis, and may influence the development of data protection legislation in other states, particularly those with close digital connections to China. Doing so requires a greater understanding of how this legislation is shaped by the Chinese political and economic context. Drawing on a thorough review of government documents, supplemented by Chinese-language academic sources, this article reviews the evolution of the two pillars of China's data protection architecture, from the early stage of fragmentation via the promulgation of the Cybersecurity Law in 2016, up to the present day. It finds that the PIPL and its attendant regulations serve to primarily regulate the relationship between large technology companies and consumers, as well as prevent cyber crime. It does not create meaningful constraints on data collection and use by the state. Even so, the PIPL bears a clear family resemblance to personal data protection regimes elsewhere in the world. In contrast, the DSL is a considerable innovation, attempting to prevent harm to national security and the public interest inflicted through data-enabled means. While implementing structures for this Law remain under construction, it will likely herald a thorough reorganization of the way through which data is collected, stored, and managed within all kinds of Chinese actors.

Introduction

The rapid expansion of digital services, the concomitant increase in data generation, collection, processing, and use, and numerous high-profile security incidents, have thrust data protection questions high on the political agenda in countries around the world, and China is no exception. Even so, China was a relative latecomer to the digital world, and dedicated data protection rules were nearly non-existent until the end of the 2000s. However, since then, China has embarked on a comprehensive legislation drive from scratch, culminating in the promulgation of the Personal Information Protection Law (PIPL) and the Data Security Law (DSL) in 2021.

As China's data protection efforts gained momentum, a few foreign researchers have devoted scholarly attention to them [1–5]. They primarily approach the topic through a comparative approach, assessing Chinese developments in the light of or in contrast with the US and European data protection. Pernot-Leplay, for instance, analyses the Chinese data protection model as a "third way" between the privacy-driven European approach and the market-oriented US conception. This is understandable: Chinese scholars and experts, several of whom have played a role in drafting laws, regulations, and standards, generally acknowledge the lessons China has derived from the European and US approaches [6–9]. However, as Don Clarke warned, using Western legal frameworks to make sense of Chinese developments risks creating blind spots concerning those elements of the Chinese legal order not easily captured in Western legal theory, but which may be crucial to understanding law is conceived and drafted, implemented, and enforced [10]. Furthermore, legal developments do not occur in a vacuum, but must be situated in the broader societal, political, and economic context in which they occur. Mere reference to potentially comparable legislative developments elsewhere can only illuminate a small part of the puzzle.

In the current literature on data protection and China, this has led to at least two important, connected oversights. A first one is the very existence of the DSL, which has not yet received significant academic scrutiny. This Law will form the cornerstone of a legal regime creating a comprehensive protection matrix for all data, personal or otherwise, from the perspective of national security and the public interest. Among major cyber powers, this undertaking is unique and therefore not easily susceptible to comparative analysis at this point in time. Second, there is a conceptual point: the current literature exclusively analyses data protection legislation in China using the concept of "privacy." In both the US [11] and the European Union [12], privacy and data protection are closely connected terms, generally referring to the prevention of harm against individuals through the use of information connected with them, for reasons including ensuring constitutional and consumer rights. In other words, the concept of privacy is often associated with liberal rule-of-law and economic values. Again, Chinese scholars too have devoted considerable attention to privacy from different perspectives [6, 13, 14]. However, "privacy" is not just an analytical concept, it is a term of art in Chinese law with very specific connotations, as will be discussed below. It does not have the constitutional status it enjoys in Europe or the USA. Indeed, the very notion of a fundamental right is absent in China's teleological, instrumental legal environment [15–18]. In short, current research suggests the Chinese data protection regime is a newly emerged but close relative of long-established systems from elsewhere in the world. But this framing obviates many of the factors animating Beijing's drive toward protecting data, the objectives it tries to achieve, and the context in which these developments takes place. While there will be obvious similarities with other legal systems, this article claims it is worthwhile understanding the distinctive particularities of the Chinese approach on their own terms, without resorting *a priori* to comparative or concept-driven analysis.

If realizing constitutional principles or liberal values is not the objective of the Chinese data protection regime, what then is its prime mover? This article argues that the answer must be sought in the Chinese policy of "cybersecurity and informatization." Chinese legislation and regulation are inextricably linked with the "bigger picture" (*daju*) of the project that the Chinese Communist Party aims to achieve. Overall, its major objectives are restoring China to a position of wealth and strength *(fuqiang*), but the specific policy implications of this have varied and evolved over time. In 2014, Xi Jinping announced a drive to turn China into a "cyber power" (*wangluo daguo*) through the combination of informatization, the introduction of digital technologies in social, economic, and political life, and cybersecurity. In other words, informatization is concerned with the realization of positive plans and policies that leverage digital capabilities for national development goals, which include economic growth and effective governance, applied by both the state and private actors [19]. Cybersecurity, in turn, forms the protective exoskeleton around this sphere of development, defending against vulnerabilities that hostile actors might exploit. Illustratively, the Chinese definition of cybersecurity does only not focus on more technical matters, such as the confidentiality, integrity, and availability of network systems and the data they contain as the US and European definitions do, but on the harm they might inflict on China's polity, economy, and society [20]. In Xi's definition, they are inextricably linked, as "two wings on the same body, two wheels of the same vehicle."

This paper suggests that the two pillars of China's data protection regime, the PIPL and the DSL, largely map onto the distinction between informatization and cybersecurity. In designing them, the Chinese government has sought to create an architecture that categorizes risks, threats, and data-related relationships between actors, and manage them accordingly. Although there is some overlap, the PIPL's primary objective is to regulate and balance the relationship between individuals and the entities collecting and using data that makes them identifiable. The DSL, on the other hand, cares little about the horizontal relationship between data subjects and controllers, but focuses on creating a comprehensive architecture to assess and manage the potential risk emanating from every single piece of data held in China, particularly against forces inimical to the integrity of the Communist Party-led regime at home and abroad. As such, it forms part of the trend of securitization of the digital sphere central to the cybersecurity and informatization efforts since 2014 [21, 22].

However, these two pillars did not appear fully fledged *ex nihilo*. They are the result of years of gradual evolution, influenced by shifts in external factors and the resolution of intellectual debates, but also by political factors including turf battles between different ministries with overlapping jurisdictions and opposition from China's tech giants. The resulting framework, thus contains compromises, responses to perceived problems, and legacy components of earlier iterations and mechanisms. Consequently, this paper adopts a process-tracing approach, in which it charts the trajectory through which the data protection regime came into being. Drawing on a comprehensive review of regulatory documents and policy plans, as well as the Chinese-language academic literature, it divides this history in three periods. First, it reviews the early beginnings of fragmentary notions of and mechanisms for data protection up to the promulgation of the Cybersecurity Law (CSL) of 2016, which outlined the foundational mandates for data protection. This includes the genesis of the public security-oriented multi-level protection system (MLPS) as well as the separation of data protection from privacy. The second phase encompasses the period between the CSL and the more extensive and specialized provisions of the DSL and the PIPL, during which there was a considerable back-and-forth between different regulators, resulting in several abortive regulatory initiatives, as well as technical data protection standards. The third stage reviews the content of the DSL and PIPL themselves, and discusses the future direction of developments of the data protection architecture they establish. The conclusion discusses the relevance of China's data protection regime for the broader data protection literature. Not only is the Chinese case worth studying in view of China's large online population and powerful tech companies, it also contains elements meriting further comparative and theoretical study.

The Genesis of Data Protection in China (1994–2011)

The development of data protection regulation has, to a significant degree, reflected the evolving perceptions and concerns of the Chinese leadership concerning the rapid introduction of digital technologies in China's state, economy, and society, and the potential impact of various forms of data abuse. This process contains various intertwined strands, each with associated risks and regulatory responses. A first one is the emergence of digitized government systems, starting with the "Golden Projects" of the 1990s [23] and continuing at present with a new Five-Year Plan for Governmental Informatization [24]. These projects intended to make the Chinese state becomes more efficient and effective at fulfilling its various tasks, ranging from public services to maintaining social stability. This requires that Chinese government authorities are able to obtain the data—including personal information—they deem necessary to do so. A second one was the development of a digital economy driven by large platform companies, whose business model was largely built on the exploita-

tion of large amounts of user data. Third, as the economic value of data rose, a large black market arose in which corporate and governmental insiders traded personal information at scale. Fourth, as informatization advanced, the vulnerability surface of data-related or enabled leaks, hacks, and attacks grew as well.

Legislative responses to these evolutions were slow in coming, with basic and broad frameworks only put in place at the end of the 2000s. Unsurprisingly for a political organization that prizes secrecy and information management, the Party leadership devoted attention to securing network information security nearly straight away. In 1994, the Ministry of Public Security (MPS) was mandated to develop a tiered approach that would impose differing levels of requirement based on the importance of specific network systems [25]. However, it would take over a decade for this "multi-level protection system" (MLPS) for information security to come into being. At first, it prioritized confidential government information [26] and later came to include "State secret information, the proprietary information of legal persons, other organizations and citizens, as well as public information, and information systems storing, transmitting and processing this information [27]." Finalized in 2007, the MLPS contained five security protection tiers, with higher tiers incurring increasing requirements and governmental scrutiny. The MLPS did not protect data *per se*. Rather, it formed a graduated protection regime for all network systems that protected them in their entirety, including their data. However, the MLPS laid the groundwork for the introduction of the DSL regime over a decade later. It constructed an institutional and conceptual framework for the protection of digital assets from the perspective of "national security, the lifelines of the economy and social stability [26]."

In the realm of personal information protection, developments were highly fragmented and remained embryonic. During the 1980s and 1990s, several laws and regulations had mandated maintaining the confidentiality of individual information in specific sectors, such as banking and legal services [28]. As China's informatization drive gained traction in the 2000s, the State Council Informatization Office commissioned Zhou Hanhua to lead the drafting of a legislative proposal for personal information protection, which was published in 2006 [29]. This "Expert Suggestion Draft" laid down 10 principles for data protection, similar to international privacy agreements and laws in Europe and Asia [1]. It also addressed data collection and processing by government bodies, This section contained fairly strict limitations on data collection as well as a requirement to register collection processes with a relevant agency in charge, although wide exceptions were included for areas such as security and policing. Third, it addressed data collection by "other data processors" in the private sector, requiring them to register with an appropriate authority. Fourth, it included restrictions on cross-border transfer of personal information, but only for private sector actors. In terms of enforcement, the Draft did not call for a dedicated data regulator, but resorted to a mix of complex administrative enforcement and judicial enforcement processes. However, Zhou's proposal was never adopted as formal legislation.

The piecemeal regulatory efforts that took place were largely reactions against specific salient forms of abuse that had started to emerge. The 2009 revision of the Criminal Law included, for the first time, provisions on the unlawful sale of personal information by government personnel or by financial, telecommunications, transportation, education, and healthcare institutions, as well as the theft or illegal acquisition of such information [30]. In 2011, the People's Bank of China issued a circular on protecting individuals' banking and financial information. Amongst others, this required that personal information collected in China should be stored within the country [31], the first instance of mandatory data localization. The same year, Ministry of Industry and Information Technology (MIIT) released regulations for Internet information services that instituted the principles of informed consent and necessity for data collection and use, created obligations to notify authorities of serious data breaches, and gave users the rights to revise and delete their personal information. They also prohibited online service providers from transferring or trading personal information. These regulations clearly indicated that the online economy had gained priority in personal information protection, but their enforcement strength was limited: the highest punishment that could be imposed was a fine of 30 000 Yuan [32]. MIIT supplemented these regulations with a 2013 technical standard that, for the first time, contained clear terminological definitions and basic norms [33]. Although this document was not legally binding, it nevertheless carried considerable normative authority.

In the separately developing area of privacy, initial notions derived from the right to reputation present in the 1986 Civil Code were developed by the Supreme People's Court, followed by protections of confidential and private personal affairs in the Civil Procedure Law, and aspects of privacy of vulnerable groups such as minors and women [28, 34]. These provisions reflected a particular reading of privacy rooted in traditional notions of shame and decency, under which certain information should not be made public [13, 35]. However, this notion expanded to encompass the individuals' autonomy to decide which aspects of their private lives they voluntarily disclosed. As such, privacy became part of a broader category of "personality rights" (*rengequan*) [36]), which also included matters such as the right to life and health, naming and portrait rights, and reputational rights. These rights were primarily seen as a part of civil law, and were included in the 2009 Tort Law [37]. However, no definition of privacy was provided, and the Law only contained one related specific provision, on confidential healthcare information.

Stumbling a More General Data Protection Framework (2012–2018)

From 2012 onward, the Chinese leadership has strived to centralize data governance, and create more generalized legislative frameworks, moving away from sector-specific, piecemeal interventions. This mirrors an overall trend in which digital regulation has been centralized, including institutional concentration of digital competences in the newly established Cyberspace Administration of China (CAC) [38]. The dominant driver for this was the rapidly growing need to govern problematic practices in the burgeoning platform economy, and the equally swift expansion of illegal data trading and other forms of abuse, particularly following the introduction of affordable mobile devices. In June 2007, only 16% of the Chinese population was online. This number rose to 70% in 2022, over 90% of whom are primarily mobile users [39]. The smartphone has facilitated the emergence of a business landscape dominated by the giant platform companies such as Alibaba, Tencent, Bytedance, Pinduoduo, and Didi, who have based their commercial models on their ability to collect and analyse user data to maximize profit and market share [40]. E-commerce revenues grew by over a hundredfold between 2011 and 2019.

On the whole, the Chinese government was highly supportive of these developments. In 2015, it issued an action plan on big data, which stated that data had become a "basic strategic resource" [41]. Yet during that period, data-related abuse became rampant as a black market for personal information emerged [42, 43]. Receiving cold calls for targeted goods and services became a regular occurrence in

Chinese daily life, much of which resulted from the illegal sale of personal information by corporate employees and contractors [44, 45], as well as government officials and departments [46]. One particularly prominent case was that of the 18-year-old Xu Yuyu, who died of a heart attack in 2016 after she was swindled out of her college tuition money in a telephone scam [47]. Other forms of online fraud equally grew rapidly [48, 49].

Consequently, developments between 2012 and 2016 largely focus on consumer protection and enforcement. An undercurrent during that period was the beginning of data securitization, as worsening relationships with the USA as well as increased concerns about terrorism at home drove authorities to devote greater attention to controlling the flow of online data. In the wake of the Snowden revelations and the use of personal information in the Russia-attributed interference in the Trump election, it had become clear that the lines between protecting personal information for the sake of the individual interest, and its potential relevance for national security, had started to blur. Rapidly, new data localization requirements were imposed in fields ranging from the credit, mapping, and healthcare sectors to online publishing and cloud services [50]. As the scholar Hong Yanqing, who would later lead the drafting of new technical standards for personal information protection, noted: "the huge amount of user information held by Alibaba, currently covering over 400 million users, is certainly personal information […] but because of its scale and granularity, it can also match the public security organs' basic national population database and even surpass it in accuracy. For the country, any eventual leak or damage of this scale of basic population data could create a serious threat to national security" [51]. This trend stimulated the drafting of the National Cybersecurity Strategy as well as the CSL. The latter contained a section on personal information protection, as well as the first mention of the term "important data," that would evolve into the DSL [52]. Yet, the implementation of the CSL would be hampered by multiple factors. The MPS was loath to transfer its data-related competences to the CAC, resulting in tussles over bureaucratic turf and overlapping claims to mandate. China's tech giants also opposed the introduction of stricter privacy laws. Tencent's TISI research institute, for instance, published repeated articles arguing that General Data Protection Regulation (GDPR) and Europe's stricter stance more generally had impeded the success of European online businesses [53]. As a result, no significant implementing regulations for the CSL were adopted in the data protection realm.

Strengthening responses to online data concerns

A first step toward a more comprehensive form of protection came in 2012, when the National People's Congress Standing Committee issued the Decision on Information Protection [54]. It reiterated the data theft prohibitions from the Criminal Law, incorporated the principles of the 2011 MIIT regulations and made them generally applicable, and prohibited unsolicited electronic communications. In terms of remedial measures, it created an obligation for online businesses to delete published personal information, or address related infringement in other appropriate ways. For the first time, it also addressed data use in government departments, prohibiting them from leaking, distorting, or selling personal information. However, these measures were part of a broader programme to impose greater control over the online sphere more broadly. The Decision required online businesses, for instance, to exercise greater control of user-generated content, and imposed real-name registration for telecommunications services. They also did not contain explicit provisions on enforcement, nor did they create or appoint a data protection regulator. As a result, the only non-criminal enforcement body was MIIT, who had little resources for doing so. Potential administrative punishment, except in criminal cases, thus remained lenient.

The Decision coincided with a strengthening of enforcement efforts. In early 2013, the Supreme People's Court, Supreme People's Procuratorate and MPS issued a notification that pushed police, prosecutorial, and judicial bodies to tackle personal data infringement more strictly, through the application of criminal prosecution. This Notice particularly focused on "a flood of illegal trading of citizens' personal data on the Internet," resulting in "telecommunications swindles, network swindles, extortion and blackmail, kidnapping and illegal loan repayment demands [55]." Targets included personnel of State bodies, financial, telecommunications, transportation, education, and healthcare work units, as well as other commercial enterprises. In support, the 2015 revision of the Criminal Law broadened the hitherto narrow basis for criminal prosecution included in the 2009 version. All illegal data sale, provision, theft, or illegal acquisition now fell under its remit, as long as they met a threshold of "grave circumstances." Maximum prison sentences increased from 3 to 7 years [56]. The Decision also led to more detailed regulations for the online services markets [57], and to the inclusion of personal information in the revised Consumer Protection Law [58]. Even so, legislative developments suggested that there was no complete consensus on specifics. For instance, the draft Anti-Terrorism Law contained an obligation to localize personal information of telecommunications service users [59], but this was dropped in the definitive version.

The CSL: integration without detail, obstacles in implementation

The CSL, which came into effect in 2017, forms the cornerstone of a new and comprehensive regime that seeks to secure the Chinese digital sphere and integrate cybersecurity-related policy areas and the bureaucratic actors involved. It encompasses elements ranging from content control to critical infrastructure protection, and from security of network products to cyber incident response. It also incorporated the MLPS, and created a first legislative basis for the two strands of data protection. First, the law incorporated the substantive provisions from the 2012 Decision. While this represented little substantive evolution, a major step forward was made in enforcement, as non-compliance with personal information protection requirements could lead to punishment ranging from a simple warning to fines of up to 1 million RMB, suspension or closure of websites, or cancellation of related business licences. Second, the law introduced the term "important data," *albeit* without offering a detailed definition. Some debate had preceded this final iteration: an earlier draft had contained the term "important business data." However, as Hong argues, the decision to retain "important data" reflects the legislator's ambition to protect national security and the public interest, as opposed to proprietary corporate concerns [51]. The notion of important data appeared twice in the CSL: a first time to mandate critical infrastructure to store personal information as well as "important data" within Chinese territory. Maximum punishment for breaching data localization rules was set at fines of 500 000 Yuan, provisional or definitive suspension of business, and revocation of business licences and permits [60].

While the CSL did, thus establish a legislative basis for both personal information and data security protection, its succinct treatment left many questions unanswered. In Hong's view, the Law did not "provide systemic thinking, let alone comprehensive institutional designs" [61] to effectively protect data. This is no strange occurrence in

the Chinese legal landscape: a law often only includes basic elements of principle, purpose, and punishment, mandating government departments and local departments to formulate more detailed implementing regulations and technical standards to provide detailed prohibitions, obligations, and procedures [62]. However, the CSL was also vague on which departments would take charge of implementing the CSL. The CAC had been created in order to coordinate and integrate the previously fragmented cybersecurity and informatization bureaucracy [63], and had taken over many of the Internet-related tasks and personnel of MIIT [38]. Accordingly, the CSL appointed the CAC in overall charge of "comprehensively planning and coordinating cybersecurity efforts and related supervision and management efforts," with other ministries responsible for work within their scope of competence. However, as the CSL had not assigned specific competences for data protection, a prolonged turf battle between the CAC and the MPS ensued, in which both institutions sought to claim territory in the data protection sphere to themselves.

Soon after the CSL took effect, the CAC issued regulations on critical infrastructure protection, which provided greater detail on the CSL's data localization requirements for personal information and important data [64]. Furthermore, these indicated that "work units providing cloud computing, big data and other such large-scale public information network services" would now fall under the scope of critical infrastructure. CAC also published draft regulations [65] and related technical standards [66] on security assessments for the export of personal information and important data. This draft's stringent provisions went far further than the GDPR or the APEC's Cross-Border Privacy Rules and would have made much of the data flows occurring within multinational companies operating in China illegal or onerous. They also went further than the CSL itself: where Article 37 only required critical infrastructure operators to undergo data export reviews, these measures applied to all "network operators." In response, the USA filed a formal protest in the World Trade Organization [67]. From the Chinese perspective, however, existing cross-border data regimes insufficiently considered national strategic concerns [68]. Even so, the regulations also met with resistance from Chinese e-commerce operators, on whom the measures would have imposed considerable compliance costs [69]. After a third draft was reportedly circulated among domestic stakeholders, the project was quietly dropped.

A total of 2 years later, CAC tried again, with a draft on cross-border transfer of personal information that retained most of the 2017 version's provisions and added greater detail on required content in data transfer contracts, reports, and audits [70]. Another draft document addressed the management of data security in general, covering a both personal information and "important data," which it defined as "data that, if divulged, may directly affect national security, economic security, social stability, or public health and safety, such as undisclosed government information or large-scale data on the population, genetic health, geography, mineral resources, etc." Standard corporate data would be excluded from this category. The draft covered a whole range of points that would be included in the PIPL, such as algorithmic content decisions on social platforms, as well as some points that would end up in the DSL, including data export security review processes. It even regulated the Internet addressing system, prohibiting domestic online traffic, or domestic users accessing domestic websites, to be routed abroad [71].

The MPS equally tried to gain greater weight in data protection. Marking its first foray into personal information, it issued guidelines on how to create internal management mechanisms and operational workflows for their protection, as well as regulating concomitant technical processes [72]. These measures partially overlapped with technical standards for personal information protection that had been drafted in the wake of the CSL. MPS also updated the MLPS [73], greatly expanding the role of data in terms of assessing the security classification tier of specific network systems.

However, none of these draft regulations, from either CAC or MPS, ever passed and took effect, largely rendering toothless the data protection provisions of the CSL. As it turned out, passing the CSL as an act of political virility had not laid an adequate basis for the creation of a detailed and practicable data protection architecture. Only one CAC initiative on data protection, provisions for children's personal information, came into force during this period [74]. For the time being, the most impactful progress was made in the fields of technical standards and sectoral self-regulation. These emerge from institutions in which companies and experts have a greater say: standard-setting bodies such as Technical Committee 260 (TC260), which oversees information security standards, and the Internet Society of China (ISC), which is the sectoral association for the digital industry. Both are closely associated with government: TC260 falls under the authority of CAC while the ISC is responsible to MIIT.

In December 2017, TC 260 issued the (unfortunately acronymed) Personal Information Security Specification [75]. Drawing clear inspiration from the GDPR, the Specification provides highly detailed definitions of important terminology, as well as procedural guidelines for information collection, storage, use, transfer, and incident response. In this sense, it goes far beyond the sparse provisions of the CSL. It outlines, for instance, how and under which circumstances data controllers should obtain consent, how to identify and handle sensitive information, and how to minimize the duration of data storage. Amongst others, it addresses points such as personalized display of information, specific functions ranging from ride hailing and transport ticketing to express parcel shipping. It has been joined by two related standards, one on de-identification of personal information in 2020, and one on personal information security impact assessment in 2021 [76]. For its part, the ISC issued a voluntary proposal on self-regulatory norms on personal information protection in 2018 [77].

Taking the Initiative in Data Protection: the DSL and PIPL

While the implementation of the data-related mandates of the CSL was stalled, the perceived importance of data in economic, social, and governmental processes continued to grow. In 2020, the Central Committee officially determined data to be a factor of production, on par with land, capital, and labor as essential to development. Simultaneously, demand continued to grow for more effective data-related regulation, particularly with regard to the data-driven business models of China's large online platform companies. Concerns had become prominent that algorithmic decision-making and content presentation could have on content distribution as well as related undesirable consumer conduct, such as shopping addiction. Again, the first initiatives here were piecemeal and reactive. Lacking a formal regulatory basis for enforcement, CAC used the existing technical standards to justify enforcement actions against Ant Financial [78], Baidu, and Bytedance, despite those not having legal binding force. These actions illustrated a shift in regulatory focus: where personal information protection efforts had hitherto largely addressed malicious activities such as data theft, the business models, and practices of China's tech giants now came under growing scrutiny. In a telling episode, Baidu CEO Robin Li came under fire after claiming Chinese Internet users did not care about privacy, and that Baidu could use their data as they chose to "exchange privacy for safety,

convenience or efficiency" [79]. The 2018 E-Commerce Law specified that where these companies used personal information-based targeted recommendations and advertising, an opt-out option had to be provided [80].

Yet at the same time, some interdepartmental frictions were ironed out. In 2019, the CAC, MIIT, MPS, and the State Administration of Market Regulation (SAMR) jointly oversaw the creation of an "App Governance Working Group" (App *zhuanxiang zhili gongzuozu*), comprising TC260 and several industry associations. Throughout the year, this Group released several standards and regulations on information collection and use in mobile apps [81]. Personal information protection was one focus point of repeated online enforcement campaigns by the MPS. One such example, the "Clean Net 2019" (Jingwang 2019) campaign, resulted in 2868 prosecuted cases involving 7647 suspected criminals [82]. Since then, the Group has conducted a continuous campaign against apps, identifying and either castigating or punishing dozens of companies, including well-known names like Baidu and Tencent [83]. In 2021, the Group issued further clarifications, determining the kinds of information that common kinds of mobile apps were permitted to collect under the principle of necessity [84], while its member MIIT circulated provisional general regulations on personal information protection in mobile apps for the solicitation of comments [85]. As such, the App Working Group demonstrated the participating bodies' ability to cooperate constructively for a prolonged period of time.

Meanwhile, within the central government, strong momentum was building for a more integrated approach toward the digital economy that would proactively shape, rather than reactively respond to, online business models. Starting in late 2020, regulatory bodies took a series of measures to better regulate competition between large platforms, fintech operations, listing on stock exchanges, and new forms of content, amongst others [86]. The PIPL, drafted between 2018 and 2021, bears clear imprints of these trends. The DSL, drafted in tandem, reflects an accompanying concern: a much greater focus on national security [87], including in the digital realm. Here, China seeks to harden networks and the data they store against as yet unforeseen threats and ensure both Chinese government institutions and business have shored up their cybersecurity practices.

The PIPL

The PIPL was passed in August of 2021, taking effect on 1 November [88]. In terms of substance, it represents further incremental evolution of the trends set by the CSL, and some of the advances made in technical standards and draft regulations, but in far greater detail and a far broader scope of application. For instance, the CSL's provisions on personal information protection only cover "network operators" in general, and only critical information infrastructure operators where data localization was concerned. The PIPL applies to all "personal information protection handlers," which includes governmental as well as corporate entities. As a result, provisions on consent needed revision: the CSL imposed consent as an absolute requirement for data collection, where the PIPL also includes necessity in response to sudden public health incidents and other emergencies, reasonable news reporting and public interest-oriented activities, and the catch-all provisions of "other circumstances provided in laws and administrative regulations." Data localization requirements are broadened to include all businesses handling personal information meeting particular quantitative thresholds, and all government bodies. Where data export is permitted, the PIPL requires passing a CAC-organized security assessment, obtaining certification from an accredited body, or concluding a contractual agreement with the foreign party that the PIPL's standards are met. The PIPL also makes a major step forward in enforcement provisions: in contrast to the 1 million Yuan maximum fine that could be imposed under the CSL, the PIPL allows fines of up to 50 million Yuan or 5% of the affected business' annual revenue.

The PIPL also contains extraterritorial elements, similar to foreign legislation such as the GDPR. For instance, the law may apply to the provision of products and services to, or conducting analysis of the activities of individuals in Chinese territory. It provides for the export of data in legal assistance, but only on application. Perhaps most importantly, reflecting the growing tensions between China and the Western world, the PIPL introduces tripwire provisions aimed at foreign private and governmental actors. On the one hand, foreign organizations and individuals who harm Chinese citizens' interests or the Chinese public interest through abusing personal information may be blacklisted by CAC. On the other, the law allows the central government to adopt retaliatory measures against foreign governments imposing discriminatory prohibitions or sanctions against the People's Republic.

While the most important function of the PIPL is to regulate online services, it also contains general provisions applicable to government departments' collection and handling of personal information. Here, a balance is sought between the need to discipline government departments, most of whom are tasked with banal tasks such as motor vehicle registration, and the need to ensure that police and security services are not impeded in their surveillance activities. To that end, the law requires that state bodies obtain consent for data collection, except where secrecy needs to be protected according to laws and regulations, or where such consent would impede the fulfilment of statutory duties and responsibilities. Following the long interagency turf war over data protection, the PIPL appoints CAC in charge of "comprehensive planning and coordination" of personal information protection, with assistance of other ministries where required. However, while the Law outlines a series of powers the CAC and related departments may exercise, it stops short of appointing a dedicated data protection regulator.

To summarize, the PIPL primarily seeks to thread the needle between three different objectives: protecting individuals from malicious or improper data collection and use, mostly by companies; stimulating the development of the digital economy, and safeguarding the public interest as Beijing defines it. Rather than creating fundamental rights or general legal principles, it does so by regulating different categories of actors and the relations between them in a highly detailed manner, depending on the potential perceived risks or harms that may arise. A secondary consideration may be to gain greater foreign recognition for data protection efforts, and facilitating international cooperation on personal data flows. Third, it still enables domestic security and police services to collect and process data for their stator purposes, as well as the use of personal information in other major state projects such as the Social Credit System.

The DSL

In contrast to the PIPL, which resembles personal data protection regimes elsewhere, the DSL, passed in June 2021, creates a new form of data regime, i.e. unique to China. The DSL not only covers personal information, it covers all data excluding state secrets [89]. Where the PIPL is primarily concerned with the relationship between a data subject and a data controller, the DSL focuses on national security and the public interest. For this reason, the National Security

Council is in overall charge of its implementation, with MPS and CAC playing a supporting role.

Where the PIPL intends to provide actionable provisions for businesses, the DSL is more programmatic, calling for the establishment of a strategy involving the "intelligentization" of public services, research into data development and technology, the formulation of data-related standards, the promotion of a cybersecurity industry, the establishment of data trading markets, and data-related education. In terms of regulatory architecture, the DSL proposes a categorized and tiered data protection system, where data is classified on the basis of "degree of importance to economic and social development; and […] the impact on national security, the public interest, or the lawful rights and interests of citizens or organizations if it is falsified, destroyed, leaked or illegally acquired, or illegally used." Furthermore, the DSL creates a new category, of "core national data" (*guojia hexin shuju*), which covers data related to "national security, the lifelines of the national economy, important aspects of people's livelihoods, major public interests, etc." This category remains distinct from "important data," which was never quite clearly defined since its first use in the CSL. Where it comes to data classification, the DSL charges local governments and regulators with drafting catalogues for their own regions and sectors. On this basis, the DSL specifically calls for the creation of three mechanisms, one for data security risk assessment, reporting, information sharing, monitoring, and early warning; one for emergency response; and one for data security review. The latter may review any data handling activity possibly affecting national security, without a possibility of appeal. Furthermore, with regard to the outside world, the DSL implements export controls for specific data categories, and reiterates the anti-sanction tripwire clause also present in the PIPL. Furthermore, the law also heavily circumscribes the provision of data to foreign judicial and law enforcement bodies.

Subsequently, the law addresses the obligations of data handlers, and the role of digital security in e-governance. These sections explicitly include the MLPS as the basis for performing data security obligations, regular risk assessment, and an obligation on individuals and organizations to cooperate with public and national security bodies who need to obtain data in the course of their duties. Government will charge ahead with e-government, but the DSL creates the foundation for a disciplinary framework to assess whether individual departments correctly fulfil data protection requirements.

In contrast to the focus on harm to individuals in the PIPL, the DSL this mainly strives to reconcile or balance two competing elements of the collective interest: national security and development objectives. The DSL is explicit about the importance of data in the reform of China's governance processes and the next step in its economic ascendance. However, it also recognizes that these very processes expand the country's vulnerability surface. The answer it provides is an integrated system covering all data, personal or non-personal, held by individuals, businesses, or government. The practice of classification already has precursors in regulations on scientific and industrial data [90], as well as earlier practice in the MLPS. Yet, the DSL, even more than the PIPL, only provides a basic framework, to which the government departments tasked with implementation must add detail. Considerable debate is ongoing on the best path for classification, for instance, as well as on the different types of harm or risk scenarios data abuse might present [91]. While the general direction of travel is clear, it will take years of further regulatory activity to deliver any appreciable level of detail. One question that will undoubtedly come to the fore is how the DSL and PIPL frameworks interact, and how potential contradictions or tensions between them might be resolved in practice. However, in the fast-moving digital arena, the march of events has necessitated quicker intervention.

General and specific implementing regulations

As with the CSL, the PIPL and DSL create mandates that instruct ministries to regulate. At the time of writing, general implementing regulations for both laws, as well as measures for the export of both personal information and important data have come out in draft. [92, 93]. The former document is mostly concerned with outlining compliance-related details and procedures. For instance, it outlines the timeframes within which companies should respond to cybersecurity incidents and the procedures for submitting breach reports, as well as transparency and notification duties toward individuals. Continuing the wave of regulatory moves against large platform companies, the regulations included an entire chapter outlining specific obligations regarding their data management practices. These go so far as to require specific interfaces in instant messaging software and the use of public identity verification mechanisms. Slightly outside the immediate realm of data protection, the draft reiterates the earlier requirement to not route domestic Internet traffic abroad, and contains one of the first explicit mentions in regulatory text of the Great Firewall, dubbed a "trans-border data security gateway." The provision of tools to penetrate or circumvent this is prohibited. The latter addresses concerns about foreign listing by companies holding personal information and important data, requiring a cybersecurity review to take place before IPOs. This specific concern gained public prominence with the botched listing of ride-sharing platform Didi, as discussed below.

The matrix-type structure of the data protection architecture means sector-specific regulation is also starting to emerge. One particular emerging area of priority is personal transportation. In June 2021, following increasing concerns about the potential security ramifications of the cameras, radars and sensors in Tesla vehicles, the CAC published draft regulations on data security in automobiles. This document covers both personal information and important data, with the latter category including national security-related information such as people and traffic flows in military or other sensitive state facilities, as well as mapping and survey data in general [94]. Again, this document creates an explicit link between the MLPS, and requires the domestic storage of all data. Soon after, the Cybersecurity Review Office created under a CSL mandate launched its first investigation, against the popular ride-hailing app Didi, citing concerns over national data security risks [95]. A total of 2 days later, CAC ordered that the popular ride-hailing app Didi be removed from app stores for "grave issues of collecting and using personal information in violation of laws and regulations" [96]. This ban came mere days after the company had completed its IPO on the New York Stock Exchange, as the latest in a long line of Chinese tech companies listing abroad under the legally dubious VIE construction [97]. Investigations for national data security concerns were also launched into three other companies that had recently listed in the USA: trucking companies Yuanmanman and Huochebang, and recruitment site Boss Zhipin [98]. These measures were followed by a draft revision of cybersecurity review measures, which explicitly indicated that data handling activities that might influence national security could trigger a cybersecurity review. More specifically, it also introduced a requirement that business holding the personal information of more than 1 million users listing on foreign markets must conduct such a review. Theft, disclosure, and illegal use of core, important, or large amounts of personal data, as well as the use of such data by foreign govern-

ments after listing on a foreign stock exchange were included as part of the risks to be reviewed [99]. With these measures, the automotive industry joins banking and healthcare as sectors with dedicated data protection frameworks, and more are likely to follow.

On the one hand, these steps blur the boundaries between personal information and data security protection, yet on the other, they clearly integrate data protection with hitherto separate processes, such as foreign stock listings. They also provide a useful first example of how the edifice to be built on the foundation of the DSL and PIPL will function, offering a greater degree of detail and granularity on important questions ranging from data-related definitions and classifications to the balance to be struck between corporate economic interests, individual well-being, and security concerns [100]. Lastly, they reflect a broader sense that Chinese technology companies should be regulated more strictly. Illustratively, well-known Internet entrepreneur Fang Xingdong claimed that an end had come to the "barbaric" growth of China's Internet, and that greater compliance would now be necessary. Moreover, he argued that the VIE structure, a legally dubious but hitherto condoned method for certain Chinese businesses to list abroad, had created not only a legal grey zone but also resulted in "hidden dangers" in national cybersecurity [101]. Perhaps ironically, but just like in the West, some of the shine has come off the prestige of major technology companies. The trend heralded by the DSL and PIPL is thus one of greater scrutiny of their activities, in an attempt to separate out the activities and functions that authorities deem desirable or not, and micromanaging the specific parameters governing them.

Demarcating privacy from personal information protection

A last point is that the relationship between privacy as determined in the Civil Code and personal information protection has been determined with some degree of clarity. Only with the Civil Code's revision in 2020 did an authoritative definition of the term privacy appear in legislation. Specifically, privacy consists of "the tranquillity of natural private persons' lives, and private and confidential (*simi*) spaces, activities and information that they do not wish others to know about" (NPC 2020) [102]. More specifically, it covers both individuals' entitlement to a "tranquil life," protecting them against unsolicited phone calls, text messages, e-mails, and other such communications, as well as entry into or disclosure of private residences, observing or disclosing private activities or private body parts, and processing information related thereto. The 2012 NPC Decision [54] had already indicated that privacy and personal information would be dealt with separately, by stating that the State protects "electronic information by which the individual identity of citizens can be distinguished as well as involving citizens' individual privacy." In other words, personal information protection would primarily come to cover questions surrounding identifiability of individuals, and providing them with autonomy over how this information is collected and used. The 2020 Civil Code [102] further underlined this view, by defining personal information as "information recorded electronically or in other ways that can be used, by itself or in combination with other information, to identify a natural person, including the name, date of birth, identification number, biometric information, residential address, telephone number, email address, health information, whereabouts, and the like, of the person." The Code also concisely laid out the hierarchical relationship between privacy protection and personal information protection, establishing priority for privacy protection. As a result, the PIPL operates largely separately from the reputation-based conception of privacy, to the extent that it doesn't even contain a single mention of the term.

Conclusion

Starting in the early 2000s, the Chinese leadership has incrementally constructed a model for data protection adapted to its perceived circumstances and requirements. Perhaps counter-intuitively, given the highly controlling nature of the Chinese regime, it has built up this structure gradually, incrementally, and cautiously. Partly, this can be explained by the complexity of the challenge, interdepartmental wrangling, and the difficulties resulting from the administrative restructuring of the cyber governance landscape. But equally importantly, the Chinese government did not want to nip the initial development of the country's digital economy in the bud by smothering it under an avalanche of regulations. This phase has now come to an end. While the imperative of using data for economic growth and government reform remains important, it is increasingly matched with a willingness of State actors to wield regulatory powers in defence of security concerns that have become ever more prominent.

The Chinese data protection model is built on two pillars: personal information protection and data security. In the former, the government seeks to rebalance the relationship between individual citizens on the one hand, and the businesses and organizations that control their data on the other. While this model resembles, and has derived ample inspiration from, the GDPR, it misses the generality of the European approach: where China has recreated the consumer protection aspect of the GDPR to a significant degree, it has not emulated the European foundational principle that privacy is a fundamental right. Most importantly, the PIPL largely leaves the power of government bodies untouched, as it does not impose any meaningful constraints on their ability to collect and process data. This is not surprising given the instrumental, teleological nature of the Chinese legal system. However, the Law recognizes the need to ensure that data flows and operations within government are properly regulated to prevent abuse and corruption. To this end, the PIPL lays the groundwork for a "disciplinary" approach to government data management, where the data gathering powers, competences, and limitations of individual departments are laid down through administrative regulations and detailed catalogues.

While all major states have fairly detailed protections for classified government information, the Chinese effort to require all data, personal or non-personal, to be assessed in the light of their importance to national security and the public interest, is a global first. Where the personal information pillar shares more than a passing resemblance with existing regulatory frameworks elsewhere in the world, the data security pillar remains, for the moment, unique to China. This has major ramifications both for academic research and policy-making. Future research on the implementation of this law will contribute much to our understanding of its effectiveness, particularly in the light of its overlap with the PIPL. Perhaps most importantly, the DSL tackles head-on a challenge, which has become an elephant in the room for Western policymakers: the fact that digital information has become a source of risk or threat to national and public security in a way not imagined even a few years ago. With the DSL, China is moving first. Perhaps it will make mistakes, but certainly, it is providing answers to questions Western governments have been unwilling or unable to ask. As such, China may well gain influence among third countries grappling with similar issues. The growing aspirations of the Chinese government and Chinese businesses to

play a greater role in the region, through the Belt-Road Initiative and other investment projects, may facilitate such normative influence.

Apart from its potential impact on governments, the DSL also presents an interesting academic challenge. In its approach, it echoes a Chinese definition of cybersecurity, i.e. primarily based on the economic, social, or political harm that information use might inflict, instead of on the more technical approach reflected in the European and US focus on confidentiality, integrity, and availability of networks and data. China's far more substance-oriented approach contrasts with the European efforts to regulate the flow of non-personal data, or the US' reliance on the NIST privacy and cybersecurity frameworks (European Commission 2019). Future research could do much to illuminate the differences and similarities, the strengths and weaknesses of these various approaches. Furthermore, given the continued importance and growing sensitivity of trans-border data flows, researchers might do well to start identifying potential areas of overlap and conflict, in order to develop mechanisms to mitigate those.

Acknowledgements

This work was supported by the Netherlands Organization for Scientific Research (NWO), grant number 016.Vidi.185.200. The author is grateful to Perry Keller, Linda van der Horst, Linnet Taylor, and Frederick Douzet for very helpful comments on earlier drafts, to the Journal of Cybersecurity's two anonymous reviewers, and to Emma Burgers for much appreciated research assistance.

References

1. Greenleaf G. *China's Proposed Personal Information Protection Act*. Privacy Laws & Business International Newsletter. 2008. http://www.austlii.edu.au/au/journals/ALRS/2008/7.html. (11 July 2022, date last accessed).
2. De Hert P, Papakonstantinou E. *The Data Protection Regime in China*. Strasbourg: European Parlement, 2005.
3. Pernot-Leplay E. China's approach on data privacy flaw: a third way between the US and the EU?. *Penn State J Law Int Aff* 2020;**8**:49–117.
4. Geller A. How comprehensive is Chinese data protection law? A systematisation of Chinese data protection law from a European perpective. *GRUR Int* 2020;**69**:1191–203.
5. Han S, Munir A. Information security technology - personal information security specification: China's version of the GDPR. *Eur Data Prot Law Rev* 2018;**4**:535–41.
6. Xu J. Evolving legal frameworks for protecting the right to Internet privacy in China. In: Lindsay J, Cheung T, Reveron D (eds). *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford: Oxford University Press, 2015.
7. Zhou H. Zhou Hanhua: Geren xinxi baohu guannian yanbian de sige jieduan [Zhou Hanhua: the four stages of the evolution of personal information protection concepts]. 2018. https://t.qianzhan.com/daka/detail/181213-ba3cf8ff.html. (11 July 2022, date last accessed).
8. Hong YG Geren xinxi anquan guifan zhende bi Oumeng yu Meiguo geng yange ma? [Is the national standard "Personal Information Security Standard" really stricter than the EU and the US?. 2018. https://www.secrss.com/articles/726. (11 July 2022, date last accessed).
9. Wang L. Ren'gequanfa de xin fazhan yu woguo minfadian ren'gequanbian de wanshan [New developments in human dignity law and the completion of the human dignity chapter in our country's Civil Code]. *Zhejiang Univ Ind Commer J* 2019;**6**:5–19.
10. Clarke D. Puzzling observations in Chinese law: when is a riddle just a mistake. In Hsu S (ed.). *Understanding China's Legal System*. New York: New York University Press, 2003.
11. Boyne S. Data protection in the United States. *Am J Comp Law* 2018;**66**:299–343.
12. Pohle J. Data privacy legislation in the European Union member states - a practical overview. *Comput Law Rev Int* 2018;**19**:97–116.
13. Lü Y. Privacy and data privacy issues in ccntemporary China. *Ethics Inf Technol* 2005;**7**:7–15.
14. Wang H. *Protecting Privacy in China: A Research on China's Privacy Standards and the Possibility of Establishing the Right to Privacy and the Information Privacy Protection legislation in Modern China*. Berlin: Springer, 2011.
15. . In: Creemers R. DeLisle J, Goldstein A, Yang G. The privilege of speech and new media: conceptualizing China's communications law in the Internet era(eds), *The Internet, Social Media and a Changing China*. Philadelphia: Penn University Press, 2014.
16. Creemers R. Party ideology and Chinese law. In Creemers R, Trevaskes S (eds). *Law and the Party in China: Ideology and organisation*. Cambridge: Cambridge University Press, 2020.
17. Clarke D. Order and law in China. GWU Leg Studies Research Paper. Washington: George Washington University Law School, 2020.
18. Zhang Q. A constitution without constitutionalism? The paths of constitutional development in China. *Int J Const Law* 2010;**8**:950–76.
19. State Council. Shisanwu guojia xinxihua guihua [Thirteenth Five-Year Plan for National Informatization]. 2016. http://www.gov.cn/zhengce/content/2016-12/27/content_5153411.htm. (11 July 2022, date last accessed).
20. Cyberspace Administration of China. Guojia wangluo kongjian anquan zhanlüe [National Cyberspace Security Strategy]. 2022. http://www.cac.gov.cn/2016-12/27/c_1120195926.htm. (11 July 2022, date last accessed).
21. Lynch DC. Xi Jinping confronts the network society. *Mod Chin* 2022;**48**:231–52. doi: 10.1177/0097700421993392.
22. Zeng J. Securitization of artificial intelligence in China. *Chin J Int Polit* 2021;**14**:417–45.
23. Lovelock P, Clark TC, Petrazzini BA. The "golden projects": China's national networking initiative. *Inf Infrastruct Pol* 1996;**5**:265–77.
24. DigiChina. National Development and Reform Commission Shisiwu tuijin guojia zhengwu xinxihua guihua [14th Five-Year Plan for National Governmental Informatization]. 2021. http://www.gov.cn/zhengce/zhengceku/2022-01/06/content_5666746.htm. (11 July 2022, date last accessed).
25. State Council. Zhonghua Renmin Gongheguo jisuansji xinxi xitong anquan baohu tiaoli [Computer Information System Security Protection Regulations of the People's Republic of China]. 1994. https://chinacopyrightandmedia.wordpress.com/1994/02/18/computer-information-system-security-protection-regulations-of-the-peoples-republic-of-china/. (11 July 2022, date last accessed).
26. National Information Security Standardization Technical Committee. Guanyu jiaqiang xinxi anquan baozhang gongzuo de yijian [Opinions concerning Strengthening Information Security Protection]. 2003. https://chinacopyrightandmedia.wordpress.com/2003/09/07/opinions-concerning-strengthening-information-security-protection/. (11 July 2022, date last accessed).
27. Ministry of Public Security. Guanyu xinxi anquan dengji baohu gongzuo de shishi yijian [Implementation Opinions concerning the Information Security Multi-Level Protection System]. 2004. https://chinacopyrightandmedia.wordpress.com/2004/09/15/implementation-opinions-concerning-the-information-security-multi-level-protection-system/. (11 July 2022, date last accessed).
28. Zhu G. The right to privacy: an emerging right in Chinese law. *Statut Law Rev* 1997;**18**:208–14.
29. Zhou H. *Geren xinxi baohu fa (zhuanjia jianyi gao) ji lifa yanjiu baogao [Personal Information Protection Law (Experts Suggestion Draft) and Legislative Research Report]*. Law Publishing House: Beijing, 2006.
30. Standing Committee of the National People's Congress. Zhonghua Renmin Gongheguo xingfa xiuzheng an [Amendments to the Criminal Law of the People's Republic of China. 2009. http://www.gov.cn/flfg/2009-02/28/content_1246438.htm. (11 July 2022, date last accessed).
31. People's Bank of China. Zuohao geren jinrong xinxi baohu gonzuo de tongzhi [Notice on Doing Well in the Protection of Personal Finan-

cial Information. 2011. http://www.gov.cn/gongbao/content/2011/content_1918924.htm. (11 July 2022, date last accessed).
32. Ministry of Industry and Information Technology. Guifan hulianwang xinxi fuwu shichang chengxu ruogan guiding [Some Provisions to Standardize Internet Information Service Market Order]. 2011. https://chinacopyrightandmedia.wordpress.com/2011/12/29/some-provisions-to-standardize-internet-information-service-market-order/. (11 July 2022, date last accessed).
33. National Information Security Standardization Technical Committee. *Xinxi anquan jishu gonggong ji shangyong fuwu xinxi xitong geren xinxi baohu zhinan [Information security technology - Guideline for personal information protection within information system for public and commercial services]*. 2012. http://std.samr.gov.cn/gb/search/gbDetailed?id=71F772D7E6DED3A7E05397BE0A0AB82A. (11 July 2022, date last accessed).
34. Standing Committee of the National People's Congress. Law of the People's Republic of China on Protection of Minors. 1991. http://www.china.org.cn/english/government/207410.htmhttp://www.china.org.cn/english/government/207411.htm. (11 July 2022, date last accessed).
35. Cao J. Protecting the right to privacy in China. *Vic Univ Wellingt Law Rev* 2005;**36**:645–64.
36. Wang L. Lun geren xinxiquan zai rengequanfa zhong de diwei [On the Status of Personal Information Right in the Law of Personality Rights]. *J Soochow Univ Philos Soc Sci Edn* 2012;**6**:68–75.
37. Standing Committee of the National People's Congress. Tort Law of the People's Republic of China. 2009. https://www.wipo.int/edocs/lexdocs/laws/en/cn/cn136en.pdf. (11 July 2022, date last accessed).
38. Creemers R. China's cyber governance institutions. LeidenAsiaCentre Report. 2022. https://leidenasiacentre.nl/en/report-chinas-cyber-governance-institutions/. (11 July 2022, date last accessed).
39. CNNIC. Di 47 ci Zhongguo hulianwangluo fazhan zhuankuang tongji baogao [47th Statistical report on the development situation of the Internet in China]. 2022. http://www.cac.gov.cn/2021-02/03/c_1613923423079314.htm. (11 July 2022, date last accessed).
40. Lee KF. *AI Superpowers: China, Silicon Valley, and the New World Order*. Boston: Houghton Mifflin, 2018.
41. State Council. Cujin dashuju fazhan xingdong gangyao [Outline of operations to stimulate the development of big data]. 2022. https://chinacopyrightandmedia.wordpress.com/2015/08/31/outline-of-operations-to-stimulate-the-development-of-big-data/. (11 July 2022, data last accessed).
42. Xinhuanet. Wangshang "heishi": nide simi xinxi jishi yuan jiu neng chadao [Online "Black Markets": your intimate information can be found for some tenners). 2017. http://www.xinhuanet.com/2017-02/17/c_1120482225.htm. (11 July 2022, date last accessed).
43. Li X., Liu J. Shei maile nide yinsi? Cheqi yonghu mingan xinxi shiluo diaocha [Who sold your privacy? An investigation of sensitive information leaks of vehicle company users]. *Xiaofeizhe baodao (Consumer Report)* 2015;**7**:
44. Mozur P. Apple customer data in China was sold illegally, police say. The New York Times. 2017. https://www.nytimes.com/2017/06/09/business/china-apple-personal-data-sold.html. (11 July 2022, date last accessed).
45. Shu M. The legal protection over personal information in China. London: Lexology. 2015. https://www.lexology.com/library/detail.aspx?g=17884797-e678-4e20-9e76-03d2fe4a9dec. (11 July 2022, date last accessed).
46. Tham E. Data dump: Chinas sees surge in personal information up for sale. 2018. https://www.reuters.com/article/us-china-dataprivacy-idUSKCN1L80IW, (11 Jully 2022, date last accessed).
47. Ding X. Personal data protection: rethinking the reasons, nature, and legal framework. *Front Law Chin* 2018; **13**:380–9.
48. Lee C. Online fraud victimization in China: a case study of Baidu Tieba, victims & offenders. *Int J Evid Based Res Pol Pract* 2021;**13**:343–62.
49. Cai T, Du L, Xin Y,. *et al*. Characteristics of cybercrimes: evidence from Chinese judgment documents. *Police Pract Res* 2018;**19**:582–95.
50. Liu J. China's data localization. *Chin J Commun* 2020;**13**:84–103.
51. Hong Y. Shuju chujing anquan pinggu: Baohu jichuxing zhanlüe ziyuan de zhongyao yihuan [Data outbound security assessment: An important part of protecting basic strategic resources]. **06**. Zhongguo Xinxi Anquan (China Information Security). 2017.
52. Creemers R. China's cybersecurity regime: Securing the smart state. Working paper 2022. 2022. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4070682. (11 July 2022, date last accessed).
53. Tencent Research Institute. Shuzi jingji shiye zhong de Oumeng "yiban shuju baohu tiaoli" [EU General Data Protection Regulation in the Perspective of Digital Economy]. 2018. https://tisi.org/15189. (11 July 2022, date last accessed).
54. Standing Committee of the National People's Congress. Quanguo renmin daibiao dahui changwu weiyuanhui guanju jiaqiang wangluo xinxi baohu de jueding [National People's Congress Standing Committee Decision concerning Strengthening Network Information Protection]. 2012. https://chinacopyrightandmedia.wordpress.com/2012/12/28/national-peoples-congress-standing-committee-decision-concerning-strengthening-network-information-protection/. (11 July 2022, date last accessed).
55. Ministry of Public Security. Zuigao renmin fayuan zuigao renmin jianchayuan gong'anbu guanyu yifa chengchu qinhai gongmin geren xinxi fanzui huodong de tongzhi [Notice concerning Punishing Criminal Activities Infringing Citizens' Personal Data]. 2013. https://chinacopyrightandmedia.wordpress.com/2013/04/23/notice-concerning-punishing-criminal-activities-infringing-citizens-personal-data/. (11 July 2022, date last accessed).
56. National People's Congress. Zhonghua renmin gongheguo xingfa (2015 xiuzheng) [Criminal Law of the People's Republic of China (2015 Revision)]. 2015. http://npc.people.com.cn/n/2015/1126/c14576-27857512.html. (11 July 2022, date last accessed).
57. Ministry of Industry and Information Technology. Dianxin he hulianwang yonghu geren xinxi baohu guiding [Telecommunications and Internet Personal User Data Protection Regulations]. 2013. https://chinacopyrightandmedia.wordpress.com/2013/07/16/telecommunications-and-internet-user-individual-information-protection-regulations/. (11 July 2022, date last accessed).
58. Standing Committee of the National People's Congress. Zhonghua renmin gongheguo xiaofeizhe quanyi baohufa [Consumer Rights Protection Law of the People's Republic of China]. 2013. https://www.chinalawtranslate.com/consumer-protection-law-including-2013-amendments/. (11 July 2022, date last accessed).
59. National People's Congress. Fan kongbuzhuyifa cao'an [Anti-Terrorism Law (Draft)]. 2014. http://www.npc.gov.cn/npc/c1481/201411/1634ef9ed5fc4204a2d5ca6b8eb8581d.shtml. (11 July 2022, date last accessed).
60. National People's Congress. Zhonghua renmin gongheguo wangluo anquan fa [Cybersecurity Law of the People's Republic of China]. 2016. http://www.cac.gov.cn/2016-11/07/c_1119867116.htm. (11 July 2022, date last accessed).
61. Hong Y. Ping "wangluo anquan fa" dui shuju anquan baohu zhi de yu shi [On the Gain and Loss of Cybersecurity Law of China on Data Protection]. *Zhengce Pinglun (Pol Rev)* 2017;**1**: 66–73. http://library.ttcdw.com/uploadfiles/zk/1507792951.pdf. (10 August 2022, date last accessed).
62. Keller P. Sources of order in Chinese law. *Am J Compar Law* 1994;**42**:711–59.
63. Xinhuanet. Zhongguo hulianwang guanli jiang dapo 'jiulong zhishui' geju [The situation of "nine dragons governing the water" in China's Internet management will be smashed]. 2014. http://politics.people.com.cn/n/2014/0307/c70731-24567726.html. (11 July 2022, date last accessed).
64. Cyberspace Administration of China. Guanxian xinxi jichu sheshi anquan baohu tiaoli [Critical Information Infrastructure Security Protection Regulations]. 2017. https://chinacopyrightandmedia.wordpress.com/2017/07/10/critical-information-infrastructure-security-protection-regulations/. (11 July 2022, date last accessed).
65. Cyberspace Administration of China. Guanyu "geren xinxi he zhongyao shuju chujing anquan pinggu banfa" gongkai zhengqiu yijian de tongzhi [Notice on the Public Consultation on the "Measures for the Security

Evaluation of the Exit of Personal Information and Important Data"]. 2017. http://www.cac.gov.cn/2017-04/11/c_1120785691.htm. (11 July 2022, date last accessed)).
66. Standardization Administration of China. Xinxi anquan jishu shuju chujing anquan pinggu zhinan [Information Security Technology - Guidelines for Data Cross-border Transfer Security Assessment]. 2017. http://std.samr.gov.cn/gb/search/gbDetailed?id=625516672A96BD9BE05397BE0A0A265C. (11 July 2022, date last accessed).
67. United States Trade Representative. Communication From the United States - Measures adopted by China relating to its cybersecurity law. 2017. (11 July 2022, date last accessed).
68. Hong Y. Kanqing APEC "kuajing yinsi baohu guize" tixi beihou de zhengzhi he jingji [Clearly see the politics and economics behind the APEC "Cross-border Privacy Protection Rules" system]. 2017. https://mp.weixin.qq.com/s/Gi59sRKAftyYcPhTVFmkTQ. (11 July 2022, date last accessed).
69. Sacks S, Triolo P, Webster G. Beyond the worst-case assumptions on China's Cybersecurity Law. 2017. https://www.newamerica.org/cybersecurity-initiative/blog/beyond-worst-case-assumptions-chinas-cybersecurity-law/. (11 July 2022, date last accessed).
70. Cyberspace Administration of China. Guanyu "geren xinxi chujing anquan pinggu banfa" gongkai zhengqiu yijian de tongzhi [Notice on publicly soliciting opinions on the "Personal Information Outbound Transfer Security Assessment Measures"]. 2019. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/. (11 July 2022, date last accessed).
71. Cyberspace Administration of China. Shuju anquan guanli banfa (zhengqiu yijian gao [Data security management measures (Draft for comment)]. 2019. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-draft-data-security-management-measures/. (11 July 2022, date last accessed).
72. Sacks S, Shi M, Creemers RLC,. *et al*. Public security ministry aligns with Chinese data protection regime in draft rules. 2018. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/public-security-ministry-aligns-chinese-data-protection-regime-draft-rules/. (11 July 2022, date last accessed).
73. Ministry of Public Security. Wangluo anquan dengji baohu tiaoli (zhengqiu yijian gao) [Regulations on Graded Cyber Security Protection (Draft for solicitation of comments)]. 2018. https://www.chinalawtranslate.com/en/regulation-on-graded-cybersecurity-protections-draft-for-solicitation-of-comments/. (11 July 2022, date last accessed).
74. Cyberspace Administration of China. Ertong geren xinxi wangluo baohu [Regulations on the Protection of Children's Personal Information Online]. 2022. https://perma.cc/2RJZ-XN98. (11 July 2022, date last accessed),
75. National Information Security Standardization Technical Committee. Xinxi anquan jishu geren xinxi Anquan guifan [Information Security Technology—Personal Information Security Specification]. 2017. https://www.tc260.org.cn/upload/2018-01-24/1516799764389090333.pdf. (11 July 2022, date last accessed).
76. National Information Security Standardization Technical Committee. Xinxi anquan jishu geren xinxi anquan yingxiang pinggu [Principles and criteria from China's Draft Privacy Impact Assessment Guide]. 2022. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-principles-and-criteria-from-chinas-draft-privacy-impact-assessment-guide/. (11 July 2022, date last accessed).
77. Internet Society of China. Geren xinxi baohu changyi shu [Proposal on Personal Information Protection]. 2018. https://chinacopyrightandmedia.wordpress.com/2018/09/14/proposal-on-personal-information-protection/. (11 July 2022, date last accessed).
78. Wang L. Nide geren xinxi anquan ma? [Is your personal information safe?]. 2018. http://tech.sina.com.cn/roll/2018-01-12/doc-ifyqqciz5880474.shtml. (11 July 2022, date last accessed).
79. Lu X, Li M, Sacks S.. What the Facebook scandal means in a land without Facebook: A look at China's burgeoning data protection regime. 2018. https://www.csis.org/analysis/what-facebook-scandal-means-land-without-facebook-look-chinas-burgeoning-data-protection. (11 July 2022, date last accessed).
80. National People's Congress. Zhonghua Renmin Gongheguo dianzi shangwu fa [E-Commerce Law of the People's Republic of China]. 2018. http://www.npc.gov.cn/zgrdw/npc/lfzt/rlyw/2018-08/31/content_2060827.htm. (11 July 2022, date last accessed).
81. App Working Group. App weifa weigui shouji shiyong geren xinxi zi pinggu zhinan [App Self-Assessment Guide for Collecting and Using Personal Information in Violation of Laws and Regulations]. 2019.
82. Ministry of Public Security. Gong'anbu tongbao "Jingwang 2019" zhuanxiang xingdong dianxing anli [The Ministry of Public Security announces typical cases of the "Net Net 2019" special action]. 2019. http://www.cac.gov.cn/2019-11/14/c_1575264987750271.htm. (11 July 2022, date last accessed).
83. Cyberspace Administration of China. Guanyu shuru fa deng 33 kuan app weifa weiguid shouji shiyong geren xinxi qingkuang de tongbao [Notification on the illegal collection and use of personal information in 33 apps including input methods]. 2022. http://www.cac.gov.cn/2021-04/30/c_1621370239178608.htm. (11 July 2022, date last accessed).
84. Cyberspace Administration of China. Changjian leixing yidong hulianwang yingyong chengxu biyao geren xinxi fanwei guiding [Regulations on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications]. 2022. http://www.cac.gov.cn/2021-03/22/c_1617990997054277.htm. (11 July 2022, date last accessed).
85. Ministry of Industry and Information Technology. Yidong hulianwang yingyong chengxu geren xinxi baohu guanli zanxing guiding [Interim Provisions on the Management of Personal Information Protection of Mobile Internet Applications]. 2021. http://www.cac.gov.cn/2021-04/26/c_1621018189707703.htm. (11 July 2022, date last accessed).
86. Naughton B. What's behind China's regulatory storm?. New York: Wall Street Journal. 2021. https://www.wsj.com/articles/what-is-behind-china-regulatory-storm-11638372662. (11 July 2022, date last accessed).
87. Goldstein A. China's grand strategy under Xi Jinping: Reassurance, reform, and resistance. *Int Secur* 2020;**45**:164–201.
88. National People's Congress. Zhonghua Renmin Gongheguo geren xinxi baohu fa [Personal Information Protection Law of the People's Republic of China]. 2021. https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/. (11 July 2022, date last accessed).
89. National People's Congress. Zhonghua Renmin Gongheguo shuju Anquan fa [Data Security Law of the People's Republic of China]. 2021. https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/. (11 July 2022, date last accessed).
90. Hong Y. Shuju anquan guanli shijiao xia de shuju fenlei yanjiu [Research on data classification from the perspective of data security management]. 2020. https://mp.weixin.qq.com/s?__biz=MzIxODM0NDU4MQ== &mid = 2247488664&idx = 1&sn = fdd8fdf8299298d273a2ab2b734248b2&chksm = 97eaa972a09d2064394ae5f08d13e0ca41ae41cef562a54566097c83ca8051544feea471ad2f&scene = 21#wechat_redirect. (11 July 2022, date last accessed).
91. Hong Y. Dui "shuju anquan fa" de lijie he renshi [Understanding and recognition of the "Data Security Law"]. 2020. https://mp.weixin.qq.com/s/iZGNGKG1Q36XaFVu0g_lHw. (11 July 2022, date last accessed).
92. Cyberspace Administration of China. Shuju chujing anquan pinggu banfa (zhengqiu yijian gao) [Outbound Data Transfer Security Assessment Measures (Draft for comment)). 2021. https://digichina.stanford.edu/work/translation-outbound-data-transfer-security-assessment-measures-draft-for-comment-oct-2021/. (11 July 2022, date last accessed).
93. Cyberspace Administration of China. Wangluo shuju anquan guanli tiaoli (zhengqiu yijian gao) [Online Data Security Management Regulations (Draft for comment)]. 2021. http://www.cac.gov.cn/2021-11/14/c_1638501991577898.htm/. (11 July 2022, date last accessed).
94. Cyberspace Administration of China. Qiche shuju Anquan guanli ruogan guiding (zhengqiu yijian gao) [Several Provisions on the Management of Automobile Data Security (Draft for comment)]. 2021.

https://digichina.stanford.edu/news/translation-several-provisions-management-automobile-data-security-draft-comment. (11 July 2022, date last accessed).

95. Cybersecurity Review Office. Dui "Didi Chuxing" qidong wangluo anquan shencha de gonggao [Announcement on launching a cybersecurity review of "Didi Travel"].2021. http://www.cac.gov.cn/2021-07/02/c_1626811521011934.htm. (11 July 2022, date last accessed).
96. Cyberspace Administration of China. Guanyu xiajia "DidiChuxing" app de tongbao [Announcement on the removal of "Didi Travel" App]. 2021. http://www.cac.gov.cn/2021-07/04/c_1627016782176163.htm. (11 July 2022, date last accessed).
97. Santoni G. Foreign capital in Chinese telecommunication companies: from the Variable Interest Entity model to the draft of the new Chinese Foreign Investment Law. *Ital Law J* 2018;**4**:589–609.
98. Cybersecurity Review Office Guanyu dui "Yunmanman" "Huochebang" "Boss Zhipin" qidong wangluo anquan shencha de gonggao [Announcement on launching a cybersecurity review of "Yunmanman", "Truck Gang", and "Boss Direct Appointment"]. 2021. http://www.cac.gov.cn/2021-07/05/c_1627071328950274.htm. (11 July 2022, date last accessed).
99. Cyberspace Administration of China. Wangluo anquan shencha banfa [Cybersecurity review measures]. 2021. https://digichina.stanford.edu/news/translation-cybersecurity-review-measures-revised-draft-comment-july-2021. (11 July 2022, date last accessed).
100. Schaefer K, Sacks S, Lu X. *With auto data, China buckles In for security and opens up for future tech*. DigiChina. 2021. https://digichina.stanford.edu/news/auto-data-china-buckles-security-and-opens-future-tech. (11 July 2022, date last accessed).
101. Fang X. Zhongguo hulianwan qiye xu bushang "hegui" qianzhang [Chinese Internet companies need to make up "compliance" debts]. 2022. https://finance.sina.com.cn/tech/2021-07-06/doc-ikqciyzk3929049.shtml. (11 July 2022, date last accessed).
102. National People's Congress. Zhonghua Renmin Gongheguo minfadian [Civil Code of the People's Republic of China]. 2020. http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8.shtml. (10 August 2022: date last accessed).