IRDG | Institut für das Recht der digitalen Gesellschaft

UNIVERSITY OF PASSAU
Faculty of Law

UNIVERSITY OF PASSAU IRDG RESEARCH PAPER SERIES NO. 22-15

ENDEAVOUR TO CONTAIN CHINAS' TECH GIANTS

Country Report on China

Sarah Lena Hünting

Juni 2022

Place of Publication

University of Passau IRDG
c/o Chair of German and European Private Law, Civil Procedure, and Legal Theory
Innstraße 39
94032 Passau

https://www.jura.uni-passau.de/irdg/

Author

Sarah Lena Hünting is a research associate at the University of Passau (Chair of Public Law, Media Law and Information Law) in parallel to her legal clerkship at the Higher Regional Court Munich.

Abstract

The report analyses current information law regulations in China and focuses on the data protection system. This includes relevant Chinese legislation and decisions from 2012 onwards. The main emphasis of the article lies on the recently enacted Personal Information Protection Law (PIPL), the formerly mainly relevant Cybersecurity Law, and its accompanying Standards. Although the PIPL's key considerations still miss implementing regulations, guidelines, and application examples, this newly enacted legislation has far-reaching effects and alludes to a stringent regime.

This report was written within the framework of a comparative research project between various countries including the research areas of legal studies, cultural studies, and business informatics.

Cite as

Hünting, S. (2022). Endeavour to Contain Chinas' Tech Giants – Country Report on China. *University of Passau Institute for Law of the Digital Society Research Paper Series No. 22-15*. https://www.jura.uni-passau.de/irdg/publikationen/research-paper-series/.

Keywords

Data Protection law, Data localisation, Law, Technology, China, Privacy, Data Disclosure.

Contents

A) Generalities 1

I) Cultural vectors of Data Disclosure 1

II) Legal System and Lawmaking 2

B) (General) Legal System of Information Law 5

I) Structure of Information Law 5

II) Allocation of Informational Legal Positions 7

III) Institutions 7

IV) Procedural Aspects 8

C) Regulations Concerning Disclosure of Personal Data 9

I) Legal Structure of Data Disclosure 9

II) Notions 14

1) (Personal) Data as Object of Protection 14
2) Allocation of Data to a Person 15
3) Reception and Recipient 16

III) Relationship between Discloser and Recipient 18

1) Provisions for Disclosure 18
   (a) Prohibited Disclosures 18
   (b) Disclosure Obligations 19
   (c) Voluntary Disclosure/Voluntariness 20
2) Recipient's Obligations 20
   (a) Requirements for Personal Data Reception 20
   (b) (Procedural) Obligations Concerning Received Personal Data 21
3) Control by Discloser – ex post 22
   (a) Transparency and Right to Request Information 22
   (b) Co-Determination and Co-Decision Concerning Data Use 22
   (c) Revocation 23
   (d) Procedural Aspects 24
4) Enforcement 24
   (a) Damages and Compensation 24
   (b) Procedural Aspects 24

IV) Objective Legal Obligations of the Recipient 25

1) Obligations Concerning Received Data 25
   (a) Dependence on Authorisation 25
   (b) Notification Obligations 26
   (c) Documentation 26
   (d) Processing Requirements 27
   (e) Prohibitions and Obligations 29
2) Monitoring 30

(a) Recipient's Self-Monitoring 30
(b) Regulated Self-Regulation 31
(c) Supervisory Authorities 31
(d) (Specific) Criminal Proescution 32
(e) Procedural Aspects 32
3) Enforcement 32
(a) Interventions Concerning Data Processing 33
(b) Interventions Concerning Business Models 33
(c) Sanctions for Processors/Processor-related Sanctions 33
(d) Sanctions for Individual Actors 34
(e) Procedural Aspects 34

D) Sources and Literature 35

E) Legal Framework 35

A) Generalities[1]

I) Cultural vectors of Data Disclosure

(Identification of cultural [pre]conditions for individual data disclosure: cultural parameters that may the decision to disclose one's personal data; cultural practices and expectations regarding data disclosure [eg taboos]; data protection and privacy discourse, particularly articulated calls for reform); narratives and stories concerning data disclosure; synonyms for 'Data Protection' and 'Privacy' in the respective language)

The need to protect personal data has been increasing in China in recent years. Influenced by Confucianism, Chinese culture deems the collective above the individual.[2] The state's focus is on moral, ethical and appropriate behavior of said individual. Considering this collective oriented culture, it has been argued that this caused the lack of privacy protection.[3] The fact that the protection of the state's interests and the social group is preferable (to those of the individual) is reflected in legal practice as well as in the way of communication.[4] Yet, culturally similar regions such as Taiwan show data protection laws going beyond the Organization for Economic Co-Operation and Development's (OECD) standards.[5] The political situation in mainland China seems to be one driving factor, which precluded the emergence of Western style privacy protection. If one follows *Case's* classification, a senior lecturer in Southeast Asia with a research focus on Comparative Politics and Southeast Asian politics, into full-, semi- and pseudo-democratic regimes, China is to be classified as a (broad) authoritarian regime.[6]

This blank can also be seen at a linguistic level, considering that the Chinese language does not encompass the concept of privacy. The equivalent is 'yin si' (隐私)[7], which means a shameful secret that should not be made public in order not to damage the reputation of the individual, his/her family or the nation.[8] The protection of privacy was, thus, previously considered necessary in areas where there was a threat of damage to reputation.

With the occurrence of the 'human flesh searches' (renrou sousuo[9]) (2006–2008),[10] the need to protect not only intimate secrets, but also increasingly other personal data developed within society. However, these simultaneously reflect the morally dominant idea that

[1] This report is part of an interdisciplinary research project on individual data disclosure: Vectors of Data Disclosure – A comparative study on the disclosure of personal data from the perspectives of legal, cultural studies, and business information systems research, supported by the Bavarian Research Institute for Digital Transformation (bidt). <https://www.bidt.digital/en/vectors-data-disclosure/>.

[2] Snejina Michailova and Kate Hutchings, 'National Cultural Influences on Knowledge Sharing: A Comparison of China and Russia' [2006] 43(3) Journal of Management Studies 394.

[3] For a detailed discussion see Tiffany C. Li, Jill Bronfman and Zhou Zhou, 'Saving Face: Unfolding the Screen of Chinese Privacy Law' [2017] Journal of Law, Information & Science 4.

[4] Xiaoyan Huang, *Technik versus Recht* (Nomos 2020) 142.

[5] The OECD issued its first Privacy Guidelines in 1980, which were updated in 2013. Christine Chen and Michael R. Fahey, 'Data protection in Taiwan: overview, Practical Law Country Q&A' (Thomson Reuter Practical Law, 29 July 2020) <https://uk.practicallaw.thomsonreuters.com/5-578-3485?transitionType=Default&contextData=(sc.Default)&firstPage=true> accessed 10 February 2022.

[6] William Case, *Politics in Southeast Asia, Democracy or less* (Routledge 2002) 8–9.

[7] Elia Zureik, *Surveillance, Privacy and The Globalization of Personal Information: International Comparisons* (McGill-Queen´s University Press 2010) 203.

[8] For further analysis of the term 'si' (private) see Philip C. C. Huang, 'Biculturality in Modern China and in Chinese Studies' [2000] 26(1) Modern China 5.

[9] Internet users try to gather all personal data of a person who has behaved immorally and put them online, to be punished by the public.

[10] Liu Han, 隐私权、言论自由与中国网民文化:人肉搜索的规制困境 ('Privacy rights, freedom of speech and Chinese netizen culture: the regulatory dilemma of "human flesh searches"'), 中外法学 [2011] 4 Peking University Law Journal, 870–871.

the bearer of the right to privacy is also part of a moral society.[11] Yet, the biggest concern is the misuse of data by private concerns, rather than the state.[12]

The domestic social economic development, international trade and economic exchange are driving factors to observe the international standard of privacy and personal data protection which China had to consider in the past few years. [13]

II) Legal System and Lawmaking

(central characteristics; sources of law and legal hierarchies; classification of legal systems); lawmakers and influential political and societal movements)

China is a unitary State, ruled by one party with an elaborate system of political, social and economic control.[14] The regions are divided into 34 administrative districts[15] which are not considered to be independent; Hong Kong and Macau as special administrative zones are conferred the necessary autonomy to diverge from China's system (Art 31 of the Constitution). The systems to be instituted in these special administrative regions shall be prescribed by law, enacted by the National People's Congress. Therefore, the Peoples Republic of China has three different jurisdictions (mainland China, Hong Kong and Macau), each having its own laws.[16] Further, China follows its 'One-China policy', considering Taiwan as part of China, applying the Hong Kong formula, 'One Country, two systems'.[17] Nevertheless, different from Hong Kong, there is a complete state apparatus in Taiwan and controversies on this view. China's view is based upon the 1992 Consensus, according to which Taiwan is bound to China.[18] This report only covers the situation in mainland China.

The Chinese Communist Party (CCP) is the dominant political party and primary political organ. Its structure and the State structure are very closely connected and fused at various junctures.[19] Leading government positions are occupied with top leaders of the party and its members are posted throughout the

[11] Liu Han, 隐私权、言论自由与中国网民文化:人肉搜索的规制困境 ('Privacy rights, freedom of speech and Chinese netizen culture: the regulatory dilemma of "human flesh searches"'), 中外法学 [2011] 4 Peking University Law Journal 878.

[12] Frank Sieren, 'China regelt Datenschutz neu' (Table China, 25 January 2022) <https://table.media/china/analyse/china-regelt-datenschutz-neu/> accessed 10 February 2022.

[13] Hong Xue, 'Privacy and personal data protection in China: An update for the year end 2009' [2010] 26 Computer Law & Security Review 289.

[14] Richard McGregor, *The Party: The secret world of China's Communist rulers* (Penguin Books 2010).

[15] 23 provinces (Taiwan is considered as one of those provinces); 5 autonomous regions; 4 directly governed cities; 2 special administrative zones.

[16] 中华人民共和国宪法 1954 (Constitution of the People's Republic of China 1954), adopted on 20 September 1954, repealed on 17 January 1975; promulgated on 17 January 1975, repealed on 5 March 1978; promulgated on 5 March 1978, repealed on 4 December 1982; promulgated on 4 December 1982, amended on 12 April 1988, amended on 23 March 1992, amended on 15 March 1999, amended on 14 March 2004, amended on 11, March 2018. Art 31, Art 62(13) Constitution of the PRC <http://www.npc.gov.cn/englishnpc/constitution2019/201911/1f65146fb6104dd3a2793875d19b5b29.shtml> accessed 10 February 2022; Joint Declaration of the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the People´s Republic of China on the Question of Hong Kong effective 27 May 1985.

[17] Under the Preamble of the Constitution of the PRC (n 15), Taiwan is part of the sacred territory of the PRC. For further analysis see Yihu Li, 'The "one country, two systems' solution to Taiwan: two comparative analyses' [2020] China International Strategy Review 270–287.

[18] Taiwan and China interpret this Agreement differently. For further information see Yu-Jie Chen and Jerome A. Cohen, 'China-Taiwan relations Re-Examined: The "1992 Consensus" and Cross-Strait Agreements' [2019] 14(1) University of Pennsylvania Asian Law Review 7.

[19] Wen-Chen Chang, Li-Ann Thio, Kevin Tan and Jiunn-rong Yeh, *Constitutionalism in Asia: Cases and Materials* (Oxford and Portland 2014) 175.

government apparatus.[20] The main organs include the National Party Congress (NPC)[21] (legislature), State Council[22] (executive) and the Supreme People's Court (judiciary). Due to its size the NPC is rather inefficient, wherefore it elects a Standing Committee to act on its behalf, when not in session (the NPC meets once a year).[23] Under Art 67 of the Constitution it is responsible for interpreting the Constitution and for supervising its implementation.

Rod Rosenstein, Deputy Attorney General of the U.S., pointed out that in China 'the law is an instrument of state power, a mechanism for rulers to maintain control and quash dissent'[24], thus following a rule through/by law instead to the rule of law.[25] The Chinese legal system is formed by many individual laws, supplemented by widely ramified secondary law. At the top of these is the Constitution (Art 5 of the Constitution), which lists the fundamental rights of Chinese citizens in its second chapter. These do not only guarantee rights but also define the citizens' duties towards society. Nevertheless, the fundamental rights contained therein cannot be enforced against the State due to the lack of constitutional jurisdiction. Human rights in China are conceived as being derived from the State itself, meaning that the state's interests remain above the individuals.[26] In addition, Art 51 of the Constitution enshrines that the exercise of fundamental rights by an individual may not impair the interests of the State or society. The mentioned human rights rather seem to be a program set which the legislature is responsible to codify by statutory regulations. Laws must be formally and materially enacted in conformity with the constitution.[27] Administrative regulations, local provisions, autonomous regulations, special regulations etc., are based on different legal systems and have different levels of development. The Constitution does neither mention international law as a source of law, nor are there any implementing provisions concerning the extent to which it is applicable.[28]Observing the legislative practice, international law is automatically implemented as part of PRC law and binding provisions prevail over domestic law.[29]

The rank of (national) law is higher than that of administrative regulations, local provisions and rules. The force of administrative regulations is higher than that of local regulations and rules.[30] Typically there is not one main law covering a legal area, but several parallel laws.[31]

---

[20] Wen-Chen Chang, Li-Ann Thio, Kevin Tan and Jiunn-rong Yeh, *Constitutionalism in Asia: Cases and Materials* (Oxford and Portland 2014) 174.

[21] Arts 57, 59, 60, 62 Constitution of the People's Republic of China.

[22] Arts 85, 89 Constitution of the People's Republic of China.

[23] Chang, Thio, Tan and Yeh, (n 20) 176.

[24] U.S. Department of Justice, Deputy Attorney General Rod J. Rosenstein Delivers Remarks at the Center for Strategic & International Studies Event on Defending Rule of Law Norms. Paper presented at the Center for Strategic & International Studies, Washington, 25 Feburary 2019 <https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-center-strategic-international> accessed 10 February 2022.

[25] In August 2018, President Xi said that the Chinese Communist Party must strengthen its leadership over the law <http://en.people.cn/n3/2018/0825/c90000-9494097.html> accessed 10 February 2022.

[26] Jyh-An Lee, 'Hacking into China's Cybersecurity Law' [2018] 53(1) Wake Forest Law Review 100.

[27] Art 5 Constitution; Art 100 Constitution <https://english.www.gov.cn/archive/lawsregulations/201911/20/content_WS5ed8856ec6d0b3f0e9499913.html> accessed 23 February 2022; Art 78 Legislation Law of the PRC, 2000 <http://www.china.org.cn/english/government/207419.htm> accessed 10 February 2022.

[28] Hongyi Chen, *An Introduction to the Legal System of the People's Republic of China* (Butterworths Asia 1992) 103.

[29] ibid.

[30] Art 88 Law on Legislation.

[31] Mathias Lejeune, 'Datenschutzrecht der Volksrepublik China' (2021) 3 PinG Privacy in Germany 109

A hierarchy is determined in accordance with Art 83 Law on Legislation, which states 'for the laws, administrative regulations, local regulations, autonomous regulations, special rules, administrative rules or local rules enacted by the same body, if a special provision is different from a general provision, the special provision shall prevail; if a new provision differs from an old provision, the new provision shall prevail'. Nevertheless, the enacted law is not coherent.[32]

This divergence can especially be seen, when looking at the rules and case law governing the transfer of property. The decisions of the Supreme People's Court, show that the separation principle is applied[33] – and that divergences are solved by case law. The contract law is based on the 'unity principle' while the rules and case law governing property are based on the 'separation principle'.[34] According to Art 51 Contract Law (1999) a contract concluded by a party without disposition right shall be invalid unless the transaction is ratified by the right owner or the contracting party receives the right. Opposing this rule, Art 3 SPC Interpretation on dealing with Sales Contract Disputes (2012) specified that 'the people's court shall not support the claim to invalidate a contract made by a buyer on the ground that the seller does not have the disposition right'. This Interpretation is influenced by the Property Rights Act (enacted 2007). According to the provision of Art 15 Property Rights Act, the contract made between the parties concerned on the creation, alteration, transfer or extinction of the property right of immovables shall become valid as of the time when the contract is concluded and the absence of an entry in the land register shall not affect the validity of the contract, unless the law provides otherwise. Opposing this, again, Art 130 Contract Law, the contract of sale in this law is a contract by which the seller transfers ownership of the object of sale to the buyer and the buyer pays the purchase price. According to the wording of this provision, it is considered that the transfer of ownership in Chinese law takes place directly based on the 'contract of sale' (again, unitary principle). The Contract Law remains unchanged and valid until today.

In principle, laws are kept simple and concise. The legal literature commonly acknowledges that Chinas legal system is characterized by broad and flexible laws.[35] They are determined through judicial interpretation or ministerial regulations, giving the government room for maneuverability and flexibility in interpreting and enforcing the laws as well as preventing them from being rapidly outdated. Law interpretations by the Standing Committee of the National People's Congress (SA-NPC)[36] and the Supreme People's Courts[37] constitute separate norm-setting acts.[38] In the development of the Chinese legal system, gaps in specialized areas of law are often first filled by administrative law provisions before a generally applicable law, often encompassing a broader regulatory framework, is enacted. Besides these statutory laws, policy norms are enacted, either by

<https://doi.org/10.37307/j.2196-9817.2021.03.13> accessed 10 February 2022.

[32] Cf Xianchu Zhang, 'The New Round of Civil Law Codification in China' [2016] 1(1) University of Bologna Law Review 135.

[33] For further information see Yuanshi Bu, *Einführung in das Recht Chinas* (2nd edn, C.H. Beck 2017) 22.

[34] Meiying Fu, 'Abstrakte Sicherheiten in China und Deutschland' (Dr. jur. thesis, Universität Freiburg 2016) 226.

[35] See generally Deborah Cao, *Chinese Law: A Language Perspective* (1st edn, Routledge 2004).

[36] Art 67 No. 1, 4 Constitution of the PRC; Art 47 Legislation Law of the PRC.

[37] Decision of the Standing Committee of the National People's Congress on Strengthening the Work of Law Interpretation (CLI.1.1006, 10 June 1981) <http://www.lawinfochina.com/display.aspx?lib=law&id=28&CGid> accessed 04 February 2022.

[38] Albert Chen, *An Introduction to the Legal System of the People's Republic of China* (1st edn, LexisNexis 1992) 94.

the State (state policies) or by the CCP. Standards are used as guidance for the implementation of laws. They set technical requirements for agricultural, industrial, service industries and social undertakings etc. which require standardization.[39] Products and services must comply to be provided.[40] The legal value of these texts is ruled by the Standardization Law (2017) which sets two kinds of standards:[41] compulsory standards and recommended standards, which the State encourages to adopt.

B) (General) Legal System of Information Law

I) Structure of Information Law

(constitutional and basic rights aspects; relevant regulations concerning intellectual property, secrecy, cybercrime [data privacy aut idem infra at C.]; Which regulations are based on international provisions [especially concerning intellectual property]?)

A first enhancement of Intellectual Property (IP) rights occurred in 1992, to access the Paris Convention for the Protection of Industrial Property and the Berne Convention. As from World Trade Organization (WTO) accession, the IPR system in China has experienced a comprehensive process of improvement and adaptations to international standards. With the Chinese Trademark Law, Patent Law, Copyright Law and further regulations in this field, China has adopted international norms and harmonized its legal system with the rest of the world in the area of IPRs.[42] Changes in material law hardly showed any effect in the actual safeguarding of informational legal positions.[43] The reason for the lack of protection was the poor legal enforcement, which changed with the complaint brought by the USA against China before the WTO arbitration court.[44]

In its IP Strategy (2008), which set a roadmap for China to become a country of advanced IP creation, utilization and protection by 2020, China committed itself to carrying out a number of judicial reforms to strengthen the protection of IP rights. The goal of becoming an 'IP Power Country' was further set out in the 2020 published plan for further implementation of the National IP Strategy to Accelerate the construction of an IP Power Country by 2020.

Although the fundamental right to freedom of speech and press has been recognized since the first Constitution of the People's Republic of China,[45] the media sector is (still) heavily restricted. Rights related to mass media law such as the right to government information, right to privacy and right to defamation, have also been recognized and protected under a variety of laws and regulations. According to Art 33(3) of the Constitution, the State respects and protects conferred human rights yet, due to the lack of a constitutional court, an enforcement of constitutional rights

[39] Art 2 Standardization Law 2017 <https://share.ansi.org/Shared%20Documents/News%20and%20Publications/Links%20Within%20Stories/China%20Standardization%20Law_English%20translation_SESEC_5.17.2017.pdf> accessed 10 February 2022.

[40] Art 25 Standardization Law 2017.

[41] Art 2 Standardization Law 2017.

[42] See Permanent Mission of the PRC to the UN Office at Geneva and other International Organizations in Switzerland, *New Progress in China's Protection of IPRs* (2005) <https://www.fmprc.gov.cn/ce/cegv/eng/zywjyjh/t193102.htm> accessed 28 January 2022.

[43] Donald P. Harris, 'The Honeymoon is Over: Evaluating the United States' WTO Intellectual Property Complaint Against China' [2008] 32 Fordham International Law Journal 2.

[44] China — Measures Affecting the Protection and Enforcement of Intellectual Property Rights (DS362, 10 April 2007) <https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds362_e.htm> accessed 28 January 2022.

[45] (n 16), Art 87 (1975); Art 28 (1978); Art 45 (1982); Art 35 (2004); Art 35 (2018).

against the State is not possible.[46] Moreover, courts do not apply constitutional norms directly.[47] The Constitution does not mention any specific fundamental rights concerning protection of personal information. These are only broached in Art 38 et seq of the Constitution, standardizing the inviolability of dignity and privacy at home. In addition, Art 40 grants protection against interference with the freedom and privacy of correspondence (an exception applies to state organs for the purpose of maintaining public security). However, as alluded before, an enshrinement in constitutional law would not grant effective and individually enforceable protection.[48] Until today, one landmark decision of the Supreme People Court referred to the Constitution, determining that private parties must abide to the constitution.[49]

While the printing press went through a transition from state-owned entities to private commercially-owned entities, TV and radio entities are still entirely state-owned with tight content censorship or self-censorship requirements.

Protective provisions of the criminal law (Artt 285, 286, 287a and 287b, which also provide for criminal liability of legal persons) are primarily directed at computer information systems instead of protecting data. In 2017, the Cyber Security Law (CSL) was enacted[50] to combat cyber criminality by ensuring network security, network operational security, critical infrastructure protection, data security and protection and legal accountability.[51] Only recently a comprehensive data protection law has been enacted, which enhances the data protection established by the CSL. China is a member of the World Intellectual Property Organization, as well as other international agreements on the protection of IPR, namely the Paris Convention, Berne Convention and TRIPs agreement, so that in principle the scope of IPR protection is the same.

The Data Security Law (DSL) grants authority to China's Central Government to establish a hierarchical data categorization system in accordance with the importance of the data to China's economy, national security, livelihood of Chinese citizens and public and private interests. This system will result in data deemed more important to China's national interest being more heavily regulated. To this point, the DSL focuses on two categories of data subject to a heightened level of regulation and protection: 'important data' and 'national core data'. The concept of 'important data' was introduced in the CSL, requiring elevated protection, a localization requirement and a prior security assessment for cross-border transfer of important data by critical information infrastructure operators ('CIIOs'). While the CSL and DSL do not define 'important data,' the DSL states that a consortium of national-level agencies will develop catalogue(s) of 'important data' and mandates that local governments and regulatory agencies develop more detailed catalogues to identify the scope of 'important data' based on their respective

---

[46] Björn Ahl, 'Hoffnung auf Rechtsreformen' [2013] ZChinR 10. Christina Eberl-Borges, *Einführung in das chinesische Recht* (Nomos 2018) 85.

[47] Björn Ahl, 'Normative oder semantische Verfassung? Der Diskurs in der Volksrepublik China um die Vereinbarkeit des Sachenrechtsgesetzes mit der Verfassung' [2008] 41(4) VRÜ 482.

[48] Qianfan Zhang, 'A constitution without constitutionalism? The paths of constitutional development in China' [2010] 8(4) International Journal of Constitutional Law 950.

[49] See generally Shen Kui and Yuping Liu, 'Is it the Beginning of the Era of the Rule of the Constitution? Reinterpreting China's First Constitutional Case' [2003] 12 Washington International Law Journal; Qi Yuling v. Chen Xiaoqi Case of Infringement of Citizen's Fundamental Rights of Receiving Education Under the Protection of the Constitution by Means of Infringing Right of Name, 13.08.2001, withdrawn on 18.12.2008.

[50] Dennis-Kenji Kipker, 'Das neue chinesische Cybersecurity Law' [2017] MMR 456.

[51] Ibid; Xiaoyan Huang, *Technik versus Recht, Zu Internetkriminalität und Datenschutz im deutsch-chinesischen Vergleich* (19 Robotik und Recht, Nomos 2020) 79.

region and sectors. 'National core data', is considered as a class of data subject to stricter regulations due to its relation to national security, the national economy, citizens' livelihoods and important public interests.

Non-personal information is only protected partially (eg by Art 37 CSG domestic storage obligation).

II) Allocation of Informational Legal Positions

(commodity/commoditization, especially 'intellectual property'; collective goods; public goods)

Intellectual property law is a specific legal system for ensuring, protecting and utilizing copyright, industrial property and other exclusive rights of creators, as well as encouraging intellectual innovations.[52] Informational Legal Positions protected under the copyright law are the exclusive rights of authors and disseminators of literary, artistic and scientific works, while patent law protects industrial inventions or creations which include inventions, utility models and designs. Other protected positions are product trademarks and service trademarks, products of geographical indications in the country, the breeder of a new plant variety by means of manual cultivation and field exploitation; scientific discoveries, domain names, well-known images, goodwill, databases, etc.

Any invention developed in China, regardless of the nationality of the inventor, requires a confidentiality examination by the Chinese patent administration department before it is applied for a patent abroad. If this requirement is circumvented, the invention can no longer be protected in China.[53] Moreover, China operates a 'first to file' principle. If two people apply for a patent on an identical invention, the first one to file the application will be awarded the patent.

Besides demanding three constitutive requirements (originality, reproducibility and human intellectual creation) the Chinese Copyright Law also lists forms of works (Art 3 Copyright Law, Art 4 Regulation for the Implementation of the Copyright Law), especially referring to 'Qu yi', typical Chinese works related to regional culture.

III) Institutions

(information supervisory authorities; private institutions/organisations [industry and sectoral associations], including international ones; public administration und cultivation/management of informational goods)

The China Trademark Office works under the State Administration for Industry and Commerce and oversees trademark registration and administration nationwide, specifically registering and administering trademarks, protecting trademark rights and handling trademark infringement and counterfeiting cases. The Copyright Office is an administrative agency responsible for regulating and distributing news, print and Internet publications in China. Moreover, there are several ministerial level authorities for different departments.[54] Formerly known as the State Intellectual Property Office (SIPO), the China National Intellectual Property Office (CNIPA), is the centralized administrative institution responsible for the protection of IP rights as well as the registration, administrative adjunction and facilitation of the establishment of the IP protection system. With its reorganization in 2018, the administration of patents, trademarks, geographical indications of origin and layout design of integrated circuits, have been centralized within the CNIPA.

---

[52] Wu Handong, '论反不正当竞争中的知识产权问题' [2013] 35(1) Modern Law Science 37.

[53] Art 19 I, IV Patent Law 2021 <https://www.wipo.int/edocs/lexdocs/laws/en/cn/cn028en.pdf> accessed 10 February 2022.

[54] Eg Administration for Industry and Commerce (AIC).

In course of the cybersecurity extension (see also C. I. below) new institutions as the National Security Committee, Central Cybersecurity and Informatization Committee and the National Security Council were established. The latter one being a subsidiary of the Communist Party of China's (CPC) Central Committee and therefore being the central decision-making and coordinating body on national security issues. Later on the CPC's Cybersecurity and Informatization Committee was established, being responsible for cybersecurity and informatization in various fields.

IV) Procedural Aspects

(Kontrolle und Durchsetzung; individuell; kollektiv; durch Verbände; obrigkeitlich [behördlich und gerichtlich])

Any citizen, legal person or organization entitled to intellectual property rights which have been infringed may bring a lawsuit to the people's court. Being civil rights, the court is empowered to order the infringer to end the infringement, to remove any negative effects caused, to apologize and compensation for any losses. Furthermore, the infringer's illegal gains may be confiscated and/or criminal detention or a fine may be adjudged.[55] The State may prosecute infringements under the Criminal Law. Therefore, the case must be brought to the Public Security Bureau for criminal investigation. If the case is accepted it is passed to the prosecution agency, which assesses whether the case may proceed to trial. Punishment includes imprisonment and penalties. Other options of individuals to enforce IP rights include administrative actions and customs seizure.

China's laws concerning IPRs are mostly consistent with its TRIPs obligations[56], nevertheless the enforcement of those laws is lacking. The reason for this issue is widely discussed among scholars, with substantial disagreement. While some doubt the power of the central government to control the provinces[57], others question the government's commitment to IP enforcement.[58]

In 2014 China established its first three intellectual property courts, adding four more IP tribunals in 2017 and finally establishing a combined trial of civil, criminal and administrative elements of IP infringements.[59] The tribunals resemble the courts yet, having cross-regional jurisdiction over the entire province. Remedies sought in civil proceedings include injunctions, damages, delivery-up of infringing goods and declaration of infringement.

Trademark counterfeiting can be enforced through the civil courts, administrative enforcement through the State Administration for Industry and Commerce (SAIC), Administration of Quality Supervision, Inspection and Quarantine (AQSIQ), State Food and Drug Administration (SFDA) and Ministry of Health (MOH) or criminal enforcement. The number of cases handled by the court system is many times lower than the amount of administrative enforcement.[60]

Copyright infringement can also be enforced administratively and through courts.

[55] Information Office State Council of the People's Republic of China, Intellectual Property Protection in China, June 1994 <https://www.mfa.gov.cn/ce/cegv//eng/bjzl/t176937.htm> accessed 04 February 2022.

[56] Yahong Li, 'The Wolf Has Come: Are China's Intellectual Property Industries Prepared for the WTO?' [2002] 20(1) UCLA Pacific Basin Law Journal 88–89.

[57] Joseph A. Massey, 'The Emperor is Far Away: China's Enforcement of Intellectual Property Rights Protection, 1986-2006' [2006] 7(1) Chicago Journal of International Law 232, 237.

[58] Lusita Lusita, 'Counterfeiting in China: A Great Challenge in Intellectual Property Protection' [2012] 9(2) Indonesian Journal of International Law 329.

[59] Richard Li, Chuanshu Xu and Hui Zhang, 'China's Specialized IP Courts' (Kluwer Patent Blog, 10 April 2017) <http://patentblog.kluweriplaw.com/2017/04/10/chinas-specialized-ip-courts/> accessed 04 February 2022.

[60] Martin Dimitrov, *Piracy and the State, The Politics of Intellectual Property Rights in China* (Cambridge University Press 2009) 189.

Responsible for copyright protection is the Ministry of Culture (MOC) and the State Administration for Industry and Commerce (SAIC). Furthermore, Copyright enforcement is mainly offered by quasi-judicial enforcement, where requests from right holders are examined in-house at the National Copyright Administration of China (NCAC) and resolved through mediation or by the imposition of an administrative punishment, including confiscating and destroying infringing goods and imposing fines.[61] Furthermore, several regions have stipulated, that in case of non-compliance with administrative injunctions, the infringer will be included in a list of dishonest persons under the public credit information system.[62]

Patent enforcement is provided by a single agency – the State Intellectual Property Office (SIPO) – providing administrative enforcement and courts.

C) Regulations Concerning Disclosure of Personal Data

I) Legal Structure of Data Disclosure

(existence of 'Data Protection Law'; mandatory and nonmandatory regulation; differentiation between public and private sector; public or private sector as a role model for regulation; general or sectoral regulation; self-regulation [codes of conduct]; basic principles of regulation [preventive ban or freedom of processing]; risk-based approach [potential for misuse; protection of certain categories of data]; privileged areas [personal and family sphere; media; research])

Personal Information Protection Law 2021[63] (PIPL)	Binding
Cybersecurity Law 2017[64]	Binding
Information Security Technology - Personal Information Security Specification 2018[65] and 2020[66]	non-binding guideline; national Standard
NPC 2012 Decision[67]	Binding

By 2014, China had taken the first steps to establish protection to personal data. Due to the late start, China has had the possibility to turn to existing US and EU models solving the same issues. The country first considered going the EU route with a comprehensive law covering the entire scope of personal data, before renouncing and resorting to an US approach. Unlike the US, data privacy right focuses solely on consumers whereas citizens (in general) do not enjoy the same level of

[61] See <https://www.ncac.gov.cn/chinacopyright/channels/12577.shtml> accessed 28 January 2022.

[62] Luo Rui, 'The power of administrative injunctions in patent infringement' (2021) China Business Law Journal <https://law.asia/administrative-injunctions-patent-infringement-china/> accessed 23 February 2022.

[63] Personal Information Protection Law of the PRC (中华人民共和国个人信息保护法) enacted by the Standing Committee of the NPC, effective 01 November 2021 <http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml>.

[64] Cybersecurity Law of the PRC (中华人民共和国网络安全法) enacted by the Standing Committee of the NPC, effective 01 June 2017. (Transaltion: <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/> accessed 10 February 2022.

[65] Information Security Technology – Personal Information Security Specification – (GB/T 35273-2017) (信息安全技术 个人信息安全规范) issued by National Information Technology Standardization Technical Committee, effective 1 May 2018.

[66] The Information Security Technology – Personal Information Security Specification (GB/T 35273-2020) (信息安全技术 个人信息安全规范) issued by National Information Technology Standardization Technical Committee, effective 01 October 2020. (Also called 'Privacy Standard') <https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf> accessed 10 February 2022.

[67] Adopted on 28 December at the 30th Committee Meeting of the 11th NPC Standing Committee <http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm> accessed 03 June 2021.

protection as part of their civil liberties. An expert responsible for drafting China's latest guidelines stated that 'we are stricter than the US, but not as strict as the EU'.[68] The enacted laws can be described as data privacy with Chinese characteristics, which are especially endorsed by the cyber-sovereignty principle (see also C. III. 2. b. below) and the separation between privacy from private actors and privacy from the government.[69] Instead of the term 'personal data', Chinese laws do not use a uniform term (see also C. II. 1. below).[70] There is no clear distinction between personal data (个人数据, 'ge ren shu ju') and personal information (个人信息, 'ge ren xin xi').[71] Data (shu ju) literally means 'referring itself to numbers' and is used in everyday language to describe information which is stored electronically. The term rather concerns the form of presentation of information, while the term 'xin xi' can be traduced as 'news' and rather focuses on the transfer of content. As equivalent to the European Data Protection laws 'personal data' term, Chinese laws use 'personal information'. This is due to different legal traditions and does not lead to terminologically inherent legal consequences.

Until recently the Chinese data protection law was rather sporadic and sectoral. The currently existing Chinese 'data protection law' has evolved from a security aspect, with a focus on the protection of persons and property (as opposed to a fundamental rights-based approach)[72] and an ex-post curative rather than ex-ante expressive effect. The governments access to data is increasing and spurred by innovations such as facial recognition. First regulations concerning businesses' use of personal data were overall more concerned with public security rather than personal privacy.[73] The development of core data protection principles came with the emergence of cloud computing, big data analytics and Edwards Snowden's revelations. With the development of the Social Credit System (SCS) the national Planning Outline called for regulating the protection and handling of personal information[74] and the Guidance on Personal Creditworthiness introduced requirements on the collection of Personal Credit Information (PCI).[75] The (local) regulations on SCS use the term PCI to refer to personal information on loans and transactions and other information that may reflect an individual's credit situation. Similarly, the Guidance on Standardizing the SCS (2020) emphasize privacy protection and

[68] Yanqing Hong, 'Responses and explanations to the five major concerns about the Personal Information Security Specification' (对《个人信息安全规范》五大重点关切的回应和解释) (2018) Weixin <https://mp.weixin.qq.com/s/rSW-Ayu6zNXw87itYHcPYA> accessed 04 February 2022.

[69] Emmanuel Pernot-Leplay, 'China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.' [2020] 8(1) Penn State Journal of Law & International Affairs 54.

[70] Abu Bakar Munir, Siti Hajar Yasin and Ershadul Karim, *Data Protection Law in Asia* (1st edn, Sweet & Maxwell 2014) 283.

[71] Lei Yi, 'Daten als eigentumsrechtlicher oder immaterialgüterrechtlicher Gegenstand in China' [2019] GRUR International 239.

[72] Anja Geller, 'How Comprehensive is Chinese Data Protection Law' [2020] 69(12) GRUR International 1195.

[73] Yanfang Wu, Tuenyu Lau, David Atkin and Carolyn A. Lin, 'A comparative study of online privacy regulations in the US and China' [2011] 35 Telecommunications Policy 613.

[74] Planning Outline for the Construction of a Social Credit System (2014–2020) – 社会信用体系建设规划纲要 – State Council Notice (14 June 2014) <https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/> accessed 02 February 2022.

[75] Guiding Opinions on Strengthening the Construction of Personal Integrity System, issued by the State Council, 23 December 2016 <https://www.chinalawtranslate.com/7079-2/> accessed 02 February 2022.

requires the government to observe principles of legality, legitimacy, necessity and minimization when collecting and using personal information.[76] There is also specific sectoral legislation as for consumer protection, banking, insurance, telecommunications and so forth, which will not be analyzed in this context.

The wrongdoing on privacy and personal information is sanctioned by the Criminal Law on several occasions.[77] The Tort Liability Law explicitly protected the right of privacy along with the right of reputation and the right of honor.[78] As part of the reform of the General Part of the Civil Code[79] (CC), Art 111 of the CC was inserted, which regulates the protection of personal information – the right to protection of privacy is conferred according to Art 110 CC and Art 1032 – and underlines the responsibility of individuals and organizations for data protection and collection. The protection of personal information is further stipulated in Art 1034. Among the general rules for personality rights (Book four of the CC) Artt 994–1000 CC confer rights regarding the prosecution of rights because of breaches concerning privacy and data protection. Chapter six establishes further measures regarding protection of personal information. According to Art 127 CC laws providing for the protection of data and network virtual property shall be applied, showing that Chinese legislation treats Personal Information as a personality and a property right.[80]

Considered as the highest level law specifically dealing with data protection issues was the 'Decision on Strengthening Information Protection on [Electronic] Networks' that was promulgated by the Standing Committee of the NPC (2012 NPC Decision). It only grants protection to Chinese citizens and also applies to the public sector.[81] It explicitly states the goal to protect network information security, the lawful interests of citizens and to safeguard national security and social order.[82] It is applicable to network service providers and other enterprise and work units that collect or use citizens' individual electronic information during their business activities.[83] The Chinese Ministry of Industry and Information Technology (MIIT) released two sets of regulation[84] (the latter one not repealing the former) as well as a set of Guidelines (more

[76] Further Improving Systems for Restraining the Untrustworthy and Building Mechanisms for Building Creditworthiness that have Longterm effect, General Office of the State Council, 07 December 2020, VII (14).

[77] Art 253a CL, Art 252 CL.

[78] Art 2 Tort Law. Tort Liability Law, effective as of 01 July 2010, as of 01 January 2021 constituting part VII of the PRC Civil Code (n 79).

[79] Civil Code of the PRC, 中华人民共和国民法典, effective 01 January 2021 <http://www.npc.gov.cn/english-npc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf> accessed 10 February 2022.

[80] Qu Bo and Hua Changxu, 'Privacy, National Security and Internet Economy: An Explanation of China's Personal Information Protection Legislation' [2020] 15(3) Frontiers of Law in China 347; See also C. II. 1.

[81] Graham Greenleaf, 'China's NPC Standing Committee Privacy Decision: A Small Step, Not a Great Leap Forward' [2013] 121 Privacy Laws & Business International Report 2.

[82] Preambel 2012 NPC Decision.

[83] Art 2 2012 NPC Decision.

[84] 2011 MIIT Regulations – Several Regulations on Standardizing Market Order for Internet Information Services (规范互联网信息服务市场秩序若干规定), (adopted 07 December 2011, effective 15 March 2013); 2013 MIIT Regulations - Regulations on Protecting the Personal Information of Telecommunication and Internet Users (电信和互联网用户个人信息保护规定), which entered into force on 1 September 2013; Information Security Technology – Guidelines for Personal Information Protection in Public and Commercial Service Information Systems (信息安全技术公共及商用服务信息系统个人信息 保护指南)) – Guidelines 2013. Voluntary standard under previous Standardization Law (GB/Z).

The Chinese executive has considerable regulatory power and its regulations have a similar effect to parliamentary acts, though ranking lower than laws and other regulations of the NPC and NPCSC, see Graham

comprehensive but only voluntary in nature), to ensure implementation. The regulations apply to the collection and use of personal user data in the process of providing telecommunications services and internet information services within China, including requirements of minimum data collection, inform and data breach notifications, applying to Internet Service Providers (ISPs) and telecommunication business operators. Also, provisions in the Consumer Protection Law 2014 and E-Commerce Law 2019 broadly referred to personal information protection, as well as local legislation and further standards.

Also binding and considered as one of the first high-level laws that regulate data protection, is the Cyber Security Law of the PRC 2017 (CSL), which focuses on cyber security law, but has a broad concept of it, encompassing information security including data protection and therefore making a step towards comprehensive data protection law. Data protection law provisions are found in Art 22(3) and Artt 40–45 of the CSL. According to the cyber-sovereignty principle (Art 1 CSL), cyberspace is subordinated to the interests and values of a country within its borders, i.e., the application of state sovereignty to cyberspace. To ensure its sovereignty over a cyberspace a country may exert control over the internet architecture, content and data flows often for security purposes.

The requirements set out by the CSL remain so general that guidance texts are required. The 2020 and 2018 Specifications, which have a strong connection to the GDPR, were issued for implementation and concretization of personal data privacy regulations (and is a resumption of the MIIT Guidelines 2013 [structurally very similar]). The Specifications are much closer to the GDPR concerning definitions on different types of personal information and requirements on childrens' personal information, regulating the relationship with an entrusted party, the record of personal information processing activities and adopting an approach for the use of de-identified information[85]. They are of non-binding nature, being labeled as 'best practice guides', being especially helpful for companies to establish an adequate data security management system.[86] Drafters complained about internal contradictions of the Laws, arguing that they had great difficulties trying to fit the Standards within the Parameters of the CSL.[87] Due to their non-binding nature no direct penalties apply when contravening.

Under the CSL, if a data activity takes place in China, China will apply its data protection law to this activity.[88] According to the Data Security Law (DSL), data processing activities outside the PRC that threaten the national security of the PRC, the public interest, or the legitimate interests of Chinese citizens or organisations, will also be pursued under the DSL. A similar provision can be found in Art 42 PIPL which stipulates that restrictive or even prohibitive measures may be taken by regulators against organisations and individuals outside China who engage in activities that harm the rights and interests of Chinese citizens or harm the national security or public interest. At the same time PIPL applies to those who process personal information about

Greenleaf, *Asian Data Privacy Laws, Trade and Human Rights Perspectives* (Oxford University Press 2017) 205; Jörg Binding and Anna Radjuk, 'Die Rangordnung der Rechtsnormen in der VR China' [2009] 11 RIW 786-789.

[85] De-identification is not referred to in the CSL.

[86] Mathias Lejeune, 'Datenschutzrecht der Volksrepublik China' (2021) 3 PinG Privacy in Germany 110 <https://doi.org/10.37307/j.2196-9817.2021.03.13> accessed 10 February 2022.

[87] Drafters noted that the CSL left them 'dancing while waring shackles' 洪延青 [Hong Yanqing], «对'个人信息安全规范' 五大重点关切的回应和解释» [Responses and Explanations to the Five Major Concerns of the 'Personal Information Security Specification'] (网安寻路人 – Wanganxunluren), 5 February 2018 <https://mp.weixin.qq.com/s/rSW-Ayu6zNXw87itYHcPYA> accessed 01 February 2022.

[88] Art 50 CSL.

individuals inside the territory of the People's Republic of China (Art 3 I) as well as those who process personal information outside the territory of China, where any of the following circumstances exists: (1) the handling activity is related to offering of any goods or services to that individual residing in China, (2) the handling activity is related to analysis and assessment of behavior of that individual residing in China, or (3) any other circumstances as provided by laws and administrative regulations (Art 3 II).

The Data Security Law, which entered into force on 01 September 2021, regulates data processing activities associated with personal and non-personal information. It is primarily concerned with data protection and data activities of entities.

The PIPL, which entered into force on 01 November 2021 regulates personal information handling activities and promotes the rational use of personal information, establishing duties for data controllers (see also C. III. 2.; C. IV. below) and rights for disclosers (see also C. III. 3. below). In terms of content, the law adopts a large part of the provisions of the 2020 Specifications. The law applies equally to companies and individuals (see also C. II. 3. below) who collect personal data from individuals within China and has extraterritorial effect.

The aforementioned regulations were introduced in the areas of private and criminal law. Processing activities by the government are mainly regulated in the Open Government Information Regulations (OGIR)[89]. However, provisions only refer to the disclosure of Personal Information and do not limit the collection of it. Personal Information protection rules for the collection and use of financial credit data can be found in the Regulations on the Administration of Credit Investigation Industry (RACII)[90]. They are lex specialis in this field, applying to all credit investigations and related activities carried out in China, including the collection, organisation, storage, further processing and provision of financial credit data by the state-held financial credit information system (FCIS).[91] Accordingly, the collection and transfer of information to the FCIS by financial institutions is subject to the RACII. This system is the most sophisticated arm of the Social Credit System (SCS). The Chinese Personal Information Protection laws enacted until 2020, did not provide comprehensive protection for the personal information processed in this system, the applicable scope of the PIPL remains to be seen.[92] There is still no legal framework concerning the construction of the SCS, a big data empowered system,[93] which until now is not unified but rather based upon multiple coexisting SCSs at different sectoral and local levels.[94] Regulations can be found at local level, while at national level, the traces of the SCS which can be found, are based upon the 'planning outline'[95] as well as further guiding opinions,

[89] Open Government Information Regulation, effective 15 May 2019 <https://www.chinalawtranslate.com/en/open-government-information-regulations-of-the-p-r-c-2019/> accessed 14 February 2022.

[90] Regulations on the Administration of Credit Investigation Industry, 'Chenxinye guanli tiaoli', effective 15 March 2013 <http://www.lawinfochina.com/display.aspx?lib=law&id=12585&CGid=&EncodingName=big5> accessed 14 February 2022; The term personal credit information is used to refer to personal information on loans, transactions and other information that may reflect an individual's credit situation.

[91] Art 2 RACII.

[92] Lu Yu and Björn Ahl, 'China's Evolving Data Protection Law and the Financial Credit Information System. Court Practice and Suggestions for Legislative Reform' [2020] 51 Hong Kong Law Journal 21.

[93] Yongxi Chen and Anne SY Cheung, 'The Transparent Self under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System' [2017] 12(2) The Journal of Comparative Law 377.

[94] Chuncheng Liu, 'Multiple Social Credit Systems in China' [2019] 21(1) Economic Sociology: The European Electronic Newsletter 22–32.

[95] State Council of the People's Republic of China, Planning Outline for the Establishment of a Social

eg: for the establishment of blacklists and redlists.[96] A first draft of a Social Credit Law was formulated in December 2020. Planning outlines are not considered to be material law, they map an implementation strategy and define the core function. Also, in many cases, existing regulation for specific sectors has been updated to include provisions stating that violations of rules will be recorded in credit files (see also C. IV. 3. e) below).

II) Notions

1) (Personal) Data as Object of Protection

(situational [spoken words etc.]; local/spatial [at home]; logical ['spheres']; informational [datum, information]; treatment of public or publicized data; limitations and expansions of notions; categories)

The term 'personal information' (个人信息) can have a different meaning, depending on the context in which it is used (see also C. I. above). Due to Art 111 CC[97] systematic position close to Art 109 CC, which establishes the right of personal liberty and dignity, it can be assumed that the data's content is decisive in this context, while the focus in Art 127 CC rather lies on the form. The latter one is positioned between protected rights, which differ according to the type of qualification of the object of protection, wherefore the form and not the content is relevant. Furthermore, the CC does not mention any form of data property or ownership, while one of the top-level policy documents[98] stated to 'establish and improve mechanism on data property transaction'.[99]

Personal information is primarily considered part of a natural person's representation on the internet,[100] whereby the possibility to individualize a natural person is always decisive. Due to the lack of possibility of direct identification of an individual, anonymized data is seen as non-personal information.

Personal data is generally referred to in laws as personal information. The definition of 'personal information' largely coincides with that of 'personal data' under Article 4(1) of the GDPR in the sense that both focus on the identification of the data subject and give similar examples (see also C. I. above).[101] While the CSL defines personal information as 'information recorded electronically or through other means, that taken alone or together with other information, is sufficient to identify a naturals persons identity'[102], the Standards[103] went further stipulating it as information that can be used to identify or track a person, also covering information reflecting the activities of an individual.[104]

Early regulations as Art 3.2 MIIT Guidelines 2013 define personal information of users as 'any information which can be attributed to a user and which can be used alone or in combination with other information to identify a

Credit System (2014-2020) (社会信用体系建设规划纲要 (2014—2020年) 的通知), 27 June 2014.

[96] Guiding Opinions on Establishing and Improving the Joint Incentive System for Trustworthiness and Joint Disciplinary System for Untrustworthiness (2016).

[97] There is a debate among legal Chinese scholars, on whether Personal Information is a legal interest or right, See Qu Bo and Hua Changxu, 'Privacy, National Security and Internet Economy: An Explanation of China's Personal Information Protection Legislation' [2020] 15(3) Frontiers of Law in China 352–354.

[98] Instruction on Improving the Market Mechanism for Allocating Essential Factors (中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见), effective 30 March 2020.

[99] Zhenbin Zuo, 'China's Data Strategies: Institutionalisation, Activation, and Layering' (to be published) 5-6.

[100] Vincent Winkler, *Rechte an Daten im Zivilrecht*, (8 Schriften zum Ostasiatischen Privatrecht, Mohr Siebeck 2021) 37.

[101] See the definition in Art 76(5) CSL and Art 3.1 2020 Specification.

[102] Art 76(5) CSL.

[103] Art 3.1, Appendix A 2020 Specification.

[104] Comparing the definition in Art 76(5) CSL and Art 3.1, Appendix A 2020 Specification.

user'. A broader definition can be found in Article 4 of the MIIT Regulation 2013, which also covers information relating to the time and place of service and other information collected by service providers in the course of providing their services. Another early definition is to be found in 2012 NPC Decision Art 1 as 'information that can identify citizens and involve their privacy'.

According to Art 4 PIPL personal information is 'all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons'. It is clarified, that anonymized data shall not be considered as personal information. It can be assumed that the use of the terms 'related, 'identified', and 'identifiable' suggests that Chinese authorities likely will take a broad approach to interpreting what constitutes personal information in practice.[105]

Further categories of personal information are being distinguished. Sensitive personal information (Art 28 PIPL)[106] is personal information that, once disclosed or illegally used, may easily cause grave harm to the dignity, personal, or property security of natural persons, including information on biometric characteristics, religious beliefs, specially designated status, medical health, financial accounts, individual location tracking, etc., as well as the personal information of minors under the age of 14 (Consistent with 2020 Specification).

2) Allocation of Data to a Person

(creation; possession/control; personal connection; differentiation between domestic and foreign nationals; treatment of multi-referential data; limitations and expansions of notions; categories)

The existing data economy system in the PRC is predominantly governed by regulations of data transfer platforms, which regulate the relationship between the parties involved in data trade. In fact, about 80% of all data in the PRC is said to be in state hands.[107] Personal information is seen as a purely negative right of defence ('non-property law character'), although this is discussed controversially due to the introduction of Art 111 sent. 1 CC.[108]

According to the first draft of the CSL the identifiable person could only be a Chinese citizen, yet, the final version broadened the definition of data subject to any natural person.[109] The protection granted by Art 76(5) CSL for personal information presupposes the capacity (and not only a possibility) to determine a natural person.

Personal data rights are enjoyed by every individual nevertheless, the Chinese government reserves the right to collect data it deems important for maintaining public security, protecting the health and property of natural persons, as well as for public opinion monitoring in the public interest.

Art 127 Var. 2 CC introduced the legal institution of 'virtual property' (xuni caichan 虚拟财产) which is to be understood as a descriptive and not a normative legal term.[110] Unfortunately no definition is provided. It is commonly understood as the establishment of de facto protection of analogue objects by means of a digital representation in virtual space, which have a certain intrinsic value and are

[105] Hui Xu, Kieran Donovan and Bianca Lee, 'China introduces first comprehensive legislation on personal information protection' (Client Alert Commentary n 2894, Latham & Watkins, 8 September 2021) 2.

[106] Also, Annex B 2020 Specification. There is no clear differentiation between sensitive and non-sensitive information as for example property, biometric, health and physiological, information is listed as sensitive (Appendix A) and non-sensitive information (Appendix B) and the categorization depending on the perceived risk.

[107] Li Keqiang, Speech (China Big Data Industry Summit, Guiyang, 25 May 2016).

[108] Simon Werthwein, *Das Persönlichkeitsrecht im Privatrecht der VR China* (4 Schriften zum Chinesischen Recht, De Gruyter 2009) 38.

[109] Art 76(5) CSL.

[110] Vincent Winkler, *Rechte an Daten im Zivilrecht*, (8 Schriften zum Ostasiatischen Privatrecht, Mohr Siebeck 2021) 54.

fundamentally non-convertible.[111] Virtual does not necessarily refer to immaterial but is characterized by being framed in a virtual space.[112]

3) Reception and Recipient

(special regulation for non-profit/non-commercial actors; the public as a [legal] recipient; use of public data; specialised/special obligations for small and medium-sizes enterprises (SMEs); differentiation between recipients and third parties [especially within company groups]; differentiation between national and international actions; outsourcing options)

The CSL applies to 'network owners, managers and network service providers or application software providers who collect, distribute or use information'[113], 'suppliers of critical network equipment and specialized network security products'[114], in short, to virtually any company. The 2020 Specifications go further and clarify that it applies to all types of organizations handling personal information,[115] defining the personal information controller as the organization or individual that has the authority to determine the purpose and methods of the processing of Personal Information.[116]

Besides regulating Personal Information processing activities in the Mainland, PIPL also applies extraterritorially. According to Art 3 s. 1 PIPL processing personal data of natural persons from inside China is subject to the PIPL and Art 3 s. 2 stipulates that the processing of personal data of natural persons located in China from outside China is also subject to the PIPL, provided that a.) the data controller aims to provide products or services to natural persons located in China; or b.) the data controller analyses, evaluates the behaviour of natural persons located in China; or c.) it is otherwise stated in laws or regulations.

A definition of 'processor' is provided in Art 73 PIPL, referring to organizations and individuals that can independently determine processing purposes and processing methods. They are subject to most of the requirements in PIPL. Furthermore, section 3 regulates personal information processing by state organs, setting limits on government departments processing, but there are exceptions for public security and national security.[117] For example there is no specific provision on the processing of personal information during criminal investigations, wherefore it can be accessed by police officers.[118] It is specified in Art 72 PIPL that the law shall not apply to the processing of personal information by natural persons for personal or family affairs.

The new law also provides special regulations for special personal information processors as important internet platforms as well as general exceptions for governmental agencies[119] to process personal information in their public functions while strictly following (other) laws and regulations. As an exemption, Art 62 PIPL requires relevant authorities (the State Internet Information Department) to establish specific personal information protection rules and standards for small-scale processors, although no definition of small-scale processors is given.

There are general requirements and specific requirements on different kinds of Personal Information processors (eg, CIIO, Non-CIIO

[111] Definition given by an Announcement of the China Court Network <https://bjgy.chinacourt.gov.cn/article/detail/2017/05/id/2864056.shtml> accessed 17 November 2021.

[112] Lin Xuxia, *Untersuchung zum Recht an virtuellen Vermögen* (1 China Legal Science 2009) 89.

[113] Arts 22, 48, 68 CSL - Definitions are given in Art 76 CSL, missing a definition for CIIO.

[114] Art 23 CSL.

[115] Art 1 2020 Specifications.

[116] Art 3.4 2020 Specification.

[117] European Data Protection Board, Government access to data in third countries, November 2021, 22, 23.

[118] European Data Protection Board, Government access to data in third countries, November 2021, 16, 20.

[119] Art 34 PIPL.

processor with a processed Personal Information amount reaching or exceeding the quantity threshold specified by the Cyberspace Administration of China ('CAC')). CIIOs[120] face stricter requirements such as data localization. According to this, personal information, whether important or not, collected and produced by critical information infrastructure operators shall be stored within China.[121] When finalised, the Draft Measures[122] would apply to cross-border transfers of personal information and important data collected and generated in China by CIIO, which requires them to undergo a security assessment.[123] Further detail and clarity regarding cross-border data transfers is not provided, neither by the CSL nor the Specifications[124]. Moreover, CIIOs need to conduct a self-security assessment[125] addressing certain criteria.[126] Please note that the requirements for cross-border transmission of Personal Information also apply to Personal Information transfer from the mainland of China to Hong Kong SAR, Macao SAR and Taiwan, as they are deemed separate jurisdictions for the purpose of Personal Information Law.

Changes introduced by PIPL require to locally store personal information, collected and generated within mainland China, applying to personal information processors, whose processing of personal information reaches the number prescribed by the State cyberspace administration and CIIOs.[127] Regulations concerning cross-border transfer can be found in Artt 38–40 PIPL. They can be divided into general requirements which demand to:

– Adopt necessary measures to ensure the foreign receiving parties' personal information processing activities reach the standard provided in PIPL (Art 38),

– Notify the individuals of the foreign receiving party's contact information, processing purpose and processing methods, categories of personal information and procedures to exercise their personal information rights over the foreign receiving party (Art 39),

– Obtain the individual's separate consent (Art 39),

– To conduct a personal information protection impact assessments in advance (Art 55), and

– In case of international agreements, treaties or other laws, provisions therein concerning cross-border transfer must be met (Art 38).

Moreover, one of the following requirements must be met:[128]

– Pass a security assessment organized by State cyberspace authorities,

– obtain a certification in relation to personal information protection by a specialized body (under provisions of State cyberspace authorities),

– enter a standard contract as formulated by the State cyberspace authorities with the overseas receiving parties to stipulate the rights and obligations of both parties, or

– fulfill the requirements stipulated in other laws or regulations, or in the rules set by the State cyberspace authorities.

[120] The definition of CIIO is left to implementing regulations.

[121] Art 37 CSL.

[122] According to Art 37 CSL measures are to be jointly formulated by the State network information departments and the relevant departments of the State Council. Draft Measures on Security Assessment of Cross-border Data Transfer (released for Public Comment on 29 October 2021 (third legislative attempt)).

[123] Arts 34, 21 CSL.

[124] Art 9.8 2020 Specifications.

[125] Art 38 CSL.

[126] Further obligations for CIIO Arts 35, 36, 39.

[127] Art 40 PIPL.

[128] Art 38 PIPL.

Further regulations can be found in industry-specific regulations, as for example the Administrative Measures on Automotive Data Security. CIIOs and personal information processors, whose processing of personal information reaches the number prescribed by the State cyberspace administration, need to further pass the impact assessment conducted by said authorities, unless laws enacted by them provide for an exemption.[129]

If any other country adopts discriminatory prohibitive, restrictive or other similar measures against the People's Republic of China in respect of the protection of personal information, the People's Republic of China may take reciprocal measures against such countries.[130]

III) Relationship between Discloser and Recipient

1) Provisions for Disclosure

(Does regulation exist? personal data as intellectual property and commercial good; data law as a framework for action; 'informational self-determination')

The State has begun to regulate the collection of Personal Information by businesses for commercial purposes while himself having wide access to citizen's Personal Information.[131] Nevertheless, private tech companies and the State collaborate on data issues, questioning the former one's autonomy. Before PIPL, data localization was required for all kind of personal information and restrictions on cross-border transfer, offering the government economic control and preventing tech firms from becoming too powerful.[132]

Moreover, until recently regulations focused more on protecting national security rather than a citizen's privacy. A right to informational self-determination as recognized by German courts does not exist. The Chinese legal system recognizes a general personality right, yet with a limited scope of protection. Only recently, protection of personal information has been introduced into the new CC in form of a general clause in need of interpretation and specification (Art 111 CC, see also C. I. above), which does not confer a right on individuals.

Different regulations on disclosure can be found for different technologies. In case of facial recognition technology in public places, PIPL requires clear indicating signs[133] and the enactment of further rules[134]. Before Personal Information is being handled it is recognized, that the individual has the right to know, to decide, to limit and to refuse.

(a) Prohibited Disclosures

(protections of secrecy; multi-referentiality; disclosure to actors abroad; public communications)

Prohibitions referring to the manner of collection can be found in various laws. Those prohibit to deceive, trick or coerce the Personal Information subject to provide Personal Information. Furthermore, it is forbidden to obtain Personal Information from illegal channels.[135]

Regulations on Chinas Social Credit Systems[136] forbid the collection of certain sensitive personal information (as genetic data, blood types, fingerprints, information on diseases and religious beliefs). Further social Credit legislation (enacted by various local

[129] Art 40 PIPL.

[130] Art 43 PIPL.

[131] Adil Nussipov, 'How China Governs Data' (The CMDS Blog, 27 April 2020) <https://medium.com/center-for-media-data-and-society/how-china-governs-data-ff71139b68d2> accessed 23 February 2022.

[132] Ibid.

[133] Art 26 PIPL.

[134] Art 62 PIPL.

[135] Art 44 CSL; Art 5.1 2020 Specifications; Art 10 PIPL.

[136] 2013 Regulations on the Administration of The Credit Investigation Industry (RACII). 'Chenxinye guanli tiaoli'.

governments)[137] prohibit to collect information on religious faith, genetics, fingerprints, blood type, illness and medical history.

(b) Disclosure Obligations

(identification obligations and prohibition of anonymity; tax and other control)

The personal information gathered by private firms (like Tencent, Alibaba) has helped the government to fill the gaps within the 'household registration record system'. This system, known as the Hukou (户口)[138], documents birthplace, address, family members and marriages. When introduced in the 1950s,[139] it was used to control movement within China. By now the control of migration has been relaxed and it has been decentralized. Nevertheless, it still confers a 'status' on the citizen, linked to social services and social welfare, wherefore the registration remains necessary.[140] Over a period of four years, 14 million people have been registered, who had never been officially counted / registered within the country.[141] These people did not legally exist until then.

It is to be noted, that government requests for Personal Information are exempt from the CSL.[142] While containing broad data protection provisions, the CSL (and various other Chinese laws/regulations[143]) also sets up requirements of real-name user registration for ICT platforms[144], allowing the Chinese government to demand access to the local data of any person who uses online services in China, for national security or criminal investigation purposes.[145]

In 2006 the credit reference centre of the People's Bank of China was established to operate and maintain the national centralized commercial and consumer credit reporting system. It is the only national scoring bureau, to which banks and other financial entities are obliged to report on their client's creditworthiness. Non-financial information is transmitted from courts, government departments,

[137] Enacted by local governments, based upon the national guideline released 2014 by the State Council ('Planning Outline for the Construction of a Social Credit System 2014-2020' – 社会信用体系建设规划纲要), being the first policy plan for the construction of the SCS at national level. Local governments already instituted their own social credit initiative beforehand <http://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm> accessed 02 February 2022.

[138] For further information see 'The Residence Registration System' [2001] 34(3) Chinese Law and Government 9–51.

[139] Ministry of Public Security, Chengshi hukou guanli zanxing tiaoli (Interim Regulations on Urban Household Administration), issued on 16 July 1951; Decree of the President of the People's Republic of China, Zhonghua renmin gongheguo hukou dengji tiaoli (Regulations on Household Registration in the People's Republic of China), 9 January 1958.

[140] Marc Colas and Suqin Ge, 'Transformations in China's Internal Labor Migration and Hukou System' [2019] Journal of Labor Research 301.

[141] Echo Huang, 'China keeps Finding Millions of People Who Never Officially Existed' (Quartz, 27 March 2017) <https://qz.com/941240/china-keeps-finding-millions-of-people-who-never-officially-existed/> accessed 01 February 2022.

[142] Max Parasol, *AI Development and the 'Fuzzy Logic' of Chinese Cyber Security and Data Laws* (Cambridge University Press 2021) 155.

[143] Eg 'WeChat Articles' – Provisional Regulations for the Development and Management of Instant Messaging Tools and Public Information Services, SIIO (now CAC), 7 August 2014; Telephone User Real Identity Information Registration Regulations, MIIT, 16 July 2013.

2013 Regulations on the Administration of The Credit Investigation Industry (RACII). 'Chenxinye guanli tiaoli'.

[144] Art 24 CSL.

[145] Also, user terms (eg WeChat, Airbnb) make clear, that information can be shared with the government to comply with applicable laws are regulations <https://technode.com/2017/09/19/now-its-official-wechat-is-watching-you-1/ ; https://technode.com/2018/03/28/airbnb-china-host-data-privacy/> accessed 31 January 2022. There is an entire market for fake WeChat accounts to avoid real-name registration <https://technode.com/2019/01/16/wechat-accounts-sale-online-fraud/> accessed 31 January 2022.

telecommunication companies and fiscal authorities. They provide individual and enterprise credit reference reports, which only cover activities that strictly deal with money.

Another record system, named Dang an (档案) (personal archives), established in 1953, stores ID numbers, employment records and education data about citizens of mainland China.

The SCS project heavily relies on a functioning flow of information.[146] Local regulations require horizontal and vertical sharing of information inside the public administration.[147]

(c) Voluntary Disclosure/Voluntariness

(protection in dependency and hierarchy contexts; access to alternatives; prohibition of coupling; (voluntary) commercialization of personal data; incentives to data disclosure and protection therefrom [protection of adolescents; competition law; nudging]; prerequisites for consent; 'privacy fatigue'; peer pressure [eg WhatsApp])

Relying upon the flow of Personal Information, especial encouragement to voluntarily disclose Personal Information can be seen within the SCS. Information subjects are encouraged to actively provide their social credit information and legal persons may share credit information accumulated during their operations.[148] Taking part in this system allows individuals to get access to diverse services and advantages.

2) Recipient's Obligations

(a) Requirements for Personal Data Reception

(Information; requirements concerning content and formalities; warnings; notifications; assurances)

Already following the earliest Art 2 2012 NPC Decision, network service providers shall abide by the principle of legality, legitimacy and necessity, clearly indicate the objective, method and scope for collection and use of information and obtain agreement from the person whose data is collected.

Similarly, under the CSL the recipient is obliged to abide by the principles of legality, propriety and necessity, as well as to make public rules for collection and use, explicitly stating the purposes, means and scope for collecting or using information (Art 41 CSL). Also, it is prohibited to collect personal information unrelated to the services provided by the network operator (Art 41(2) CSL/ similarly 5.2 2020 Specification – 'directly related').

Information duties are promulgated under Art 5.5 2018/2020 Specification, according to which the Recipient should provide data subjects with a privacy policy or other form of notice, informing them of the scope and ways in which their personal information is collected, processed and disclosed, including the following information:

– the identity of the data controller, including its registered name, registered address, principal office, a telephone number and/ or an e-mail address;

– a list of personal information collected for each business purpose. Where sensitive personal information is involved, relevant consent shall be explicitly marked or highlighted;

– the location of storage, retention period, means of use / processing and scope of the personal information collected;

[146] Marianne Von Blomberg, 'Social Credit System and China's Rule of Law' [2018] 2 The Mapping China Journal 78, 88.

[147] Art 6 I Hubei Provincial Social Credit Information Management Regulations (01 July 2017), Standing Committee of the 12th Hubei Provincial People's Congress.

[148] Art 13 Shanghai Municipal Social Credit Regulations (01 October 2017), Standing Committee of the Shanghai People's Congress; Art 17, 18 Hebei Provincial Social Credit Information Regulations (01 January 2018); Art 14 I Hubei Provincial Social Credit Information Management Regulations (01 July 2017), Standing Committee of the 12th Hubei Provincial People's Congress.

– the purposes sought by the data controller, i.e. what the data controller uses the data for (for instance, supplying goods and services, creating a user account, processing payments, managing subscriptions to the newsletters, etc.). These should be as comprehensive as possible, as additional purposes will require new consent;

– circumstances under which the data controller will transfer, share, assign personal information to third parties (including intra-group entities) or publicly disclose personal information, the types of personal information involved in these circumstances, the types of third party data recipients and the respective security and legal responsibilities of the entities; the rights of data subjects and mechanisms for them to exercise such rights, eg methods to access, rectify or delete their personal information, to de-register their accounts, withdraw their consent, obtain copies of their personal information and restrict automated decision by the data system etc.;

– potential risks for providing personal information as well as possible consequences for not providing the data;

– data security capabilities of and data security protection measures to be adopted by the data controller and, when necessary, the compliance certificates related to data security and personal information protection; and

– channels and procedures for making inquiries and lodging complaints by data subjects, as well as external dispute settlement body and contact information.

The information in the privacy policy must be true, accurate and complete. The contents of the privacy policy must be clear and easy to understand and ambiguous language should be avoided. The privacy policy should be made available to the data subject when collecting consent and published publicly and easily accessible. When changes occur to the information provided in the privacy policy, the data subjects should be notified of such changes and further consent may need to be obtained. Consent is required for the collection of personal information for each specific business function.[149] Exceptions to consent, as for example for Personal Information related to public safety, can be found under Art 5.4 Specification 2020.

According to PIPL, before collecting Personal Information one must truthfully, accurately and completely notify the following matters in clear and easy-to-understand language:

– the name and contact information of the Personal Information processor;

– the purposes, methods, categories of the processed Personal Information and the preservation period (generally, it shall be the shortest period necessary to achieve the processing purpose);

– methods and procedures for individuals to exercise their rights provided in the Personal Information Law; and

– other matters provided by laws or administrative regulations.[150]

Exceptions to this notification requirement are stipulated under Art 18 PIPL. To handle Personal Information, consent or one of the new lawful bases set out in Art 13 PIPL must be given (see also C. IV. 1. D) below). The collection of personal information shall be limited to the smallest scope for realizing the handling purpose and excessive personal information collection is prohibited.[151]

(b) (Procedural) Obligations Concerning Received Personal Data

(purpose dedication/limitation; technological and organisational measures; data security; deletion and retention; further transmission and limitations thereto, also concerning transmission abroad)

[149] Art 5.4 a) Specification 2020. For further specifications concerning consent see also C. IV. 1. D. below.

[150] Art 17 PIPL.

[151] Art 6 PIPL.

Throughout the Specifications it is stipulated that personal information should only be used in accordance with a person's legitimate rights and interests (合法权益).[152] The 'data quality principle' is not clearly stated in the CSL. Provisions concerning gathered personal information can be found in Artt 40–42, prohibiting the tampering with or destroying the data collected.[153] Yet, a requirement to ensure that the data is accurate, relevant or up-to-date is not given anymore. It exists in the 2013 MIIT Guideline and was clearly expressed in the 2018 Specification draft, yet not mentioned in the final version.

The CSL has many requirements regarding infrastructure security and monitoring. On personal data the law especially requires security but does not expressly mention the appropriateness criterion.[154] The appropriateness security criterion is explicitly mentioned in Art 4 f) 2018 Specification, requiring recipients to possess security capabilities that match potential security risks and adopt adequate administrative and technical measures to protect.

Due to the cyber-sovereignty principle (see also C. I. above), requirements of localization of data storage and restrictions on cross-border data transfers apply. Chinas government's stance on data localization is that it protects individuals' privacy, but also China's economic development and reduces its exposure to foreign intelligence.[155]

Operators must stick to the strict data minimization principle, with data processing permitted for only what is necessary to fulfil the purposes.[156] It is further specified that data should be deleted once the purpose specified is achieved.[157] If a data controller wants to use personal information for a purpose different than the one specified at the time of data collection, it shall seek explicit consent from the individual.[158] Moreover, the Personal Information Controllers should de-identify the Personal Information immediately after collection[159] and employ encryption and other security measures for the transmission and storage of sensitive Personal Information.[160]

Similar principles as under the Cybersecurity Law can be found in Art 5–9 PIPL (legality, openness, transparency, quality of personal information, responsibility for processing personal information, propriety and sincerity).

3) Control by Discloser – ex post

(a) Transparency and Right to Request Information

The CSL stipulates in Art 41 that network operators shall make public the rules for collection and using personal data and expressly notify the purpose, methods and scope of such collection and use. The Specifications are more detailed, stating that the scope, purpose and rules of personal data processing should be publicly available and be clear, understandable and fair as well as subject to external supervision.[161] The same principle has been included in Art 7 PIPL.

(b) Co-Determination and Co-Decision Concerning Data Use

(restrictions for use; reservation of consent; revocation of consent; contestation and objection; special rules for international contexts; technical requirements for the act of permission/consent)

In previous laws to the 2018 Specification, automated processing or profiling was not mentioned. It was introduced in Art 3.7 2018

[152] Arts 4 a); 5.6 e) 2020 Specifications, yet not specifying what these are/might be.

[153] Art 42 CSL.

[154] Art 40, Art 42(2) CSL.

[155] Aimin Qi, Guosong Shao and Wentong Zheng, 'Assessing China´s Cybersecurity Law' [2018] 34(6) Computer Law & Security Review 1353.

[156] Art 4 d) 2020 Specification.

[157] Art 6 l) 2020 Specification.

[158] Art 7.3 a) 2020 Specification.

[159] Art 6.2 2020 Specification.

[160] Art 6.3 2020 Specification.

[161] Art 4.e) 2020 Specifications.

Specification, which defines profiling and requires that in case of an automated decision-making the data controller should provide means for data subjects to lodge a complaint (Art 7.10).

Under PIPL individuals generally have the right to know and the right to decide relating to their personal information and have the right to limit or refuse the handling of their personal information by others unless laws or administrative regulations stipulate otherwise (Art 44).

PIPL confers data subjects[162] a right to access and copy their personal information from personal information processors, to obtain and reuse their personal information for their own purposes across services (data portability) (Art 45; but it does not specify the prerequisites or procedures for processors)[163] as well as to correct and delete personal information. The data portability right confers an individual the possibility to request the transfer of personal information to a personal information processor designated by him or her, the personal information processor shall provide the means for the transfer if the conditions set by the state internet information department are met. The law does not specify the conditions for the exercise of the right but leaves it to the Internet information department to formulate the relevant rules.

These rights were already covered in previous regulations such as the 2018/2020 Specifications.

(c) Revocation

(Data portability; deletion; 'right to be forgotten / to forget')

No previous regulations such as the 2012 NPC Decision provide a right of access, modification and deletion. Nevertheless, the 2012 NPC Decision provides a right to erasure which is less far-reaching than the right to be forgotten in the EU. This right has been confirmed in the CSL but is limited to the cases in which the network operator has violated laws or agreements between the parties.[164] The 2020 Specification is in line with this, going further by requiring controllers to also notify third parties, with whom data has been shared to delete it (still only where a law or an agreement has been breached).[165]

The 2020 Specification Art 8.6 grants individuals a data portability right. This requires data controllers to give their collected personal information to data subjects or directly transfer them to a third party. Yet it only concerns individuals' basic information and information about their identities, health, psychological, education and work information. Similar rights are conferred by PIPL (right to data portability (Art 45), Right to rectify (Art 46), Right to delete (Art 47)) which can also be invoked by relatives in case of death of the data subject[166]. Individuals also have a right to withdraw consent and personal information processors must provide individuals with a convenient means of withdrawing consent.[167]

In May 2016, the Haidian District People's Court in Beijing ruled in favor of Baidu, China's main search engine, against a plaintiff invoking the 'right to be forgotten'.[168] The judges ruled there was no right to be forgotten in Chinese law, but that this kind of personal interest might be protected under the right to personality, if legitimate. Yet, in this case the information was relevant and useful to the

[162] Art 44–48 PIPL.

[163] It is unclear whether Chinese Law enforcement and judicial authorities will follow eg GDPR principles.

[164] Art 43 CSL.

[165] Art 8.3 b) 2020 Specification.

[166] Art 49 PIPL.

[167] Art 15 PIPL.

[168] Ren Jiayu v. Beijing Baidu Netcom Technology Co., Ltd. Beijing Haidian District First Interm People´s Ct. 25 December 2015, Global Freedom of Expression – Columb. U. <https://globalfreedomofexpression.columbia.edu/cases/ren-jiayu-v-baidu/> accessed 04 February 2022.

public because the information was recent and the plaintiff still worked in the same field, wherefore the interest in having the information removed was not legitimate.

(d) Procedural Aspects

(costs for and effectivity of the rights of the affected persons [information, etc]; consumer appropriateness)

Similar to Art 49 CSL[169], Art 50 PIPL holds the processor responsible for establishing a mechanism to accept and process applications for exercising personal rights by individuals. If such a request is rejected, the reasons shall be stated. The individual may bring a lawsuit in a people's court according to law (see also C. III. 4. B. above). PIPL does not specifically require processors to inform data subjects how they can complain.

4) Enforcement

(a) Damages and Compensation

([material and immaterial] damages; reparations; disgorgement of profits; punitive damages)

There is no independent liability based upon the infringement of personal information (Art 111 CC) as an object of protection of property rights within the meaning of Art 1166 Alt. 1 CC. Art 111 only confers a legal interest, so that the protection of personal information must be determined based on a balancing exercise in the individual case.

Material damages can be claimed according to Art 1182 CC, immaterial damages according to Art 1183 CC.

In Personal Information related legal actions, the burden of proof that they are not at fault is on the Personal Information processor.[170] According to PIPL, processors infringing rights and interests and causing harm to data subjects shall be liable for damages and other civil liabilities. The processor will be held liable to pay damages to the relevant individuals if he cannot prove his innocence, regarding the infringement of rights and interests of personal information. The damages shall be determined based on the loss suffered by the victim or the benefits gained by the Personal Information Processor.[171] If the loss and profit are difficult to be ascertained, the amount of the damages shall be decided on the actual circumstances.[172]

(b) Procedural Aspects

('threshold' for legal protection; right to initiation; burden of proof and evidentiary privileges; dispute value; 'small claims'; alternative dispute resolution; rights to bring/press charges; 'rational apathy')

China follows a territorially based jurisdiction rule.[173] The territorial competence concerning civil claims is ruled in Chapter 2, Section 2 of the Civil Procedure Law.[174] According to Chinese law courts exercise personal jurisdiction in intellectual property infringement cases are solely based on the location of the server, which was extended to all internet torts.[175] The court located at the place where the tort occurs or at the defendant's domicile shall have jurisdiction, according to Art 28 Civil Procedure Law, which is clarified by Art 24 2015 Interpretation, stating that this encompasses the place where the tort activity is committed and where the result of the tort occurs. Art 25 2015 Interpretation refers to internet torts, adding to the place of tort places where computers and other information equipment used to commit the tort are located. The SPC Provisions on infringement of the Right of Dissemination stipulated, that where the location is difficult to identify or outside of China, the

[169] Similar Art 8.8 2020 Specification.

[170] Art 69 PIPL.

[171] Art 69 PIPL.

[172] Art 69 PIPL.

[173] Jiej Huang, 'Personal Jurisdiction based on the location of a server: Chinese Territorialism in the Internet Era?' [2019] 36 (1) Wisconsin International Law Journal 90–91.

[174] Arts 22–35 Civil Procedure Law.

[175] Interpretation of the Supreme People's Court on the Application of the Civil Procedure Law of the PRC, effective 04 February 2015. Referred to as 2015 Interpretation.

place where the computer or other equipment on which the infringement is discovered shall be the decisive location.[176]

Those who infringe stipulations of the CSL and cause harm to others are liable according to the rules of the civil law and thus in tort.[177] In case of infringements constituting a violation of public security management, public security administrative sanctions are given and in case of a crime, criminal responsibility is pursued.[178]

Individuals may file a lawsuit if personal information processors refuse their requests to exercise their rights under PIPL.[179] This provision clarifies the individual's right of action against the personal information processor for refusing the personal information subject to exercise his or her rights under the Personal Information Protection Law, such as the right to know, the right to decide, the right to restrict refusal, the right to access and copy, the right to portability, the right to correction, the right to deletion, the right to interpretation, etc. and will enrich the types of civil litigation related to infringement of personal information rights.

Further, if a personal information processor has infringed on the rights and benefits of a large number of individuals, consumer organizations stipulated by law (eg China Consumer Association)[180] or organizations designated by relevant authorities can file a lawsuit.[181] As such the Supreme People's Procuratorate issued an official notice, stating that public interest actions for personal information protection cases will be the focus of its work in the future.

Moreover, any organization or individual has the right to complain or report illegal personal information processing activities to the departments performing duties of personal information protection. Upon this, the departments receiving such complaints or reports shall process them according to the law and notify the complainants or reporters of the results. To provide better access, these departments are required to make public their contact information for accepting complaints or reports.[182]

IV) Objective Legal Obligations of the Recipient

1) Obligations Concerning Received Data

(a) Dependence on Authorisation

(of business models, processing variants, terms and conditions)

As of 2015, China's system was transformed from a system subject to permission for all companies to operate to a system in which prior clearance is only required in certain blacklisted industrial sectors.[183] The list, which is regularly updated, contains provisions for domestic and foreign investors, as well as joint venture requirements. There is no requirement of registration for collecting Personal Information in China.[184] To register in China, companies must apply for a business license.

---

[176] Interpretation of the Supreme People's Court of the PRC on Several Issues Concerning the Application of Law in the Hearing Civil Dispute Cases Involving Infringement of the Right of Dissemination on Information Networks, effective 01 January 2013.

[177] Art 74(1) CSL.

[178] Art 74(2) CSL.

[179] Art 50 PIPL.

[180] For further information see Dan Wei, 'Enforcement and Effectiveness of Consumer Law in the People's Republic of China' in Hans W. Micklitz and Geneviève Saumier (eds), *Enforcement and Effectiveness of Consumer Law* (Springer International Publishing 2018).

[181] Art 70 PIPL.

[182] Art 65 PIPL.

[183] Opinions on Implementing the Negative List for Market Access (国务院关于实行市场准入负面清单制度的意见) October 2015.

[184] Papan Tang, 'Data Protection and Cybersecuirty Law in China' (CMS, 5 March 2021) <https://cms.law/en/int/expert-guides/cms-expert-

PIPL prohibits sharing domestically stored Personal Information with a foreign government without previous authorization by the Chinese government. In case of foreign judicial or law enforcement bodies, the request has to be filed by said body directly with the competent government authorities in China.[185]

Although a requirement of approval is not mentioned, according to Art 53 PIPL, if an organization outside of China handles PI of persons inside China, it will have to set up a special organization or designate a representative inside China. The name of the organization or individual is to be submitted to Chinese authorities that have the authority to oversee personal information protection.

(b) Notification Obligations

(regarding business models and business activities; regarding processing activities)

Notification duties only arise in specific situations. When Personal Information is shared with other Personal Information handlers or transferred abroad it is necessary to notify individuals of the (overseas) recipient's name and contact information, processing purposes, processing methods, categories of Personal Information, the methods by which individuals may exercise their rights provided in the Personal Information Law and other relevant matters.[186]

In case of a data breach, previous rules only mandated the notification of authorities by the data controller.[187] The CSL requires to inform authorities as well as individuals.[188] This is concretized by the Specifications which further require the affected entities to record a set of information about the incident, assess its impact and report it in a timely manner, as well as promptly informing data subjects.[189] Data subjects shall receive individual information via email, telephone, push notification or other means. A public alert is sufficient in case of difficulties.[190] A clear timeframe is not given.

Similar notification duties arise under PIPL although an exception is promulgated according to which processors may choose not to inform individuals if they consider that the measures taken can prevent any harm arising from the leakage of, tampering with, or loss of information.[191] Nevertheless, if authorities consider that the leakage may cause harm to an individual, they can require processors to notify the individual.

(c) Documentation

(accountability)

Personal Information Controllers must maintain records of processing activities of collected and used Personal Information[192] but no requirements concerning the accountability of Personal Information Controllers can be found in the 2018/2020 Specifications.

Prior to processing sensitive personal information, a personal information protection impact assessment is to be carried out and relevant reports and records must be retained for at least three years.[193] The same applies when implementing automated decision-making, entrusting others with the processing, for cross-border transfers and for other personal information processing activities that have a

guide-to-data-protection-and-cyber-security-laws/china> accessed 02 March 2022.

185 Art 41 PIPL.

186 Art 39 PIPL.

187 Graham Greenleaf and Scott Livington, 'China´s New Cybersecurity Law – Also a Data Privacy Law?' [2017] 19 University of New South Wales Law Research Series 5.

188 Art 42 CSL.

189 Art 10.2 2020 Specifications.

190 Art 10.2 2020 Specifications.

191 Art 57 PIPL.

192 Art 11.3 2020 Specifications.

193 Art 55, 56 PIPL.

significant impact on individuals' rights and interests.[194]

(d) Processing Requirements

(prohibition subject to permission; balancing of interests; restrictions for terms and conditions; business practices; APIs/interfaces for third parties)

Personal information can either be processed by the recipient, jointly, with a third parties entrusted by the controller or by providing Personal Information to other processors when certain requirements are met.[195] The CSL[196] establishes consent as the only legal basis for data collection and processing and has a loose conception of it, allowing for implicit consent. Neither the CSL nor the 2018 Specifications use the term implied but drafters clarified that explicit consent is only required if it is expressly mentioned.[197] Nevertheless, the CSL always requires consent and does not allow collection or processing by default. Yet, Art 5.5a 2018 Specification requires explicit consent for the collection of sensible personal information, while implied consent is generally sufficient for the collection of personal information.[198] Furthermore, they included a series of exemptions to obtaining consent[199] when collecting personal information in the following situations:

– directly related to national security and national defense;

– directly related to public safety, public health and significant public interests;

– directly related to criminal investigation, prosecution, trial and judgment enforcement, etc.;

– when safeguarding the major lawful rights and interests such as life and property of Personal Information subjects or other persons and it is difficult to obtain the consent of the Personal Information subject;

– when the Personal Information subject voluntarily opened the collected Personal Information to the general public;

– when the Personal Information is collected from legitimate public information channels, such as the legitimate news reports and open government information;

– when necessary to sign and perform a contract according to the Personal Information subject's request;

– when necessary to maintain the safe and stable operation of the provided products or services, such as to detect and handle product or service malfunctions;

– when necessary for the Personal Information controller, as a news agency, to make legal news reports;

– when necessary for the Personal Information controller, as an academic research institute, to conduct statistical or academic research in the public interest, which also has de-identified the Personal Information when providing academic research or results externally;

– when other situations specified by laws and regulations.

The 2020 Specification clarified that the term 'consent' includes explicit and authorized consent. Explicit consent[200] refers to the behavior of the personal information subject who voluntarily makes a statement in paper or electronic form through written or verbal means, or makes an affirmative action on his or her own to expressly authorize the specific processing of his or her personal information.

---

194 Art 55 PIPL.

195 Art 9.1 2020 Specifications; Art 21 PIPL.

196 Art 42(1) CSL.

197 Samm Sacks, 'China´s Emerging Data Privacy System and GDPR' (CSIS, 9 March 2018) <https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr> accessed 10 February 2022.

198 Art 5.3 Specification 2018.

199 Art 5.4 a–g 2018; Art 5.4 a–k 2020 Specifications.

200 Art 3.6 2020 Specifications.

Affirmative action includes the personal information subject actively ticking a box, clicking 'agree', 'register', 'send', 'call', or providing the personal information by filling out a form etc.

In contrast, 'authorized consent'[201] refers to the act of express authorization by the personal information subject for the specific processing of his or her personal information, which includes both authorization through positive actions (ie express consent) and authorization through negative inactions.

Personal information processing shall 'have a clear and reasonable purpose', 'directly related to the processing purpose' and 'limited to the smallest scope for realizing the processing purpose'. Art 5 PIPL specifies that Personal Information shall be handled in accordance with the principle of lawfulness, legitimacy, necessity and good faith and no manner of means that is misleading, fraudulent or coercive is allowed in Personal Information handling. It is worth noting that the PIPL puts necessity in equal importance with lawfulness, legitimacy and good faith, demonstrating that necessity has become a focus of Personal Information protection administration. The necessity requirement obliges companies to ensure that their Personal Information handling is directly related to intended purposes and their Personal Information collection is limited to the minimum scope necessary for achieving the purposes.

PIPL breaks away from the legislative style of the Cyber Security Law, which has authorized consent as the only lawful basis and adds a number of new lawful bases for handling (which includes personal information collection and processing[202] personal information). It is to be noted that the legitimate interest of the data controller or processor is still not recognized as a separate legal basis. Personal information is to be processed under one of the legal bases set out in Article 13. The most relevant legal bases for organizations processing personal information include 'necessary to conduct human resources management'. The necessity for HR management in this provision is limited to that generated from 'lawfully formulated labor rules and structures and lawfully concluded collective contracts'. The emphasis on 'in accordance with the labor regulations and collective contracts established by law' reflects the legislator's attempt to strictly limit the scope of the processing of employees' personal information in consideration of the inherent inequality in labor relations.[203]

Further legal bases are the processing 'necessary for the performance of a contract to which the individual is a party' and 'necessary for the performance of legal duties and legal obligations'. Another legal basis is the processing of 'personal information already disclosed by persons themselves or otherwise lawfully disclosed.'[204] Whereby according to Art 27 (consistent with Art 1036(2)[1] CC) a person can 'clearly refuse' the processing on their personal information already disclosed and that consent from such person is still required if the processing of their personal information has 'a major influence on individual rights and interests'. Disclosed personal information shall be processed 'within a reasonable scope'. To define 'reasonable' factors such as the use of the personal information at the time of disclosure, the individual's expectation of privacy and the impact of the use of the disclosed information on the rights and interests of the individual shall be taken into account. The specific standards are still to be clarified by law enforcement and judicial decisions.[205]

---

[201] Art 3.7 2020 Specifications.

[202] Art 4(2) PIPL.

[203] Han Kun Law Offices, 'A New Chapter in the Spotlight: A Brief Overview of the Personal Information Protection Law' (Han Kun Law Offices, 21 August 2021) <A New Chapter in the Spotlight> accessed 04 November 2021.

[204] Art 27 PIPL.

[205] Han Kun Law Offices, 'A New Chapter in the Spotlight: A Brief Overview of the Personal Information

Another legal basis is the processing when 'necessary to protect any natural person's life, health and property safety under emergency circumstances or public health emergency events' or when Personal Information is processed 'within the reasonable scope for conducting news reports, public opinion-based supervision and other activities for the public interest'. Lastly, Personal Information can be processed 'in other circumstances provided by laws or administrative regulations'.

Consent remains a legal basis and is only valid if individuals voluntarily and explicitly provide such consent and with full knowledge of the details of the personal information processing.[206] Parents' or other guardians' consent is required when the minor is under 14.[207]

The concept of 'separate consent', is introduced in Art 14 PIPL, '[w]here laws or administrative regulations provide that a separate consent or written consent is required in order to process personal information, those provisions shall prevail'. There is currently no definition or specific procedure for obtaining separate consent. Separate consent is required when:

– The processor provides the Personal Information processed to any other Personal Information processor,[208]

– discloses the processed Personal Information to the public,[209]

– uses personal image and identification information collected in public space for any purpose other than maintaining public safety,[210]

– sensitive Personal Information is being processed,[211] or

– Personal Information is provided to any party outside the PRC.[212]

When processing sensitive data, the recipient must have a specific purpose and necessity of the data collection and follow stringent data protection measures.[213] The requirement of separate consent can be otherwise specified by other laws. Installation of image collection and personal identity recognition facilities in public premises shall be for the purpose of ensuring public security and signages shall be displayed. Information of personal images and personal identification collected shall only be used for the purpose of ensuring public security and shall not be used for other purposes, unless separate consent from individuals has been obtained.[214]

(e) Prohibitions and Obligations

(prohibition of processing variants [eg profiling]; criminal prohibitions; restrictions under competition regulations; prohibition of abuses [of power/market power]; further transmission to third parties, especially governmental bodies; elicitation from abroad)

Theft and unlawful sale of personal information is forbidden under Art 44 CSL. By requiring consent for the transfer of personal information (as long as it is not anonymized) the CSL presupposes the possibility to transfer personal information to third parties.[215] Nevertheless, it is unclear whether consent is required for every transfer. The 2020 Specification require the Personal Information Controller to pay full attention to risks, when sharing and transferring Personal Information and set out further requirements, when Personal Information is shared and transferred not due

Protection Law' (Han Kun Law Offices, 21 August 2021) <A New Chapter in the Spotlight> accessed 04 November 2021.

206 Art 14 PIPL.

207 Art 31 PIPL.

208 Art 23 PIPL.

209 Art 25 PIPL.

210 Art 26 PIPL.

211 Art 29 PIPL.

212 Art 39 PIPL.

213 Art 28(2) PIPL.

214 Art 26 PIPL.

215 Art 42(1) CSL.

to acquisition, merger, reorganization or bankruptcy.[216]

Personal Information controllers shall in principle not store, share or publicly disclose original personal biometric information.[217] In principle, biometric information shall not be shared or transferred.[218]

A definition for automated decision-making is provided in Art 73 PIPL, referring to 'the use of computer programs to automatically analyze or assess individual behaviors and habits, interests and hobbies, or situations relating to finance, health, or credit status, etc. and engage in decision-making activities'. Restrictions on this process include the requirement of transparency of the process and the fairness and justice of the result. Personal information processors may not engage in unreasonable differential treatment of individuals in trading conditions such as trade price. This provision[219] targets the trend of 'differential pricing on existing users'. Furthermore, information push delivery, or commercial sales to individuals through automated decision-making methods, shall simultaneously provide the option to avoid targeting an individual's characteristics or a convenient method for the individual to refuse or opt out of targeting.[220]

Also Art 16 PIPL restricts image collection or personal identity recognition in public venues. Image collection or personal identity recognition in public venues can only be used for safeguarding public security, except if individuals' separate consent is obtained (see also C. IV. 1.d. above).

2) Monitoring

(a) Recipient's Self-Monitoring

(self-restrictions; compliance mechanisms; internal responsibilities [company privacy officers; ombudspersons)

The MIIT Regulations 2013 required an annual 'self inspection' of security measures (see also C. IV. 3. below).

Besides informing users and competent government departments in case of a leak, the CSL requires recipients to take remedial measures.[221]

Under previous law, there was no obligation to appoint a data protection officer. However, Art 11.1 b) of the 2020 Specification requires data controllers to appoint a person responsible for personal data protection (reminding of the GDPR's data protection officer), who should be inhouse if the controller crosses the defined thresholds (when processing personal data of more than 1 million citizens in one year or when processing sensitive personal data of more than 100,000 citizens, as generally when the company has more than 200 employees) and a data protection department.

Responsibilities of this person are listed in Art 11. 1) of the 2020 Specification including the data protection impact assessments. Under the 2020 Specifications it is recommended best practice for data controllers to establish a personal information impact assessment system,[222] to assess security risks associated with personal information processing activities and identify effective protection measures.[223] This has been changed with the PIPL, which obliges to carry out an impact assessment only in specific circumstances. The National Standardization Technical Committee for

[216] Art 9.2 2020 Specifications.

[217] Art 6.3 c); Art 9.4 f) 2020 Specifications.

[218] Art 9.4 f) 2020 Specification.

[219] Art 24 PIPL.

[220] Art 24 PIPL.

[221] Art 42 CSL.

[222] Art 11.4 2020 Specification.

[223] Further data protection impact assessments are to be carried out in specific circumstances, eg, fusion of Personal Information collected for different business purposes (Art 7.6 b)); when using an automated decision-making system (Art 7.7).

Information Security has published the 'Guidance for Personal Information Security Impact Assessment' (PIIA Guidelines) which was implemented on 1 June 2021.

Foreign processors subject to Art 3(2) PIPL are obliged to appoint a data protection representative or designated agency, within China and report the name and contact info of that representative to the Chinese supervisory authority.[224]

The processors obligations concerning internal administrative measures, staffing and organization and security measures are stipulated in Art 51–56 PIPL. Specific obligations on personal information processors that provide important Internet platform services with a large number of users and complex business types are enshrined in Art 58 PIPL. Generally, internal administrative measures oblige the processor to formulate internal management systems and operating rules on personal information processing.[225] Moreover, regular personal information compliance auditing must be audited[226] and personal information protection impact assessments need to be conducted.[227] If the amount of personal information processed reaches a certain threshold a personal information protection officer is to be appointed, whose contact information is to be made public.[228] In form of security measures, processors have to classify and implement categorized management on personal information, adopt technical security measures to protect personal information such as encryption and de-identification[229] and carry out access control and regular security education and training for employees. Moreover, a personal information security incident response plan should be formulated and implemented.[230]

(b) Regulated Self-Regulation

(sectoral and industry associations)

A public-private partnership project[231], including the CAC, MIIT, Ministry of Public Security, Standardisation Administration of China, Alibaba, Ant Financial, AutoNavi, Didi, created templates for complying with the Specifications (Privacy Management Templates)[232]. These serve as explanations for customers and employees how the company protects and uses data (and thereby complies with the Specifications).

(c) Supervisory Authorities

(data protection authorities; competition authorities; economic oversight authorities)

There are several regulators responsible for data protection enforcement efforts. Besides the MIIT and the Ministry of Public Security, which are responsible for network security protection, supervision and management efforts within the scope of their responsibilities, the Cyberspace Administration of China (CAC) has a general responsibility for planning and coordination cybersecurity efforts.[233] The same measure also refers to 'other relevant authorities'. Therefore, different authorities are responsible for data protection for their own sectors (in accordance with the sectoral approach). The administrative law enforcement of CSL is still performed by different departments on their own. The CAC, the authority in charge of telecommunication, the public security authority and other relevant

[224] Art 53 PIPL.

[225] Art 51 PIPL.

[226] Art 54 PIPL.

[227] Art 55 PIPL.

[228] Art 52 PIPL.

[229] Art 51 PIPL.

[230] Art 51 PIPL.

[231] Lu Xiaomeng, Li Manyi and Samm Sacks, 'What the Facebook Scandal Means in a Land without Facebook: A look at China's Burgeoning Data Protection Regime' (CSIS, 25 April 2018) <https://www.csis.org/analysis/what-facebook-scandal-means-land-without-facebook-look-chinas-burgeoning-data-protection> accessed 01 February 2022.

[232] Annex C and Annex D 2020 Specifications.

[233] Art 8 CSL.

authorities of the State Council all could take charge of protection, supervision and administration of cyber security, which leads to the existence of the problem of unclear power and responsibility as well as cross law enforcement among aforesaid administrative law enforcement authorities.

Under the new legislation, the CAC is responsible for coordinating the protection of personal information and regulatory work; Ministries of the State Council shall be responsible for protecting and administering personal information within their purview.[234]

(d) (Specific) Criminal Proescution

(focus) prosecution units for informational offences; [situational/special] investigators)

Personal information protection authorities shall refer illegal personal information processing activities that come to their attention while carrying out their duties to public security authorities if the activities may constitute criminal offences.[235] In certain circumstance, the Personal Information processor and their responsible officials may even face criminal liability. The relevant offences include infringement on citizens'[236] Personal Information, refusing to perform the obligation of information network security management[237] and illegally disclosing state secrets[238].

(e) Procedural Aspects

(investigation powers; resources of monitoring institutions)

The current enforcement structure is decentralized and consists of many departments at different levels, which leads to inconsistency.[239] Within this multi-level structure the CAC takes a leading and coordinating role, and other supervisory authorities are limited to their respective designated areas. The CAC is directly under the Central Committee of the Chinese Communist Party, with rising power and expanding territory.[240] Investigations by responsible authorities may involve an inquiry of parties concerned, reviewing contracts and other records, conducting on-side inspections and inspecting equipment and articles relevant to Personal Information processing activities. [241] The departments are equipped with proper tools for the investigation and enforcement nevertheless, there are no standards for these supervisory mechanisms' independence.[242]

3) Enforcement

Enforcement in the PRC depends on the specific data protection laws and regulations breached, as they are scattered across various laws and additional laws or regulations may be applicable depending on the industry or type of information at hand. Generally, the civil and criminal sanctions and administrative penalties for data protection breaches include warnings, orders to rectify, fines, confiscation of unlawful income, compensation to victims, cancellation of licenses, prison sentences, shutting down of websites and prohibition on engaging in certain types of business in the future.[243]

---

[234] Art 60 PIPL.

[235] Art 64 PIPL.

[236] Art 253 Criminal Law of the PRC.

[237] Art 286 Criminal Law of the PRC.

[238] Art 111 Criminal Law of the PRC.

[239] Zhaofeng Zhou, 'China's Personal Information Protection Law – What do you need to know?' (fieldfisher, 23 August 2021) <https://www.fieldfisher.com/en/insights/china's-personal-information-protection-law-what-d> accessed 02 March 2022.

[240] AJ Caughey and Shen Lu, 'How the CAC became Chinese tech's biggest nightmare' (protocol, 11 March 2022) <https://www.protocol.com/china/china-cac-tech-crackdown> accessed 24 March 2022.

[241] Art 63 PIPL.

[242] European Data Protection Board, *Government access to data in third countries* (EDPS/2019/02–13, 2021) 23, 24.

[243] Baker McKenzie, 'Data Protection Enforcement in China (PRC)' (Global Compliance News) <https://www.globalcompliancenews.com/data-privacy/data-protection-enforcement-in-china-prc/> accessed 02 March 2022.

The 2012 NPC-Decision lacked any enforcement mechanism. It says the 'relevant competent agency' will use its existing powers 'to prevent, halt and investigate'. The MIIT regulations provide for the supervision and administration by the MIIT and Chinese authorities at multiple levels of government.[244] Latter ones provided greater detail regarding how supervision and inspection is to be carried out[245] and set a requirement of annual 'self inspection' of security measures and response to what is found.[246]

Under the CSL, the CAC (Cyberspace Administration of China) is responsible for the planning and coordination of cybersecurity and relevant supervisory and administrative work, while the MIIT (Ministry of Industry and Information Technology), the public security department and other relevant departments are responsible for the supervision and administration of personal information protection in their respective sectors. The CAC is also responsible for the enforcement of PIPL. Also many major cities within China have established their own branch of the CAC. In case that illegal processing of Personal Information is suspected of a crime, the case shall be transferred to the public security organ.[247]

(a) Interventions Concerning Data Processing

(restriction and prohibition of data processing)

Art 66 PIPL provides that 'if personal information is handled in violation of the provisions of this Law, or if personal information is handled without taking the necessary safety protection measures in accordance with the provisions, the department responsible for the protection of personal information shall order rectification, issue a warning, confiscate the illegal income and order the suspension or termination of services for the application that handled personal information in violation of the law'.

(b) Interventions Concerning Business Models

(competition and economic supervision; government/public monopolies)

Recently, several opinions addressed to all local governments were released on cracking down monopolies and unfair competition in China's internet economy.[248] Further rules were released at the beginning of this year to curb anti-competitive behavior, such as sharing sensitive consumer data. The PIPL, however, does not regulate the use of certain business models. The State cyberspace administration may prohibit or restrict the provision of Personal Information to overseas organization or individuals, whose activities damage the rights and interests of the PRC's citizens or endanger the national security or public interest.[249] Special further regulations on handling and transferring financial information are released by the People's Bank of China. For example PRC banks are not allowed to disclose this kind of information offshore. Similar regulations can be found in the Security Law and the State Secrets Law. Also private sectors have additional requirements as for example the health sector.[250]

(c) Sanctions for Processors/Processor-related Sanctions

(prohibition orders concerning business activities; corporate sanctions; revenue-based sanctions)

The competent government department can order the critical information infrastructure operator who violated the data localization requirements to take corrective action,

[244] Art 3 MIIT Regulations 2011.

[245] Art 17 MIIT Regulations 2013.

[246] Art 16 MIIT Regulations 2013.

[247] Art 64 PIPL.

[248] Eduardo Baptista, 'China state planner to punish monopolies in internet platform industry' *Reuters* (Beijing, 19 January 2022).

[249] Art 42 PIPL.

[250] Anupam Chander and others, 'Achieving Privacy' [2021] 74(4) SMU Law Review 644.

confiscate its illegal income, impose a fine and may order it to suspend relevant business operations, cease operation for rectification or close down the website and even revoke its business license, a remedy even more serious than financial penalties.[251]

The CSL does not allow authorities to issue highly deterrent fines like the GDPR does in the EU, based on the companies' turnover. Infringements can be fined between one to ten times the amount of unlawful gains, where there are no unlawful gains, the fine is up to RMB 1,000,000 RMB as well as a fine to persons directly responsible (between RMB 10,000 and RMB 100,000). Furthermore, authorities may order the business to temporarily suspend its operations, shut down the website or even cancel business licenses and relevant operations permits.[252]

If personal information is processed in violation of PIPL or without fulfilling personal information protection duties in accordance with PIPL, authorities may order for rectification, issue warnings and confiscate any unlawful income. If the personal information processor refuses to rectify he shall be liable to a fine up to RMB 1,000,000.[253]

In case of serious infringements, personal information protection authorities above the provincial level may issue an order of rectification, confiscate any unlawful income and impose a fine up to RMB 50,000,000 or 5% of its annual revenue of the last year. The personal information protection authorities may also issue an order of suspension of business or operation for rectification, notify authorities in-charge for cancellation of business permits or licenses.[254]

(d) Sanctions for Individual Actors

([managing] directors' liability; individual criminal sanctions)

The person in-charge who is directly responsible and other personnel who bear direct responsibility shall be liable to a fine between RMB 10,000 and RMB 100,000.[255] In case of serious infringement, the person in-charge who is directly responsible for and other personnel who bear direct responsibility shall be liable to a fine between RMB 100,000 and RMB 1,000,000 and may be barred from serving as directors, supervisors, senior officers and personal information protection officers in corporations within a certain period of time.[256]

(e) Procedural Aspects

(priority of data regulation enforcement; resources of enforcers; shaming impact/pillorying effectof breaches/violations)

The practical procedures of enforcement of the PIPL remain to be seen. Nevertheless, shortly after the release of PIPL, Yahoo ended its presence in mainland China, being the latest US tech company to take this step. The law contributes to what these companies characterize as a 'challenging market' from which they prefer to opt out.[257] Protection practices have received increased attention, mainly targeted at issues of public order.[258] Previous to the enactment of PIPL, the government launched several campaigns on mobile apps to tackle illegal Personal Information collection and processing and to conduct an enforcement action against mobile apps to target

[251] Art 66 Measures to Assess whether Personal Information and Important Data can be Moved outside of China.

[252] Art 64 CSL.

[253] Art 66 PIPL.

[254] Art 66 PIPL.

[255] Art 66 PIPL.

[256] Art 66 PIPL.

[257] Karoline Kan, 'Yahoo pulls out of China over "challenging" business conditions' *BBC News* (2 November 2021).

[258] Anupam Chander and others, 'Achieving Privacy' [2021] 74(4) SMU Law Review 644.

gambling, pornography and other disfavored content.[259] There is currently no estimate of the amount China's public sector spends to enforce the regulations.[260]

Contraventions of the requirements of the PIPL may be entered into credit files and publicized, having a possible effect on the social credit score.[261] A 'negative' credit score might affect the future qualification to take part in government projects, receive government support or to become a government supplier, as well as making it difficult to conduct everyday business operations.

D) Sources and Literature

Xiaoyan Huang, *Technik versus Recht* (Nomos 2020).

Vincent Winkler, *Rechte an Daten im Zivilrecht*, (8 Schriften zum Ostasiatischen Privatrecht, Mohr Siebeck 2021).

Max Parasol, *AI Development and the 'Fuzzy Logic' of Chinese Cyber Security and Data Laws* (Cambridge University Press 2021) 94–126; 154–208.

Qu Bo and Hua Changxu, 'Privacy, National Security and Internet Economy: An Explanation of China's Personal Information Protection Legislation' [2020] 15(3) Frontiers of Law in China 339-366.

Graham Greenleaf, *Asian Data Privacy Laws, Trade and Human Rights Perspectives* (Oxford University Press 2017).

Paul C. Johannes, 'Datenschutz und Datensicherheit in China, Überblick zu PIPL und DSL' [2022] ZD 90 et seq.

E) Legal Framework

Civil Procedure Law of the People's Republic of China as promulgated on 9 April 1991 <http://www.npc.gov.cn/zgrdw/english-npc/Law/2007-12/12/content_1383880.htm>.

Copyright Law of the People's Republic of China as amended 27 October 2001 <http://www.asianlii.org/cn/legis/cen/laws/cloproc372/>.

Criminal Law of the People's Republic of China as amended on 14 March 1997 <https://www.fmprc.gov.cn/ce/cgvienna/eng/dbtyw/jdwt/crimelaw/t209043.htm >.

Cybersecurity Law of the People's Republic of China (中华人民共和国网络安全法) as promulgated on 6 November 2016 <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/>.

Cybersecurity Law of the People's Republic of China as promulgated on 7 November 2016 <http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml>.

Decision oft he 30th Committee Meeting of the 11th NPC Standing Committee as adopted on 28 December 2012 <http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm>.

Hebei Provincial Social Credit Information Regulations as promulgated on 1 January 2018 <
https://credit.gansu.gov.cn/credit/c117024/202203/2001599.shtml>.

[259] Thomas Zhang, 'China's Personal Information Protection Law: Compliance Considerations from an IT Perspective' (China Briefing, 11 December 2020) <https://www.china-briefing.com/news/data-privacy-china-personal-information-protection-law-it-compliance-considerations/> accessed: 02 March 2022; Jiaxing Li, 'Chinese regulators order mobile apps to rectify mishandling of user data' (KrASIA, 23 August 2021) <https://kr-asia.com/chinese-regulators-order-mobile-apps-to-rectify-mishandling-of-user-data> accessed 02 March 2022; Anupam Chander and others (n 258) 644.

[260] Anupam Chander and others (n 258) 645.

[261] Art 67 PIPL.

Hubei Provincial Social Credit Information Management Regulations as promulgated on 01 July 2017 <http://rst.hubei.gov.cn/zfxxgk/zc/qtzdgkwj/201912/t20191227_1799988.shtml>.

Information Security Technology – Guidelines for Personal Information Protection in Public and Commercial Service Information Systems (信息安全技术公共及商用服务信息系统个人信息 保护指南) as promulgated 1 Feburary 2013 <https://chinacopyrightandmedia.wordpress.com/2013/01/21/information-security-technology-guidelines-for-personal-information-protection-on-public-and-commercial-service-information-systems/>.

Information Security Technology – Personal Information Security Specification – (GB/T 35273-2017) (信息安全技术 个人信息安全规范) as promulgated on 29 December 2017 <https://www.chinesestandard.net/PDF.aspx/GBT35273-2017>.

Information Security Technology— Personal Information Security Specification as promulgated on 3 June 2020 <https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf>.

Interim Regulations on Urban Household Administration as promulgated on 16 July 1951 <http://www.gd.gov.cn/zwgk/gongbao/1951/7/content/post_3352652.html>.

Open Government Information Regulation as promulgated on 15 May 2019 <https://www.chinalawtranslate.com/en/open-government-information-regulations-of-the-p-r-c-2019/>.

Patent Law of the People's Republic of China as amended on 17 October 2020 <https://www.wipo.int/edocs/lexdocs/laws/en/cn/cn028en.pdf>.

Personal Information Protection Law of the People's Republic of China as promulgated on 20 August 2021 <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/>.

Personal Information Protection Law of the People's Republic of China (中华人民共和国个人信息保护法) as promulgated on 20 August 2021 <http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml>.

Personal Information Specification as promulgated on 1 May 2018 <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-personal-information-security-specification/>.

Provisional Regulations for the Development and Management of Instant Messaging Tools and Public Information Services as promulgated on 7 August 2014 <https://chinacopyrightandmedia.wordpress.com/2014/08/07/provisional-regulations-for-the-development-and-management-of-instant-messaging-tools-and-public-information-services/>.

Regulation on the Administration of Credit Investigation Industry as promulgated on 21 January 2013 <http://www.lawinfochina.com/display.aspx?lib=law&id=12585&CGid=&EncodingName=big5>

Regulations on Household Registration in the People's Republic of China as promulgated on 9 January 1958 <https://www.tandfonline.com/doi/abs/10.2753/CLG0009-4609340352?journalCode=mclg20>.

Regulations on Protecting the Personal Information of Telecommunication and Internet Users (电信和互联网用户个人信息保护规定) as promulgated in 28 June 2013 <https://chinacopyrightandmedia.wordpress.com/2013/07/16/telecommunications-and-internet-user-individual-information-protection-regulations/>.

Several Regulations on Standardizing Market Order for Internet Information Services (规范互联网信息服务市场秩序若干规定) as amended 07 December 2011 <https://chinacopyrightandmedia.wordpress.com/2011/12/29/some-provisions-to-standardize-internet-information-service-market-order/>.

Shanghai Municipal Social Credit Regulations as promulgated on 23 June 2017 <https://www.shanghai.gov.cn/nw48050/20200824/0001-48050_112971.html>.

Standardization Law of the People's Republic of China as promulgated on 4 November 2017 <https://www.sesec.eu/app/uploads/2018/01/Annex-I-China-Stadnardization-Law-20171104.pdf>.

Telephone User Real Identity Information Registration Regulations as promulgated on 28 June 2013 <https://chinacopyrightandmedia.wordpress.com/2013/07/16/telephone-user-real-identity-information-registration-regulations/>.

The Information Security Technology – Personal Information Security Specification (GB/T 35273-2020) (信息安全技术 个人信息安全规范) as promolugated on 6 March 2020 <https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf>.

中华人民共和国宪法 1954 (Constitution of the People's Republic of China 1954) as amended on 11 March 2018 <http://www.npc.gov.cn/englishnpc/constitution2019/201911/1f65146fb6104dd3a2793875d19b5b29.shtml>