How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective

In China, there is no unified data protection law similar to the EU’s General Data Protection Regulation (GDPR). As a result, there are many different relevant regulations. Among other things, this makes enforcement and comprehension more difficult. To alleviate this problem and assess the comprehensiveness of Chinese data protection, this article uses the GDPR as a frame to organise and systematise the most important Chinese regulations. Binding and non-binding as well as enacted and draft provisions are included to show the dynamic progress and the general direction of Chinese law. While from a European data protection perspective there still are numerous deficiencies, the general development is positive.

I. Introduction

Recently, the Chinese government has shown an increased interest in building a stronger data protection regime, which has led to many different legislative efforts. Despite this, Chinese data protection law is mostly viewed as being fragmentary, insufficient, ineffective and difficult to understand. And indeed, there does exist a vast amount of relevant national, local and sector-specific regulations that affect the comprehensibility of this field of law. As the European General Data Protection Regulation (GDPR) is considered to be one of the most comprehensive and modern data protection regimes, it serves in this analysis as a framework for structuring and systematising these numerous legal provisions. This can be used to organise Chinese law to make it more understandable, especially for those who are familiar with the GDPR. Furthermore, it will be possible to assess the comprehensiveness of Chinese law, since gaps and rules that go beyond the European law will stand out. Thus, while being aware of the great differences of the two legal systems, this article intentionally uses an European perspective to review the above-mentioned assumptions. In doing so, it restricts itself to Chinese regulations with a nationwide scope of application. Additionally, it includes important draft regulations to present a perspective for possible future developments.

II. General provisions

1. Subject matter and objectives

As there is no unified law on data protection in China, the numerous regulations have to be seen in combination to determine the current standard. The GDPR, on the other hand, strives to align the laws of the EU Member States, although it leaves some options at the discretion of the national legislatures. It aims to balance the protection of personal data with the free flow of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

Sarah Wang Han and Abu Bakar Munir, ‘Information Security Technology – Personal Information Security Specification: China’s Version of the GDPR?’ (2018) 4 EDPL 355.

Xiao Cheng (程晓), ‘On Civil Liability of Infringing Personal Information’ (论侵害个人信息的民事责任) (2020) 42(2) Jinan Journal (济南学报) 39, 40.

6 Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C326/47 (TFEU), art 288(2). Nicholas F III Palmieri, ‘Data Protection in an Increasingly Globalized World’ (2019) 94 Ind L J 297, 308; Ding, ‘Personal Data’ (n 1) 380.

of data.\(^8\) Furthermore, it emphasises the protection of fundamental rights, particularly underlining the right to the protection of personal data.\(^9\) In contrast, the Chinese Constitution\(^10\) only indirectly recognises a right to privacy.\(^11\) Additionally, the Constitution is widely regarded as irrelevant, as there is neither a constitutional court nor any possibility to assert constitutional rights.\(^12\) In the absence of a fundamental basis, there is an ongoing intensive academic debate concerning general questions such as the direction, level, focus and legal nature of data protection law, with some stressing the civil right to privacy to justify a higher level of protection.\(^13\) Many recommend the European or US approach, while others prefer a special Chinese direction, focusing on social control and societal interests.\(^14\)

The Chinese legislators show a clear preference towards stronger data protection. They increasingly include data protection regulations when creating or amending general laws such as the Tort Liability Law,\(^15\) the Consumer Protection Law,\(^16\) the Criminal Law\(^17\) and the General Provisions.\(^18\) These regulations are rather unspecified and not comprehensive.\(^19\) More promising and detailed is the long-awaited Civil Code of the People’s Republic of China (PRC) (中华人民共和国民法典) (Civil Code), which was passed on 28 May 2020 by the National People’s Congress (NPC) and will enter into force on 1 January 2021.\(^20\) According to Art. 1260 Civil Code, the Tort Liability Law and the General Provisions will be abolished upon entry into force of the Civil Code. Alongside these general regulations, the lawmakers have introduced more specialised provisions. The ‘Standardizing Regulations 2012’ were among the first binding regulations dealing with internet information services and containing rules concerning the protection of personal information.\(^21\) A relatively general and short but important legislative basis is the binding ‘Decision 2012’ of the Standing Committee of the National People’s Congress (NPCSC), one of the central legislative organs.\(^22\) To support its implementation, the Ministry of Industry and Information Technology (MIIT) enacted the binding ‘Protection Regulations 2013’.\(^23\) More comprehensive and better organised are the ‘Guidelines 2013’, which are not legally binding but serve as an important orientation for courts, public authorities, lawyers, companies and possibly future legislation.\(^24\) Structurally very similar and equally non-binding is the ‘Standard 2020’, which entered into force on 1 October 2020 and whose previous version has already been used by the government against transgressors.\(^25\) It regulates the entire data processing cycle extensively and strengthens individual rights.\(^26\)

Another central binding regulation is the ‘Cybersecurity Law of the PRC’ (中华人民共和国网络安全法) (CSL), which came into force on 1 June 2017. Although it mainly states the protection of cybersecurity and national security as its aims, the CSL is a positive step towards a more comprehensive data protection

---

8. GDPR, art 1. See also Palmer (n 7) 308.
9. This right derives from the Charter of Fundamental Rights of the European Union (2007) OJ L113/1, art 7, and the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended), art 8. For an overview, see Schütz (n 7) 306-308; Fung and Gao (n 12) 206-207; Personal Information Protection: From Personal Control to Social Control (‘Personal Information’, from ‘Individual Control to Social Control’) (2014) 40(3) Chinese Journal of Law 84, 85-87.
10. Mao, ‘Personal Data Rights in the Era of Big Data’ (2019) 77(1) Chinese Journal of Law 20-34.
11. China’s network legislators show a clear preference towards stronger data protection. They increasingly include data protection regulations when creating or amending general laws such as the Tort Liability Law, the Consumer Protection Law, the Criminal Law and the General Provisions. These regulations are rather unspecified and not comprehensive. More promising and detailed is the long-awaited Chinese Civil Code (民法典) (Civil Code), which was passed on 28 May 2020 by the National People’s Congress (NPC) and will enter into force on 1 January 2021. According to Art. 1260 Civil Code, the Tort Liability Law and the General Provisions will be abolished upon entry into force of the Civil Code. Alongside these general regulations, the lawmakers have introduced more specialised provisions. The ‘Standardizing Regulations 2012’ were among the first binding regulations dealing with internet information services and containing rules concerning the protection of personal information. A relatively general and short but important legislative basis is the binding ‘Decision 2012’ of the Standing Committee of the National People’s Congress (NPCSC), one of the central legislative organs. To support its implementation, the Ministry of Industry and Information Technology (MIIT) enacted the binding ‘Protection Regulations 2013’. More comprehensive and better organised are the ‘Guidelines 2013’, which are not legally binding but serve as an important orientation for courts, public authorities, lawyers, companies and possibly future legislation. Structurally very similar and equally non-binding is the ‘Standard 2020’, which entered into force on 1 October 2020 and whose previous version has already been used by the government against transgressors. It regulates the entire data processing cycle extensively and strengthens individual rights.

---

Daten: Die Rechtslage in China’ in Louisa Specht-Riemenschneider, Nikola Werry and Susanne Werry (eds), Datenschutz in der Digitalisierung (Erich Schmidt Verlag 2019) 440, 457.
12. Binding and Radjuk (n 3) 329. Hua Wang (ed), ‘Chinese Constitution’ (2013) 126 Harv L Rev 1966, 1973-1980, 1993.
13. Greenleaf, Data Privacy (n 3) 196; W. Wang, ‘Redefining Privacy’ (n 1) 116; Ma and Roth (n 2) 355.
14. See eg Mingyi Ye (叶明益), ‘On the Basic Categories of the Right to Personal Information’ (论个人信息的基本范畴) (2012) 125 Tsinghua University Law Journal (清华大学法学期刊) 143, 145; Ding, ‘Private Law’ in 194-196, 200; Dual Attributes (n 1) 69-70; Gao (n 9) 91-94, 99; Hao Wang (王海), ‘The Conception of the Path to Civil Law Protection of Internet Privacy (网络隐私权保护路径之探讨)’ (2017) 39(10) Jinan University Journal 35-36; Zhenghuan Xie (谢正淳), ‘Data Privacy Protection in the Data-driven Era – From Personal Control to the Fiduciary Duty of Data Controllers (数据驱动时代的数据隐私保护——从个人信息到数据控制者的义务)’ (2020) 37(2) Studies in Law and Business (法商研究) 71, 78.
15. Compared to the previous version of the GDPR, which focuses on individual rights, the US law is sector-specific, market-oriented and less strict, see Paul M Schwartz, ‘The EU-US Privacy Collision: A Turn to Institutions and Procedures’ (2013) 126 Harv L Rev 1966, 1973-1980, 1993-1997, Xie (n 13) 78; Ding, Dual Attributes (n 1) 76; Ding, ‘Personal Data’ (n 2) 381 ff; Gao (n 9) 93-97, 100; Qinghai Sun (孙庆海) and Jianwen Wang (王建文), ‘The Legal Logic and Legal Regulation of the “Public Nature” of Personal Information in the Age of Big Data (大数据时代下个人信息的法律逻辑与法律规范)’ (2018) http://olaw.cssn.cn/fxyd20180601/20180605_4659795.shtml accessed 20 July 2020.
16. eg arts 36, 62 of the Tort Liability Law of the PRC (中华人民共和国侵权责任法) which entered into force on 1 July 2010.
17. The amendment of the Law of the PRC on the Protection of Consumer Rights and Interests (消费者权益保护法) which entered into force on 15 March 2014.
18. See arts 253-1, 285-286 of the Criminal Law of the PRC (中华人民共和国刑法) which entered into force on 4 November 2017 following its 10th Amendment.
19. The reform of the General Provisions of the Civil Law of the PRC (中华人民共和国民法通则) of the NPC entered into force on 1 October 2017, arts 110 l, 127 introduce the protection of personal information as a part of the civil law for the first time, see Mingyi Ye (叶明益), ‘Tort Law Protection of Personal Information (个人信息的侵权责任保护)’ (2018) 40(4) Chinese Journal of Law 83, Ling Yu, ‘Reconstruction of an

---

11 Legal Logic and Legal Regulation of the “Public Nature” of Personal Information in the Age of Big Data (大数据时代下个人信息的法律逻辑与法律规范) (2018) http://olaw.cssn.cn/fxyd20180601/20180605_4659795.shtml accessed 20 July 2020.
system.27 Like many national laws, it is merely supposed to be a broad basic framework, which results in vague language, enforcement difficulties and criticism from the private sector.28 Thus, the Cyberspace Administration of China (CAC) released the ‘Administrative Measures on Data Security (Draft for Comment)’ (数据安全管理办法（征求意见稿）) (Draft Administrative Measures) on 28 May 2019, which provide binding rules for implementing the higher-ranking CSL.29 They aim to protect personal information, adopting many rules of the former version of the Standard 2020 and showing much resemblance to the GDPR, which had become effective just one year before.30

Last but not least, the Draft for a Law of the PRC on the Protection of Personal Information (中华人民共和国个人信息保护法（草案）) (Draft Law), proposed by several delegates of the NPC in 2017, shows promise as a binding and more comprehensive data protection law.31 For the first time, a national law mentions the protection of the right to personal information as a primary objective, indicating a growing recognition of its importance.32 While its final form is not clear, the NPCSC spokesman stated that a Law on the Protection of Personal Information will be adopted in 2020.33

2. Material scope

The GDPR applies to ‘the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of [it]’.34 Article 2 Draft Law employs almost exactly the same wording. The Draft Administrative Measures apply to the use of networks for data activities, excluding purely family and personal matters, just like Art. 2(2)(c) GDPR.35 The Standardizing Regulations 2012 and Protection Regulations 2013 apply to providers of internet information services, which are understood broadly and include e.g. providers of e-commerce services, social media, online advertising and mobile services.36 The Tort Liability Law and parts of the Civil Code also address network users.37 Most significant is the complete exclusion of processing by public actors in the older provisions.38 In contrast, the CSL, the Standard 2020 and at least in part the Civil Code apply to the processing of personal information by private and public actors.39 The Criminal Law punishes certain acts relating to personal information and is even stricter towards state offenders.40 In summary, many differences exist among the Chinese provisions, the exclusion of state actors in the older ones being the most far-reaching.

3. Territorial scope

In contrast to the extraterritorial applicability of the GDPR,41 the Chinese legislation mostly concentrates on domestic compliance and courts do not tend to apply domestic laws to internet companies whose server is not based in China.42 A reason for this might be the strict data localisation and internet censorship rules, which restrict information flows, making extraterritoriality less important.43

4. Definitions

The definitions of ‘personal data’ of Art. 4(1) GDPR and of ‘personal information’ in the Chinese regulations overlap considerably, as the identifiability of the ‘data subject’44 is the central requirement and similar examples are given.45 Furthermore, Art. 3.1 and Appendix A Standard

---

27 CSL, arts 1, 3; Jyb-An Lee, ‘Hacking into China’s Cybersecurity Law’ (2018) 53 Wake Forest L Rev 37, 87, 104; Feng (n 1) 72.
28 Palmieri (n 7) 318; Aimin Qi, Guosong Shao and Wentong Zheng, Draft Law, art 3. Jyh-An Lee, Measuring Other than by Automated Means of Personal Data (2018) 53 Wake Forest L Rev 57, 87, 104; Feng (n 1) 72.
29 CSL, arts 1, 3. Jyh-An Lee, Assessing China’s New Cybersecurity Law and U.S.-China Dual Attributes (2018) 58 Santa Clara L Rev 137, 140, 152f, 159.
30 Jeffrey A. Wasserstrom, The Standard 2020 and at Least in Part the Civil Code, art 1039 Obligations of State Organisations to Keep the Personal Information of Natural Persons Known to Them in the Course of Performing Their Duties Confidential (2018) 58 Santa Clara L Rev 137, 140, 152f, 159.
31 The definitions of personal data in the Interpretations of the Supreme People’s Procuratorate on Several Issues Concerning the Application of Law in Handling Criminal Cases Involving the Infringement of Citizens’ Personal Information (中华人民共和国最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释) (Interpretations of Criminal Cases) Fa Shu (2017) 10 (法

Downloaded from https://academic.oup.com/grr/article/69/12/1191/5909207 by guest on 01 January 2021
2020 far exceed the GDPR in regard to detail and guidance, giving a thorough explanation and listing many examples. Concerning 'consent', Arts. 3.6 f. Standard 2020 and Arts. 3.10 f. Guidelines 2013 state almost the same as Art. 4(11) GDPR, the difference being in their express definitions of explicit and implied consent.ropolis As to 'profiling' and 'pseudonymisation', only Arts. 3.8 and 3.15 Standard 2020 offer definitions that resemble the GDPR. Article 20 Draft Administrative Measures and Art. 3.14 Standard 2020 define 'anonymisation' in the same way as Rec. 26 GDPR. Definitions of 'filing systems' similar to Art. 4(6) GDPR are given in Art. 44(9) Draft Law, Art. 3.1 Guidelines 2013 and Art. 76(1) CSL.

Unlike Art. 4(2) GDPR, of the enacted binding legal provisions only the new Art. 1035 Civil Code defines 'processing' by briefly listing use, handling, transmission, provision and disclosure. In contrast, the Guidelines 2013, Draft Law and Standard 2020 specify the individual stages of a processing cycle in a well ordered and detailed way, surpassing the GDPR. They Concerning the main parties, Art. 4(7)(8) GDPR characterises the 'controller' as the person determining the purposes and means of the processing, while the 'processor' performs the processing on behalf of the controller. Most regulations that apply to the controller also apply to the processor. Though In the absence of a unifying data protection law, the Chinese terms are not consistent, which complicates their application. The actors closest to the definition of the European controller are called 'internet information service providers', 'internet service providers', 'network operators', 'information controllers', 'personal information managers', 'personal information controllers' and 'information processing subjects', whereas those resembling the European processor are referred to as the 'personal information recipients' and 'persons entrusted with the processing'. Though the terms may in part sound misleading from a European perspective, the differences between the Chinese and the European definitions are not substantial. Thus, for the sake of simplification, the terms controller and processor are used in the following. Most regulations only mention controllers, omitting processors. Approving of this, some Chinese scholars argue that the same duties apply, anyway. Apart from that, the CSL stipulates stricter rules for 'critical information infrastructures', another broadly defined term that includes 'important industries and fields'.

All in all, despite the existence of some extensive definitions in the non-binding provisions, most Chinese regulations lack many basic definitions.

### III. Principles

#### 1. Principles relating to the processing of personal data

Article 5 GDPR enumerates lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability as processing principles and provides respective explanations.

While their regulations seen in combination reflect all of the principles listed in Art. 5 GDPR, of the Chinese regulations merely mention briefly 'lawfulness, legitimacy and necessity' as processing principles. In contrast, the majority of the non-binding and draft regulations contain almost all of the European principles and nearly identical explanations, adding the principle of individual consent and in part the principle of subject participation, listing the information subjects' rights to access, correct, delete and withdraw consent to their personal information.

#### 2. Lawfulness of processing and conditions for consent

While Art. 6(1) GDPR sets out six exhaustive legal bases for processing, most of the enacted binding Chinese provisions only consider consent to be a legitimate legal basis, which at first glance leads to a higher degree of protection. Concerning consent itself, the GDPR is much clearer and stricter, however. Many Chinese regulations allow implied consent without adding specifications or requirements apart from information duties, in part only requiring explicit consent for sensitive personal information. Some add that deception, misleading and

---

54 CSL, arts 33-38. Huang (n 42) 194 f; Balke (n 28) 154.
55 Consumer Protection Law, art 29; General Provisions, arts 111, 127; Civil Code, arts 1035, 1039, 1225; Standardizing Regulations 2012, arts 11-14; Decision 2012, arts 2, 4, 10; Protection Regulations 2013, arts 9 f; CSL, arts 30, 40 f; Draft Administrative Measures, arts 20, 31.
56 Consumer Protection Law, art 29(1); Civil Code, art 1035; Decision 2012, art 2; Protection Regulations 2013, art 5; CSL, art 41. Standardizing Regulations 2012, art 4 enumerates 'equality, voluntariness, fairness and integrity'. The Draft Administrative Measures name no principle at all.
57 Guidelines 2013, art 4.2; Standard 2020, art 4; Draft Law, arts 4-10.
58 Consumer Protection Law, art 29(1); Decision 2012, art 2; Protection Regulations 2013, art 9(1); Guidelines 2013, art 5.2.3; CSL, arts 41 f. Palmieri (n 7) 309; Xie (n 13) 78; Gao (n 9) 85; Binding (n 3) 332.
59 GDPR, arts 4(1), 61(1)af and resc 32 f. 421. See also Klaus Wiedemann, 'The ECJ's Decision in “Planet49” (Case C-673/17): A Cookie Monster or Much Ado About Nothing?’ (2020) 51 IIC 543, 545-549.
60 Consumer Protection Law, art 29; Civil Code, art 1035; Standardizing Regulations 2012, art 11; Protection Regulations 2013, art 9; Guidelines 2013, arts 5.2.2 f; Standard 2020, arts 5.4, 9.2(2); CSL, art 41; Draft Administrative Measures, arts 8 f, 22, 27; Draft Law, arts 2011 f, 22(2)af, 37(1)af. Inc. as to the definition of consent see above II. 4, Daniel Albrect, 'Chinese Cybersecurity Law Compared to EU-NIS Directive and German IT-Security Act: When Cybersecurity Not Only Protects Interests of the Masses but Ultimately Also Safeguards National Sovereignty' [2018] CRI 1, 4; Wang Han and Munir (n 5) 538 f; Ma and Roth (n 2) 359.
61 Guidelines 2013, arts 5.2.3, 5.2.7, 5.3.4; Standard 2020, arts 5.4(2), 9.2(3), 9.3(2), 9.4(2); Draft Administrative Measures, art 9.
coercion are forbidden as a means of obtaining consent. Only Art. 11(2) Draft Administrative Measures and Art. 8.4 Standard 2020 mention the possibility to withdraw consent as in Art. 7(3) GDPR. All the more prominent, Appendix C of the Standard 2020 clearly and in great detail describes how express consent is to be obtained, providing a template that sets out many options on individual aspects. In summary, despite the greater requirements for consent, the Chinese law is not necessarily more protective as its rules concerning consent itself are less strict.

Nevertheless, as to alternative legal bases, there is a clear movement in the direction of the GDPR especially on the part of the more recent and draft regulations. Articles 11(1), 13(2)(b) Standardizing Regulations 2012 and Art. 1035(1) Civil Code very generally allow other laws and administrative regulations to provide additional legal bases. Beyond that, the Draft Law, the Standard 2020 and in part the Draft Administrative Measures include substantial portions of all the legal bases in the GDPR, adding ‘national security and national defence security’ as public interests. However, since the CSL only accepts consent and possibly ranks higher than the enacted regulations, the legality of the alternative legal bases will remain unclear until the Draft Law enters into force.

### 3. Conditions applicable to child’s consent

Where personal data of children below the age of 16 are concerned, Art. 8(1) GDPR requires the consent of the holder of parental responsibility. Article 5.2.7 Guidelines 2013 on the one hand extends this requirement to persons with limited legal capacity and on the other hand restricts it to cases of sensitive personal information. Article 12 Draft Administrative Measures and Art. 5.4(4) Standard 2020 lower the age limit to 14. Of the binding and adopted regulations, it was the new Civil Code that first introduced – quite broad – rules for this case. In principle it requires the consent of the guardians to the processing of any personal information of those under their guardianship, which means minors under the age of 18 and adults with no or limited civil capacity.

### 4. Processing of special categories of personal data

Prominent Chinese scholars support the theory of ‘strengthening at both ends, tripartite balance’ (两头强化, 三方平衡理论), by which the interests in the protection and use of personal data are to be strengthened simultaneously. While consent requirements for personal information are to be lowered, a high level of protection is to be provided for sensitive personal information. Consequently, these scholars advocate a clear differentiation between the two categories, a differentiation that in most cases does not yet exist. Only the Guidelines 2013 and the Standard 2020 define sensitive personal information.

In contrast to Art. 9(1) GDPR, both definitions are non-exhaustive and more general, describing it as information that could adversely affect the information subject if leaked or misused. The Standard 2020 gives a longer explanation and enumerates many examples, some of which go beyond the GDPR, e.g. identification numbers, bank account numbers, information on property, credit, transactions and personal information of children under the age of 14. A reason for these differences might be that unlike the fundamental rights-oriented protection of the GDPR, the Chinese regulations mostly evolved within a security context, making the safety of persons and property the main criterion. The higher level of protection consists of the requirement of express consent, similar to Art. 9(2)(a) GDPR, and additional information duties.

Article 15 Draft Administrative Measures adds the obligation to file a record to the local network information department, containing, among others, the purpose, scope, type and duration, but excluding the data content itself. Going further than this, Art. 9.4(6) Standard 2020 forbids the disclosure of personal biometric information without exception. In summary, merely non-binding or draft provisions regulate sensitive personal information.

### IV. Rights of the data subject

#### 1. Transparency and modalities for the exercise of rights

Article 12(1)(5) GDPR obliges controllers to provide information in a ‘concise, transparent, intelligible and easily accessible form’ as well as free of charge, unless requests are unfounded or excessive. Articles 13 f. GDPR differentiate information obligations depending on whether information was collected from the data subject or not. In addition, the controller is required to ‘facilitate the exercise of data subject rights’ by providing ‘mechanisms to request’ and responding ‘without undue delay and at the latest within one month’.

According to Art. 29(1) Consumer Protection Law, the controller is required to disclose the rules for the processing of personal information. Article 2(1) Decision 2012 and Art. 41(1) CSL add the obligation to inform information subjects of the manner, content and purpose of the processing. Moreover, controllers have to establish a complaint and reporting system and handle complaints ‘in a timely manner’.

62 Protection Regulations 2013, art 9(3); Standard 2020, art 5.1; Draft Administrative Measures, arts 11(1), 13.

63 Standard 2020, arts 5.6, 9.5; Draft Administrative Measures, art 27; Draft Law, arts 20, 22(2) f, 25(1), 37 f.

64 Wang Han and Munir (n 5) 537. The Draft Law and the CSL would both be issued by the NPCSC and the former would take precedence as the newer and more specific law, see Legislative Law of the PRC (as amended in 2015) (中华人民共和国立法法 (2015年修正)) (Legislative Law), art 92. The Civil Code, on the other hand, is newer but not necessarily more specific than the CSL. In such situations, art 94 of the Civil Code requires the NPCSC to decide which law takes precedence.

65 Civil Code, arts 17, 27 f, 34 f, 1035(1), 1037(1).

66 Xinhao Zhang (弥新宝), ‘From Privacy to Personal Information: Theory and Adaption of Practice for the Revaluation of Interests (从隐私到个人信息: 理论与实践的变革对利益重估)’ in a timely manner.

67 Guidelines 2013, art 3.7; Standard 2020, art 3.2 and Appendix B.

68 See especially GDPR, rec 51.

69 Guidelines 2013, art 5.2.3; Standard 2020, arts 5.4, 9.2(3), 9.4(3).

70 GDPR, art 12(2) and rec 59.

71 CSL, art 49(1).
Standardizing Regulations 2012, Protection Regulations 2013, Draft Law and Standard 2020, requiring controllers to publish valid contact information, accept complaints and respond within 15 or, as in the case of the Standard 2020, 30 days. Furthermore, the controllers should make transparent the channels for accessing and correcting information and the consequences of refusing to provide personal information. The Guidelines 2013, Draft Administrative Measures, Draft Law and Standard 2020 give a more detailed list concerning the information, and the last three in particular largely cover the requirements of the GDPR. In addition, Art. 14 Draft Administrative Measures and Art. 5.4 Standard 2020 undertake a differentiation as in Arts. 13 f. GDPR. Going beyond the GDPR, Art. 5.5 and Appendix D Standard 2020 explain the functions of the privacy policy and provide a very detailed and long template combined with writing requirements, which contain very comprehensive rules that are clear and easy to understand and could also inspire the European legislator.

Structurally similar to Arts. 13(4), 14(5) GDPR but broader in content, Art. 8.7(5) Standard 2020 and in part Arts. 27, 38 Draft Law non-exhaustively exempt controllers from the obligation to respond to requests or disclose information, e.g., if they are directly related to national security, public safety, major public interests or criminal prosecution, if the information subject is abusing his or her rights, if it will cause serious damage to the legitimate rights and interests of the information subject or others and if commercial secrets are involved. The uncertainty concerning e.g. ‘major public interests’ and the relative openness of these exceptions could lead to substantive limitations to the information obligations. Nevertheless, the Standard 2020, an enactment of the Draft Administrative Measures and the Draft Law would establish comprehensive information obligations and meet many demands of Chinese scholars and practitioners. In particular, the binding obligations could alleviate issues such as the lack of privacy policies in many companies or the absence of contact or user rights information.

2. Right of access

According to Art. 15 GDPR, the data subject has the right to know whether his or her personal data are being processed, and to obtain a copy of these data as well as certain information from the controller. Reasonable fees are only allowed for further copies. In contrast, no enacted binding Chinese regulation provides such a right. Article 21 Draft Administrative Measures lays down that the controller shall ‘inquire’ when receiving a corresponding request, leaving details unclear and stressing the controller’s obligation rather than the individual’s right. Articles 1036(1), 1225(2) Civil Code shift the focus by stating that a natural person may examine and copy his or her personal information and medical records, and Arts. 14, 28 Draft Law explicitly employ the headline ‘right of access to information’. Less vaguely, Art. 5.3.7 Guidelines 2013 adds that the controller has to inform the data subject ‘truthfully and free of charge whether or not he or she possesses personal information, the contents [thereof] and the status of the processing […]’, unless the cost or frequency of the request exceeds a reasonable range.’ According to Art. 8.1 Standard 2020 and Arts. 28 (1), 38 Draft Law the access comprises the personal information or its type, its source and purpose and the identity or type of recipients, which falls short of the broader coverage of Art. 15 GDPR. Articles 29, 38 Draft Law allow copies to be made of the said data, which may be subject to an appropriate fee. Article 8.6 Standard 2020 limits the content of copies to basic personal data, personal identity information, and health, physiological, education and work information. Article 28(2) Draft Law further limits the right by listing exceptions, namely if it would be harmful to the national or public interest, public order or morals, if it would lead controllers to perform their duties unfairly, if access is inappropriate due to the nature of personal information and – similar to the sole limitation ground in Art. 15(4) GDPR – if vital interests of third parties are affected.

3. Rectification and erasure (‘right to be forgotten’)

According to Art. 16 GDPR, data subjects have the right to rectification of their personal data without undue delay. In comparison, Art. 13 Standardizing Regulations 2012 is quite restrictive, limiting such a right to information uploaded by users. Article 5.3.6 Guidelines 2013, Art. 43 CSL, Art. 8.2 Standard 2020 and Art. 1036(1) Civil Code give information subjects a more general right, obliging the controller to correct or supplement the information. Article 21 Draft Administrative Measures adds the obligation to undertake the corrections within a ‘reasonable time and at a reasonable cost.’ Articles 15, 30 (1), 38 Draft Law further require controllers to update outdated personal information and provide an explanation when deciding not to make changes. Thus, some enacted binding regulations provide a right to rectification, which is considerably weakened due to the lack of a corresponding right to access.31 Again, the non-binding and draft provisions show more promise.

Article 17 GDPR gives information subjects the right to obtain the erasure of their personal data without undue delay, e.g. if they are no longer necessary for the original purposes, if the data subject withdraws consent or objects, without there being any other legal ground for processing, and if the data have been unlawfully processed. Without links to corresponding rights for information subjects, Arts. 5.5.2–5.5.4 Guidelines 2013 and in part Arts. 20, 31 Draft Administrative Measures, Arts. 6.1, 6.4 Standard 2020 and Art. 30(2) Draft Law oblige

74 Standardizing Regulations 2012, arts 11(2), 14; Protection Regulations 2013, arts 8, 12; Standard 2020, arts 8.7f; Draft Law, arts 31, 38.
75 Protection Regulations 2013, art 9(2).
76 Guidelines 2013, art 5.2.2. Standard 2020, arts 5.4 f; Draft Administrative Measures, arts 7-9; Draft Law, arts 21, 26, 36, 38.
77 Sun and Wang (n 14); Ding, ‘Private Law’ (n 2) 203; Miao Qu (gement) and others, ‘Data Controversy – Inventory of Data-Related Controversies in 2019 (数据之争——2019年数据相关争议盘点)’ (2020) <http://news.zhuchani.com/article/9015.html> accessed 20 July 2020.
78 Ying Zhu (朱颖), ‘Study on Privacy Policies for Mobile Apps in China – Analysis Based on 96 Mobile Apps (我国移动 APP隐私保护政策研究——基于96个移动应用 APP的分析)’ (2017) 39(12) Jinan Journal 107, 110-113; Sun and Wang (n 14); Xu (n 3) 251.
79 GDPR, art 15(3).
80 Regarding the CSL see Feng (n 1) 73; Palmieri (n 7) 321.
81 Palmieri (n 7) 321.
82 For more details see Globocnik (n 41).
controllers to delete personal information as soon as the purpose has been achieved, if the user’s account has been cancelled, when the notified retention period ends and if the purpose cannot be continued due to bankruptcy or dissolution. In contrast, Art. 13 Standardizing Regulations 2012 provides for a right to delete personal information, albeit limited to that uploaded by users. Without being subject to this limitation, Art. 8 Decision 2012 provides a right to erasure where the legitimate rights and interests of the information subjects are violated. Article 5.5.1 Guidelines 2013 additionally allows ‘legitimate reasons’ and requires that the deletion is carried out ‘in a timely manner’. In contrast, Art. 43 CSL, Art. 1036(2) Civil Code, Art. 8.3 Standard 2020 and similarly Arts. 18 f. Draft Law base the right on the violation of legal norms or processing agreements. Article 36(2) Tort Liability Law and Art. 1195 Civil Code give injured persons a right to deletion against network service providers if another ‘network user uses a network service to commit an infringement’. Only Art. 21 Draft Administrative Measures gives a general right to request deletion of personal information and a corresponding obligation for the controller. Consequently, a right to deletion exists in various forms. However, the enacted regulations do not reach the level of the European ‘right to be forgotten’, where the withdrawal of consent is in principle not connected to any conditions and is possible at any time. Apart from this, there is no consensus whether such a ‘right to be forgotten’ should be introduced at all, some doubting its technical feasibility and others having competition concerns.

4. Right to restriction of processing

Instead of deletion, Art. 18 GDPR provides the right to restrict processing in certain cases, making processing only possible with the consent of the data subject and subject to a number of other conditions. Furthermore, the data subject should be informed before the restriction is lifted. Only Arts. 17, 30(3)(4) Draft Law provide a similar right, albeit for different reasons: if the deletion is prohibited by law, regulation or contract, if it would harm the legitimate interests of the information subject, if it is impossible due to the storage method, or is excessively expensive or inappropriate. In such cases, any processing has to be notified to the information subject and requires consent except where it serves the protection of major interests of the information subject and others or the public interest.

5. Right to data portability

To strengthen the control of data subjects and increase competition among digital services and their interoperability, Art. 20(1) GDPR gives data subjects the right to receive the personal data they provided to a controller in a ’structured, commonly used and machine-readable format’ and to transmit them to another controller. The data subject can also ‘have the personal data transmitted directly from one controller to another, where technically feasible.’ In China, only non-binding and draft provisions offer a basic right to data portability. Articles 16, 38 Draft Law and Art. 8.6 Standard 2020 state that information subjects have the right to obtain their personal information or have controllers transmit them directly to others, where technically feasible. The latter regulation restricts this to basic personal data, personal identification, health, physiological, education and work information, possibly because it is only these that are deemed sufficiently relevant to the information subjects. Unlike the GDPR, they do not limit this right to data provided by the information subjects.

6. Right to object

According to Art. 21 GDPR, data subjects have the right to object to processing if their interests prevail, which requires a balancing of interests except for cases of direct marketing. Irrespective of the interests, Art. 5.2.3 Guidelines 2013 allows express opposition to the collection or deletion of personal information. Article 7 Decision 2012 and Art. 8.4(2) Standard 2020 give information subjects the possibility to refuse to receive electronic messages or commercial advertisements based on their personal information. The most advanced provision is Art. 23(1) Draft Administrative Measures, which obliges controllers to show explicitly when user data and algorithms are used for targeted marketing and gives users the right to object to such marketing, after which personal information has to be deleted. In sum, especially the non-binding and draft Chinese rules appear more specific.

7. Automated individual decision-making

Unlike Art. 22(1) GDPR, Art. 7.7 Standard 2020 does not require the decision to be based solely on automated decision-making, but much more broadly applies whenever automatic decision-making mechanisms are used in information systems that can ‘significantly affect the rights and interests’ of information subjects. It obliges public and private controllers to conduct an information security impact assessment before the first use and at least once a year, take appropriate measures, provide information subjects with complaint channels and support the manual review of the results. While the consequences have some similarity to Art. 22(2)(3) GDPR, the Chinese norm probably has more relevance due to its broader range of application.

V. Controller and processor

1. General obligations

Unlike Ch. 4 GDPR, only three Chinese regulations divide the obligations and responsibilities between different actors. Article 4.1.4 Guidelines 2013 provides that processors have to adhere to the Guidelines and the contract with the controller when collecting personal information. Showing a few more similarities to Art. 28(1)(3) GDPR

83 GDPR, arts 17(1)(b), 7(3). See also Liao (n 31) 70 f; Ye, ‘Tort Law Protection’ (n 18) 98.
84 Ye, ‘Tort Law Protection’ (n 18) 98; Luo (n 31) 78-80.
85 GDPR, art 18(3).
86 Draft Law, art 30(5)(6).
87 GDPR, rec 68. See Paul de Hert and others, ‘The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services’ (2013) 34 CLS Rev 193, 194-196, 200, 202 f.
88 GDPR, art 20(2).
but still falling quite short, Art. 11 Protection Regulations 2013 provides that the controller shall ‘supervise and manage’ the processor and shall ‘not entrust an agent who does not meet the requirements of these Regulations’. Lastly, Art. 9.1 Standard 2020 adds that controllers cannot let processors process outside of the consent given to themselves, and that controllers shall assess information security impacts, define the responsibilities and record the processing. Processors, on the other hand, must promptly tell controllers when deviating from their requirements or when unable to provide adequate security, assist controllers in responding to requests from information subjects and delete all personal information after the termination of their relationship. Concerning joint controllers, only Art. 9.6 Standard 2020 provides, less comprehensively than Art. 26 GDPR, that they must determine their respective responsibilities regarding information security and clearly inform the information subject. As a result, obligations similar to those in Ch. 4 GDPR mostly apply only to the controller. This is the case e.g. for the duty to cooperate with authorities or to keep relevant records.

A special Chinese obligation without a counterpart in the GDPR is real-name registration, which has already existed extensively in many fields for more than a decade. It is given broad coverage by Art. 6 Decision 2012 and Art. 24(1) CSL, which obliges controllers that provide network access or other services to ‘require users to provide true identity information’ and otherwise not to offer services to them. Otherwise, following Art. 61 CSL and in part Art. 11 Decision 2012, administrative fines, business suspensions, closures of websites and withdrawals of the business license are possible. These rules are very controversial. On the one hand, they are supposed to support the enforcement of the law against defamatory speech, fraud and other kinds of cyber criminality and to strengthen network and data security. On the other hand, many fear negative implications for privacy and freedom of speech, as it reduces online anonymity and increases the possibilities of state monitoring. After all, anonymity can be vital for those who wish to express critical and sensitive comments about politics, society and other subjects without risking damage to their reputation and more serious harm. Studies show that after the implementation of such rules the amount of politically sensitive content fell significantly, which caused some to assume that such rules were mainly introduced to reduce such speech. Furthermore, a weak data protection system raises concerns regarding the security of identity data transmissions. Accordingly, less restrictive measures appear preferable.

2. Security of personal data

Article 111 General Provisions and Arts. 12 f. Standardizing Regulations 2012 state that controllers shall strengthen information security without explaining how this is to be accomplished. A little more concretely, other regulations include the legal duty to carry out technical and other necessary measures for this purpose and to take immediate remedial action in the event of data breaches. Articles 13, 15 f. Protection Regulations 2013, Art. 6 Draft Administrative Measures and in part Art. 4.1.3 Guidelines 2013 add more specific measures that already exceed those of the GDPR in number such as data security education, training, plans for data security, risks and emergencies, clarification of responsibilities, internal control mechanisms, evaluation and protection systems, periodic self-inspections, commission of independent evaluation agencies, clarification of responsibilities, access controls and secure storage of information carriers. Article 19 Draft Administrative Measures further lists data classification, backup and encryption. Most extensive is the Standard 2020, containing all of the above-mentioned provisions and including additional, data minimisation, the separation of the roles of security managers, data operators and auditors as well as automated audit systems. Articles 21, 25, 34, 38 CSL contain many of the above-mentioned measures, but formulate these in regard to network security in general and limit some duties to critical information infrastructures. All in all, the Chinese regulations do not differentiate the measures in regard to the risks in the same way as the GDPR. However, as Chinese legislation has a stronger focus on security than the GDPR, it generally provides more details, guidance and clarity in this area.

Once more unlike the GDPR, the newer and draft Chinese provisions contain obligations to provide timely information to competent authorities and information subjects whenever data breaches occur and not only if it is ‘likely to result in a high risk to the rights and freedoms of natural persons’. However, only Arts. 10 ff. Standard 2020 describe the contents of such surveillance, see Moritz Buchi and others, ‘The Chilling Effects of
communication, which are almost identical to those of the GDPR, but without a specific time frame and adding recommendations for autonomous prevention and remedial measures.

3. Data protection impact assessment and prior consultation

Article 35(1) GDPR provides that when processing is ‘likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact […] on the protection of personal data’. The norm adds detailed rules as to the procedure and content of this assessment. If the results indicate that there is a high risk, the controller should consult the supervisory authority.

Before the disclosure of personal information, Art. 27 Draft Administrative Measures obliges controllers to assess the possible security risks, naming a few exceptions such as anonymisation or necessity for the national security and public interest. More detailed but still quite different from the GDPR is the Standard 2020, which more generally requires data protection impact assessments in cases where processors are involved or when sharing, transferring or publicly disclosing personal information. In both cases, there is no obligation to consult authorities, although this could be helpful and necessary.

4. Data protection officer

Following Art. 37(1) GDPR, a data protection officer is obligatory if ‘the processing is carried out by a public authority or body’ or when the ‘core activities’ involve data subjects or sensitive data on a large scale. In the remaining cases, the designation is voluntary. Chinese regulations vary, sometimes simply obliging every controller and sometimes being limited to state organs or important and sensitive personal information. However, only Arts. 17, 18(2) Draft Administrative Measures and Art. 11.1 Standard 2020, like Arts. 37(5), 38(2)(3) GDPR, require that controllers have to support the officer to maintain his or her independence and that the officer must have the necessary professional qualities. Concerning the tasks, only Art. 11.1(4) Standard 2020 and in part Art. 4.1.3(1) Guidelines 2013 are more elaborate, covering those enumerated in Art. 39(1) GDPR. The Standard 2020 further requires the development of a privacy policy, a policy concerning access to the personal information and the establishment of a list of the types, quantity, sources and recipients of the personal information held by the organisation. Especially the last measure could prove to be useful for examinations.

To sum up, unlike the GDPR, some regulations contain a more general duty to appoint a data protection officer. On the other hand, there is mostly no mention of independence, and the tasks are less well described. Exceptions to the latter are the Guidelines 2013 and the Standard 2020, which list even more than the GDPR and could serve as a positive example.

5. Codes of conduct and certification

Articles 7, 21 Protection Regulations 2013 and Art. 11 CSL quite generally state that internet industry associations should strengthen industry self-discipline and formulate self-regulatory management systems, but, unlike the GDPR, do not specify any requirements or consequences. More similar to the GDPR but still less concrete, Art. 39 Draft Law stipulates that self-regulatory norms by non-State organs ‘shall have the same effect as this Law if they meet the standards [of] this Law and are approved by the competent authorities.’ However, there is as yet no enacted provision resembling Art. 41 GDPR that gives the possibility to legally enforce or monitor self-regulatory regulations, which weakens the power of the Chinese measures. Data protection certification is briefly mentioned in Art. 34 Draft Administrative Measures, in contrast with the more developed Arts. 42 f. GDPR. Nonetheless, the implementation of voluntary provisions such as the Guidelines 2013 and the Standard 2020 that provide a higher protection level than the binding ones may indicate that China’s policy-makers generally favour self-regulation to stricter norms.

VI. Transfers of personal data to third countries

Concerning cross-border transfers of personal data, Arts. 44-50 GDPR require an adequacy decision from the Commission concerning the level of data protection in the third country or other safeguards such as binding corporate rules or approved codes of conduct. In China, regulations concerning state secrets and other specific matters can be very restrictive in this regard. Article 5.4.5 Guidelines 2013, on the other hand, simply requires the express consent of the information subject, specific legal provisions or the consent of the competent authorities. The only norm similar to the GDPR is Art. 24 Draft Law. It provides a requirement of a minimum protection standard like Art. 45 GDPR, mainly referring to equivalence and adding violations of Chinese laws or public order and morality as rather vague prohibition grounds. Especially the latter could allow arbitrary decisions by the responsible departments, making cross-border transfers more difficult and unpredictable.

However, before the Draft Law is enacted, Art. 37 CSL is the most important norm in this area. It lays down that personal information and undefined ‘important data’...
‘collected and generated by operators of critical information infrastructures in the course of their operations in [...] China’ shall be stored within the country. Only if it is ‘really necessary’ and a security assessment does not indicate any dangers is transfer possible.120 The scope of this data localisation rule could be extended to all controllers upon enactment of the binding ‘Draft Measures for Transfer’.121 Experts doubt that the responsible authorities have enough capacities to fulfil these obligations.122 Nevertheless, strict data localisation is seen as an important means to achieve cyberspace sovereignty and network security, the main goals of the CSL.123 Beyond that, it is supposed to strengthen supervision and legal enforcement.124 However, as foreign enterprises are forced to run domestic servers for their users in China, significant costs and worries concerning the security of those servers arise.125 Domestic companies, on the other hand, criticise that this rule may hinder their global operations and expansion.126 Others fear the growing control of the government.127 All of this causes Art. 37 to be one of the most controversial regulations in the CSL.128

VII. Independent supervisory authorities

The GDPR requires each Member State to have independent public authorities responsible for monitoring and facilitating a consistent application of the GDPR throughout the EU.129 Such an independence does not exist in China, since the authorities are subordinated to the central government.130 Moreover, instead of a central authority with broad responsibilities, many different state authorities are involved, leading to inconsistent implementation, coordination issues and unforeseen results.131 As a consequence, businesses often have to deal with many different authorities for one processing act, which creates inefficiencies and costs.132 Furthermore, some legal provisions do not clearly state the competent authority nor specifically list their tasks and powers, creating much uncertainty.133 One important reason for these issues is the lack of an enacted comprehensive data protection law and the insufficient efforts to align the data protection regulations.134

VIII. Remedies, Liability and Penalties

1. Right to lodge a complaint and right to an effective judicial remedy

Articles 77-79 GDPR give information subjects and, in the case of Art. 78 GDPR, natural and legal persons the right to lodge a complaint with a supervisory authority and to an effective judicial remedy against supervisory authorities, controllers or processors. Article 9 Decision 2012, Art. 4.1.2 Guidelines 2013 and Art. 14(1) CSL entitle individuals and organisations to complain or report to competent authorities, the former provision also adding a right to sue. Under Arts. 15(2), 47 Consumer Protection Law consumers and consumer associations have the same rights, making it the only law containing a norm similar to Art. 80 GDPR.

2. Right to compensation and liability

Under Art. 82(1) GDPR, ‘any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.’ Controllers and processors are not exempt from liability unless they prove that they were in no way responsible for the damaging act, which is quite difficult.135 Thus the GDPR provides for strict civil liability, which largely releases data subjects from the burden of proof and makes it easier for them to claim damages.136

In contrast, Art. 74(1) CSL briefly states that ‘whoever violates [...] this Law and causes damage to others shall be subject to civil liability’. There is no further guidance concerning e.g. the burden of proof, and it is disputed whether this norm imposes strict liability or not.137 Similarly, Art. 11 Decision 2012 stipulates civil liability for those violating the civil rights and interests of other people, without clarifying whether there is a right to compensation.138 Such a right is expressed briefly in Art. 50 Consumer Protection Law. Article 30 Draft Administrative Measures only mentions civil liability in the context of data security incidents in third-party applications. Articles 40 f. Draft Law stipulate civil liability and compensation for damage if violations of the provisions of the Draft Law caused personal or property damage or non-material losses to the information subject. Moreover, Art. 42 Draft Law regulates joint violation,
giving the information subject the right to claim damages from two or more relevant controllers if they are unable to identify the infringer.

The Tort Liability Law and the Civil Code are much more extensive and, since the latter will replace the former, very similar in their wording. Both include almost identical exceptions to liability, such as if the acts were carried out within the scope of the consent given, if it was reasonably necessary to protect the public interest or the lawful rights and interests of the natural person and if information has been disclosed legally. For both, compensation for losses is a central form of civil liability. They regulate joint and several liability similarly to Art. 82(4)(5) GDPR. Alongside material damage, serious non-material damage is also compensated and there is much guidance concerning this. The regulations stipulate fault-based liability. Strict liability only applies to medical institutions that infringe the patient’s privacy, personal information or medical records. However, proving fault can be very difficult due to the speed and immateriality of virtual data traffic, leading to a low number of civil cases. Thus, from a data protection perspective, strict or at least tiered liability systems appear preferable.

3. Administrative fees and penalties

According to Art. 83(1) GDPR, administrative fines imposed by the supervisory authorities shall be ‘effective, proportionate and dissuasive’. They can be imposed in addition to warnings, reprimands, temporary or definitive limitations including processing bans, withdrawal of certifications or the suspension of data flows to third

countries. Article 83(2) GDPR lists some relevant factors when determining the fine, such as the nature, gravity and duration of the infringement. In the case of certain infringed regulations, the fines may amount to 10,000,000 or 20,000,000 EUR or 2 or 4% of the total worldwide annual turnover of the preceding financial year. Especially for cases not covered by Art. 83 GDPR, Member States are required to establish criminal or administrative sanctions that are ‘effective, proportionate and dissuasive’. All of these strict penalties are the main incentive for compliance with the GDPR.

In China, some regulations criminalise, for example, the illegal sale or provision of personal information, where a sentence of up to three years imprisonment and a fine is possible, or, where ‘circumstances are particularly serious’, up to seven years. There are many more regulations concerning administrative measures, which are also the main tool to ensure compliance. Most vaguely, Art. 43 Draft Law merely stipulates administrative responsibility in cases of violations. Article 11 Decision 2012 briefly mentions that fines are possible. Article 56 (1)(i) Consumer Protection Law adds more concrete amounts for the fines, stating that the fine imposed may be ‘not less than one and not more than ten times the unlawful proceeds’ or, in the absence of such, up to 500,000 RMB. Articles 16-19 Standardizing Regulations 2012 and Arts. 22 f. Protection Regulations 2013 regulate fines in more detail, linking the violation of specific regulations to specific penalties, which may amount up to 30,000 RMB. Most extensive are Arts. 59-75 CSL, which contrast with the other regulations of the CSL in their level of detail, indicating that the CSL mainly depends on these sanctions for its enforcement. However, even its highest fine of up to 1,000,000 RMB (roughly 130,000 EUR) is still very low compared to Art. 83 GDPR.

Apart from monetary penalties, in particular the Consumer Protection Law, CSL and the Draft Administrative Measures list many different kinds of administrative measures that exceed those of the GDPR. Sanctions can consist of a warning, order to correct, confiscation of the illegal proceeds, suspension or closure of the business, website or communication groups, cease and desist order, revocation of relevant business licences, temporary or definitive ban from the profession, property freezing, detention up to five days and the recording and publishing of these sanctions in the ‘Social Credit Register’ and other forms of ‘public exposure’ such as the public announcement of these measures. Particularly noticeable are the numerous so-called ‘name and shame’
sanctions, which, in contrast to the EU, have a long tradition in China as tools for social control. In particular, recording in the Social Credit Register and publication thereof is an unusually strong ‘name and shame’ sanction, as this in turn can lead to a high number of additional negative consequences. To create incentives for conformity, the ‘Social Credit System’ is expected to rate the trustworthiness of all citizens and companies in China by analysing large amounts of behavioural data. In view of the severe issues of legal enforcement, the Chinese government and the media present it as a crucial tool for making citizens and companies comply with the law. Although it is still evolving, its central idea of ‘trust-breaking here, restrictions everywhere’ leads to a strong focus on manifold connected punishments rather than rewards, and already affects the lives of many people. The right of appeal against administrative acts is most likely not sufficient to exclude disproportionate sanctions.

IX. Conclusion

In China, there is no unified data protection law comparable to the GDPR. Instead, relevant provisions are contained in many different regulations, which in combination show the level of data protection. From a European perspective, the enacted binding Chinese provisions are too general and leave many important aspects unregulated, already starting with the absence of clear definitions. Except for administrative sanctions, the non-binding and draft regulations are much more comprehensive and detailed, often equal to or even exceeding the GDPR.

One reason for these issues is the above-mentioned legal fragmentation and the lack of a central competent authority, resulting in many overlapping and vague responsibilities. These circumstances also make enforcement very difficult, as investigations by the NPCSC in 2017 concerning the CSL and another independent study from 2019 have shown. Accordingly, there is a need for a comprehensive, unifying law on data protection and corresponding adjustments of the other regulations as well as a centralised independent supervisory authority with broad competences.

Another reason could be that in the context of data protection, the Chinese government strongly focuses on national security and stability instead of fundamental rights. This could also explain the relative lack of a balancing of interests in Chinese law as compared to the GDPR. Additionally, this most likely accounts for some of the biggest differences to the GDPR, such as the obligatory real-name registration and the design of the data localisation rules. These two measures could be detrimental to the protection of personal data, as they, for the sake of security, extend state access to a large amount of data held by the private sector. Seen in combination with numerous other laws authorising state access, the image of a growing surveillance system becomes reality, beginning with the ‘hukou’ (户口) household registration system, which controls the mobility of citizens, and ending with the emerging Social Credit System. In this context, influential Chinese scholars stress the value of data as a resource for social management by the state, which could serve as a justification for refraining from a strict regulation of the public sector. Mirroring this, most of the earlier regulations only apply to the private sector, unlike the more recent laws and the draft regulations. However, as the government strongly pursues ambitious data processing projects such as the Social Credit System, it is very likely that at least in certain sectors there will continue to be exceptions for state actors.

Despite these problems, there are a lot of positive dynamic developments in the Chinese data protection legislation. The CSL and the new Civil Code signify important steps towards a stronger national data protection regime. Furthermore, many drafts are evolving that strongly emphasise privacy protection alongside security interests and indicate that legislation will largely continue to move in the European direction. While it is not clear whether and in what form the drafts will be enacted, the Chinese government shows much willingness to develop a more comprehensive data protection system. The pressure to do so is increasing as the data protection awareness of the population grows.

156 Florian Thünen and Björn Alpermann, ‘Technologie gegen den Werteversfall? Chinas “Soziales Bonitätsystem”’ [2018] Forschung & Lehre 474, 476.
157 Yu-Jie Chen, Ching-Fu Lin and Han-Wei Liu, “Rule of Trust”: The Pressure and Perils of China’s Social Credit Megaproject (2018) 32 Colum J Asian L 1, 13-19.
158 Notification of the State Council concerning the Issuance of the Planning Outline for the Construction of a Social Credit System (2014-2020) (国务院关于印发社会信用体系建设规划纲要（2014-2020年）的通知) Guo Fa [2014] 21 (国务院 [2014] 21号) (Planning Outline), ex preamble and cl 1(1)(3), 3(2)(5), 5(1); Feng (n 1) 67.
159 Planning Outline, preamble and cl 1(2)(3). Mareike Ohlberg, ‘Central Planning, Local Experiments: The Complex Implementation of China’s Social Credit System’ [2017] 2 ErK 5, 13 <www.merics.org/en/china-monitor/central-planning-local-experiments> accessed 20 July 2020; Larry Catà Backer, ‘Next Generation Law: Data-Driven Governance and Accountability-Based Regulatory Systems in the West, and Social Credit Regimes in China’ [2018] 28 Cal Interdisc LJ 123, 127 f, 130-136, 169 f; Karen Li, Xin Wang and Amy Shields Dobson, ‘We’re Just Data: Exploring China’s Social Credit System in Relation to Digital Platform Ratings’ (in Chinese) (2019) 4(2) Global Media and China 220, 221.
160 Notification of the General Office of the Communist Party of China Central Committee and the State Council on ‘Opinions on Accelerating the Construction of Credit Supervision, Warning and Disciplinary Mechanisms for Dishonest Persons Subject to Enforcement’ (中共中央办公厅国务院办公厅印发《关于推进失信被执行人信用监督、警示和惩戒机制建设的意见》的通知) Zhong Ban Fa [2016] 64 (中共中央 [2016] 64号) of 25 September 2016, art 1(1). Yongxi Chen, ‘A Đế Đà Ý Vu? The Social Credit System and Faisha (Legalism)’ (Verfassungsblog, 28 June 2019) <https://verfassungsblog.de/a-dej-a-yu-the-social-credit-system-and-faisha/> accessed 20 July 2020; Chen, Lin and Liu (n 157) 13-19; Wong and Dobson (n 159) 224.
161 Greenleaf, Data Privacy (n 3) 220; eg Consumer Protection Law, art 59.
162 Qi, Shao and Zheng (n 28) 1348; Ding, ‘Private Law’ (n 2) 196; Binding (n 3) 335 f; Zhang (n 66) 44.
163 Feng (n 1) 74 f. See also Xu (n 3) 252.
164 Zhang (n 66); Liming Wang (王立明), ‘Promoting the Ordrely Development and Sharing of Data (促进数据有序开发和共享)’ (2019) <http://opinion.china.com.cn/opinion_57_211357.html> accessed 20 July 2020; Feng (n 1) 81.
165 Palmen (n 7) 316, 327.
166 Feng (n 1) 67; Greenleaf, Data Privacy (n 3) 195.
167 See the very often cited paper Zhang (n 66) 45 f, 48, 56. See also Feng (n 1) 74.
168 Zhang (n 66) 39; Binding (n 3) 336.
169 Feng (n 1) 69; Kipker, ‘Cybersecurity Law’ (n 93) 460.
170 Yun Liu (刘云), ‘The Development of European Personal Information Protection Law and its Reform and Innovation (欧洲个人信息保护法的发展历程及其制度改革)’ (2017) 39(2) Jizian Journal 72; Feng (n 1) 83; Xu (n 3) 252.
171 Ding, ‘Personal Data’ (n 1) 380 f; Feng (n 1) 62 f, 68, 78 f.
172 Sun and Wang (n 14); Feng (n 1) 76-78; Xie (n 13) 71; Zhu (n 78) 107; Yu (n 18) 467; Binding (n 3) 327, 334 f.
All in all, although from a European point of view the Chinese data protection law is still ‘fragmentary, insufficient, ineffective and hard to understand’, it has already improved considerably and will continue to move in a positive direction when the draft provisions are enacted.

ACKNOWLEDGEMENTS
I would like to thank Klaus Wiedemann, Meiting Zhu, Dr. Simon Apel and the reviewers for their very valuable contributions and insightful comments. All translations are my own.