Ca' Foscari
University
of Venice

Master's Degree in
Languages, Economics and Institutions
of Asia and North Africa
Second Cycle (D.M. 270/2004)

Final Thesis

Personal Data Protection in Contemporary China and the Impact of Covid-19

Supervisor
Ch. Prof. Renzo Riccardo Cavalieri

Graduand
Sara Angela Beacco
Matriculation Number
880450

Academic Year
2020-2021

Table of Contents

前言

根据技术进步和中国政府进一步加强信息化进程以确保国家经济增长和国家安全的意愿，中华人民共和国建立的隐私和个人数据保护法律框架在过去几十年中以极快的速度不断发展。在不同的立法、行政和部门法律法规中制定了隐私和个人数据保护要求和义务，创建了一个“累积”框架，主要侧重于私营部门，而仅部分涵盖公共机构，其中隐私和个人数据保护不被视为两套独立的权利和利益（例如在欧盟的 GDPR 中发生的情况）。

近期，特别是全国人民代表大会五年立法计划更新后的2018年，中国一直在转变对隐私和个人数据的看法，通过在2020年批准的新《中国民法典》进一步将两者区分为独立的法律制度，并通过在2021年底通过《个人信息保护法》和《数据安全法》的出台，对个人资料保护采取更为全面的方法。

中国的数据保护制度在为私营部门设定严格义务和要求的同时，使中国政府能够从私营单位获取数据，特别是来自数字企业的数据，（这些企业）需要对用户实施实名登记制度，并且必须为公安机关提供技术支持和数据获取。许多私营企业还必须遵守严格的数据本地化要求，禁止跨境传输个人信息和重要数据，除非事先通过中国当局的安全评估。

尽管在法律方面取得了一些有意义的进步，尤其是在用户数据隐私权领域，但中国法律法规中对个人信息的保护仍然存在执行困难，尤其是法律没有设立独立的数据保护机构，而是授执法权予国务院不同部门。

另一方面，数字和信息通信技术公司已将收集和处理用户的个人信息和数据作为其发展战略的核心，中国政府越来越依赖这些企业提供的技术支持和数据来实现其治理目标。数字企业与中国政府建立了特殊的沟通渠道，增强了企业影响数字领域政策和法律制定程序的能力，尤其是在收集和处理被这些企业视为专有资产的数据方面。

2019年12月爆发的新冠病毒疫情进一步提高了数字企业与中国政府对中国公民个人信息的访问。由于与地方政府合作开发和实施集成在两个最受欢迎的中国超级应用程序支付宝和微信中的COVID-19联系人跟踪应用程序，疫情使数字企业有机会更深入地掌握其用户的敏感个人信息。

这些“健康码”应用程序汇集了不同的数据源，以评估人口流动和互动，担当数字疫情预防工具，要求高风险用户实施自我隔离和隔离措施。这些应用程序的实施和传播对通过这些技术手段收集的个人信息的公平处理、数据责任和数据安全带来了质疑。

即使在疫情紧急情况结束后，健康码可能的正常化和扩展也开启了个人数据保护领域的新讨论，并可以设想私营数字企业与中国政府之间甚至更密切的合作。

本论文重点分析 Covid-19疫情如何影响当代中国的隐私权和个人数据保护。为此，本论文分为三个章节。

第一章描述了当代中国社会如何看待隐私和个人数据保护的概念：社会价值观、历史背景和政府制度，以及西方的影响如何影响当代中国隐私概念的定义和演变。此外，同一章还介绍了中国的隐私保护法律框架，从其国际义务和宪法价值，到更详细、更具行业性的数据隐私法律法规，这些都架构了中国在这一问题上的法律背景。

隐私权最初是通过名誉权和尊严权等其他相关人格权间接保护的，后来由于最高人民法院的司法解释和《中华人民共和国侵权责任法》，隐私权被确立为一项单独的权利。同时，《中华人民共和国刑法》首次引入个人信息保护规定。隐私和个人信息保护被作为同一组权益进行监管，并且仅针对某些行业，特别是在信息通信技术和电信领域实施了第一批严格的数据隐私义务和要求。然而，在过去十年中实施的大量数据隐私法律和法规最终确实扩大了其可涵盖私营企业的普遍性，并向公共机构提供了更多的一般规定。自 2020 年以来，中国进入了一个新的过渡阶段，隐私权与个人

信息保护被分离为两个截然不同的法律制度，在新的《中国民法典》中制定，并在《个人信息保护法》和《数据安全法》中为私人和公共当事人规定了更全面的义务。

第二章通过着重于告知私营部门的主要隐私义务、哪些是最相关的用户隐私权，以及与公共部门的相互作用，重点介绍了这些法律法规在私营部门的运作情况，尤其是中国政府获取私营部门数据的程度。

第三章分析了中国重大传染病防治工作中的个人信息披露问题。首先描述了重大卫生紧急情况下的监管方面，然后描述了在 Covid-19 紧急情况下专门为保护个人信息而颁布的法律文书。新型冠状病毒突显了保护中国公民个人数据的问题。为了能够实施旨在抗击病毒的限制和控制措施，中国当局主要依靠大量使用技术工具，尤其是由私营企业实施的健康码移动应用程序，如支付宝健康码和微信健康码。第三章描述了这些应用程序的开发和实施，并进一步描述了与通过这些技术工具收集和处理的个人信息、位置和健康数据的收集和处理有关的主要隐私和个人数据保护问题。

Introduction

The privacy and personal data protection legal framework established in People's Republic of China has been evolving in the last decades at a speedy pace according to technological advances and the willingness of the Chinese Government to further enhance the informatization process in order to ensure the country's economic growth and national security. Privacy and personal data protection requirements and obligations have been devised in different legislative, administrative and sectorial laws and regulations, creating a "cumulative" framework which mainly focuses on the private sector and only in part covers public institutions, where privacy and personal data protection are not conceived as two separate set of rights and interests (as it happens for example in the European Union's GDPR). More recently, and especially after the update of the National People's Congress' five-year legislative plan in 2018, China has been shifting its view on privacy and personal data, by further distinguishing the two into separate legal regimes provided in the new Chinese Civil Code approved in 2020, and by leaning towards a more comprehensive approach on personal data protection with the issuing of the Personal Information Protection Law and the Data Security Law at the end of 2021.

The Chinese data protection regime, while setting stringent obligations and requirements for the private sector, enables more than hinders the access of the Chinese Government to private sector data, especially from digital enterprises that are required to implement a real-name registration system for users, and have to provide technical support and access to data to public security organs. Many private sector companies also have to abide by strict data localization requirements prohibiting cross-border transfer of personal information and important data unless prior passing a security assessment from Chinese authorities. Despite some meaningful legal advancements, especially in the realm of user's data privacy rights, the protection of personal information devised in Chinese laws and regulations still suffers from enforcement difficulties, especially as the laws do not establish an independent Data Protection Authority (DPA) but empowers different State Council departments with enforcement powers. On the other hand, digital and Information Communication Technology (ICT) companies have made the collection and processing of their users' personal information and data the core of their growing strategy, and the Chinese Government is relying more and more on the technological support and data provided by these enterprises to realize its governance goals. Digital enterprises have established special channels of communication with the Chinese Government

that have enhanced their ability to influence policy and law-making processes in the digital realm, especially in regard to the collection and processing of data that are treated as a kind of proprietary asset by these enterprises.

The access of digital enterprises and the PRC Government to Chinese citizens' personal information has been furtherly enhanced by the outbreak of the Coronavirus pandemic in December 2019. The emergency situation has given digital enterprises the opportunity to grasp even more in-depth sensitive personal information of its users thanks to the collaboration with local Governments in the development and implementation of contact-tracing applications integrated in the two most popular Chinese super-applications, Alipay and WeChat. These "Health Code" applications pool different data sources in order to assess population movement and interactions, and act as a digital preventive tool by requiring high-risk users to implement self-isolation and quarantine measures. The implementation and diffusion of these applications have raised questions on fair processing, data accountability and data security of personal information collected through these technological means. The possible normalization and expansion of Health Codes even after the end of the pandemic emergency has opened new discussions in the realm of personal data protection and could envisage and even closer collaboration between private digital enterprises and the Chinese government.

This paper focuses on analyzing how the Covid-19 pandemic has impacted on the right to privacy and personal data protection in contemporary China. For this purpose, this work is divided into three chapters. The first chapter delineates how the concept of privacy and personal data protection is perceived in Chinese contemporary society: how social values, historical background and governmental institutions have influenced the definition and evolution of the idea of privacy in contemporary China, along with influence from the West. Furthermore, the same chapter provides a description of the Chinese legal framework for privacy protection, starting from its international obligations and Constitutional values to the more detailed and sectorial data privacy laws that have been shaping the Chinese legal background on the matter. The right to privacy has been initially protected indirectly through other related personality rights such as the right to reputation and the right to dignity and has been subsequently established as a separate right thanks to Judicial Interpretations and the PRC Tort Liability Law. At the same time, provisions on the protection of personal information have been introduced for the first time in the PRC Criminal Law. Privacy and personal information protection have been regulated as a single set of rights and interests, and the first stringent data privacy obligations and requirements have been implemented only for certain industries, especially in

the ICT and telecommunication fields. The numerous data privacy laws and regulations implemented in the last decade however did ultimately expand to encompass the generality of the private sector, with more general provisions afforded to public institutions. Since 2020, China has entered a new transition phase where the right to privacy is being separated from personal information protection as two distinct legal regimes, devised in the new Chinese Civil Code and with more comprehensive sets of obligations for both private and public parties established in the Personal Information Protection Law and Data Security Law.

The second chapter focuses on how these many laws and regulations operate in the private sector, by highlighting the main privacy obligations informing the private sector and which are the most relevant users' privacy rights, and the interplay with the public sector, especially the extent to which the Chinese government has access to private-sector data.

The final chapter analyzes the disclosure of personal data in the prevention and control of major infectious diseases in the PRC, by first describing the regulatory aspects that come into play during major health emergency situations, and which legal instruments for the protection of personal information have been specifically published during the Covid-19 emergency period. The novel coronavirus has accentuated and highlighted the pervasiveness of the government and the problems of protecting the personal data of Chinese citizens. In order to be able to implement restrictive and control measures aimed at fighting the virus, Chinese authorities have mainly relied on massive use of technological tools, especially Health Code Mobile Applications that have been implemented by private enterprises, such as Alipay Health Code and WeChat Health Code. The third chapter describes the development and implementation of these applications and furtherly depicts the major privacy and personal data protection issues that have emerged in relation to the collection and processing of personal information, location and health data collected and processed through these technological tools.

CHAPTER 1

Privacy and Personal Data Protection in Contemporary China

1.1. The Concept of Privacy and Personal Data Protection in Contemporary China

Nowadays privacy and personal data protection have become central values in many countries, due to the technological advances that have shaped the way personal information is collected, processed, and disposed.

Not only the definition of privacy has dramatically changed throughout history, but this concept is also perceived differently between Western and Asian countries, especially in China where the concept of privacy is still connected to reputation and dignity and is more understood as a protection from other individual's interference more than a protection from the government intrusion on citizens' private lives.

In these last decades, technology advancement has also surfaced the need for protection of a new right, the right to data protection, which has been formally separated from the right to privacy in many legislations, especially in the European Union. This has not happened however in China, where the right to data privacy is not regulated by a comprehensive law but data privacy provisions can be found in numerous legislative, administrative and sectorial laws.

1.1.1. The Concept of Privacy in the Chinese Society

The concept of privacy always existed throughout history as it is related to key values inscribed in human nature such as human dignity and independence, even if the content and definition of privacy differs according to the historical period, society, culture and even from individual to individual.

Nowadays the vast majority of nations recognize privacy as a fundamental human right. Many countries directly protect privacy in their Constitution, and when there is no explicit mention, national courts have still recognized implicit constitutional rights to privacy.[1]

[1] SOLOVE Daniel J., 2008, *Understanding Privacy*, Cambridge, Harvard University Press, pp. 2-3.

However, defining what privacy actually means and entails remains a cumbersome task as there is no general agreement on a clear definition of the term. Privacy remains an elusive concept, and many argue that because of this lack of a generally agreed definition of privacy courts and laws often struggle to recognize when privacy interests are to be protected.[2] The modern concept of privacy has primarily developed out of a Western moral and legal framework that puts individual rights before collective values,[3] and this in turn has had a heavy influence on many Asian countries' legislations on privacy, including China.

Nonetheless, Contemporary China still retains a different concept of privacy compared to Western Countries. The main preconception about privacy in China is that it was a concept imported from West since the nineteenth century that never existed in Chinese society before.[4] In reality, Ancient China always had some forms of protection of privacy, although this was more an indirect consequence of the protection provided by the moral principle of *Lǐ* (礼) that regulated civil disputes and not from a formal legal protection of the right to privacy.[5]

Privacy in modern China has however been affected by the Western definition that sees privacy as an individual right, as the importation of Western privacy laws ultimately prevented China from developing its own privacy legal culture.[6] Nevertheless China still carries a unique vision on the meaning of privacy even today, as it is understood more as a collective right than an individual right.

The idea of privacy in contemporary Chinese society continues even today to be shaped by traditional values. Originally, the concept of privacy in China was expressed with the word *Yīnsī* (阴私) that can be translated as "shameful, embarrassing acts or secrets that should not be disclosed to the public". This word lacked a positive connotation and involved the safeguarding of family secrets around indecent or unethical acts such as rape or molestation.[7] Breaches of *Yīnsī* were regarded as minor civil matters and were expected to be settled by society itself through mediatory measures rather than individuals seeking external agencies to enforce their

[2] SOLOVE Daniel J., 2008, *Understanding Privacy*, Cambridge, Harvard University Press, p.7.
[3] LI Tiffany, BRONFMAN Jill, ZHOU Zhou, 2017, "Saving Face: Unfolding the Screen of Chinese Privacy Law", *Journal of Law, Information, and Science (Forthcoming)*, p. 3.
[4] MCDOUGALL Bonnie S., 2004, "Privacy in Modern China", *History Compass*, Vol. 2, Issue 1, pp. 1-8.
[5] WANG Hao, 2011, *Protecting Privacy in China, A Research on China's Privacy Standards and the Possibility of Establishing the Right to Privacy and the Information Privacy Protection Legislation in Modern China*, Springer-Verlag Berlin Heidelberg, p. 33.
[6] LI Tiffany, BRONFMAN Jill, ZHOU Zhou, 2017, "Saving Face: Unfolding the Screen of Chinese Privacy Law", *Journal of Law, Information, and Science (Forthcoming)*, p. 3.
[7] XU Jinghong, 2015, "Evolving Legal Frameworks for Protecting the Right to Internet Privacy in China". In LINDSAY Jon R., CHEUNG Tai Ming, REVERON Derek S., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, New York: Oxford University Press, pp. 243-244.

own rights.[8] Daily civil conduct and civil disputes were regulated by the Confucian theory of *Lǐ* that placed morality as the central value to govern a society.[9] These doctrines focused on setting a border between family and outsiders more than establishing an individual right of protection of private life, as the family was understood as the basic functional unit and individuals were bound to specific obligations and duties according to their family role.

Moreover, Confucian values permeated traditional Chinese society and imposed a strict social hierarchy and a limitation to personal life.[10] An individual's rights were subordinate to the rights of family unit, community, and the country, as Confucianism imposed very specific roles enshrined in the so-called *five constant relationships* (五伦, *Wǔ Lún*).[11] These principles posed heavy obligations on some individuals (mainly the wife, the son and younger children) while giving absolute privileges to others (such as the father, husband and elder brother).[12]

Ancient Chinese law focused more on the protection of government powers and social interests rather than the protection of individual rights and civil matters, and as a result there was no clear separation between private and public law.[13] Individual rights were indirectly protected by imposing duties and obligations on individuals.[14] Law in traditional China was imposed from above, and rights were provided according to social status, as a consequence the protection of privacy was understood as a flexible privilege and mainly applied to the ruling class, so it could be enjoyed towards individuals that were ranked lower socially and economically, but not vice versa.[15]

Another aspect that helped shape the notion of privacy in traditional China was the concept of "saving face", which is still now a contemporary issue in modern China. "Face" is a unique

[8] WANG Hao, 2011, *Protecting Privacy in China, A Research on China's Privacy Standards and the Possibility of Establishing the Right to Privacy and the Information Privacy Protection Legislation in Modern China*, Springer-Verlag Berlin Heidelberg, p. 38.
[9] *Ibidem*, pp. 35-36.
[10] XU Jinghong, 2015, "Evolving Legal Frameworks for Protecting the Right to Internet Privacy in China". In LINDSAY Jon R., CHEUNG Tai Ming, REVERON Derek S., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, New York: Oxford University Press, pp. 243-244.
[11] These five major relationships were between the emperor and the subject, between husband and wife, between father and son, between elder brother and younger brother and between friend and friend.
LI Tiffany, BRONFMAN Jill, ZHOU Zhou, 2017, "Saving Face: Unfolding the Screen of Chinese Privacy Law", *Journal of Law, Information, and Science (Forthcoming)*, p. 4; WANG Hao, 2011, *Protecting Privacy in China, A Research on China's Privacy Standards and the Possibility of Establishing the Right to Privacy and the Information Privacy Protection Legislation in Modern China*, Springer-Verlag Berlin Heidelberg, p. 37.
[12] WANG Hao, 2011, *Protecting Privacy in China, A Research on China's Privacy Standards and the Possibility of Establishing the Right to Privacy and the Information Privacy Protection Legislation in Modern China*, Springer-Verlag Berlin Heidelberg, pp. 37-38.
[13] *Ibidem*, p. 35.
[14] *Ibidem*.
[15] LI Tiffany, BRONFMAN Jill, ZHOU Zhou, 2017, "Saving Face: Unfolding the Screen of Chinese Privacy Law", *Journal of Law, Information, and Science (Forthcoming)*, p. 8.

concept in Chinese, and it's expressed through the words *Miànzi* (面子) and *Liǎn* (脸).[16] "Face" means to present a respectable identity to the community, and it's connected to a person's prestige and morality. As we noted, the term *Yīnsī* was connected to shameful acts that people did not want to disclose to the public, so privacy in Ancient China acted as a prevention over the shame that would lead to a loss of face. As the loss of face would reflect not only on the individual but on its entire family, this reinforced the idea that shame had to be kept within the family household and not be shared with the outside community.[17]

In the nineteenth century, during the late Qing dynasty, China became increasingly in contact with Western values and ideas and began to be influenced more by Western legal systems, mainly by Civil Law systems. The 1911 *Civil Law Draft* of the Qing dynasty and the 1925 *Civil Law Draft* of the Republic of China presented for the first time a right to personality, even though they didn't come into force in the end.[18] Listed with many other rights, the first reference of the right to privacy was in Article 195 of the *Civil Law Code of the Republic of China* enacted between 1929 and 1932, the first ever Chinese Civil Code.[19]

Even though Western values, such as individualism, began shaping the Chinese way of thinking, including its conception on human rights, both the Nationalist Republic of China (R.O.C.) and the Communist People's Republic of China (P.R.C.) continued to stress the superiority of public interests, institutions, and services over the private ones. After the founding of the PRC in 1949, the Communist authorities began to impose severe restrictions to personal life in order to implement a planned economic system. State control became so persistent that the government played a role even in providing employment and influencing marital decisions.[20] The process of collectivization and the founding of the rural communal kitchens led individuals and families to have very low control not only on their own private property but also on intangible goods like their right to personal physical space or right to their own privacy.[21]

---

[16]WANG Hao, 2011, *Protecting Privacy in China, A Research on China's Privacy Standards and the Possibility of Establishing the Right to Privacy and the Information Privacy Protection Legislation in Modern China*, Springer-Verlag Berlin Heidelberg, p. 39.

[17] LI Tiffany, BRONFMAN Jill, ZHOU Zhou, 2017, "Saving Face: Unfolding the Screen of Chinese Privacy Law", *Journal of Law, Information, and Science (Forthcoming)*, p. 10.

[18] XU Jinghong, 2015, "Evolving Legal Frameworks for Protecting the Right to Internet Privacy in China". In LINDSAY Jon R., CHEUNG Tai Ming, REVERON Derek S., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, New York: Oxford University Press, p. 244.

[19] *Ibidem*.

[20] *Ibidem*.

[21] LI Tiffany, BRONFMAN Jill, ZHOU Zhou, 2017, "Saving Face: Unfolding the Screen of Chinese Privacy Law", *Journal of Law, Information, and Science (Forthcoming)*, p. 5.

After Mao's death in 1976, Deng Xiaoping inaugurated a new era with the implementation of far-reaching economic reforms and open up policies. There are three main factors that helped in enhancing privacy needs: the wide-ranging economic changes, the urbanization process and the introduction and development of new technologies. Elements of market economy began to be introduced in the planned economic system that was implemented during Maoist era. Private ownership and the pursuit of individual interests became important components of this new "socialist market economic system". At the same time the opening to Western countries helped the circulation of new values such as freedom, equality, individualism, and ultimately the right to privacy.[22] The urbanization process also posed new conditions for the development of privacy by increasing the disconnection of the individual with the family and collective units of the past.[23] Technological advancement and especially the popularization of the internet helped in the transformation of privacy ideas, but at the same time brought many privacy issues in new forms.[24]

All these elements supported the re-evaluation of the concept of private life among academics, politicians but also the Chinese citizens, that started giving importance to privacy and expressing concern over the protection of this emerging right.[25] First of all, there was more self-awareness amongst individuals of a right to privacy, so that if they did not want an information to be made public, they would decline to answer questions on the plea that this is their privacy. Even the relationship between parents and children was shaped by this new concept of privacy, as the latter started protesting against parents' intrusion in their room or of their personal diary and mail, whereas in the past there was the idea that no secret should be kept between parents and their children, as privacy was understood more as a line between the family and the community and not between individuals per se.[26] Second, Chinese citizens became less inclined to interfere with someone's else privacy: before the 1980s the practice of *Zhuojian* (捉奸)[27] of a person having an extramarital affair was still common, but now Chinese citizens started to regard it as a personal affair and did not wish to interfere.

---

[22] WANG Hao, 2011, *Protecting Privacy in China, A Research on China's Privacy Standards and the Possibility of Establishing the Right to Privacy and the Information Privacy Protection Legislation in Modern China*, Springer-Verlag Berlin Heidelberg, p. 41.
[23] LI Tiffany, BRONFMAN Jill, ZHOU Zhou, 2017, "Saving Face: Unfolding the Screen of Chinese Privacy Law", *Journal of Law, Information, and Science (Forthcoming)*, p. 2.
[24] WANG Hao, 2011, *Protecting Privacy in China, A Research on China's Privacy Standards and the Possibility of Establishing the Right to Privacy and the Information Privacy Protection Legislation in Modern China*, Springer-Verlag Berlin Heidelberg, p. 42.
[25] YAO-HUAI, Lü, 2005, "Privacy and data privacy issues in contemporary China", *Ethics and Information Technology*, Issue 7, p. 8.
[26] *Ibidem.*
[27] The practice of catching the adulterers in the act of having an extramarital relationship. *Ibidem.*

As the demands for more privacy kept on growing in the Chinese contemporary society, a gradual change had also been occurring in the PRC's legislative terminology. In these last years the scope of privacy has gradually expanded, shifting away from the ancient definition of privacy that sees it as nothing more than a shameful secret. Xu Jinghong identified three periods of the evolution of the right to privacy in the Chinese legislation:

- from 1949 to 1981, Chinese legislation defined privacy with the ancient word *Yīnsī* (阴私), restricting the scope of privacy protection to the aspect of shameful or embarrassing private affairs;
- from 1982 to 2002, the word *Yǐnsī* (隐私), which apparently was coined to correspond to the English word "privacy", began to appear and gradually replace the ancient word *Yīnsī*. The words were often used interchangeably;
- from 2003 to 2012, the Chinese legislation began to introduce the concept of "personal information", that has gradually been expanded to the online realm thanks to the SC-*NPC Decision on Strengthening Network Information Protection* issued in 2012.[28]

Today the concept of privacy still retains some Chinese characteristics. The concept of privacy is understood more in a collectivistic manner by Chinese society, as personal privacy continues to be limited by social benefits and national interests.[29] China still stresses group rights more than political and individual rights, while human rights are still a contested issue.[30] As Yao-Huai Lü states:

> "Even in contemporary China, along with increasing valuation of individual interests – even though the new collectivism leaves some space for individual privacy, the opinion that the collective is more important than the individual still makes it impossible to have a sense of privacy as strong as Western societies that, by contrast, begin with individualism as the foreground assumption undergirding privacy conceptions."[31]

Another aspect that distinguishes the Chinese concept of privacy from the Western notion is its relation with the right of reputation and dignity. Chinese individuals, law and courts continue to mostly associate the right to privacy with the right to reputation and dignity.[32] Article 140 of

[28] XU Jinghong, 2015, "Evolving Legal Frameworks for Protecting the Right to Internet Privacy in China". In LINDSAY Jon R., CHEUNG Tai Ming, REVERON Derek S., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, New York: Oxford University Press, pp. 244-245.
[29] YAO-HUAI, Lü, 2005, "Privacy and data privacy issues in contemporary China", *Ethics and Information Technology*, Issue 7, p. 11.
[30] WANG Zhizheng, 2017, "Systematic Government Access to Private-Sector Data in China". In CATE Fred H., DEMPSEY James X., *Bulk Collection: Systematic Government Access to Private-Sector Data*, New York: Oxford University Press, p. 243.
[31] YAO-HUAI, Lü, 2005, "Privacy and data privacy issues in contemporary China", *Ethics and Information Technology*, Issue 7, p. 12.
[32] "The data protection regime in China – In-depth Analysis for the LIBE Committee", *Directorate-General for*

the *Opinions of the Supreme People's Court on Several Issues concerning the Implementation of the General Principles of the Civil Law of the PRC for Trial Implementation*, issued in 1988, explicitly establishes a connection between the right to privacy and right of reputation.[33] In addition, the Chinese Constitution implicitly establishes the right to privacy through its Article 38 that states that "the personal dignity of citizens of the People's Republic of China is inviolable".[34]

In addition, the right to privacy in China is assumed to be a protection against fellow citizens interference rather than against government intrusion of their private life.[35] The government still exercises tight control over society, moreover it detains extensive powers of investigation, seizure, and search whenever state security and social order are at stake, as China's legal system grants extensive access to private sector data.[36]

1.1.2. The Definition of Personal Data Protection in China

Technology has always been challenging the notion of privacy throughout the years, especially after the creation of the internet and computers in 1960s. From its early application in the military and for academic purposes, the Internet has continuously expanded its services and it has become truly popular for commercial use.[37] Since the birth of the Internet many other technologies have been developed: from personal computers, smartphones, search engines and machine learning, to the most recent cloud computing, Internet of Things and Artificial Intelligence technologies. The creation of this new digital world has however challenged the protection of private life and personal information as the enormous amount of digital data generated can be collected, stored, processed, and transferred from a place to another in an easy

Internal Policies of the Union (European Parliament), https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf, accessed 17-03-2021

[33] WANG Faye Fangfei, 2014, *Law of Electronic Commercial Transactions – Contemporary Issues in the EU, US, and China*, London, Routledge, pp. 175-176.

[34] "中华人民共和国宪法", Zhōnghuá rénmín gònghéguó xiànfǎ, http://www.gov.cn/guoqing/2018-03/22/content_5276318.htm, accessed 01-10-2021. English Official Translation: http://www.npc.gov.cn/englishnpc/constitution2019/201911/1f65146fb6104dd3a2793875d19b5b29.shtml, accessed 01-10-2021.

[35] WANG Zhizheng, 2017, "Systematic Government Access to Private-Sector Data in China". In CATE Fred H., DEMPSEY James X., *Bulk Collection: Systematic Government Access to Private-Sector Data*, New York: Oxford University Press, p. 243.

[36] *Ibidem*.

[37] WANG Faye Fangfei, 2014, *Law of Electronic Commercial Transactions – Contemporary Issues in the EU, US, and China*, London, Routledge, pp. 6-7.

and far-reaching way. Technology advancement has led many legislators to introduce a "data protection right".

The "data protection" or "data privacy" right concerns the use of information about people and comprises of a set of principles related to the collection, accuracy, security, use, access, deletion etc. of digital data.[38]

China, similarly to the U.S. Data Protection Regime, doesn't have a general comprehensive law on data privacy, but rather establishes data rights and obligations through many legislative, administrative, and sectorial laws. Moreover, the right to privacy and the right to data privacy have not been formally distinguished like they are in the European Union legislation[39], so it is not possible to talk about a data protection regime in China without mentioning the more

[38] GREENLEAF Graham, 2014, *Asian Data Privacy Law*s, New York, Oxford University Press, p. 5.

[39] In the European Union the right to data privacy has been formally separated from the right to privacy protection in 2009 with the ratification of the Treaty of Lisbon. The distinction between these two rights has been first and foremost drawn out in their legal definition: the right to privacy is enshrined in Article 8 of the European Convention for Human Rights and Article 7 of the EU Charter for Fundamental Rights. These articles provide for the protection of four main areas of privacy: private life, family life, home, and communications; in addition, Article 8.2 sets forth the conditions of interference to the right to privacy. The right to data protection is set forth in Article 16 of the Treaty on the Functioning of the European Union (TFEU) and in Article 8 of the EU Charter, that states:
"Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority."
Another factor that further separates the two rights is their interpretation by EU courts: the right to privacy is not interpreted in a restrictive way by the two main European Courts that supervise this right, the European Court of Human Rights in Strasbourg and the EU Court of Justice in Luxembourg. The Courts do not attempt to define the content of what constitutes the right to privacy, consequently privacy is not seen as a bundle of specific rights but rather is approached case by case by the Courts. The right to data protection on the other hand has been envisioned as a set of principles, with specific definitions and notions such as "personal information", "data subject", "data controller" or "filing system". Data protection is understood as a "technical right": it requires auxiliary legislation to make its principles and requirements concrete in personal data processing instances and requires an independent national data protection authority (or DPA) as an enforcement mechanism. Nonetheless, there are many instances where the scope of the right to privacy and right to data protection differ, although many times there is an intersection and overlap between the content of the two rights, so much that jurisprudence in the European Union has considered privacy to be at the core of data protection. Still, we can find some substantial differences between the two rights: the right to data protection revolves around the processing of personal data, but not all personal data necessarily infringe upon privacy, while privacy itself is broader of a concept as it can apply also to the processing of data that is not personal and encompasses a physical aspect that data privacy does not contain. Also, data privacy protection is applied to data that lie outside the sphere of family and personal affairs, whereas the right to privacy is not so restricted.
"The data protection regime in China – In-depth Analysis for the LIBE Committee", *Directorate-General for Internal Policies of the Union (European Parliament),*
https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf, accessed 17-03-2021; GELLERT Raphaël, GUTWIRTH Serge, 2013, "The legal construction of privacy and data protection", *Computer Law & Security Review*, Vol. 29, Issue 5, pp. 523-526; "Article 8 - Protection of personal data", *EU Charter of Fundamental Rights*, https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data, accessed 20-09-2021; KOKOTT Juliane, SOBOTTA Christoph, 2013, "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR", *International Data Privacy Law*, Vol. 3, No.4, p. 223

general provisions adopted to protect the right to privacy in the Chinese Constitution, Civil and Tort Liability Law and Criminal Law, as the two terms are often used interchangeably. The main legal instruments on data privacy protection have been issued by the Standing Committee of the National People's Congress (SC-NPC), which is the second-highest legislative organ of the PRC, and by the Chinese Ministry of Industry and Information Technology (MIIT).[40]

China's emerging data privacy problems were spurred by the popularization of the Internet in the 1990s.[41] Chinese Internet has special features that make the Chinese digital landscape unique in the world: on one hand, there is a pervasive censorship that limits the access of citizens to certain websites (e.g. Western social media) and limits and monitors the scope of the conversations that can be published (e.g. on social and political rights); on the other hand, China has the biggest e-commerce market in the world with leading platforms like Alibaba (阿里巴巴, *Ālǐbābā*), Taobao (淘宝, *Táobǎo*) and TMall (天猫, *Tiānmāo*). Internet has become a useful tool for the spread of privacy, although new threats to the protection of private life have surfaced from it. Since privacy in China has still a close connection with the idea of reputation and "face", one of the main problems resulting from the popularization of the Internet has been the so-called phenomenon of *Human Flesh Search Engines* (人肉搜索, *Rénròu Sōusuǒ*), that is defined as "the use of the Internet to find embarrassing information about a person and harass them".[42]

The first steps towards a more comprehensive approach of the protection of personal digital data in China is the issuing of the SC-NPC *Decision on Strengthening Network Information Protection* in 2012, and the SC-NPC *Cybersecurity Law of the PRC* in 2018. It is however only since last year that China has decided to give special attention to the protection of personal data, as the new *Civil Code of the PRC* (taking effect on January 1st, 2021) presents a new dedicated section to personality rights; moreover, China is drafting two new comprehensive laws on data protection: the *Data Security Law of the PRC* and the *Personal Information Protection Law of the PRC*.

[40] "The data protection regime in China – In-depth Analysis for the LIBE Committee", *Directorate-General for Internal Policies of the Union (European Parliament)*, https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf, accessed 17-03-2021.
[41] YAO-HUAI, Lü, 2005, "Privacy and data privacy issues in contemporary China", *Ethics and Information Technology*, Issue 7, p. 9.
[42] XU Jinghong, 2015, "Evolving Legal Frameworks for Protecting the Right to Internet Privacy in China". In LINDSAY Jon R., CHEUNG Tai Ming, REVERON Derek S., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, New York: Oxford University Press, pp. 242-260

The first definition of "user's personal data" in Chinese legal texts can be found in the *2011 MIIT Regulations*, which is at a lower level of a SC-NPC law, that defines personal data as "any information that relates to a user and that separately or in combination with other information may be used to identify the user".[43] It is however the SC-NPC *PRC Cybersecurity Law* that defines "personal information" with a similar wording but with the addition of "personal biometric information" in its list.[44] Article 3 of the *2013 MIIT Guidelines* (which are not legally binding documents) also defines "sensitive personal information" as follows:

> "The information that would have an adverse impact on the subject of personal information if disclosed or altered. […] For example, the sensitive personal information may include identity card numbers, mobile phone numbers, race, political viewpoint, religion, or biometric information, fingerprint and so forth."[45]

[43] Art. 11 of 'Several Regulations on Standardizing Market Order for Internet Information Services', Decree of the Ministry of Industry and Information Technology (No. 20), 7 December 2011, in force 15 March 2012. From GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, pp. 205-210.
[44] "中华人民共和国网络安全法", Zhōnghuá rénmín gònghéguó wǎngluò ānquán fǎ, https://www.pkulaw.com/chl/4dce14765f4265f1bdfb.html, accessed 03-11-2021. English Translation: "Cybersecurity Law of the People's Republic of China", https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/, accessed 03-11-2021.
[45] GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, p. 211.

1.2. The Chinese General Legal Framework for Privacy Protection: A Fragmented Reality

1.2.1. International Obligations

Since its entry the World Trade Organization in 2001, the People's Republic of China has gradually become more involved with and integrated in the international community. However, the only international document relating to the protection of privacy as a right that has been signed by the PRC is the 1966 *International Covenant on Civil and Political Rights,* whose article 17 states:

> "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks."[46]

Although it was signed in 1998, China has still not undertaken any ratification process.

China is one of the 21 member economies of the Asia-Pacific Economic Cooperation (APEC), an international organization that doesn't have a constitution or treaty but operates by consensus. APEC has developed a set of principles of data privacy protection in 2004, namely the *APEC Privacy Framework.* The Framework is not binding and can be undertaken on a voluntarily basis, but China has not yet indicated that it will be involved in the APEC Cross-Border Privacy Rules system.[47]

Therefore, China nowadays doesn't carry any international obligations regarding privacy protection.

1.2.2. The Chinese Constitution: Is Privacy recognized as a human right?

The Chinese Constitution (中华人民共和国宪法, *Zhōnghuá rénmín gònghéguó xiànfǎ*) is the supreme law of the PRC. It's the fundamental legal document that sits at the top of the hierarchy of legal norms in the People's Republic of China and all Chinese laws should be made in accordance with it. There only have been four Constitutions in the history of the PRC: the *Constitution of 1954*, the *Constitution of 1975*, the *Constitution of 1978*, and the current

[46] "International Covenant on Civil and Political Rights", https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx, accessed 07-10-2021.
[47] GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, p. 197.

Constitution of 1982.[48] Human rights provisions are introduced in Chapter 2 of the Constitution. The Constitution of the PRC does not explicitly mention a right to privacy protection, although a general privacy protection framework is provided by Articles 37, 38, 39 and 40. The Chinese modern word for "privacy", 隐私, is not even present in the constitutional text, nor in its English official translation.[49] Articles 37 and 39 respectively protect freedom of person of Chinese citizens and freedom of residence, both deemed as "inviolable" (不受侵犯， *bù shòu qīnfàn*). Article 38 protects the personal dignity of citizens and prohibits to use any means to insult, libel or falsely accuse citizens.[50] Personal dignity is a concept that is very closely related to privacy, and both Chinese citizens and lawmakers still find a close connection between dignity, reputation and the idea of privacy. Personal dignity therefore encompasses several aspects, including a right to name, right to portrait, and right to privacy.[51] Article 40 protects the freedom and privacy of correspondence. Instead of using the Chinese word for privacy here the Chinese legislator decided to use the word 秘密 (*Mìmì*), which is then translated as "confidentiality" in the official translation.[52] This Chinese word is usually translated as "secret" or "clandestine, confidential", and oftentimes doesn't have a positive connotation. In the Constitutional text, it is also present as 国家秘密 (*Guójiā mìmì*) in Articles 53 and 76, literally translated as "State Secrets". According to the *China Legal Information Center* (中国普法网，*Zhōngguó pǔfǎ wǎng*), a website under the leadership of the Ministry of Justice of the PRC designed to introduce the Chinese legal system to English speakers, the concept of freedom and privacy of correspondence finds the following definition: "Anyone may not conceal, destroy and discard, open and read or eavesdrop citizens' correspondence (including telegraph, telephone, mail and other lawful electronic contacts)".[53]

Although these four articles prohibit unlawful intrusion and search of one's home and correspondence and unlawful detention or restriction of a citizen's personal freedom by private

[48] WANG Hao, 2011, *Protecting Privacy in China, A Research on China's Privacy Standards and the Possibility of Establishing the Right to Privacy and the Information Privacy Protection Legislation in Modern China*, Springer-Verlag Berlin Heidelberg, p.50.
[49] *Ibidem.*
[50] *Ibidem*.
[51] *Ibidem*, p. 52.
[52] "中华人民共和国宪法", Zhōnghuá rénmín gònghéguó xiànfǎ, http://www.gov.cn/guoqing/2018-03/22/content_5276318.htm, accessed 01-10-2021. English Official Translation: http://www.npc.gov.cn/englishnpc/constitution2019/201911/1f65146fb6104dd3a2793875d19b5b29.shtml, accessed 01-10-2021
[53] "What is freedom and privacy of correspondence?", https://www.chinadaily.com.cn/m/chinalic/2017-06/16/content_29774939.htm, *China Legal Information Center*, accessed 11-10-2021.

actors, extensive powers of investigation and censorship are given to the Government whenever state security is at stake. Article 40 provides:

> "Except in cases necessary for national security or criminal investigation, when public security organs or procuratorial organs shall examine correspondence in accordance with procedures prescribed by law, no organization or individual shall infringe on a citizen's freedom and confidentiality of correspondence for any reason."[54]

This article therefore represents the legal basis with which the government of the PRC legitimizes its interference in the private sector, giving the possibility to specific governmental bodies to access the personal information of citizens and organizations.[55]

More generally, the concept of human rights is understood differently in China, so the Chinese Constitution ought not be perceived in the same way as western constitutions.[56] The Western human rights model had been heavily criticized during the Maoist era as a propaganda tool of Western policy against socialist countries.[57] During the process of opening towards the West (改革开放, *Gǎigé Kāifàng*) that began in the 1970s, the term "human rights" became more and more a focal point in China's foreign relations and internal politics, in particular following the events in Tiananmen Square in 1989.[58] The 2004 amendment brought a revision of Article 33 with the introduction of a new paragraph: "the State shall respect and protect human rights".[59]

Despite these advancements, human rights under the Chinese Constitution are mainly protected against private parties without mentioning or extending protection against governmental actions.[60] Moreover, Chinese governmental rights will always prevail on citizens' basic

---

[54] "中华人民共和国宪法", Zhōnghuá rénmín gònghéguó xiànfǎ, http://www.gov.cn/guoqing/2018-03/22/content_5276318.htm, accessed 01-10-2021. English Official Translation: http://www.npc.gov.cn/englishnpc/constitution2019/201911/1f65146fb6104dd3a2793875d19b5b29.shtml, accessed 01-10-2021.

[55] WANG Zhizheng, 2017, "Systematic Government Access to Private-Sector Data in China". In CATE Fred H., DEMPSEY James X., *Bulk Collection: Systematic Government Access to Private-Sector Data,* New York: Oxford University Press, p. 245.

[56] "The data protection regime in China – In-depth Analysis for the LIBE Committee", *Directorate-General for Internal Policies of the Union (European Parliament*), https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf, accessed 17-03-2021.

[57] CHEN Dingding, 2005 "Explaining China's Changing Discourse on Human Rights, 1978-2004", *Asian Perspective*, Vol. 29, No. 3, pp. 162-163.

[58] *Ibidem*, pp. 168-169.

[59] "中华人民共和国宪法", Zhōnghuá rénmín gònghéguó xiànfǎ, http://www.gov.cn/guoqing/2018-03/22/content_5276318.htm, accessed 01-10-2021. English Official Translation: http://www.npc.gov.cn/englishnpc/constitution2019/201911/1f65146fb6104dd3a2793875d19b5b29.shtml, accessed 01-10-2021.

[60] WANG Hao, 2011, *Protecting Privacy in China, A Research on China's Privacy Standards and the Possibility of Establishing the Right to Privacy and the Information Privacy Protection Legislation in Modern China*, Springer-Verlag Berlin Heidelberg, p. 51.

rights.[61] The latter concept is explicitly expressed in the constitutional treaty in numerous articles, the most emblematic of which is Article 51, which states:

> "When exercising their freedoms and rights, citizens of the People's Republic of China shall not undermine the interests of the State, society or collectives, or infringe upon the lawful freedoms and rights of other citizens."[62]

Another prominent aspect of the Chinese Constitution, unlike most Western Constitutions, is the absence of a constitutional control body. The People's Supreme Court, the highest judicial organ of the PRC, cannot determine whether legislation is "unconstitutional". In addition, Chinese Constitution is regarded as "non justiciable"[63], meaning that courts cannot interpret the Constitution and cannot refer directly to constitutional provisions as basis of judicial adjudication. It therefore becomes impossible to develop a constitutional right to privacy through case law as it happens, for example, in the US (where privacy can be protected under the Fourth Amendment).[64]

The most notable case regarding infringement of constitutional rights is the *Qi Yuling vs. Chen Xiaoqi* case. This case refers indirectly to the protection of the right of privacy, as it is a case of identity theft. The defendant (Chen Xiaoqi) and the plaintiff (Qi Yuling) both graduated from the same high school, after which Chen fraudulently impersonated Qi to pursue higher education. The case was first treated as an infringement of the *General Principles of Civil Law* (GPCL) by the Shandong Court, afterwards the matter was forwarded to the Supreme People's Court that ruled in favor of Qi on the basis that her constitutional right of education (Article 46) was infringed.[65] In 2008 the SPC officially withdrew this decision, and in 2016 it issued a regulatory document that forbad direct citation of constitutional provisions by courts.[66] Therefore Chinese Constitution's provisions on privacy protection are considered of limited relevance as they cannot be referred to in cases of civil liability.

---

[61] *Ibidem*.
[62] "中华人民共和国宪法", Zhōnghuá rénmín gònghéguó xiànfǎ, http://www.gov.cn/guoqing/2018-03/22/content_5276318.htm, accessed 01-10-2021. English Official Translation: http://www.npc.gov.cn/englishnpc/constitution2019/201911/1f65146fb6104dd3a2793875d19b5b29.shtml, accessed 01-10-2021.
[63] GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, p. 196.
[64] FENG Yang, 2019, "The future of China's Personal Data Protection Law: challenges and prospects", *Asia Pacific Law Review*, Vol. 27, Issue 1, p. 69.
[65] GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, p. 196.
[66] ZHAO Bo, FENG Yang, 2021, "Mapping the development of China's data protection law: Major actors, core values, and shifting power relations", *Computer Law & Security Review*, Vol. 40, pp. 12-13.

1.2.3. Civil Law and Tort Liability Law

China came into contact with Western civil law towards the end of the 19th century. However, despite attempts at codification by the Qing in 1911, the first and only (so far) example of the Chinese Civil Code was promulgated between 1929 and 1930 by the Nationalist government of the Republic of China. During the Maoist era, the breakdown of relations with the USSR inaugurated a period known as the "ten years of disorder" (十年乱, *Shí Nián Luàn*), during which all law-related activities were suspended. Civil law essentially disappeared because personal relationships were *de facto* considered to be of collective interest.

In the 1980s, with the beginning of the reformation phase inaugurated by Deng Xiaoping, China began to imitate the language, techniques and institutions of foreign civil law. The Chinese legislator in this period opted to adopt a series of separate legislative acts rather than drafting a comprehensive Civil Code, like the *General Principles of Civil Law* (GPCL) in 1986, the *Contract Law of the PRC* in 1999, the *Property Law of the PRC* in 2007 and the *Tort Liability Law of the PRC* in 2009 to cite a few.[67]

For almost three decades, the only civil legal document that implicitly regulated the right to privacy was the GPCL. Like the Chinese Constitution, this law did not explicitly mention privacy per se, but a series of related topics were the object of GPCL provisions. These provisions were contained in Chapter V: Civil Rights (第五章:民事权利, *Dì wǔ Zhāng: Mínshì Quánlì*), more specifically in Section 4: Personal Rights (第四节:人身权, *Dì sì Jié: Rénshēnquán*).[68]

Article 99 of the GPCL protected the right to name of both natural and legal persons. Articles 100 and 102 respectively regulated the right to portrait of individual citizens and right to honour of natural and legal persons. Article 101 also provided that:

> "Citizens and legal persons shall enjoy the right of reputation. The personality of citizens shall be protected by law, and the use of insults, libel or other means to damage the reputation of citizens or legal persons shall be prohibited"[69]

[67] WANG Liming, 2019, "The modernization of Chinese civil law over four decades", *Frontiers of Law in China*, Vol. 14, Issue 1, 42-44.
[68] "中华人民共和国民法通则-1986", *Zhōnghuá rénmín gònghéguó mínfǎ tōngzé*, https://www.pkulaw.com/chl/4202520b3be0ae24bdfb.html?keyword=%E6%B0%91%E6%B3%95%E9%80%9A%E5%88%99, accessed 15-10-2021. English Translation: "General Principles of the Civil Law of the People's Republic of China - 1986", https://www.pkulaw.com/en_law/4202520b3be0ae24bdfb.html, accessed 15-10-2021.
[69] *Ibidem*.

This Article established a right of reputation that in judicial practices has been expanded and intended to encompass the right to privacy. The Supreme People's Court (SPC) is a judicial organ that directs judicial activity with its own Interpretative Opinions, that, although not a formal source of law of the RPC, *de facto* have a quasi-legislative function and are binding to lower courts. This is a unique feature among legal systems, and it has to be taken into account as SPC Interpretations have often integrated law provisions. The SPC issued three Opinions relating to privacy protection in the GPCL, namely the *Opinions on Several Questions concerning the Implementation of the GPCL* in 1988, the *Reply to Several Questions on Adjudicating the Cases of the Rights of Reputation* in 1993, and the *Interpretation of the Supreme People's Court Regarding issues of Ascertaining the Liability of Compensation for Spiritual Damage for Tort* in 2001. The first two did not recognize the right to privacy as a separate right from reputation, but instead explained how various forms of disclosure of personal information had to be treated as an invasion or infringement of the right of reputation.[70] The 2001 SPC Interpretation however put privacy on the same level of other personality rights, as its Article 1 stated:

> "If someone infringes upon other's privacy or other personality interests, and the aggrieved party, taking tort as the cause to get compensation for spiritual damage, brings a suit to a People's Court, the People's Court shall accept it according to law"[71]

A further step revealing increasing willingness by the courts to establish a separate right to privacy was the *Wang Fei v. Zhang Leyi, Daqi.co and Tianya.com* case in 2008.[72] The wife of Wang Fei, Jiang Yan, committed suicide after discovering her husband extra-marital affair. Her friend, Zhang Leyi, posted on the two web platforms personal information about the plaintiff and also blog entries of the deceased wife that documented the pain and suffering she was experiencing before her suicide. This blog sparked outcry among net users, who started a human-flesh search that ended up in displaying personal information of the plaintiff and his supposed mistress. As a consequence, the two were forced to leave their job, as a result of a heavy damage to their reputation. Court proceedings found Zhang Leyi and Daqi.com guilty of invading the plaintiff privacy and ordered the defendants to pay the plaintiff. This case is important as the Court defined the right to privacy as follows:

[70] GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, p.200.
[71] *Interpretation of the Supreme People's Court Regarding issues of Ascertaining the Liability of Compensation for Spiritual Damage for Tort*, Art. 1. Translation from YAO-HUAI, Lü, 2005, "Privacy and data privacy issues in contemporary China", *Ethics and Information Technology*, Issue 7, p. 10.
[72] ONG Rebecca, 2012, "Online vigilante justice Chinese style and privacy in China", *Information & Communications Technology Law*, Vol. 21, Issue 2, p. 136.

> "privacy means private life, information, space and peace of private life related to a person's interests and personality that he does not intend to share with others. The right to privacy is infringed by the disclosure or publication of private information that a person does not want to disclose to others concerning his private life, private areas or domestic tranquility and connected with his interests of his body."[73]

The Court went further to identify five factors determining whether infringement of privacy occurred: a) the manner by which the private information was acquired, (b) the manner by which the information was disclosed, (c) the scope of disclosure, (d) the purpose of disclosure and (e) the consequences of disclosure.[74]

The first ever civil law that recognized the right to privacy as a separate right was the *Tort Liability Law* (TLL) issued in 2009. Article 2 provides that tortious liability arises from infringement of civil rights, including the right to privacy, that has been listed separately from other personality rights (such as the right of name, right of reputation, right of honor, right to portrait) for the first time in a civil law.[75] This Law however does not contain any definition of the right to privacy, even if Article 52 poses additional obligations for medical institutions to protect patients' privacy.[76]

TLL poses additional obligations and tortious liability on Internet Service Providers (ISPs), content providers and net users. Article 36 states:

> "Internet users and internet service providers shall bear tort liability if they utilize the internet to infringe upon civil rights of others.
>
> If an internet user commits tort through internet services, the infringed shall be entitled to inform the internet service provider to take necessary measures, including, inter alia, deletion, blocking and disconnection. If the internet service provider fails to take necessary measures in a timely manner upon notification, it shall be jointly and severally liable with the said internet user for the extended damage.
>
> If an internet service provider is aware that an internet user is infringing on the civil rights and interests of others through its internet services and fails to take necessary measures, it shall be jointly and severally liable with the said internet user for such infringement."[77]

[73] ONG Rebecca, 2012, "Online vigilante justice Chinese style and privacy in China", *Information & Communications Technology Law*, Vol. 21, Issue 2, p. 134.
[74] *Ibidem*.
[75] "Tort Liability Law of the People's Republic of China", http://www.npc.gov.cn/zgrdw/englishnpc/Law/2011-02/16/content_1620761.htm, accessed 16-10-2021.
[76] GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, p.202.
[77] "Tort Liability Law of the People's Republic of China", http://www.npc.gov.cn/zgrdw/englishnpc/Law/2011-02/16/content_1620761.htm, accessed 16-10-2021.

Before this law, ISPs and content providers had no obligations or restrictions on information dissemination by net users. Through TLL, ISPs and content providers can be jointly or severally held liable whenever there is both knowledge and failure to take appropriate measures to stop tortious actions from net users.[78] However, TLL happens to have been primarily used to resolve disputes between individuals rather than against corporations.[79]

In 2014 the Supreme People's Court issued the *Provisions on Several Issues concerning the Application of Law to Adjudicate Civil Disputes involving Infringement of Personal Rights Via Information Networks*. These provisions stated that courts should accept cases involving disclosure by net users and net service providers of both personal and generic information. At the same time, the SPC Provisions listed some exemptions that therefore did not constitute basis for tort claims: a) Disclosure with written consent and within legal scope; b) disclosure for the public interest; c) disclosure by educational or scientific entity for academic research or statistical analysis.[80]

After Xi Jinping became China's paramount leader in 2013, a new strong emphasis has been put on legal reforms. On 6 August 2015 the five-year legislation Plan of the 12th National People's Congress was updated, mentioning the drafting of a new comprehensive Civil Code.[81] In 2017 the NPC issued the *General Provisions of the Civil Law of the People's Republic of China* (中华人民共和国民法总则, *Zhōnghuá rénmín gònghéguó mínfǎ zǒngzé*), intended to be the first book of the new Chinese Civil Code that was going to be issued in 2020. This Law officially substituted the GPCL 1986. Articles 110 and 111 respectively address the right to privacy of natural persons and the right to protection of personal information by formally distinguishing the two. Article 111 poses certain obligations to both individuals and organizations about ensuring safety of information and lawfully collecting, using, processing and transferring personal information of others.[82]

The new Chinese Civil Code officially came into effect on 1st January 2021. The Civil Code not only provides a clear definition of the right to privacy for the first time but also contains a

[78] ONG Rebecca, 2012, "Online vigilante justice Chinese style and privacy in China", *Information & Communications Technology Law*, Vol. 21, Issue 2, p. 140.
[79] GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, p.202.
[80] LI Tiffany, BRONFMAN Jill, ZHOU Zhou, 2017, "Saving Face: Unfolding the Screen of Chinese Privacy Law", *Journal of Law, Information, and Science (Forthcoming)*, p. 22.
[81] TIMOTEO Marina, 2019, "China Codifies. The First Book of the Civil Code between Western Models to Chinese Characteristics", *Opinio Juris in Comparatione*, Vol.1, Issue 1, pp. 51-72.
[82] "中华人民共和国民法总则- 2017", *Zhōnghuá rénmín gònghéguó mínfǎ zǒngzé*, https://www.pkulaw.com/chl/c6f2d80ee8c0c709bdfb.html, accessed 16-10-2021. English Translation: "General Provisions of the Civil Law of the People's Republic of China - 2017", https://www.pkulaw.com/en_law/c6f2d80ee8c0c709bdfb.html, accessed 16-10-2021.

specific chapter on personality rights. It is revolutionary in a sense as it doesn't only distinguish privacy from personal information protection but sets out basic principles for it and provides obligations for data processors and rights of individuals related to personal information, with similar wording to European Union's GDPR.[83] As many provisions have a data privacy focus, we will dedicate a more detailed section on the new Chinese Civil Code in chapter 1.4.1.

1.2.4. Criminal Law

The first Criminal Law of the PRC (中华人民共和国刑法, *Zhōnghuá rénmín gònghéguó xíngfǎ*) was issued in 1979. This law was however revised in 1997, and since then eleven amendments have been issued. The 1997 Criminal Law of the PRC already contains some articles related to the protection of the right to privacy: Article 245 addresses illegal physical search of others and illegal search of others' residences by providing a maximum penalty of three years of prison or criminal detention; Article 252 provides a maximum of one year of prison or criminal detention for those who hide, destroy, or illegally open others' letters; Article 253 provides a maximum of two years for postal workers who open, hide, or destroy mail or telegrams without authorization; Article 284 addresses uses of special monitoring or photographing equipment.[84] Both Article 252 and Article 284 provide such measures only if the infringement has "severe consequences", however no definition of this term is provided and no criteria is laid out to address what is to be considered a severe circumstance.

In 2009 the Standing Committee of the National People's Congress issued *Amendment VII to the Criminal Law of the PRC* (中华人民共和国刑法修正案(七)", *Zhōnghuá rénmín gònghéguó xíngfǎ xiūzhèng àn (qī)*). For the first time, China established a criminal law provision on personal information with the introduction of Article 253(a). The Article is divided into three paragraphs, the first of which states:

> "Any staff member of a State organ, or an institution of finance, telecommunication, transportation, education, or health care, etc., who in violation of State regulations, sells or illegally provides citizens' personal information obtained by the aforesaid entity during the

[83] LAU Nanda, GUO Gavin, GONG James, "China Cybersecurity and Data Protection: China's Civil Code lays foundation for data protection", *China Investments E-Bulletin - Herbert Smith Freehills*, https://www.lexology.com/library/detail.aspx?g=89f22cb9-ff6c-41c1-9c55-3f94c6ef5faa, accessed 16-10-2021.
[84] "中华人民共和国刑法(1997修订)", *Zhōnghuá rénmín gònghéguó xíngfǎ (1997 xiūdìng)*, https://www.pkulaw.com/chl/9ec4004a183a7d8cbdfb.html, accessed 18-10-2021. English Translation: "Criminal Law of the People's Republic of China (1997 Revision)", https://www.pkulaw.com/en_law/9ec4004a183a7d8cbdfb.html?keyword=criminal%20law%201997, accessed 18-10-2021.

course of performing duties or providing services shall, if the circumstances are serious, be sentenced to a fixed term of imprisonment of not more than three years or criminal detention and be concurrently imposed with a fine, or shall be imposed with a fine alone."[85]

The limitations presented in this paragraph are evident: the illegal provisions or sale of personal information constitute criminal offense only if carried out by staff members of State organs or specific industries; moreover, it requires "serious circumstances", which are undefined. Subsequent case law, like the *Roadway case*, suggests that this paragraph is actually intended to encompass all industries with access to large amounts of personal data, such as marketing companies like Roadway.[86]

The second paragraph of Article 253(a) is interpreted more broadly, as the same penalties of the first paragraph will apply to any person that illegally obtains personal information by theft or other means, when circumstances are serious.[87] Therefore, any individual, regardless of its industry, can be prosecuted on the basis of this paragraph.[88]

The third paragraph imposes a monetary penalty to entities committing crimes specified in the first two paragraphs, while the person in charge of the entity or the person directly responsible for the crime may also be subject to imprisonment or criminal detention.[89]

Despite the fact that Article 253(a) does not define or delineate the scope of personal information, it has been the most used Article to enforce the right to privacy in the Chinese judicial system. While civil litigation regarding this specific right is underused, with Article 36 of *Tort Liability Law* not having had major commercial impact yet, the use of Article 253(a) has become more common, with notable cases like the *Roadway case*.

[85] "中华人民共和国刑法修正案(七)", *Zhōnghuá rénmín gònghéguó xíngfǎ xiūzhèng àn (qī)*, https://www.pkulaw.com/chl/e9381f0afa80a487bdfb.html, accessed 19-10-2021. English Official Translation: "Amendment VII to the Criminal Law of the People's Republic of China", http://www.npc.gov.cn/zgrdw/englishnpc/Law/2011-02/15/content_1620636.htm, accessed 19-10-2021.
[86] GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, p.198.
[87] "中华人民共和国刑法修正案(七)", *Zhōnghuá rénmín gònghéguó xíngfǎ xiūzhèng àn (qī),* https://www.pkulaw.com/chl/e9381f0afa80a487bdfb.html, accessed 19-10-2021. English Official Translation: "Amendment VII to the Criminal Law of the People's Republic of China", http://www.npc.gov.cn/zgrdw/englishnpc/Law/2011-02/15/content_1620636.htm, accessed 19-10-2021.
[88] "The data protection regime in China – In-depth Analysis for the LIBE Committee", *Directorate-General for Internal Policies of the Union (European Parliament)*, https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf, accessed 17-03-2021.
[89] "中华人民共和国刑法修正案(七)", *Zhōnghuá rénmín gònghéguó xíngfǎ xiūzhèng àn (qī),* https://www.pkulaw.com/chl/e9381f0afa80a487bdfb.html, accessed 19-10-2021. English Official Translation: "Amendment VII to the Criminal Law of the People's Republic of China", http://www.npc.gov.cn/zgrdw/englishnpc/Law/2011-02/15/content_1620636.htm, accessed 19-10-2021.

Shanghai Roadway D&B Marketing Service Co. Ltd. was fined one million yuan and four of its executives imprisoned for two years on the basis of Article 253(a) of the Criminal Law of the PRC for having purchased personal information on 150 million Chinese consumers.[90]

Another important provision introduced by Amendment VII is the inclusion of two new paragraphs in Article 285, which address crimes related to computer information systems, such as unlawful invasion or control.[91]

In 2015, *Amendment IX to the Criminal Law of the People's Republic of China* (中华人民共和国刑法修正案(九), *Zhōnghuá rénmín gònghéguó xíngfǎ xiūzhèng àn (jiǔ)*) expanded the scope of application of the first paragraph of Article 253(a), by providing that "anyone who sells or provides personal information, in violation of national provisions, to third parties is subject to punishment".[92] Moreover, if circumstances are "extremely serious", custodial penalty can be increased to a maximum of seven years.[93]

Additionally, the IX Amendment introduces new provisions in Article 286 for network service providers (which include both ISPs and content providers), which can be subject to fines and criminal punishment if they illegally leak users' information with serious consequences.[94]

The latest development in Criminal Law related to the protection of personal data is the 2017's *Interpretation on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Infringing on Citizens' Personal Information* (最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释， *Zuìgāo rénmín fǎyuàn, zuìgāo rénmín jiǎncháyuàn guānyú bànlǐ qīnfàn gōngmín gèrén xìnxī xíngshì ànjiàn shìyòng fǎlǜ ruògān wèntí de jiěshì*) jointly issued by the Supreme People's Court and the Supreme People's Procuratorate. Article 1 of the Interpretation defines the scope of "citizens' personal

---

[90] "The data protection regime in China – In-depth Analysis for the LIBE Committee", *Directorate-General for Internal Policies of the Union (European Parliament)*, https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf, accessed 17-03-2021; GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, p.199.

[91] "中华人民共和国刑法修正案(七)", *Zhōnghuá rénmín gònghéguó xíngfǎ xiūzhèng àn (qī),* https://www.pkulaw.com/chl/e9381f0afa80a487bdfb.html, accessed 19-10-2021. English Official Translation: "Amendment VII to the Criminal Law of the People's Republic of China", http://www.npc.gov.cn/zgrdw/englishnpc/Law/2011-02/15/content_1620636.htm, accessed 19-10-2021.

[92] LI Tiffany, BRONFMAN Jill, ZHOU Zhou, 2017, "Saving Face: Unfolding the Screen of Chinese Privacy Law", *Journal of Law, Information, and Science (Forthcoming)*, p. 23.

[93] "中华人民共和国刑法修正案(九)", *Zhōnghuá rénmín gònghéguó xíngfǎ xiūzhèng àn (jiǔ),* https://www.pkulaw.com/chl/6c18c6f3a93ad220bdfb.html, accessed 19-10-2021. English translation: "Amendment (IX) to the Criminal Law of the People's Republic of China", https://www.pkulaw.com/en_law/6c18c6f3a93ad220bdfb.html, accessed 19-10-2021.

[94] LI Tiffany, BRONFMAN Jill, ZHOU Zhou, 2017, "Saving Face: Unfolding the Screen of Chinese Privacy Law", *Journal of Law, Information, and Science (Forthcoming)*, p. 23.

information" specified in Article 253 of the Criminal Law of the PRC as "various information recorded electronically or in other ways that can identify a specific natural person alone or in combination with other information, or that can reflect the activities of a specific natural person, including Name, ID number, communication contact information, address, account password, property status, whereabouts, etc."[95] In addition, the Interpretation lists detailed rules for determining what could constitute a serious circumstance, and specific thresholds for criminalizing data abuse.[96]

Criminal Law remains the preferred way to prosecute privacy and personal data infringement rather than resorting to civil and administrative remedies, with 4911 criminal cases related to identity theft only in 2017.[97] However, due to lack of human and financial resources, enforcement agencies have adopted a selective approach as only the most serious criminal cases regarding personal information infringement are *de facto* being prosecuted, and this has led to data abuse still being a widespread issue in China.[98]

[95] 第一条　刑法第二百五十三条之一规定的"公民个人信息"，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。
"最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释", *Zuìgāo rénmín fǎyuàn, zuìgāo rénmín jiǎncháyuàn guānyú bànlǐ qīnfàn gōngmín gèrén xìnxī xíngshì ànjiàn shìyòng fǎlǜ ruògān wèntí de jiěshì*, https://www.pkulaw.com/chl/88d3a698daf58033bdfb.html, accessed 19-10-2021. Translation provided by author.
[96] FENG Yang 2019, "The future of China's Personal Data Protection Law: challenges and prospects", *Asia Pacific Law Review,* Vol. 27, Issue 1, pp. 71-72.
[97] ZHAO Bo, FENG Yang, 2021, "Mapping the development of China's data protection law: Major actors, core values, and shifting power relations", *Computer Law & Security Review*, Vol. 40, p. 5.
[98] FENG Yang 2019, "The future of China's Personal Data Protection Law: challenges and prospects", *Asia Pacific Law Review,* Vol. 27, Issue 1, pp. 71-72.

1.3. Data Protection Laws in China

The People's Republic of China has yet to adopt a comprehensive law on data protection. This doesn't mean however that personal data has not been regulated in China: several laws have been issued during the last two decades, that primarily regulate the private sector. Public sector remains fairly unregulated and even when it is vague definitions and exemption rules still grant the Government extensive rights of intrusion into citizens' personal data.[99]

1.3.1. 2012 SC-NPC Decision on Strengthening Network Information Protection

On December 28, 2012, the Standing Committee of the National People's Congress issued the *Decision on Strengthening Network Information Protection* (全国人大常委会关于加强网络信息保护的决定, *Quánguó réndà chángwěi huì guānyú jiāqiáng wǎngluò xìnxī bǎohù de juédìng*). It is composed of 12 articles and its focus is on the protection of online personal information, which mainly applies to the private sector, although it is one of the first legal documents also featuring a legal provision on the public sector. The need for a high-level regulation on the matter of personal data protection has been spurred not only by the rapid development of e-commerce in China and Internet technologies advancement that enhanced issues like online fraud and human-flesh searches, but also stems from the fact that ISPs and content providers in China seldom self-regulate, with no limitations on collection of personal information or monitor measures carried out on employees.[100] The many scandals involving personal data breaches but also the lacking privacy protection practices of many internet operators sparked outcry among the population and triggered a national response in the Chinese government. A perfect example of this is the dispute that escalated between *Tencent QQ* and *Qihoo 360* in 2010 which demonstrated that without effective legislation internet companies did not effectively protect the right to privacy, as they both accused the other of carrying out spying activities on its thousands of users.[101]

The aim of the Decision is to protect security of network information in order to safeguard citizens' and legal persons' rights and public security, its scope however happens to fall outside

[99] WANG Zhizheng, 2017, "Systematic Government Access to Private-Sector Data in China". In CATE Fred H., DEMPSEY James X., Bulk Collection: *Systematic Government Access to Private-Sector Data*, New York: Oxford University Press, pp. 243-244.
[100] XU Jinghong, 2015, "Evolving Legal Frameworks for Protecting the Right to Internet Privacy in China". In LINDSAY Jon R., CHEUNG Tai Ming, REVERON Derek S., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, New York: Oxford University Press, pp. 250-251.
[101] *Ibidem*, p. 251.

the Internet context suggested by its title, as most of its provisions are referred to both "network service providers and all enterprises and institutions that collect or use citizens' personal electronic information during their provision of services".[102] The wording used suggests that even brick and mortar stores that collect information at point of sale and store it electronically could be included in the scope of the Decision.[103]

According to the Decision, no individual or organization may illegally steal, obtain or provide or may sell electronic information of others (Article 1). In addition, the Decision imposes some general principles and obligations on network service providers and enterprises mentioned above. When collecting personal data of others, they shall follow principles of legality, legitimacy and necessity, while clearly stating the purpose, methods and scope of collection. Consent shall be obtained from network users, and rules for collection and use of data shall be disclosed to the public (Article 2).[104] They shall maintain strict confidentiality of information (Article 3) and provide technical and remedial measures to ensure data security (Article 4). There is also a provision prohibiting all individuals and organizations to send commercial messages to users without their consent or request (Article 7). Network service providers also have the obligation to cease information transmission or eliminate information that is illegally published or transmitted by net users and report the relevant records to supervisory departments (Article 5), with whom they shall cooperate and provide technical support (Article 10).[105]

The Decision 2012 also requires real name provisions for telecommunication services, meaning that network service providers in this field shall require users to provide true information on their identities (Article 6). Some general users' rights are listed in Articles 8 and 9, like the right of deletion of information that infringes on their right to privacy or other legal rights, or that discloses their personal identity, or the right to report or file accusations with the supervisory authorities about criminal acts involving network information.[106]

The Decision also includes a provision on the public sector, as Article 10 states:

---

[102] "全国人大常委会关于加强网络信息保护的决定", *Quánguó réndà chángwěi huì guānyú jiāqiáng wǎngluò xìnxī bǎohù de juédìng*, http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm, accessed 23-10-2021. English Translation: WANG Ted, 2016, "The NPC Standing Committee Decision on Strengthening the Network Information Protection", *Chinese Law and Government, Taylor & Francis Group*, Vol. 48, No. 1, 13–14.
[103] GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, pp. 204-205.
[104] "全国人大常委会关于加强网络信息保护的决定", *Quánguó réndà chángwěi huì guānyú jiāqiáng wǎngluò xìnxī bǎohù de juédìng*, http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm, accessed 23-10-2021. English Translation: WANG Ted, 2016, "The NPC Standing Committee Decision on Strengthening the Network Information Protection", *Chinese Law and Government, Taylor & Francis Group*, Vol. 48, No. 1, 13–14.
[105] *Ibidem*.
[106] *Ibidem*.

> "State organs and their staff shall maintain confidentiality concerning the electronic information of individual citizens they learn of during the fulfillment of their duties, and shall not leak, alter, or damage and destroy such information, or sell it or illegally provide it to others."[107]

This provision is very general and doesn't extend the other obligations imposed on private network service providers and enterprises to the public sector.

Article 11 sets penalties for those violating the provisions contained in the Decision, ranging from simple warnings to monetary fines, to revocation of business licenses and deletion of website. All violations may also be recorded in social credit files and publicly announced.[108]

The terminology used in the Decision has been adopted in other laws such as the 2013 Amendments to the Consumer Law of the PRC, as well as other implementing regulations, such as the 2013 Ministry of Industry and Information Technology Regulations.[109]

Although this law represents a very important step in the evolution of the Chinese legal framework concerning data protection on the Internet and has the merit of providing for the first time a general set of data protection principles, it still has some shortcomings, especially if we try to compare it to the EU data protection model, which is one of the strictest in the world. The concept of "electronic information" or "processing" is not defined clearly in the Decision, and Article 2 lacks some basic data protection principles such as the rights of information, access, correction and also the right to be forgotten.[110] An enforcement mechanism is not provided by the Decision as it doesn't clearly state which authority will enforce the requirements it established.

1.3.2. PRC Law on the Protection of Consumer Rights and Interests

The SC-NPC issued the *Law of the People's Republic of China on Protection of Consumer Rights and Interests* (中华人民共和国消费者权益保护法, *Zhōnghuá rénmín gònghéguó xiāofèi zhě quányì bǎohù fǎ*) in 1993. Originally, this law didn't have an explicit provision on

[107] "全国人大常委会关于加强网络信息保护的决定", *Quánguó réndà chángwěi huì guānyú jiāqiáng wǎngluò xìnxī bǎohù de juédìng*, http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm, accessed 23-10-2021. English Translation: WANG Ted, 2016, "The NPC Standing Committee Decision on Strengthening the Network Information Protection", *Chinese Law and Government, Taylor & Francis Group*, Vol. 48, No. 1, 13–14.
[108] *Ibidem*.
[109] GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, p. 205.
[110] "The data protection regime in China – In-depth Analysis for the LIBE Committee", *Directorate-General for Internal Policies of the Union (European Parliament)*, https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf, accessed 17-03-2021.

privacy or data protection. Only Article 25 provided that "Business operators may not insult or slander consumers, may not search the body of consumers or the articles they carry with them, and may not violate the personal freedom of consumers."[111] Article 32, in addressing the duties of China's consumer associations, provided that they should assist consumers in instituting legal proceeding when their rights and interests as consumers are infringed, and to expose and criticize acts harmful to the legal rights of the consumers.[112] Nonetheless, consumers associations were not empowered to deal with privacy issues in an effective way.[113]

In 2013 the Standing Committee issued the first significant Amendment of the PRC Consumer Law concerning the collection and use of personal information of consumers by all industries. The Amendment included provisions whose key terminology was almost identical with the articles issued in the *Decision on Strengthening Network Information Protection* of 2012. The new Article 29 of the PRC Consumer Law, pursuant Article 2 of the Decision 2012, demanded operators collecting and using consumers' personal information to follow principles of legality, legitimacy and necessity, and state purpose, methods and scope of use of such information, previous obtainment of consumers' consent. Rules for collection and use should be made public to consumers. Article 29 also features elements of Article 3, 4 and 7 of the Decision, as operators are demanded to treat information from consumers in a confidential manner (as in Article 3), to take both technical and remedial measure to ensure security (as in Article 4) and prevent unsolicited marketing messages to consumers (as in Article 7).[114] Use of personal information shall be made in accordance with agreements with consumers or in accordance with applicable laws, and such information cannot be sold or illegally provided to others.[115]

The new Article 50 of the amended PRC Consumer Law provides civil liability for operators who infringe upon the personal dignity, liberty and personal information protection of consumers. Operators not only have the obligation to stop infringement, but should also restore

[111] "中华人民共和国消费者权益保护法*", Zhōnghuá rénmín gònghéguó xiāofèi zhě quányì bǎohù fǎ*, https://www.pkulaw.com/chl/f9d6438c22a2f335bdfb.html, accessed 25-10-2021. English Translation: "Law of the People's Republic of China on Protection of Consumer Rights and Interests", https://www.pkulaw.com/en_law/f9d6438c22a2f335bdfb.html?keyword=consumer, accessed 25-10-2021.
[112] *Ibidem*.
[113] WANG Hao, 2011, *Protecting Privacy in China, A Research on China's Privacy Standards and the Possibility of Establishing the Right to Privacy and the Information Privacy Protection Legislation in Modern China*, Springer-Verlag Berlin Heidelberg, pp. 187-188.
[114] "中华人民共和国消费者权益保护法(2013修正)", *Zhōnghuá rénmín gònghéguó xiāofèi zhě quányì bǎohù fǎ (2013 xiūzhèng)*, https://www.pkulaw.com/chl/a347c82e6a7d13aabdfb.html, accessed 26-10-2021. English translation from: TIAN George Yijun, in GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, p. 209.
[115] *Ibidem*.

consumers' reputation, eliminate the impact of their actions, offer apologies and pay damages to consumers.[116]

Article 56(9) empowers relevant administrative departments to issue enforcement measures that range from warnings, monetary fines, confiscation of illegal earnings, suspension or rectification of acts from operators to even rescinding their business license if offences are serious.[117]

The 2013 Amendment also provides the State Administration of Industry and Commerce (SAIC) to assist the Ministry of Industry and Information Technology in regulating China's consumer market, particularly in the e-commerce field.[118] Although SAIC has now been merged into the new State Administration for Market Regulation (SAMR), in 2015 it actually issued a new regulation related to consumer rights, namely the *Measures for Punishment of Infringements of Consumer Rights and Interest* (侵害消费者权益行为处罚办法, *Qīnhài xiāofèi zhě quányì xíngwéi chǔfá bànfǎ*), which defines similar provisions set in the PRC Consumer Law. Article 11 of the Measures defines consumer personal information as "information collected by an enterprise operator during the sale of products or provision of services, that can, singly or in combination with other information, identify a consumer".[119]

The provisions set in the PRC Consumer Law lack detail, and same as the Decision 2012 do not provide data subject rights of access, correction and deletion of personal information, nor do they mention an effective enforcement mechanism. Processing and disclosure of consumers' information is only limited by agreements and law provisions, with no explicit mention of purpose of collection or minimal use.[120] Nevertheless the new advancements set in the 2013 Amendment are important for two reasons: first, it expanded the scope of protection of personal information set by the Decision 2012, as Amendment 2013 applies to all consumers transaction, both online and offline, and not only to the Internet and telecommunication services field.

[116] "中华人民共和国消费者权益保护法(2013修正)", *Zhōnghuá rénmín gònghéguó xiāofèi zhě quányì bǎohù fǎ (2013 xiūzhèng)*, https://www.pkulaw.com/chl/a347c82e6a7d13aabdfb.html, accessed 26-10-2021. English translation from: GREENLEAF Graham, 2013, "Data Protection Widened by China's Consumer Law Changes", *Privacy Laws & Business International Report*, Vol. 126, pp. 127-128.
[117] *Ibidem*.
[118] GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, p. 218.
[119] "侵害消费者权益行为处罚办法", *Qīnhài xiāofèi zhě quányì xíngwéi chǔfá bànfǎ*, http://www.saic.gov.cn/fgs/lflg/fgfb/201504/t20150403_154911.html, accessed 26-10-2021. English Translation from: LI Tiffany, BRONFMAN Jill, ZHOU Zhou, 2017, "Saving Face: Unfolding the Screen of Chinese Privacy Law", *Journal of Law, Information, and Science (Forthcoming)*, p. 16.
[120] GREENLEAF Graham, 2013, "Data Protection Widened by China's Consumer Law Changes", *Privacy Laws & Business International Report*, Vol. 126, pp. 127-128.

Second, its wording shows consistency in the Standing Committee of NPC law-making policies regarding protection of personal data.[121]

1.3.3. MIIT Regulations 2011 and 2013

At a lower level but still relevant as many of their provisions will be adopted afterwards in the PRC Cybersecurity Law, we find some legal instruments issued by the Ministry of Industry and Information Technology (MIIT). The Ministry of Industry and Information Technology is a department of the PRC State Council whose role has become pivotal in the area of personal information protection, as it has the power to issue administrative laws, either named Regulations or Provisions, that fall within its scope of action, although these must be consistent with both SC-NPC and State Council legislation.[122]

As scandals revolving around privacy and data protection on the Internet kept on permeating Chinese society, the MIIT enacted two important implementing regulations, namely the *Several Provisions on Regulating the Market Order of Internet Information Services* (规范互联网信息服务市场秩序若干规定， *Guīfàn hùliánwǎng xìnxī fúwù shìchǎng zhìxù ruògān guiding*) in 2011 and the *Provisions on Protecting the Personal Information of Telecommunications and Internet Users* (电信和互联网用户个人信息保护规定，*Diànxìn hé hùliánwǎng yònghù gèrén xìnxī bǎohù guiding*) in 2013.[123] Although these are sectorial provisions as they only regulate the Internet and telecommunications field, they nonetheless present strong data protection features that resemble the level of protection afforded to individuals by the OECD Guidelines.[124]

---

[121] "The data protection regime in China – In-depth Analysis for the LIBE Committee", *Directorate-General for Internal Policies of the Union (European Parliament),* https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf, accessed 17-03-2021.

[122] GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, pp. 204-205.

[123] "规范互联网信息服务市场秩序若干规定", *Guīfàn hùliánwǎng xìnxī fúwù shìchǎng zhìxù ruògān guiding*, https://www.pkulaw.com/chl/c513bd8a91c45ac4bdfb.html, accessed 28-10-2021. English Translation: "Several Provisions on Regulating the Market Order of Internet Information Services", https://www.pkulaw.com/en_law/c513bd8a91c45ac4bdfb.html?keyword=Internet%20Information%20Services, accessed 28-10-2021.
"电信和互联网用户个人信息保护规定", *Diànxìn hé hùliánwǎng yònghù gèrén xìnxī bǎohù guiding*, https://www.pkulaw.com/chl/f0f7c6124531c3bebdfb.html?keyword=%E7%94%B5%E4%BF%A1%E5%92%8C%E4%BA%92%E8%81%94%E7%BD%91%E7%94%A8%E6%88%B7%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A4%E8%A7%84%E5%AE%9A, accessed 28-10-2021. English Translation: "Provisions on Protecting the Personal Information of Telecommunications and Internet Users", https://www.pkulaw.com/en_law/f0f7c6124531c3bebdfb.html, accessed 28-10-2021.

[124] "The data protection regime in China – In-depth Analysis for the LIBE Committee", *Directorate-General for Internal Policies of the Union (European Parliament),*

The 2011 MIIT Regulation applies to "those engaged in internet information services and activities related to internet information services within the territory of the People's Republic of China" (Article 2)[125], that has been interpreted as encompassing all entities providing information to internet users, not only Internet companies.[126] This Regulation contains additional principles, from general principles of "equality, free will, fairness and good faith" that must be followed during provision of internet information services in Article 4, to more specific additional data privacy principles expressed in Articles 11-14.[127] Article 11, other than providing a definition for "user's personal information" (用户个人信息, *Yònghù gèrén xìnxī*), which include "any information that relates to a user and that separately or in combination with other information may be used to identify the user"[128], also defines the principle of minimal collection, stating that Internet Information Service Providers (IISPs) may not collect information for a purpose other than the provision of their services, unless otherwise required by the law.[129] Moreover, purpose notification is required, that is the user not only shall give consent but has to be notified of the "method, content and purpose of collecting and processing user's personal information" (Article 11).[130] Article 13 empowers users to use, modify and delete the information updated by them. IISPs shall not provide users' personal information and must not transfer the data without authorization.[131] No access or correction rights are granted in the MIIT Regulations 2011. It's important to highlight that whenever the Regulation refers to "information uploaded by users", this expression limits its scope of application and doesn't comprehend data collected from third parties or generated by transaction.[132]

---

https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf, accessed 17-03-2021.

[125] "规范互联网信息服务市场秩序若干规定", *Guīfàn hùliánwǎng xìnxī fúwù shìchǎng zhìxù ruògān guiding*, https://www.pkulaw.com/chl/c513bd8a91c45ac4bdfb.html, accessed 28-10-2021. English Translation: "Several Provisions on Regulating the Market Order of Internet Information Services", https://www.pkulaw.com/en_law/c513bd8a91c45ac4bdfb.html?keyword=Internet%20Information%20Services, accessed 28-10-2021.

[126] GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, pp. 205-206.

[127] *Ibidem*.

[128] "规范互联网信息服务市场秩序若干规定", *Guīfàn hùliánwǎng xìnxī fúwù shìchǎng zhìxù ruògān guiding*, https://www.pkulaw.com/chl/c513bd8a91c45ac4bdfb.html, accessed 28-10-2021. English Translation from: GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, p. 210.

[129] "规范互联网信息服务市场秩序若干规定", *Guīfàn hùliánwǎng xìnxī fúwù shìchǎng zhìxù ruògān guiding*, https://www.pkulaw.com/chl/c513bd8a91c45ac4bdfb.html, accessed 28-10-2021. English Translation: "Several Provisions on Regulating the Market Order of Internet Information Services", https://www.pkulaw.com/en_law/c513bd8a91c45ac4bdfb.html?keyword=Internet%20Information%20Services, accessed 28-10-2021.

[130] *Ibidem*.

[131] *Ibidem*.

[132] GREENLEAF Graham, 2012, "China's Internet Data Privacy Regulations 2012: 80% of a Great Leap Forward?", Privacy Laws & Business International Report, Issue 116, p. 3.

The 2013 MIIT Regulation applies to both IISPs and also Telecommunications Business Operators (TBOs). It has a broader scope than the 2011 MIIT Regulation as it was issued as an implementing regulation for the SC-NPC Decision 2012, and at the same time its Article 4 expands the scope of the definition of "user's personal information" to "other information, as well as the time, and place of the user using the service and other information, collected by TBOs and IISPs in the process of providing services".[133] Informed consent is required to collect and use data, but both in the 2011 MIIT Regulation and the 2013 MIIT Regulation there are no specifications on actions that have to be taken to demonstrate such consent, nor do they provide differentiation between data collected directly from the users and third-parties data.[134] Although both Regulations do not provide an independent enforcement mechanism and lack provisions on State organs, the 2013 MIIT Regulation contains more complete rules on data protection as it lays out more detailed security protection provisions, a sound internal security system, data breach notifications, providers' liability, and provides users with "channels to consult and correct information".[135]

1.3.4. PRC Cybersecurity Law

While China's Internet had been experiencing a dramatic growth, also thanks to the popularization of mobile smartphones, that went from 17 million in 2008 to almost 1.09 billion in only ten years,[136] the issue of cybersecurity had been emerging as a daunting challenge to China's leadership. The Chinese government had to deal not only with a general lack of network protection capabilities that brought frequent leakage of personal information and the development of a flourishing cybercrime black market, but also security threats posed by foreign cyberattacks from other countries.[137] One of the most notable cases that affected not only China but sparked outcry in the whole international community was the scandal brought by the Snowden Revelations. Edward Snowden disclosed the global surveillance activities that the U.S. National Security Agency (NSA) was carrying out in cooperation with

[133] GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, p. 210.
[134] *Ibidem* p. 211.
[135] *Ibidem*, pp. 210-215; GREENLEAF Graham, LIVINGSTON Scott, 2016, "China's New Cybersecurity Law – Also a Data Privacy Law?", *Privacy Laws & Business International*, Issue 144, p. 4.
[136] QuestMobile, 2018, "QuestMobile: 2017 China mobile Internet report", https://www.questmobile.com.cn/blog/en/blog_130.html, accessed 03-11-2021. In YANG Fan, XU Jian, 2018, "Privacy concerns in China's smart city campaign: The deficit of China's Cybersecurity Law", *Asia and the Pacific Policy Studies*, Vol. 5, Issue 3, p. 536.
[137] LI Yuxiao, XU Lu, 2015, "China's Cybersecurity Situation and the Potential for International Cooperation". In LINDSAY Jon R., CHEUNG Tai Ming, REVERON Derek S., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, New York: Oxford University Press, pp. 226-229.

telecommunication companies. China had also been the target of such surveillance operations, with the NSA allegedly hacking multiple Chinese telecommunication companies in Hong Kong and also tapping the backbone network of Tsinghua University.[138]

The new Chinese leadership under Xi Jinping brought a shift in the country's policies surrounding Internet security. In February 2014, the Chinese Communist Party (CCP) announced the creation of the *Internet Security and Informatization Leading Small Group* (网络安全和信息化领导小组, *Wǎngluò ānquán hé xìnxī huà lǐngdǎo xiǎozǔ*), with President Xi as its chairman. Its aim is to promote the informatization of China and enhance the country's national security.[139] Leading Groups are CCP's deliberative committees that have the power to influence the Standing Committee by giving policy recommendations.[140]

The Cybersecurity Law of the PRC is the result of the efforts put in by the Chinese leadership in trying to enhance security of information networks. The Cybersecurity Law is placed among a series of policy initiatives and legislation issued in the precedent years and aimed at strengthening national security protection, such as the PRC National Security Law (which already entitles the Chinese Government with vast authority to establish a cybersecurity system), and the PRC Counterterrorism Law, though the Cybersecurity Law represents the most comprehensive law on the issue.[141]

The *Cybersecurity Law of the People's Republic of China* (中华人民共和国网络安全法, *Zhōnghuá rénmín gònghéguó wǎngluò ānquán fǎ*) was passed on November 7, 2016, by the SC-NPC, and it officially came into effect on June 1, 2017. The passage of this law has been fairly controversial, as many private sector actors (especially foreign businesses), raised concerns on certain law provisions that could enhance government intrusion and intellectual property theft.[142]

The Cybersecurity Law main purpose is to "guarantee cybersecurity, safeguard cyberspace sovereignty, national security and public interest, protect the lawful rights and interests of citizens, legal persons and other organizations, and promote the sound development of

[138] *Ibidem*, p. 228.
[139] POLLPETER Kevin, 2015, "Chinese Writings on Cyberwarfare and Coercion". In LINDSAY Jon R., CHEUNG Tai Ming, REVERON Derek S., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, New York: Oxford University Press, p. 146.
[140] HSU Kimberly, MURRAY Craig, 2014, "China and International Law in Cyberspace", *U.S.-China Economic and Security Review Commission Staff Report*, p. 5.
[141] LEE Jyh-An, 2018, "Hacking into China's Cybersecurity Law", *Wake Forest Law Review*, Vol. 53, No. 1, pp. 63-65.
[142] *Ibidem*, p. 60.

economic and social informatization." (Article 1).[143] It sets additional obligations to network operators (网络运营者， *Wǎngluò yùnyíng zhě*), which are defined in Article 76(2) as comprising of network owners, managers, and network service providers. The same Article also contains the definition of Personal Information (个人信息，*Gèrén xìnxī*) in its fifth paragraph:

> "Personal information" refers to all kinds of information, recorded electronically or through other means, that taken alone or together with other information, is sufficient to identify a natural person's identity, including but not limited to natural persons' full names, birth dates, national identification numbers, personal biometric information, addresses, telephone numbers, and so forth."[144]

This is the first high-level law giving a definition of the term, although the exact same formulation was already present in Article 11 of the 2011 MIIT Regulations that similarly defines "user's personal information". Nonetheless, it is the first time that "personal biometric information" is included in the definition of personal information.[145] Still, the Cybersecurity law makes no distinction between "personal information" and "sensitive personal information", which can only be currently found in non-mandatory national guidelines, specifically, in the 2013 MIIT Guidelines.[146] However, special provisions of the law are addressed to operators of "Critical Information Infrastructures" (关键信息基础设施的运营者， *Guānjiàn xìnxī jīchǔ shèshī de yùnyíng zhě*, CII), mainly in the field of data localization and data sovereignty (Article 37). CIIs include, but are not limited to, public communication and information services, power, traffic, water resources, finance, public service, e-government information infrastructures (Article 31).

Requirements of personal information protection are mainly incorporated in Chapter IV of the Law, namely the Chapter on "Network Information Security" (网络信息安全，*Wǎngluò xìnxī ānquán*). The principles of confidentiality and of informed consent and notice are defined

[143] "中华人民共和国网络安全法", *Zhōnghuá rénmín gònghéguó wǎngluò ānquán fǎ*, https://www.pkulaw.com/chl/4dce14765f4265f1bdfb.html, accessed 03-11-2021. English Translation: "Cybersecurity Law of the People's Republic of China", http://www.lawinfochina.com/Display.aspx?LookType=3&Lib=law&Id=22826&SearchKeyword=&SearchCKeyword=&paycode=, accessed 03-11-2021.
[144] "中华人民共和国网络安全法", *Zhōnghuá rénmín gònghéguó wǎngluò ānquán fǎ*, https://www.pkulaw.com/chl/4dce14765f4265f1bdfb.html, accessed 03-11-2021. English Translation: "Cybersecurity Law of the People's Republic of China", https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/, accessed 03-11-2021.
[145] GREENLEAF Graham, LIVINGSTON Scott, 2016, "China's New Cybersecurity Law – Also a Data Privacy Law?", *Privacy Laws & Business International*, Issue 144, p. 3.
[146] "Regulating electronic means to fight the spread of COVID-19: Argentina, Australia, Brazil, China, England, European Union, France, Iceland, India, Iran, Israel, Italy, Japan, Mexico, Norway, Portugal, Russian Federation, South Africa, South Korea, Spain, Taiwan, Turkey, United Arab Emirates." *The Law Library of Congress, Global Research Directorate*, https://www.loc.gov/item/2020714995/, accessed 10-02-2021.

respectively in Articles 40 and 41, reaffirming the same provisions already established in the SC-NPC Decision 2012, which in combination with the new Cybersecurity Law has been referred to as "One Law One Decision" (一法一决定, *Yī fǎ yī juédìng*) in official reports by the former Supreme People's Court President, Wang Shengjun.[147] Article 41 also defines the collection limitation principle that prohibits network operators to collect personal information unrelated to the service they provide. Compared with the wording used in the two MIIT Regulations of 2011 and 2013, it is notable that the standard set in Cybersecurity Law is more moderate as collection can be carried out if personal information is "related to" the service operators provide, and not if it is "necessary for" the aforementioned service as provided in the MIIT Regulations.[148] Disclosure limitations are addressed in Article 42, which prohibits to disclose information unless the person involved gives consent, or the processed information renders such individual unidentifiable and there is no way to recover its identity from the information. The same Article also defines data breach remedial measures and notification, that in comparison with previous legislation adds a new requirement to notify users of the data breach. Another significant new element provided by the Cybersecurity Law is that individuals are explicitly given the power to request deletion and correction of their personal information (Article 43). Notably, the right of access to such information and to data quality (meaning accuracy, completeness and timeliness of personal information collected) are missing in the Cybersecurity Law.[149]

One of the most controversial articles of the Cybersecurity Law is Article 37 regarding cross-border data transfers. This Article sets data localization requirements for CII operators, meaning they are required to store personal information and "other important data" within Mainland China. Whenever such data needs to be transferred outside Chinese borders, operators must go through a security assessment conducted by the Cyberspace Administration of China (CAC) and relevant State Council departments and obtain approval from authorities.[150] This provision raised concern not only because its scope seems to be too broad, as the term "other important

[147] WANG Shengjun, "Report concerning the Inspection of the Implementation of the 'Cybersecurity Law of the People's Republic of China' and the 'National People's Congress Standing Committee Decisions concerning strengthening Online Information Protection'", https://digichina.stanford.edu/work/report-concerning-the-inspection-of-the-implementation-of-the-cybersecurity-law-of-the-peoples-republic-of-china-and-the-national-peoples-congress-standing/, accessed 03-11-2021.
[148] GREENLEAF Graham, LIVINGSTON Scott, 2016, "China's New Cybersecurity Law – Also a Data Privacy Law?", *Privacy Laws & Business International*, Issue 144, p. 4.
[149] *Ibidem*, p. 5.
[150] "中华人民共和国网络安全法", *Zhōnghuá rénmín gònghéguó wǎngluò ānquán fǎ*, https://www.pkulaw.com/chl/4dce14765f4265f1bdfb.html, accessed 03-11-2021. English Translation: "Cybersecurity Law of the People's Republic of China", https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/, accessed 03-11-2021.

data" remains undefined, and procedures for carrying out security assessment are not provided, but also because it entails considerable costs for foreign companies in terms of data management, as they will need to build local data centers in China or seek local data storage services.[151] Additionally, foreign companies feared that this provision might potentially increase the risk of data leaks, especially if combined with the fact that the Cybersecurity Law grants the Chinese government broad access to private sector data. On this matter, Article 28 requires network operators to "provide technical support and assistance to State organs in safeguarding national security and investigating criminal activities in accordance with the law".[152] Companies may be required to provide access or decryption of user's confidential information or create backdoors for government intrusion,[153] increasing the risk of this information being lost, passed to competitors or used by the authorities.[154] These concerns led more than 50 U.S., European and Japanese companies to sign a letter to Premier Li Keqiang in June 2016 criticizing the law, prompting the Cyberspace Administration of China to delay execution of data localization requirements until the end of 2018.[155]

Lastly, another prominent provision in the Cybersecurity Law is the requirement for "network operators handling network access and domain name registration services for users, handling stationary or mobile phone network access, or providing users with information publication or instant messaging services" to implement a real-name registration scheme, with the additional prohibition to provide services to those refusing to supply real identity information (Article 24).[156] Limiting cyberspace anonymity has become a major policy goal for the Chinese government that aims at fostering an healthy internet environment in which rumors, vulgarity, pornography and other unhealthy information should be eliminated.[157] Critics have however argued that real-name provisions may not only prevent users from exercising their constitutional

[151] LEE Jyh-An, 2018, "Hacking into China's Cybersecurity Law", *Wake Forest Law Review*, Vol. 53, No. 1, pp. 79-82.
[152] "中华人民共和国网络安全法", *Zhōnghuá rénmín gònghéguó wǎngluò ānquán fǎ*, https://www.pkulaw.com/chl/4dce14765f4265f1bdfb.html, accessed 03-11-2021. English Translation: "Cybersecurity Law of the People's Republic of China", https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/, accessed 03-11-2021.
[153] LEE Jyh-An, 2018, "Hacking into China's Cybersecurity Law", *Wake Forest Law Review*, Vol. 53, No. 1, pp. 72-73.
[154] WAGNER Jack, "China's Cybersecurity Law: What You Need to Know", *The Diplomat*, https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/, accessed 04-11-2021.
[155] *Ibidem*; LEE Jyh-An, 2018, "Hacking into China's Cybersecurity Law", *Wake Forest Law Review*, Vol. 53, No. 1, pp. 60-61.
[156] "中华人民共和国网络安全法", *Zhōnghuá rénmín gònghéguó wǎngluò ānquán fǎ*, https://www.pkulaw.com/chl/4dce14765f4265f1bdfb.html, accessed 03-11-2021. English Translation: "Cybersecurity Law of the People's Republic of China", https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/, accessed 03-11-2021.
[157] LEE Jyh-An, LIU Ching-Yi, 2016, "Real-Name Registration Rules and the Fading Digital Anonymity in China", *Washington International Law Journal*, Vol. 25, No. 1, pp. 15-16.

rights, such as their freedom of expression, but could also pose serious threats to privacy protection as hackers may steal identity information from network operators.[158]

1.3.5. PRC E-Commerce Law

One of the latest advancements in the realm of personal data protection is the promulgation of the *E-Commerce Law of the People's Republic of China* (中华人民共和国电子商务法, *Zhōnghuá rénmín gònghéguó diànzǐ shāngwù fǎ*), adopted at the Fifth Session of the Standing Committee of the 13th National People's Congress on August 31, 2018, and effective from January 1, 2019.

E-commerce has had an explosive development in China, with Alibaba as the market leading firm. Its two main platforms, Taobao and Tmall, already surpassed Amazon and eBay's combined gross merchandise value in 2012.[159] Another more recent addition to the electronic commerce market is Tencent's integration of an online shopping feature in its instant messaging platform WeChat (known as Weixin in China, 微信, *Wēixìn*).[160] Chinese legislators had to face a number of issues due to the rapid expansion of the market, as e-commerce platforms and operators tend to treat user data as a kind of proprietary asset and have little or no interest in upgrading their data protection regime.[161] It is interesting to note that Alibaba used to have two different privacy policies for Alibaba.com (the global trade platform) and Alibaba.com.cn (the Chinese platform), in which the former was updated in 2009 while the latter remained unchanged since the company's foundation in 1999. Although similar, Alibaba.com presented more advanced provisions on collection, third-party data transfer and amendments to privacy policy than Alibaba.com.cn.[162] The Chinese Government often seeks support and cooperation from these digital companies in order to achieve its governance goals, and this in turn has given these enterprises, and especially e-commerce platforms, much bargaining power in terms of

[158] *Ibidem*, pp. 15-18; LEE Jyh-An, 2018, "Hacking into China's Cybersecurity Law", *Wake Forest Law Review*, Vol. 53, No. 1, p. 89.
[159] FU Tao, 2019, "China's personal information protection in a data-driven economy: A privacy policy study of Alibaba, Baidu and Tencent", *Global Media and Communication*, Vol. 15, Issue 2, pp. 195-213.
[160] KHARPAL Arjun, "Tencent launches new online shopping feature in WeChat app, in a challenge to rivals Alibaba and JD", *CNBC News*, https://www.cnbc.com/2020/07/16/china-tech-giant-tencent-launches-new-online-shopping-feature-in-wechat-app.html, accessed 06-11-2021.
[161] LI Yuxiao, XU Lu, 2015, "China's Cybersecurity Situation and the Potential for International Cooperation". In LINDSAY Jon R., CHEUNG Tai Ming, REVERON Derek S., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, New York: Oxford University Press, p. 233.
[162] WANG Faye Fangfei, 2014, *Law of Electronic Commercial Transactions – Contemporary Issues in the EU, US, and China*, London, Routledge, pp. 180-182.

protecting their corporate interests, and the final version of the E-Commerce Law can be taken as an exemplar case of this power relation.[163]

The first draft of the E-Commerce law presented a provision that granted e-commerce users the right of self-determination of his/her personal data (Article 45), and in general posed heavy data protection obligations to e-commerce operators. However, both the second draft and the final version of the legal document deleted these data requirements as a consequence of heavy pressure from digital enterprises and support from deputies within the Congress. [164] Nonetheless, the current PRC E-Commerce Law still affords some level of data privacy protection to users. The law applies to all businesses selling goods or proving services through the network, with the exclusion of certain categories, such as "financial products and services, and services of providing news and information, audio and video program, publication and cultural products through information network" (Article 2).[165] Among E-commerce operators' obligations, listed in Article 5, there is network safety and personal information protection, which is further broken down in the obligation to abide by laws and administrative regulations on personal information protection during collection and use (Article 23), to publicize the manner and procedure for search, correction, deletion of user information and user deregistration without setting unreasonable conditions and provide it in a timely manner upon identity verification, and in case of deregistration, delete user's information unless retention is required by law (Article 24).[166] E-commerce operators also needs to provide authorities with e-commerce data when required by law (Article 25).[167]

Similar requirements are provided for e-commerce platform operators, that shall develop the service agreement and transaction rules of the platform under the principles of openness, fairness and impartiality (Article 32) and also publicize service agreement and transaction rules at a conspicuous position of its homepage (Article 33). E-commerce platform operators shall require real name registration for e-commerce operators and hand over their identity information to market regulation authorities and taxation authorities (Article 27 and 28).[168]

---

[163] ZHAO Bo, FENG Yang, 2021, "Mapping the development of China's data protection law: Major actors, core values, and shifting power relations", *Computer Law & Security Review*, Vol. 40, pp. 8-9.
[164] *Ibidem*, p. 9.
[165] "中华人民共和国电子商务法", *Zhōnghuá rénmín gònghéguó diànzǐ shāngwù fǎ*, https://www.pkulaw.com/chl/3f020f79c1e5316ebdfb.html, accessed 07-11-2021. English Translation: "E-Commerce Law of the People's Republic of China", https://ipkey.eu/sites/default/files/documents/resources/PRC_E-Commerce_Law.pdf, accessed 07-11-2021.
[166] *Ibidem*.
[167] *Ibidem*.
[168] *Ibidem*.

1.3.6. Non-Mandatory National Guidelines

Given the lack of a comprehensive law for data privacy and personal information protection, and the fact that current legislation has not yet effectively established an independent Data Protection Authority (DPA), a number of Chinese Administrations and Ministries have issued their own regulations and guidelines concerning data protection provisions. We already named two regulations from the Ministry of Industry and Information Technology, namely the *2011 MIIT Regulation* and the *2013 MIIT Regulation*. In 2013 the Ministry also issued in combination with the State Administration of Quality Supervision, Inspection and Quarantine (AQSIQ, now dissolved) and the Standardization Administration of the People's Republic of China (SAC) the *Guidelines for the Protection of Personal Information 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, *Xìnxī ānquán jìshù gōnggòng jí shāngyòng fúwù xìnxī xìtǒng gèrén xìnxī bǎohù zhǐnán*).

Although voluntary in nature, these Guidelines are of significant importance as they have a broader scope than previous regulations and laws, in the sense that they apply to "guiding the protection of personal information in information systems by all types of organizations and institutions other than government organs and other institutions performing public management duties, such as service institutions in telecommunications, finance, and medical care, etc." (Article 1).[169] They not only define key terminology such as "sensitive personal information" (Article 3.8), "information system" (Article 3.1), and the relevant parties involved such as "data subject" "data controller" "data processor" and "third-party agencies" (Article 3), but also delineate a series of eight data privacy principles that a data controller should follow (Article 4.2).[170] These basic principles include provisions of clear purpose, minimum and sufficiency, public notification, personal consent, quality assurance, safety guarantee, good faith and data accountability, with notable absence of data rights of access and correction.[171]

[169] "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", *Xìnxī ānquán jìshù gōnggòng jí shāngyòng fúwù xìnxī xìtǒng gèrén xìnxī bǎohù zhǐnán*, https://www.pkulaw.com/chl/0ff5bc705d989a1abdfb.html?keyword=%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8%E6%8A%80%E6%9C%AF%E5%85%AC%E5%85%B1%E5%8F%8A%E5%95%86%E7%94%A8%E6%9C%8D%E5%8A%A1%E4%BF%A1%E6%81%AF%E7%B3%BB%E7%BB%9F%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A4%E6%8C%87%E5%8D%97, accessed 08-11-2021. English Translation: "Information Security Technology – Guidelines for the Protection of Personal Information in Public and Commercial Service Information Systems", https://www.pkulaw.com/en_law/0ff5bc705d989a1abdfb.html, accessed 08-11-2021.
[170] *Ibidem*.
[171] GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, pp. 209-210.

Other institutions have been in charge of issuing data privacy related Guidelines or National Standards (which are either mandatory or recommended), such as the Cybersecurity Administration of China (CAC), the Ministry of Public Security (MPS) and the Standardization Administration of China (SAC). The MPS for example issued in 2019 some Guidelines aimed specifically at the protection of Internet personal information security, with the SAC further addressing more specific provisions in its Guidelines on topics such as de-identification of personal information, cybersecurity practices for mobile applications and guidelines for notice and consent in 2020.

An important nonmandatory document that has further provided additional protection for processing sensitive personal information is the *Information security technology— Personal information (PI) security specification* (信息安全技术 个人信息安全规范， *Xìnxī ānquán jìshù gèrén xìnxī ānquán guīfàn*), first issued in 2018 by the State Administration for Market Supervision and SAC and revised in 2020. The 2020 version defines sensitive personal data as including location records and health records and demands additional security measures such as encryption during transmission and storage of such data.[172]

[172] "Regulating electronic means to fight the spread of COVID-19: Argentina, Australia, Brazil, China, England, European Union, France, Iceland, India, Iran, Israel, Italy, Japan, Mexico, Norway, Portugal, Russian Federation, South Africa, South Korea, Spain, Taiwan, Turkey, United Arab Emirates." *The Law Library of Congress, Global Research Directorate*, https://www.loc.gov/item/2020714995/, accessed 10-02-2021.

1.4. Towards a more Comprehensive Regulation

In the past decades, China's personal information protection has been established through a series of laws and regulations that generally cover the private sector and partly the public one, though it wasn't formally established as a full-fledged right separate from the right to privacy but treated more as a subset interest, similarly to what happens in the US privacy model.[173]

However, China has been shifting its view on privacy and data privacy protection in these last years, by moving closer to what Chinese scholars call a "dual model" (二元制, *Èr yuán zhì*) which establishes privacy and personal information as two separate civil rights.[174] The *General Provisions of the Civil Law of the People's Republic of China* issued in 2017 already provided such formal distinction by establishing the right to privacy of natural persons in Article 110 and a separate civil interest of personal information protection in Article 111. The General Provisions however did not specify the scope and boundaries of the two rights, nor they established different legal regimes for their protection, thus creating ambiguity and confusion in judicial practice. It is the New Chinese Civil Code, effective from January 1st, 2021, that further expanded and clarified the two concepts by laying the foundation of two different legal regimes in its Chapter VI, namely the *Right to Privacy and Personal Information Protection* Chapter (隐私权和个人信息保护, *Yǐnsī quán hé gèrén xìnxī bǎohù*) contained in the Book of Personality Rights.[175]

Other than the recognition of a formal distinction between the right to privacy and personal information protection, there have been legislative efforts to improve data protection by issuing two new comprehensive laws, firstly announced in September 2018 when the NPC updated its five-year legislative plan: the *Personal Information Protection Law* (中华人民共和国个人信息保护法, *Zhōnghuá rénmín gònghéguó gèrén xìnxī bǎohù fǎ*), effective from November 1st,

[173] US privacy laws consider personal information protection as part of the right to privacy, and data privacy provisions can be found in different sectorial laws. CUI Shujie, QI Peng, 2021, "The legal construction of personal information protection and privacy under the Chinese Civil Code", *Computer Law & Security Review*, Vol. 41, Art. 105560, pp. 3-4.

[174] LI Yongjun 李永军, 2017, "*Lùn "mínfǎ zǒngzé" zhōng gèrén yǐnsī yǔ xìnxī de "èr yuán zhì" bǎohù jí qǐngqiú quán jīchǔ*", 论《民法总则》中个人隐私与信息的 "二元制" 保护及请求权基础 (The Research on the "Dual System" Protection and Claim Basis of the Personal Privacy and Information in The General Principles of Civil Law), 浙 江 工 商 大 学 学 报 *Journal of Zhejiang Gongshang University*, Vol. 31 (3), pp. 11-12.

[175] "中华人民共和国民法典", *Zhōnghuá rénmín gònghéguó mínfǎ diǎn*, https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E6%B0%91%E6%B3%95%E5%85%B8, accessed 30-12-2021. English Translation: "Civil Code of the People's Republic of China", https://npcobserver.com/wp-content/uploads/2020/11/Civil-Code_Eng_July-2021-version.pdf, accessed 31-12-2021.

2021, and the *Data Security Law* (中华人民共和国数据安全法, *Zhōnghuá rénmín gònghéguó shùjù ānquán fǎ*), effective from September 1st, 2021.

1.4.1. The New Chinese Civil Code 2020

The New Chinese Civil Code has been officially adopted by the NPC on May 28, 2020. Despite its structure being fairly similar to the German Civil Code (*Bürgerliches Gesetzbuch,* BGB), the Chinese Civil Code of 2020 presents features that are unique among legal systems, one of the most controversial one has been the introduction of a separate Book entirely dedicated to Personality Rights (人格权, *Réngé quán*).[176] The introduction of this Book generated many debates, as many legal scholars argued that personality right provisions should be included in other parts of the Code, mostly in the Part on Tort Liability. However Chinese legislators stressed the importance of having a separate part of the Code that could effectively implement the constitutional protection for "personal dignity."[177] This has not been the first time that personality rights, and in particular the concept of personal information protection as such have come under academic scrutiny. The first draft of the *General Provisions of the Civil Law of the People's Republic of China* issued in 2017 did not contain any rules for personal information protection, but after two notable cases sparked outcry among the public, the legislature opted to introduce personal information provisions that ultimately became Article 111.[178]

Chapter VI of the Book IV of Personality Rights regulates two different and separate civil rights: the right to privacy, understood in Article 1032 as "the undisturbed private life of a natural person and his private space, private activities, and private information that he does not want to be known to others", and the right to protection of personal information, defined in Article 1034:

> "Personal information is the information recorded electronically or in other ways that can be used, by itself or in combination with other information, to identify a natural person,

[176] TIMOTEO Marina, 2019, "China Codifies. The First Book of the Civil Code between Western Models to Chinese Characteristics", *Opinio Juris in Comparatione*, Vol.1, Issue 1, pp. 54-55; 66.
[177] WEI Changhao, "2020 NPC Session: A Guide to China's Civil Code (Updated)", https://npcobserver.com/2020/05/21/2020-npc-session-a-guide-to-chinas-civil-code/, *NPC Observer*, accessed 31-12-2021.
[178] The two cases both involved telephone scams. In the first case, 18-year-old student Yuyu Xu died of cardiac arrest after having her tuition funds swindled in a telephone scam that stole her personal information. Similarly, the second case involved a Professor of Tsinghua University that was scammed out of 18 million Yuan. CUI Shujie, QI Peng, 2021, "The legal construction of personal information protection and privacy under the Chinese Civil Code", *Computer Law & Security Review*, Vol. 41, Art. 105560, p. 8.

including his name, date of birth, identification number, biometric information, residential address, telephone number, email address, health information, whereabouts, and the like."[179]

The definition is fairly identical to the one provided in the PRC Cybersecurity Law, however the Chinese Civil Code distinguishes two kinds of personal information, by providing in Article 1034(3) that "private personal information" (私密信息, *Sīmì xìnxī*), which remains undefined, shall be regulated by provisions on the right to privacy. Thus, two different legal regimes will be applied: one for privacy and private personal information, and one for general personal information protection. The Chinese Civil Code therefore recognized that there exists some overlap between the right to privacy and the right to personal information protection, and that certain types of personal information could bring civil damage not only if processed unfairly, but also if disclosed to the public.

The Civil Code explicitly establishes privacy as a personality right, and further lays out a series of activities that result in breach of such right (Article 1033), including intruding upon another person's private life, private spaces, private activities, a person's body and through processing a person's private information, unless provided by law or previous obtainment of consent by the holder.[180]

The remainder of the Chapter deals with the protection of personal information, which is protected by law but still not explicitly established as a personality right. The PRC Civil Code introduces the concept of "personal information processing" (个人信息的处理, *Gèrén xìnxī de chǔlǐ*), defined as collection, storage, use, process, transmission, provision, disclosure, and the like of the personal information (Article 1035).[181] A personal information processor, although not explicitly defined in the Chinese Civil Code, is assumed then to both encompass the concept of a personal data controller and processor as defined under the GDPR.[182]

---

[179] "中华人民共和国民法典", *Zhōnghuá rénmín gònghéguó mínfǎ diǎn,* https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E6%B0%91%E6%B3%95%E5%85%B8, accessed 30-12-2021. English Translation: "Civil Code of the People's Republic of China", https://npcobserver.com/wp-content/uploads/2020/11/Civil-Code_Eng_July-2021-version.pdf, accessed 31-12-2021.

[180] *Ibidem*.

[181] *Ibidem.*

[182] The *General Data Protection Regulation* is the latest advancement in the realm of personal information protection in the European Union and considered to be one of the most comprehensive and strictest international legal documents on the issue. The GDPR lays out different definitions and obligations for data controllers, which determine both purpose and means of processing of personal information, and data processors, which only processes data on behalf of the controller.
LAU Nanda, GUO Gavin, GONG James, "China Cybersecurity and Data Protection: China's Civil Code lays foundation for data protection", *China Investments E-Bulletin - Herbert Smith Freehills*, https://www.lexology.com/library/detail.aspx?g=89f22cb9-ff6c-41c1-9c55-3f94c6ef5faa, accessed 16-10-2021.

Articles 1035 and 1038 state the obligations of personal information processors, which are consistent with many of the obligations already included in other PRC data privacy laws. Other than obtaining consent before processing personal information, processors shall clearly state processing rules and purpose, method, and scope of the information processing, which shall not violate any law or administrative regulation. It is also prohibited to provide such information to others unless the processed information cannot be used to identify any individual. Processors shall take both technical and remedial measures to ensure data security.[183]

It is interesting to note that, although Article 1039 also provides obligations for State organs and chartered institutions and their staff (that is, to keep confidential the privacy and the personal information of natural persons during the performance of their responsibilities and not disclose or illegally provide such information to others), it does not extend private parties obligations to the public sector.

A further advancement in the realm of personal information protection laid out in the new PRC Civil Code is the explicit introduction of individuals rights to personal information, which include rights to be informed, of access, copy, correction, objection and deletion of their personal information (Articles 1035-1037).[184]

Civil liability provisions are listed in Article 1036, which provides cases where a processor does not bear it, that is when he acts within the scope of consent given, processes information that has been made publicly available unless expressly forbidden by the individual, and when the processor acts in name of protection of public interest or legal interest of the individual.[185]

To reinforce the legal protection afforded to personal information, the Supreme People's Court issued a Notice, also effective from January 1, 2021, where both a "privacy protection dispute" and a "personal information protection dispute" have been added as a cause of action of civil cases.[186] Thanks to the Notice, it is now possible to bring civil claims to court on the basis of infringement of a natural person's personal information protection.

---

[183] "中华人民共和国民法典", *Zhōnghuá rénmín gònghéguó mínfǎ diǎn,* https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E6%B0%91%E6%B3%95%E5%85%B8, accessed 30-12-2021. English Translation: "Civil Code of the People's Republic of China", https://npcobserver.com/wp-content/uploads/2020/11/Civil-Code_Eng_July-2021-version.pdf, accessed 31-12-2021.

[184] *Ibidem*.

[185] LAU Nanda, GUO Gavin, GONG James, "China Cybersecurity and Data Protection: China's Civil Code lays foundation for data protection", *China Investments E-Bulletin - Herbert Smith Freehills*, https://www.lexology.com/library/detail.aspx?g=89f22cb9-ff6c-41c1-9c55-3f94c6ef5faa, accessed 16-10-2021.

[186] "最高人民法院印发《关于修改＜民事案件案由规定＞的决定》的通知 (2020)", *Zuìgāo rénmín fǎyuàn yìnfā "guānyú xiūgǎi <mínshì ànjiàn ànyóu guīdìng >de juédìng" de tōngzhī (2020),*

Although the new Civil Code of the PRC has the merit of introducing a more comprehensive protection of personal information distinct from the right to privacy in the realm of civil law, some questions are left to be answered, such as the remedies available to individuals in case their legitimate rights regarding personal information are denied, or the scope of private personal information that is to be protected by laws on the right to privacy.[187] In addition, the New Civil Code of the PRC does not take the further step of labelling certain types of personal information as "sensitive".

1.4.2. PRC Personal Information Protection Law

In addition to the formal separation of privacy from personal information protection enshrined in the New PRC Civil Code, the Chinese leadership seems to be moving away from its previous approach of regulating personal information protection with sectorial laws and departmental regulations, and finally proceed towards a more comprehensive approach to personal information protection with the promulgation of the *Personal Information Protection Law* (中华人民共和国个人信息保护法, *Zhōnghuá rénmín gònghéguó gèrén xìnxī bǎohù fǎ*, PIPL).

Attempts at regulating the realm of personal information protection in a comprehensive manner had already been made in 2007, when a draft of the *Personal Information Protection Act*, drafted by the Institute of Law at the Chinese Academy of Social Sciences was taken under consideration, covering both the private and public sector, even though it never reached the law-making process.[188] This early draft bears some similarities with the newly enacted PIPL, as they both cover an advanced set of data privacy principles (apparently influenced by international principles), while still not establishing an independent DPA but allowing a set of ministries enforcement powers.[189]

The Personal Information Protection Law not only recollects relevant provisions from other specific Chinese data privacy laws and regulations (such as the PRC Cybersecurity Law, E-commerce Law, Consumer Rights Law, the MIIT Regulations etc.), and non-mandatory privacy

http://lawinfochina.com/display.aspx?id=34794&lib=law, accessed 02-01-2022. English Translation: "Notice by the Supreme People's Court of Issuing the Decision to Amend the Provisions on the Causes of Action of Civil Cases (2020)", http://lawinfochina.com/display.aspx?id=34794&lib=law, accessed 01-01-2022.

[187] LAU Nanda, GUO Gavin, GONG James, "China Cybersecurity and Data Protection: China's Civil Code lays foundation for data protection", *China Investments E-Bulletin - Herbert Smith Freehills*, https://www.lexology.com/library/detail.aspx?g=89f22cb9-ff6c-41c1-9c55-3f94c6ef5faa, accessed 16-10-2021.

[188] GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, p. 208.

[189] *Ibidem*.

standards (such as the MIIT Guidelines and the PI Security Specification), but also introduces advanced data privacy protection rules such as a set of personal information protection principles, clear data privacy user's rights, new legal bases for personal information processing and specific rules for automated decision-making, image collection or personal identity recognition in public places, additional obligations for sensitive personal information, and stringent cross-border data transfer requirements.[190]

The PIPL has a broader scope than the past fragmented data privacy laws of China, as Article 3 clearly states that it is applicable to activities of processing personal information of natural persons within the PRC, but also applies to the handling of personal information outside PRC's border whenever the processing purpose is to provide products or services to natural persons inside the borders, or when analysing or assessing activities of natural persons inside the borders or again when other circumstances provided in laws or administrative regulations are present.[191] Thus, the Law presents an extra-territorial effect that is much similar to the one featured in the EU GDPR.[192]

A new definition of personal information that rejects the previous list-based outline used in previous laws and regulations, and also the newly enacted Civil Code of the PRC, is devised in Article 4 of the PIPL:

> "Personal information is all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including information after anonymization handling."[193]

---

[190] XU Hui, DONOVAN Kieran, LEE Bianca, "China Introduces First Comprehensive Legislation on Personal Information Protection", https://www.lw.com/thoughtLeadership/china-introduces-first-comprehensive-legislation-on-personal-information-protection#:~:text=On%20August%2020%2C%202021%2C%20the,effect%20on%20November%201%2C%202021., *Latham & Watkins Data Privacy & Security Practice*, accessed 02-01-2022.

[191] "中华人民共和国个人信息保护法", *Zhōnghuá rénmín gònghéguó gèrén xìnxī bǎohù fǎ*, https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A4%E6%B3%95, accessed 04-01-2022. English Translation: "Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021", https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/, accessed 04-01-2022.

[192] ROBINSON Mark, LAU Nanda, GONG James, "China cybersecurity and data protection: Review of 2020 and outlook for 2021", *Herbert Smith Freehills*, https://sites-herbertsmithfreehills.vuturevx.com/95/24431/compose-email/china-cybersecurity-and-data-protection--review-of-2020-and-outlook-for-2021.asp?sid=3e6b986b-17d9-4d66-a1ff-bb17e5da30f7, accessed 15-02-2021.

[193] "中华人民共和国个人信息保护法", *Zhōnghuá rénmín gònghéguó gèrén xìnxī bǎohù fǎ*, https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A4%E6%B3%95, accessed 04-01-2022. English Translation: "Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021", https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/, accessed 04-01-

This more general characterization of personal information is likely aimed at responding better to the ever-changing technological environment, so that the Law doesn't have to be updated frequently. Article 4 specifies for the first time that anonymized data is exempt from being considered personal information. The same Article also defines "personal information processing" in the same way as Article 1035 of the new PRC Civil Code, with the addition of "deletion of personal information" (个人信息的.....删除, *Gèrén xìnxī de…shānchú*).[194] The PIPL falls short on further distinguishing non-private personal information from the concept of private personal information devised in the New Chinese Civil Code, never mentioning the term in its entire transcript, not providing any additional provision to better comprehend when personal information have to be regulated under the right to privacy protection or under the personal information protection regime. It does however define the concept of "sensitive personal information" in Article 28, which is generally consistent with the definition of the PI Security Specification:

> "Sensitive personal information means personal information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons grave harm to personal or property security, 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."[195]

Additional obligations must be met when processing sensitive personal information, that can be processed only if there is a specific purpose, and separate consent from individual is obtained.

Another difference between the PRC Civil Code and the PIPL seems its characterization of the term "personal information processor": while in the Civil Code the term seems to encompass both the concept of a "data controller" and a "data processor" as devised in the EU GDPR, Article 73 of the PIPL defines the same term as "organizations and individuals that, in personal information handling activities, autonomously decide handling purposes and handling methods", which is almost identical to the definition of "data controller" envisioned in Article 4(7) of EU GDPR.[196] At the same time, distinguished from personal information processors, Article 59 of PIPL stipulates that "entrusted persons accepting entrusted handling of personal information" (接受委托处理个人信息的受托人, *Jiēshòu wěituō chǔlǐ gèrén xìnxī de shòutuō*

2022.
[194] *Ibidem*.
[195] *Ibidem*.
[196] "Regulation (EU) 2016/679 of the European Parliament and of the Council*", Official Journal of the European Union*, https://eur-lex.europa.eu/eli/reg/2016/679/oj, accessed 04-01-2022.

rén) shall take necessary measures to safeguard the security of the personal information and assist personal information processors.[197] The term used in Article 59 is akin to the concept of "data processor" as devised by the EU GDPR.[198] This is the first law of the PRC ever providing a formal distinction between who controls data and who merely processes it.

The new Personal Information Protection Law establishes for the first time a system of multiple legal bases for processing personal information, specifically listed in Article 13. Apart from the already existing consent-based criteria, processing of personal information can be carried out when necessary for concluding or fulfilling a contract, for fulfilling statutory duties, to respond to sudden public health incidents or protect natural persons' lives and health, to implement activities for the public interest such as news reporting, to process personal information disclosed by persons themselves and for any other circumstance provided in laws and administrative regulations.[199] Articles 14 and 15 establish unprecedented provisions on the procedure to obtain consent, which has to be given by individuals under the precondition of full knowledge, and in a voluntary and explicit statement. The concept of separate (or written) consent is introduced whenever laws or administrative regulations provide it, and when processing sensitive personal information (Article 29). Individuals have the right to rescind such consent and processors have to provide a convenient way to withdraw it.

Personal information protection principles are provided in Articles 5-9. Many of these principles were already listed in other PRC data privacy laws, such as the principles of legality, propriety, necessity, and sincerity, however PIPL is the first law of the PRC to clearly elaborates on these principles, for example in Article 6 the principle of necessity establishes that:

---

[197] "中华人民共和国个人信息保护法", *Zhōnghuá rénmín gònghéguó gèrén xìnxī bǎohù fǎ*, https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A4%E6%B3%95, accessed 04-01-2022. English Translation: "Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021", https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/, accessed 04-01-2022.

[198] XU Hui, DONOVAN Kieran, LEE Bianca, "China Introduces First Comprehensive Legislation on Personal Information Protection", https://www.lw.com/thoughtLeadership/china-introduces-first-comprehensive-legislation-on-personal-information-protection#:~:text=On%20August%2020%2C%202021%2C%20the,effect%20on%20November%201%2C%202021., *Latham & Watkins Data Privacy & Security Practice*, accessed 02-01-2022.

[199] "中华人民共和国个人信息保护法", *Zhōnghuá rénmín gònghéguó gèrén xìnxī bǎohù fǎ*, https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A4%E6%B3%95, accessed 04-01-2022. English Translation: "Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021", https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/, accessed 04-01-2022.

> "Personal information handling shall have a clear and reasonable purpose, and shall be directly related to the handling purpose, using a method with the smallest influence on individual rights and interests.
>
> The collection of personal information shall be limited to the smallest scope for realizing the handling purpose, and excessive personal information collection is prohibited."[200]

Other personal information protection principles include principles of openness and transparency, data quality, and responsible processing of personal information.

Individual rights related to personal information are clearly stated in Articles 44-48 of the PIPL. All of them are already enshrined in the New Civil Code of the PRC, with the exception of the new right of "data portability" enshrined in Article 45. There has been controversy over the introduction of such right, as a matter of fact both the first and second draft of PIPL didn't mention it, but in the end, it was introduced in the final version of the Law.[201] The right of data portability enables individuals to request that their personal information be transferred to a personal information handler they designate, as long as conditions of the Cyberspace Administration of China are met.

Articles 51-56 stipulate the obligations of personal information processors, which include staffing and organization obligations, internal administrative measures and security measures. Similar to the PRC Cybersecurity Law (which defines additional obligations for Critical Information Infrastructures, or CII), the PIPL provides additional obligations to "Personal information processors providing important Internet platform services, that have a large number of users, and whose business models are complex" (Article 58)[202], even though the thresholds to ascertain if a business has to be included in this categorization have still to be laid out by future regulations.

---

[200] "中华人民共和国个人信息保护法", *Zhōnghuá rénmín gònghéguó gèrén xìnxī bǎohù fǎ*, https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A4%E6%B3%95, accessed 04-01-2022. English Translation: "Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021", https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/, accessed 04-01-2022.

[201] ZHANG Lu, 2021, "Personal information of privacy nature under Chinese Civil Code", *Computer Law & Security Review*, Vol. 43, p. 5.

[202] "中华人民共和国个人信息保护法", *Zhōnghuá rénmín gònghéguó gèrén xìnxī bǎohù fǎ*, https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A4%E6%B3%95, accessed 04-01-2022. English Translation: "Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021", https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/, accessed 04-01-2022.

One of the most controversial parts of the PIPL is the cross-border data transfer requirements laid out in Chapter III. Such requirements were previously regulated by the PRC Cybersecurity Law but only for CII operators (CIIOs), the PIPL however sets general requirements for all personal information processors, while adding additional obligations to CIIOs and to processors who reach the processing quantity thresholds prescribed by relevant authorities.[203] It is notable the absence of "derogatory provisions" under the PIPL, such as the possibility to transfer personal information data outside China by obtaining the consent of the individual or when it is necessary of performance of a contract, which are usually present in other data protection legislation of other countries.[204] To transfer personal information outside Chinese borders, at least one of the following conditions shall be met: to pass a security assessment organized by the State cybersecurity, undergoing personal information protection certification, concluding a contract with the foreign side consistent with standards laid out by the State cyberspace and informatization department (Article 38).[205]

In comparison with previous PRC data privacy laws, the PIPL sets out stricter penalties for unlawful processing of personal information in violation of the aforementioned law, by increasing the maximum penalty of a personal information processor to CNY50 million, or 5% of its annual revenue of the last year under grave circumstances (Article 66).[206]

1.4.3. PRC Data Security Law

Two months before the promulgation of PIPL (June 2021), another important comprehensive law regarding data privacy has been issued by the SCN-NPC: the PRC Data Security Law (中华人民共和国数据安全法, *Zhōnghuá rénmín gònghéguó shùjù ānquán fǎ*, DSL).

---

[203] XU Hui, DONOVAN Kieran, LEE Bianca, "China Introduces First Comprehensive Legislation on Personal Information Protection", https://www.lw.com/thoughtLeadership/china-introduces-first-comprehensive-legislation-on-personal-information-protection#:~:text=On%20August%2020%2C%202021%2C%20the,effect%20on%20November%201%2C%202021., *Latham & Watkins Data Privacy & Security Practice*, accessed 02-01-2022.

[204] XIAO Tangfei 肖腾飞, SHEN Yanru 申燕茹, "*Gèrén xìnxī bǎohù fǎ zhìdù liàngdiǎn jiěxī"* 《个人信息保护法》制度亮点解析, *Deloitte*, https://www2.deloitte.com/cn/zh/pages/risk/articles/personal-information-protection-law-analysis.html, accessed 05-01-2022.

[205] "中华人民共和国个人信息保护法", *Zhōnghuá rénmín gònghéguó gèrén xìnxī bǎohù fǎ*, https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A4%E6%B3%95, accessed 04-01-2022. English Translation: "Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021", https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/, accessed 04-01-2022.

[206] *Ibidem*.

While the main focus of the Personal Information Protection Law is to regulate the fair processing of personal information, the Data Security Law main aim is to ensure the security of data during its processing, both in mainland and outside China (Article 2). Similar to PIPL, this law has thus an extra-territorial effect, in particular it is also applied to data processing activities outside China when such activities "harm the national security, the public interest, or the lawful rights and interests of citizens or organizations of the PRC".[207]

The definition of "data" and "data processing" elaborated in Article 3 of DSL is identical to the definition of "personal information" and "personal information processing" devised in the PIPL, with the exception that the PIPL excludes anonymized data from the realm of personal information, while the definition of "data" in the DSL refers to any information record in electronic or other form, whether it is anonymized or not. The Law also elaborates a definition of "data security":

> "Data security" refers to ensuring data is in a state of effective protection and lawful use through adopting necessary measures, and to possessing the capacity to ensure a persistent state of security.[208]

Articles 53 and 54 however specify how data processing activities regarding State Secrets are to be regulated by the Law of the PRC on the Protection of State Secrets and military data processing activities are to be formulated separately by the Central Military Commission, thus the DSL will not apply to these two types of data processing activities.[209]

While the DSL only applies to aforementioned activities, at the same time, the Cybersecurity Law of the PRC still regulates limited network activities occurring outside of the PRC that attack, infringe, interfere with, or damage critical information infrastructure in the PRC and lead to severe consequences. Moreover, the Cybersecurity Law still applies to CIIOs, for example for cross-border transfer of "important data" and when conducting national security reviews of network products and services.[210] The concept of "important data" is defined nor in the Cybersecurity Law nor the Data Security Law, the 2017 *Guidelines for Cross-Border Data*

---

[207] "中华人民共和国数据安全法", *Zhōnghuá rénmín gònghéguó shùjù ānquán fǎ*, https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E6%95%B0%E6%8D%AE%E5%AE%89%E5%85%A8%E6%B3%95, accessed 06-01-2022. English Translation: "Data Security Law of the People's Republic of China", https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/, accessed 06-01-2022.

[208] *Ibidem*.

[209] *Ibidem*.

[210] XU Hui, DONOVAN Kieran, "China's New Data Security Law: What to Know", https://www.lw.com/thoughtLeadership/china-new-data-security-law-what-to-know, *Latham & Watkins Data Privacy & Security Practice*, accessed 06-01-2022.

Transfer Security Assessments specifies how the term refers to data collected or derived in the PRC that closely relates to national security, economic development, and public interests. Moreover, Appendix A of the Guidelines provide a list of "important data" in various industries.[211]

The DLS main aim is to establish a data security framework, comprising of a set of systems and measures that apply in different situations, such as a data security risk management system, an emergency response system for data security incidents, a data security review system, a data export control system and a counter-measure system against discriminatory international measures.[212]

Articles 27-36 of the DSL devise the obligations for entities and individuals carrying out data activities. General obligations include the need of establishing a data security management system for the entire workflow, organizing and conducting data security education and training, adopting corresponding technical measures to ensure data security (Article 27), strengthening risk monitoring (Article 29), conduct risk assessments of important data (Article 30), obtaining administrative permits for the provision of services related to data processing (Article 34).[213] It is notable that Article 36 establishes that "domestic organizations and individuals must not provide data stored within the mainland territory of the PRC to the justice or law enforcement institutions of foreign countries without the approval of the competent authorities of the PRC"[214], which is also consistent with Article 41 devised in the PIPL.

The DSL also regulates the processing of data necessary to safeguard national security or investigate crimes by public security authorities and national security authorities, who shall undergo strict approval procedures according to relevant State provisions (Article 35).

[211] *Ibidem*.
[212] *Ibidem*.
[213] "中华人民共和国数据安全法"，*Zhōnghuá rénmín gònghéguó shùjù ānquán fǎ*, https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E6%95%B0%E6%8D%AE%E5%AE%89%E5%85%A8%E6%B3%95, accessed 06-01-2022. English Translation: "Data Security Law of the People's Republic of China", https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/, accessed 06-01-2022.
[214] *Ibidem*.

CHAPTER 2

Data Privacy Protection in the Private Sector and the Interplay with the Chinese Government

2.1. Data Privacy Obligations informing the Private Sector

The previous Chapter shows how data privacy legislation in China has been progressing from a fragmented and cumulative framework towards a more comprehensive legal regime that is separate from the protection of the right to privacy. One of the most significant differences of the Chinese data protection regime in comparison with data privacy laws in the US and the European GDPR is that the rules for personal information processing in China are mainly formulated for the private sector while public actors are not extended the same obligations or requirements. Above all the legislative instruments described above, some do contain some general provisions for the public sector, but it is usually only a general requirement of maintaining confidentiality and not leaking or selling personal or electronic information during fulfilment of their duties.[215] Moreover, the Cybersecurity Law of the PRC and the non-binding PI Security Specification apply only in part to the processing of personal information by public actors.[216] However, it is only the newly enacted Personal Information Protection Law (PIPL) that covers for the first time the processing of personal information by both public and private sectors.

Before the enactment of the PIPL, data privacy obligations were scattered among different laws, regulations, and non-binding legal instruments, that were often sectorial in nature, meaning they covered only certain industries, forming nonetheless a "cumulative" effect that broadly covered all the private sector. Since the PIPL was only passed more than a year after the outbreak of the Covid-19 pandemic, it is relevant to our paper to investigate the data privacy principles and obligations of the private sector in China emerging from the dispersive and complicated framework established during the previous decades.

Data privacy obligations are usually derived from a set of principles that establish the fundamental legal basis under which subjects of data privacy laws have to carry out collection and processing of personal information. Most of the international data privacy instruments and

[215] Such as Article 10 of SC-NPC Decision of 2012, or Article 1039 of the New Chinese Civil Code.
[216] GELLER Anja, 2020, "How Comprehensive is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective", *GRUR International*, Vol. 69, Issue 12, p. 1193.

major data privacy laws worldwide clearly establish such set of principles.[217] Nevertheless, Chinese data privacy laws and regulations fail to explicitly mention a clear set of principles that can be compared to the one issued in the European Union, as the only legal documents directly providing a list of principles are the 2013 MIIT Guidelines and the PI Security Specification (2020 revision), which are both not legally binding documents.[218] However, some principles for the fair collection and processing of personal information can be inferred by several provisions dispersed among the different data privacy laws mentioned in Chapter 1.

2.1.1. Collection and Processing Principles

All SC-NPC laws related to the collection and processing of personal information that have been issued in the last decade only generally state briefly fair processing principles of "legality, legitimacy and necessity", which are not further defined in the laws.[219] In addition, the MIIT Regulations of 2011 provide that principles of "equality, free will, fairness and good faith" to be followed by Internet Information Service Providers during provision of services.[220] It is only the newly enacted Personal Information Protection Law that lists but also describes an advanced set of principles in Articles 5-9 that cover almost all data privacy principles devised by the European model, as it is partly modelled after the GDPR.[221]

---

[217] The eight principles established in the 1980 OECD Guidelines and the1981 CoE Convention are considered the most basic set of principles that a data privacy law should abide by, and they comprise of a Collection limitation principle, a Data quality principle, a Purpose specification principle, a Use limitation principle, a Security safeguards principle, an Openness principle, an Individual participation principle and an Accountability principle. A more advanced set of data privacy principles are also known as "European principles" as they are mainly enshrined in the 1995 EU Directive and the 2001 CoE Convention. They comprise of: Fair and lawful processing, Minimal collection, Data export restrictions, Prior checking, Deletion, Sensitive data protections, Automated processing controls and Direct marketing opt-out. In addition, a "third-generation" set of data protection principles is arising from the new European GDPR, which include provisions on automated profiling, data portability, right to copy and be forgotten, and new concepts like "implementation by design" and "implementation by default".
GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, pp. 54-57; 546-547.

[218] GELLER Anja, 2020, "How Comprehensive is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective", *GRUR International*, Vol. 69, Issue 12, p. 1194.

[219] Article 2 of 2012 Decision; Article 29 of Consumer Protection Law, Article 5 of Cybersecurity Law.

[220] 2011 MIIT Regulations, Article 4. GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, p. 210.

[221] The processing principles of PIPL comprises of principles of legality, propriety, necessity, and sincerity, with the further prohibition of handling information in a misleading, swindling, coercive, or other such ways (Article 5), purpose notification, limitation and minimal collection principles (Article 6), openness and transparency principle (Article 7), data quality principle (Article 8) and accountability of the data processor - which is akin to the definition of a data controller in GDPR – (Article 9).
"中华人民共和国个人信息保护法", *Zhōnghuá rénmín gònghéguó gèrén xìnxī bǎohù fǎ*, https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A

Although not explicitly listing a set of principles, SC-NPC data privacy laws and MIIT regulations do still afford a general data protection framework by providing a set of obligations that the private sector must carry out during collection and processing of personal information:

Limited Collection: following the principle of "necessity" stated in each SC-NPC data privacy law and MIIT Regulation, collection of personal information shall be carried out by clearly stating purpose, methods and scope, and by previous obtaining consent from individuals, which has been the only legal basis for the processing and collection of personal information in the PRC until the enactment of the PIPL.[222] This new Law has envisioned a total of other six legal bases by which data processors can collect data without previous obtaining consent from individuals: for example, whenever collection is necessary to conclude or fulfil a contract, or to conduct human resources management, to fulfil statutory duties and responsibilities or statutory obligations, or respond to sudden public health incidents or protect natural persons' lives and health. Even if consent is considered to be a stronger legal basis, the dispersive legal framework that was in place before the PIPL was still weakened by the fact that no PRC legislation specified which actions be taken to demonstrate that consent was given in a lawful and transparent way.[223] Article 14 of the PIPL clearly specifies that consent has to be obtained from individuals under the precondition of full knowledge, and in a voluntary and explicit statement. Separate or written consent shall be given under certain circumstances, for example when collecting and processing sensitive personal information.

Minimal Collection: limiting collection to the smallest scope for realizing its processing purpose was not clearly established in the 2012 Decision, as the only limitation to collection and processing was not to violate provisions of the law or the agreement between the parties (Article 2). However, both the 2011 MIIT Regulations (Article 11) and 2013 Guidelines set out a stringent requirement for data minimization, prohibiting the collection be limited to data "required" for the provision of services. Moreover, the Guidelines explicitly establish the principle of "minimum and sufficiency".[224] The Cybersecurity Law devised however a more morbid approach to data minimization as collection was limited to personal information "related

4%E6%B3%95, accessed 04-01-2022. English Translation: "Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021", https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/, accessed 04-01-2022.

[222] Article 2 of 2012 Decision, Article 29 of Consumer Protection Law, Article 9 of 2013 MIIT Regulations, Article 41 of Cybersecurity Law. GELLER Anja, 2020, "How Comprehensive is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective", *GRUR International*, Vol. 69, Issue 12, p. 1194.

[223] GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, p. 211.

[224] *Ibidem*.

to" (and not required for) the service provided (Article 41), creating ambiguity to when the stricter standard from the MIIT regulations applies. The enactment of the PIPL clarified the issue, as it is the first SC-NPC law clearly establishing that "collection shall be limited to the smallest scope for realizing the processing purpose" (Article 6).[225]

Purpose Notification: All SC-NPC Data Privacy Laws, MIIT Regulations and Guidelines, and also the New Chinese Civil Code clearly indicate that purpose has to be specified before collection and during processing of personal data. Moreover, rules for the collection and processing shall be disclosed to the public, which can be interpreted as a general obligation to publish a privacy policy.[226]

Use and Disclosure Limitation: the 2012 Decision expressly provides that processors shall maintain confidentiality and not leak, tamper, destroy or provide illegally personal information (Article 3), however data processing was again not limited to purpose but rather to agreement between the parties and provisions of law (Article 2). Both the Decision 2012 and the MIIT Regulations in addition did not specify limitations for third parties' data or data generated indirectly by transactions. The Cybersecurity Law adds an exception where information can be provided if after processing there is no way to identify a specific individual and it's not possible to recover such identifiability (Article 42). The same requirement has been reiterated by Article 1038 of the New Civil Code, with the addition in Article 1035 that personal information cannot be "excessively processed". Article 6 of PIPL establishes that information processing shall be directly related to the processing purpose, and processing has to be carried out in a way that has the least impact on personal rights and interests.

Openness and Transparency: this principle has not been clearly stated in any SC-NPC Data privacy law, in MIIT Regulations or in the 2013 MIIT Guidelines. However, a general requirement of publicly disclosing rules of processing is present in each of these legal instruments. The Cybersecurity Law provides that data processors have to establish a complaint and reporting system, and such complaints from users have to be handled in a timely manner (Article 49). The PRC E-Commerce Law obliges e-commerce operators to publicize manner and procedure for search, correction, deletion and deregistration that have to be set up without

[225] "中华人民共和国个人信息保护法", *Zhōnghuá rénmín gònghéguó gèrén xìnxī bǎohù fǎ*, https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A4%E6%B3%95, accessed 04-01-2022. English Translation: "Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021", https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/, accessed 04-01-2022.

[226] Article 2 of 2012 Decision; Article 29 of Consumer Protection Law, Article 41 of Cybersecurity Law,

posing unreasonable requirements (Article 24). The 2013 MIIT Regulation and the PI Security Specification of 2020 also require data processors to publish valid contact information and respond to complaints within 15 (MIIT Regulation) or 30 days (PI Specification).[227] The PIPL is currently the only SC-NPC law that clearly states the principle of openness and transparency in its Article 7.

Data Retention: No mention on neither a general obligation of notifying users of data retention periods nor actual data retention periods can be found in the Decision 2012, where there is only a general requirement of not destroying personal information collected. However, specific data retention periods were already provided in the Regulation on Internet Information Service of the People's Republic of China (互联网信息服务管理办法, *Hùliánwǎng xìnxī fúwù guǎnlǐ bànfǎ*) issued in 2000, whose Article 14 requires Internet service providers to keep records of each user's time spent online, user account, IP address or domain name, phone number, etc., for 60 days, and provide it authorities when required.[228] The Cybersecurity Law strengthened this requirement by requiring network logs be kept for at least six months, in accordance with other data retention provisions (Article 21).[229] This provision sparked controversy as it doesn't only generate considerable costs for network operators, but also users' personal information will be exposed to a higher risk of leakage.[230] On another hand, data retention related to processing has been explicitly limited in the new PIPL, where Article 19 states:

"Except where laws or administrative regulations provide otherwise, personal information retention periods shall be the shortest period necessary to realize the purpose of the personal information processing."[231]

Moreover, data retention has to be explicitly notified to individuals "truthfully, accurately, and fully" per Article 17.

[227] GELLER Anja, 2020, "How Comprehensive is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective", *GRUR International*, Vol. 69, Issue 12, p. 1196.
[228] ZHANG Laney, 2013, "China: NPC Decision on Network Information Protection", https://www.loc.gov/item/global-legal-monitor/2013-01-04/china-npc-decision-on-network-information-protection/, *Library of Congress*, accessed 22-10-2021.
[229] GREENLEAF Graham, LIVINGSTON Scott, 2016, "China's New Cybersecurity Law – Also a Data Privacy Law*?", Privacy Laws & Business International*, Issue 144, p. 10.
[230] LEE Jyh-An, 2018, "Hacking into China's Cybersecurity Law", *Wake Forest Law Review*, Vol. 53, No. 1, p. 88.
[231] "中华人民共和国个人信息保护法", *Zhōnghuá rénmín gònghéguó gèrén xìnxī bǎohù fǎ*, https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A4%E6%B3%95, accessed 04-01-2022. English Translation: "Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021", https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/, accessed 04-01-2022.

Data Quality: there has been a notable absence of data quality provisions in data privacy laws of the PRC. There are no requirements or obligations on timeliness and accuracy of personal information in the MIIT Regulations. The 2013 MIIT Guidelines do mention a basic principle of quality assurance where data processors need to ensure that the confidentiality, integrity and availability of personal information are all up to date.[232] The new Personal Information Protection Law however explicitly requires data processors "to ensure the quality of personal information and avoid adverse effects on individual rights and interests from inaccurate or incomplete personal information" (Article 8).[233]

Accountability of Data Processors: all relevant data privacy laws of the PRC require data processors to be accountable and accept complaints from users and remedy various types of privacy breaches (2012 Decision, 2011 MIIT Regulation). Moreover, the 2012 Decision requires data processors to strengthen their management of information that is posted by their users, and when publication or transmission of such information is prohibited by law they shall eliminate it, record it and provide it to relevant authorities (Article 5). As we have seen with other principles, the most stringent requirements for data accountability are devised in the non-binding 2013 MIIT Guidelines, that provide "clear definition of responsibilities, taking of appropriate measures, and recording processing so as to facilitate retrospective investigation".[234] With the enactment of the PIPL, this principle is finally being reiterated in a SC-NPC law.

Data Security: the previous fragmented framework that was set in place did afford some level of data security protection, although both 2012 Decision and Consumer Protection Law had rather general requirements of enacting technical measures to prevent leakage, damage or loss of personal data and consequent remedial measures in cases of data breach.[235] The 2011 MIIT Regulation already provided a mandatory notification provision in case of data breach, the most notable shortcoming however was that notification was required to authorities, but not users. The 2013 MIIT Regulation further expanded data security protection by merely listing which

[232] GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, p. 213.
[233] "中华人民共和国个人信息保护法", *Zhōnghuá rénmín gònghéguó gèrén xìnxī bǎohù fǎ*, https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A4%E6%B3%95, accessed 04-01-2022. English Translation: "Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021", https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/, accessed 04-01-2022.
[234] GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, p. 215.
[235] Article 5 of 2012 Decision, Article 29 of Consumer Protection Law.

aspect of a business must pay attention to security.[236] The 2013 MIIT Guidelines set out more stringent requirements, comprising of "data security education, training, plans for data security, risks and emergencies, clarification of responsibilities, internal control mechanisms, evaluation and protection systems, periodic self-inspections, commission of independent evaluation agencies, clarification of responsibilities, access controls and secure storage of information carriers.[237] Notably, data breach notification to data subjects was only required in the 2013 MIIT Guidelines, until the enactment of the Cybersecurity Law, whose Article 42 finally required to inform users in cases of leakages, information destruction or loss of information. The same provision has been reiterated in Article 1038 of the new Chinese Civil Code. The Cybersecurity Law already contains most of the requirements provided in the 2013 MIIT Guidelines, but some of the more stringent obligations are only required for Critical Information Infrastructures. Both PIPL and the new Data Security Law of the PRC set stringent standards for data security in the private sector. It is interesting to highlight how the Chinese personal information protection framework that result from all these complex legal instruments show how Chinese regulations mostly evolved within a security context, making the safety of persons and property the main criterion instead of focusing on building a fundamental rights protection framework like the GDPR.[238]

2.1.2. Real Name Registration Provisions

If the several yet fragmented data privacy laws of China did afford a general level of personal information protection in the private sector, it is also true that these laws have also helped in limiting cyberspace anonymity through the establishment of a real-name registration system.

Article 6 of the 2012 Decision provides that all "network service providers that conduct Internet access services and handle fixed telephone, mobile phone, and other network access procedures for users, or provide users with information dissemination services" must require real identity information from users when enter into agreements or confirming provision of services with users.[239] This doesn't mean however that a person must use its real name whenever providing

[236] GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, p. 213.
[237] GELLER Anja, 2020, "How Comprehensive is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective", *GRUR International*, Vol. 69, Issue 12, p. 1198.
[238] *Ibidem*, p. 1195.
[239] "全国人大常委会关于加强网络信息保护的决定", *Quánguó réndà chángwěi huì guānyú jiāqiáng wǎngluò xìnxī bǎohù de juédìng,* http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm, accessed 23-10-2021. English Translation: WANG Ted, 2016, "The NPC Standing Committee Decision on Strengthening the Network Information Protection", Chinese Law and Government, *Taylor & Francis Group*, Vol. 48, No. 1, 13–14.

information online, but rather that Internet Service Providers need to be able to identify who is the content provider, thus still allowing the use of pseudonym as long as ISPs are able to identify the individual behind it.[240]

A similar requirement for real-name registration has been reiterated in the Cybersecurity Law, Article 24, which expand its scope also to instant messaging platforms, and prohibits network operators to provide services to users refusing to give real identity information. Network operators failing to do so may be subjected to monetary fines, temporary suspension of operations, cancellation of permits, business licenses and closing down of websites. Moreover, persons directly in charge or responsible personnel may also face monetary fines (Article 61). In addition to the general obligation devised in Article 28 of providing technical support to public security agencies, the system devised in the Cybersecurity Law empowers regulatory authorities with extended monitoring and investigative powers.[241]

Real-name requirements have been fairly controversial, as on one hand they have been implemented to support enforcement of the law against cyber criminality, on the other hand studies clearly show that, after implementation of real name registration rules, politically sensitive content fell considerably, meaning that real name provisions have significantly helped in curtailing the freedom of speech of Chinese users.[242] Real name provisions also create a high risk of data leakage and breach by hackers by creating more opportunities to steal such data from network operators.

2.1.3. Data Export Limitations

Another contentious provision in China's data privacy laws has been the introduction of stricter data localization obligations and data export requirements. Before the enactment of the PRC Cybersecurity Law in 2017, the obligation of storing personal information and important financial data within mainland China was already in place in the banking sector, and it had become common practice in some industries.[243] Article 37 of the Cybersecurity Law however imposed data localisation of personal information and undefined "important data" to all Critical

[240] GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press p. 196.
[241] LEE Jyh-An, 2018, "Hacking into China's Cybersecurity Law", *Wake Forest Law Review*, Vol. 53, No. 1, pp.72-73.
[242] GELLER Anja, 2020, "How Comprehensive is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective", *GRUR International*, Vol. 69, Issue 12, p. 1198.
[243] CHANDER Anupam, LÊ Uyên, 2015, "Data Nationalism", *Emory Law Journal*, Vol. 64, Issue 3, pp. 686-688; LEE Jyh-An, 2018, "Hacking into China's Cybersecurity Law", *Wake Forest Law Review*, Vol. 53, No. 1, p. 78.

Information Infrastructure operators, comprising of "public communication and information services, power, traffic, water, finance, public service, electronic governance and other critical information infrastructure that if destroyed, losing function or leaking data might seriously endanger national security, national welfare and the people's livelihood, or the public interest" (Article 31).[244]

All operators from these industries are therefore barred from transferring such data outside of Chinese borders unless it is "truly necessary" for business requirements. Whenever such necessity is stated, the CII operators shall pass a security assessment that has ultimately been devised in the *Guidelines for Cross-Border Data Transfer Security Assessments* issued in 2017 and formulated by the Cyberspace Administration of China (CAC).

Data localization requirements and data export obligations have further been expanded in the new Personal Information Protection Law. According to Article 38, when all personal information processors need to transfer such data for business or other requirements, they must either pass a security assessment by the CAC, or undergoing personal information protection certification conducted by a specialized body, or again concluding a contract with the foreign receiving side in accordance with standards formulated by the CAC.[245]

Under these conditions, CII operators, together with personal information processors processing personal information reaching quantities provided by the State cybersecurity and informatization department, do still have stricter data localisation obligations as Article 40 of the PIPL explicitly requires them to store personal information within mainland China, and only when strictly necessary, export it outside borders (with a copy still remaining within China) by previously passing a security assessment procedure carried out by CAC.

PIPL also sets out the general obligation of always notifying users of the data export and the contact information, purpose and method of processing of the foreign personal information

[244] "中华人民共和国网络安全法", Zhōnghuá rénmín gònghéguó wǎngluò ānquán fǎ, https://www.pkulaw.com/chl/4dce14765f4265f1bdfb.html, accessed 03-11-2021. English Translation: "Cybersecurity Law of the People's Republic of China", http://www.lawinfochina.com/Display.aspx?LookType=3&Lib=law&Id=22826&SearchKeyword=&SearchCKeyword=&paycode=, accessed 03-11-2021; https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/, accessed 03-11-2021.

[245] "中华人民共和国个人信息保护法", *Zhōnghuá rénmín gònghéguó gèrén xìnxī bǎohù fǎ*, https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A4%E6%B3%95, accessed 04-01-2022. English Translation: "Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021", https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/, accessed 04-01-2022.

processors, as well as procedures to exercise their personal information rights (Article 39). PIPL also mandates that whenever personal information is disclosed to another entity, separate consent must be obtained from individuals to do so (Article 25). Moreover, a personal information protection impact assessment has to be carried out prior to data exports (Article 55).

To better implement the new data export and localisation requirements, the Cyberspace Administration of China issued on 29 October 2021 the *Draft Measures of Security Assessment of Cross-border Data Transfer* (数据出境安全评估办法, *Shùjù chūjìng ānquán pínggū bànfǎ*) that is currently being opened for public comment. The Draft Measures provide clarification on the thresholds under which personal information processors other than CII operators shall undertake mandatory personal information security assessment: in particular, it is mandatory when the data transfer is carried out by data processors who handles over 1 million individuals' personal information or when transferring the personal information of more than 100,000 individuals or the sensitive personal information of more than 10,000 individuals; or again when "important data" is being transferred.

2.1.4. Sensitive Data Provisions

If compared with the stricter EU Data Protection Model, a remarkable absence in the cumulative data privacy framework laid out in the last decade by the PRC is the one regarding sensitive data provisions. Sensitive data has not been defined in any SC-NPC Law, and not even in the New Chinese Civil Code, that only distinguishes private personal information (that have to be protected under the privacy protection provisions) and non-private personal information (which otherwise are ruled under the separate protection of personal information). The only legal document defining the term "sensitive personal information" and requiring separate obligations and requirements for its processing is the 2013 MIIT Guidelines, which list a series of data that can be considered sensitive and requires the obtainment of explicit consent from individuals.

Another non-binding instrument depicting in details the type of personal information to be considered sensitive is the PI Security Specification of 2020, whose list encompasses data that partly go beyond the list provided in the GDPR, for example: identification numbers, bank

account numbers, information on property, credit, transactions and personal information of children under the age of 14 are all to be considered sensitive personal information.[246]

The newly enacted PIPL has however dedicated a special section to the processing of sensitive personal information (Articles 28-32), by reiterating the same definition from the 2013 MIIT Guidelines, and by requiring a specific purpose, a need to fulfil, and strict protection measures to process such information. Article 29 requires express separate consent to be obtained, not specifying if the other six legal basis for processing personal information that is not sensitive can be applied. If the individual whose sensitive personal information is under 14 years old, consent from guardians shall be obtained and specific rules be drawn out for the processing of such information (Article 31). Users have to be notified of the possible effect that the processing of sensitive personal information could have on their rights and interests (Article 30), and, when administrative regulations provide it, a license may be needed to process sensitive personal information or additional restrictions may be required (Article 32).

Under the PIPL a data processor that processes sensitive personal information is required to undergo a prior personal information protection impact assessment (Article 55).

2.1.5. Automated Decision-Making Provisions

Requirements for automated decision-making was only laid out in the non-mandatory PI Security Specification, which has been updated in 2020. The Security Specification sets out additional obligations to processors (both private and public) who employ automated decision-making techniques in information systems, such as conducting an information security impact assessment before first use (similar to the European data privacy principle of "prior checking", by which data systems which raise potentially high levels of risk should be identified and examined before they operate[247]), and each year after it starts operating, take appropriate measures and empower subjects with complaint channels.[248]

The new Personal Information Protection Law introduces the concept of automated decision-making by defining it in its Article 73:

[246] GELLER Anja, 2020, "How Comprehensive is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective", *GRUR International*, Vol. 69, Issue 12, p. 1195.
[247] GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, p. 56.
[248] GELLER Anja, 2020, "How Comprehensive is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective", *GRUR International*, Vol. 69, Issue 12, p. 1197.

"Automated decision-making" refers to the activity of using computer programs to automatically analyze or assess personal behaviors, habits, interests, or hobbies, or financial, health, credit, or other status, and make decisions [based thereupon]."[249]

Article 24 sets out additional obligations regarding automated decision-making mechanisms, providing transparency of decision-making and fair handling of the results, while prohibiting unreasonable differential treatment of individuals in trading conditions such as trade price. Processors need to provide channels to individuals to refuse the targeting of their personal characteristics.

2.2. User's Data Privacy Rights

Remarkably, the lack of a clear definition of user's data privacy rights has been the weakest element in the dispersive data privacy laws and regulations devised by the PRC. Even if some general rights are provided in the SC-NPC laws, such as a restricted right to deletion of personal information, what generally weakens the whole data privacy protection system devised to users is the notable absence of explicit rights of access and correction. An advanced set of user's rights was however already in place in non-binding regulations, such as the 2013 MIIT Guidelines and the PI Security Specification. Many of these rights have been reiterated in the new Personal Information Protection Law, which has also introduced a new right to data portability, similarly to the one present in the European GDPR. To better comprehend the breadth of user's rights that are now protected in relation to the collection and processing of personal information in the PRC, the following listing is partly constructed on the GDPR set of rights, which contain the most advanced set of individual's rights regarding data privacy, and the rights' list provided in the PIPL.

Right to be informed: in each of the legal instruments described in Chapter 1, there is a general obligation to inform users on the method, scope and purpose of collection and processing, and shall publicly disclose rules on collection and processing. Similar to the requirements imposed

[249] "中华人民共和国个人信息保护法", *Zhōnghuá rénmín gònghéguó gèrén xìnxī bǎohù fǎ*, https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A4%E6%B3%95, accessed 04-01-2022. English Translation: "Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021", https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/, accessed 04-01-2022.

by the European GDPR, the new PIPL has established in Article 17 that personal information processors shall explicitly notify individuals truthfully, accurately, and fully. The privacy notice must contain a detailed set of information, ranging from the name and contact of the personal information processor, purpose, handling methods, categories of processed personal information, methods and procedures for individuals to exercise the rights and others provided by relevant regulations, and name, contact, purpose and methods of processing of any separate entity entrusted with the processing of such personal information. Special provisions of the PIPL also demand a notice to users on the use of automated decision-making, when transferring users' data outside Chinese borders, when handling sensitive personal information, and in addition it requires a special notice when processing personal information of children under 14 years old.

Right of Access: no explicit right of access can be found in any SC-NPC data privacy law before the enactment of the new Chinese Civil Code and the PIPL. Although the Cybersecurity Law requires network operators to establish a network information security complaint and reporting systems (Article 49), this doesn't imply rights of access and rectification to their own personal data. Only non-mandatory data privacy standards such as the 2013 MIIT Guidelines and PI Security Specification directly provide for rights of access and rectification. The New Chinese Civil Code is the first legal document of the PRC clearly providing individuals of access and copy rights regarding their personal information (Article 1036), and additionally to their own medical records (Article 1225). The PIPL reiterates these two rights in its Article 45, but provides exceptions in Article 18, which states that personal data processors are permitted not to notify users when laws or administrative regulations provide that confidentiality shall be preserved or notification is not necessary. PIPL additionally provides access and copy of personal information of a deceased person to "their next of kin" (Article 49).

Right to Copy: akin to the right of access, the right to obtain a copy of personal information was only included in non-mandatory Guidelines and Standards until the enactment of the new Civil Code and the PIPL. Article 45 of the PIPL requires the copies of personal information to be provided in a "timely manner".

Right of Rectification: Article 13 of the 2011 MIIT Regulations provides that users have the right to use, modify and delete the personal information uploaded by them. However, there is no provision on personal information originating from third parties.[250] Both Article 43 of the

[250] GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press, p. 215.

Cybersecurity Law and Article 1036 of the Civil Code provide users with the right to request correction whenever discovering that personal information gathered or stored by network operators has errors. Article 46 of the PIPL also provides users with the right to correct, complete or supplement personal information that has to be carried out by processors in a timely manner after verification.

Right of Deletion: this right was generally present in all SC-NPC data privacy laws, even if it was restricted to certain conditions. For example, Article 8 of the 2012 Decision granted users the right of deletion in case users discovered electronic information that discloses their personal identity, violates their privacy, or otherwise violates their legal rights, or if users are subject to harassment by electronic information of a commercial nature. The 2013 MIIT Regulations, although providing that collection and processing must cease when a user cancels an account, does not require that account data be deleted.[251] Again in this case the most advanced provisions on deletion were included in the 2013 MIIT Guidelines, that provided that deletion to be carried out in a timely manner and for "legitimate reasons", with additional requirements to delete personal information when purpose is achieved, or to provide de-identification measures when there is continued processing, or again devising procedures in case of bankruptcy and insolvency.[252] The PIPL establishes a right of deletion that is similar to the one provided in the GDPR, as individuals can request erasure whenever purpose has been achieved, is impossible to achieve, or the personal information is no longer necessary to achieve purpose; when processors cease the provision of products or services, or the individual rescinds its consent; when there has been unlawful processing, and other circumstances provided by relevant regulations. The right devised in the PIPL however does not quite reach the same level of the "right to be forgotten" drawn out in GDPR, where withdrawal of consent is possible at any time.[253]

Right to Object: similar to the right of deletion, the right to object personal information processing was limited to the prohibition of sending commercial electronic messages to the fixed telephone, mobile phone, or personal e-mail of an electronic information recipient without consent or request and when there was express rejection (Article 7 of the 2012 Decision, Article 29 of the Consumer Protection Law). The 2013 MIIT Guidelines again explicitly provide the user's right of refusal to processing or deletion of personal information (Article 5). Article 44

[251] *Ibidem*.
[252] *Ibidem*.
[253] GELLER Anja, 2020, "How Comprehensive is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective", *GRUR International*, Vol. 69, Issue 12, p. 1197.

of the PIPL reiterates this right and also empowers the individual of the right to limit the processing of its personal information. Article 24 additionally empowers the user to refuse targeting their individual's characteristics through automated decision-making techniques.

Right to Data Portability: a new right that has only been devised in the Personal Information Protection Law is the right of an individual to transfer their personal information to a personal information processor they designate, always in respect to conditions posed by the CAC (Article 45).

2.3. Shifting Power Relations: Difficulties in Implementation and the Bargaining Power of Chinese Digital Enterprises

Despite the meaningful legal advancements on personal data protection, especially in the private sector, the effectiveness of the data privacy legal framework set up in the PRC has been weakened by several factors, the first and foremost being a lack of an efficient enforcement mechanism administered by and independent Data Protection Authority (DPA).

There is no SC-NPC law granting responsibility of supervising compliance of data privacy laws and regulations to a single specific agency or authority, but it is rather established that enforcement powers be given to a set of State Council departments, sector-specific government authorities, and relevant departments of local government.[254] The Cyberspace Administration of China is in charge of coordination of these multiple governmental departments and for network data security, that include but are not limited to the Ministry of Industry and Information Technology (MIIT), State Administration for Market Regulation (SAMR), China Banking and Insurance Regulatory Commission (CBIRC), etc.[255] The lack of a central data protection authority whose main mandate is personal data protection has led to poor implementation and to enforcement difficulties, for example leading to confusion on to which agency individuals or enterprises are eligible to submit complaints.

The main enforcement tool to ensure compliance in the many PRC Data privacy laws are administrative penalties, many of which have no counterpart in the fellow European General

[254] LUO Duoqun, WANG Yanchen, "China - Data Protection Overview", https://www.dataguidance.com/notes/china-data-protection-overview, accessed 18-01-2022.
[255] *Ibidem*.

Data Protection Regulation.[256] Almost all SC-NPC laws and MIIT Regulations provide the possibility to administer sanctions such as monetary fines, both to data processors and relevant employees, but also to provide for warnings, confiscation of illegal income, revocation of licenses, suspension or closure of business, banning employees from accessing the profession, and even adverse publicity sanctions such as the publishing of the sanctions in a "social credit file" and public announcement provisions.[257]

The serious difficulties in implementing data privacy protection provisions can be shown for example in the Report conducted by the SC-NPC in 2017 on the implementation of the new Cybersecurity Law provisions as well as the 2012 Decision. The document reported that "the situation in user personal information protection work is grim", with half of the interviewees encountering excessive collection of personal information; in addition, more than 60% of individuals had been subject to "dictator clauses", where relevant enterprises use their own advantageous position to force the collection and use of user information, and if this is not accepted, the product in question cannot be used, or services received.[258] Moreover, according to the report, after individuals discovered that their personal information was leaked or abused, reporting, filing complaints, and filing cases was deemed to be difficult.[259]

Another factor contributing to the weakening of the PRC data privacy framework is the fact that the major actors that are able to shape China's data protection regime (mainly the Chinese government, digital enterprises and the public) often have contrasting values that ultimately cause personal data protection to be put in second place. Zhao and Feng argue that legal advancements in the realm of personal data protection mainly happen in those areas where these actors' interests meet, especially when personal data protection is seen as instrumental in upholding public security and facilitating economic growth.[260] Private digital enterprises have undergone a booming expansion in the last decades that has enhanced both their economic and political power, especially the ones known as the "Big Three" or with the acronym BAT, namely Baidu, Alibaba and Tencent. These companies have an enormous hold on personal

[256] GELLER Anja, 2020, "How Comprehensive is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective", *GRUR International*, Vol. 69, Issue 12, p. 1201.
[257] *Ibidem*.
[258] WANG Shengjun, "Report concerning the Inspection of the Implementation of the 'Cybersecurity Law of the People's Republic of China' and the 'National People's Congress Standing Committee Decisions concerning strengthening Online Information Protection'", https://digichina.stanford.edu/work/report-concerning-the-inspection-of-the-implementation-of-the-cybersecurity-law-of-the-peoples-republic-of-china-and-the-national-peoples-congress-standing/, accessed 03-11-2021.
[259] *Ibidem*.
[260] ZHAO Bo, FENG Yang, 2021, "Mapping the development of China's data protection law: Major actors, core values, and shifting power relations", *Computer Law & Security Review*, Vol. 40, pp. 11-13.

information data, and the Chinese Government is relying more and more on the technological support provided by these enterprises to realize its governance goals. This has led to an increasing bargaining power that digital enterprises have gained, supported by the establishment of special communication channels between these private companies and the government, that have been collaborating on the expansion and enactment of big data policies also thanks to the wide access of the Chinese government to data held by the private sector.[261]

Digital enterprises have established special channels of communication with the Chinese Government that has enhanced their ability to influence policy and law-making processes in the digital realm, especially in regard to the collection and processing of data that are treated as a kind of proprietary asset by these enterprises.

2.3.1. Privacy Policy Evolution of the "Big Three": Alibaba, Tencent and Baidu

The three main private digital enterprises that have been expanding in the Chinese market through their multi-service and integrated platforms are Alibaba Group, Tencent and Baidu. These companies have taken collection and processing of their users' personal information, in particular in the fields of big data extraction and analysis, as their core growing strategy. The Chinese government highly relies on the access to these companies' users' data to achieve its governance goals, and at the same time the three enterprises have become very active in collaborating with the PRC government in State-coordinated research projects, both in the technological field (such as facial recognition, AI, big data etc.), and also in social control policies (for example with the Social Credit Systems created by Tencent, namely Tencent Credit, and Alibaba, namely Sesame Credit).

Alibaba is the major e-commerce player in the PRC, with leading B2B (such as the international Alibaba.com and AliExpress.com or the Chinese domestic portal 1688.com), B2C (Tmall), and C2C platforms (Taobao). The company however has expanded in recent years to other fields, such as online payments (Alipay and Ant Financial), logistic networks (Cainiao), supermarket retail chains (known as Hema or Freshippo[262]), food delivery services (Ele.me), cloud

[261] *Ibidem*, p. 8.
[262] Hema, founded in 2016, is a self-operated retail chain supermarket of Alibaba Group, integrating online and offline retail capabilities, notable for using data analytics for offering customized recommendations for consumers.
CHOUDHURY Sahely Roy, "Jack Ma's Alibaba is doubling down on its supermarket strategy",

computing services (Alibaba Cloud), entertainment (Youku Tudou) and communication and collaboration platforms (DingTalk).[263]

Tencent, since its founding in 1998, has also become one of the major Chinese conglomerate in the entertainment and technology industry, with major instant-messaging applications such as Tencent QQ and WeChat, and notable entertainment divisions such as Tencent Games, Tencent Music, Tencent Video and Tencent Comic. Baidu is China's largest search engine, providing multiple Internet-related services, and currently expanding to Artificial Intelligence-related sectors, including intelligent driving and smart devices.[264]

All of these three companies have published their own privacy statements, which although generally complying with the fragmented data privacy legislation set out in the PRC, still allow these companies to process an enormous amount of data that help in designing new products and services, other than providing existing ones.

Alibaba Group hasn't devised a general privacy policy but distinguishes different privacy statements in each of its platforms. It is interesting to highlight how the international platform of Alibaba.com and the Chinese equivalent portal 1688.com (former Alibaba.com.cn) have two different privacy policies, with the former in the past being more advanced in terms of personal data protection than the latter.[265] A study conducted in 2013 shows how the privacy policy of the Chinese portal had not changed since Alibaba's foundation in 1999, while the privacy policy of the international platform was updated in 2009. The study highlights how the international platform of Alibaba.com had more advanced and detailed provisions on transfer of information to third parties: 1688.com allowed such transfer whenever a third-party affiliates or partners with Alibaba, while the international platform allowed data transfer only if users responded to relevant third-party marketing, promotion or advertising messages.[266] The Chinese privacy policy also clearly stated that one purpose of collection was for statistical analysis for trade and service promotion. Both of them did not provide users' notification in case the privacy policy got revised (although Alibaba.com stated that changes in the policy will be published in the homepage), and in addition did not provide a choice to opt-out of the privacy policy, requiring

https://www.cnbc.com/2017/07/18/alibaba-hema-stores-blend-online-and-offline-retail.html, *CNBC News*, accessed 19-01-2022.

[263] Alibaba Group, "*Yèwù fànchóu*", 业务范畴, https://www.alibabagroup.com/cn/about/businesses, accessed 19-01-2022.

[264] Baidu, "Company Overview", https://ir.baidu.com/company-overview/, accessed 19-01-2022.

[265] WANG Faye Fangfei, 2014, *Law of Electronic Commercial Transactions – Contemporary Issues in the EU, US, and China*, London, Routledge, pp. 181-182.

[266] *Ibidem*.

users to contact Alibaba in writing in case they did not agree to changes.[267] A more recent study on Alibaba's (based however on Taobao) privacy policy carried out in 2019 shows that, although there is general compliance with data privacy law provisions, it still does not limit collection to its strict purpose but use the information to design new products and services. Moreover, all privacy policies do not expressively mention that usage of data will come to an end after deregistration.[268] All enterprises published their privacy statement on their site requiring obtainment of consent before service provision and clearly stated purpose, method and scope of collection, however only Tencent provided users with avenues to consult and correct their personal information, and Alibaba in particular still had no clear notification for users in case of change of policy or company ownership.[269] The use of jargon and technicalities rendered difficult user's understanding of the privacy policy.[270]

The privacy policies of all of the relevant Alibaba platforms have been updated before or immediately after the entry into force of the Personal Information Protection Law.[271] All Alibaba platforms now clearly state user's rights, for example 1688.com lists rights of access, correction, supplement, deletion, deregistration, rescinding of consent and limitation of scope, opt-out of automated-decision making, and the right to contact the platform. Tencent's privacy statement was also updated in November 2021 in a similar way, by also providing an email to users to exercise their statutory and regulatory rights (dataprotection@tencent.com) and by informing that no automated decision-making techniques are employed by Tencent products, as any emails from Tencent are sent only in response to inquiries submitted by users and for service messages only.[272]

Baidu's privacy policy was last updated in April 2021, stating a very similar set of users' rights to the one provided by Alibaba platforms, but with more detailed instructions on how to exercise them.[273] Tencent privacy policy does not specify any provision on transfer of data outside Chinese borders, Baidu on the other hand has dedicated a special section setting strict data storage within Mainland China.

---

[267] *Ibidem*.
[268] FU Tao, 2019, "China's personal information protection in a data-driven economy: A privacy policy study of Alibaba, Baidu and Tencent", *Global Media and Communication*, Vol. 15, Issue 2, pp. 206-207.
[269] *Ibidem*.
[270] *Ibidem*.
[271] Alibaba.com (16/01/2022), 1688.com (29/10/2021), Taobao (1/11/2021), Tmall (31/10/2021), Alipay (30/11/2021) to name a few.
[272] Tencent Privacy Policy. "*Téngxùn gōngsī wǎngyè jí wèn xún tíjiāo yǐnsī zhèngcè*", 腾讯公司网页及问询提交隐私政策, https://www.tencent.com/zh-cn/privacy-policy.html, accessed 20-01-2022.
[273] Baidu Privacy Policy, "*Bǎidù yǐnsī zhèngcè zǒngzé*", 百度隐私政策总则, http://privacy.baidu.com/policy, accessed 20-01-2022.

There is no clear section that provides for different legal bases for collection and processing of personal information other than consent as provided by the PIPL in any of the previously stated privacy policies. Even though minimal collection and processing is devised by the PIPL, many of these platforms still state the designing of new products and services as a purpose of collecting and processing personal information.

2.4. Chinese Government Access to Private-Sector Data

Contrasting to the more stringent obligations and requirements provided for the private sector, the public sector has been fairly unregulated in the realm of personal information protection until the enactment of the PIPL, which features a specific section of "Specific Provisions on State Organs Processing Personal Information" (国家机关处理个人信息的特别规定, *Guójiā jīguān chǔlǐ gèrén xìnxī de tèbié guiding*, Articles 33-37). Moreover, many laws provide for the PRC Government access to private-sector data, which have been fundamental in fulfilling the Government policy goals (for example on big data, or on social control policies).

The Chinese Government is the strongest actor in informing the direction of data privacy legislation, and as such many legal advancements in the realm of data privacy protection have gone hand in hand with the need to improve network safety and security through the expansion of surveillance systems with the rationale of enhancing public and national security, more than for truthfully establishing an individual right to data protection.[274] That is why one of principal law explicitly authorizing government access to private-sector information is the State Security Law: whenever state security is at stake, individuals and organisation cannot refuse to provide relevant information to authorities (Article 18), which on the other hand have to previously pass an internal approval procedure (Article 10).[275] Government authorities are also extended vast monitoring and surveillance powers in name of public and national security. Real-name provisions and strict data localization requirements have enhanced authorities' power of surveillance, as important data cannot be exported outside Chinese borders without a previous assessment by authorities and individuals are required to identify themselves with their real

[274] ZHAO Bo, FENG Yang, 2021, "Mapping the development of China's data protection law: Major actors, core values, and shifting power relations", *Computer Law & Security Review*, Vol. 40, pp. 4-6.
[275] WANG Zhizheng, 2017, "Systematic Government Access to Private-Sector Data in China". In CATE Fred H., DEMPSEY James X., *Bulk Collection: Systematic Government Access to Private-Sector Data*, New York: Oxford University Press, p. 245.

identity when accessing the network and applying for relevant services. As the real identity of users are detained by private data processors, channels to access such identification data held by the private sector are established with the relevant authorities. The Chinese government both relies on technical support provided by network operators (provided in the Cybersecurity Law) and the data they have access to achieve different policy goals.

The complex organizational apparatus established by the Chinese Government, both at the legislative and institutional level, through its many surveillance systems (ranging from the oldest one such as the *Hùkǒu* 户口 household registration system that limited the mobility of Chinese citizens to the diffused censorship of the Chinese Internet and millions of surveillance cameras with facial recognition features devised by the Skynet and the SharpEyes surveillance systems, to the more recent Smart Cities Projects and social control policies related to the Social Credit System) is a system that is institutionally ready to tackle and curtail its citizens fundamental rights in the name of national and public security.

CHAPTER 3

Disclosure of Personal Data in the Prevention and Control of Major Infectious Diseases: the Covid-19 Case Study

3.1 China's Response to the Covid-19 Epidemic and the Central Role of Chinese Digital Platforms

The access of digital enterprises and the PRC Government to Chinese citizens' personal information has been furtherly enhanced by one of the most unexpected events happening during this century: the outbreak of the worldwide Covid-19 pandemic caused by the SARS-CoV-2 virus (severe acute respiratory syndrome Coronavirus 2). Originating from Wuhan, Hubei, where the first confirmed patients were documented in December 2019, and also where the most stringent lockdown and quarantine measures were implemented, the virus soon spread to other Chinese provinces and abroad, prompting the World Health Organization to declare the Covid-19 outbreak a "public health emergency of international concern" on 30 January 2020.[276]

In the fight against the spread of the Novel Coronavirus, the Chinese Government has sought to implement an "elimination strategy", aimed at containing the dissemination of the virus and keeping the number of cases to zero or a very low level with strict and aggressive control measures.[277] Different measures have been implemented in different provinces and cities, according to their risk level, mainly based on number of deaths and confirmed cases and significance of population movement.[278] As of January 2022, 138.310 confirmed cases have been reported in China, 80,695 of which had been reported only in the first two months since

[276] World Health Organization, "Statement on the second meeting of the International Health Regulations (2005) Emergency Committee regarding the outbreak of novel coronavirus (2019-nCoV)", https://www.who.int/news/item/30-01-2020-statement-on-the-second-meeting-of-the-international-health-regulations-(2005)-emergency-committee-regarding-the-outbreak-of-novel-coronavirus-(2019-ncov), accessed 26-01-2022.
[277] LU Guangyu, RAZUM Oliver, JAHN Albrecht, ZHANG Yuying, SUTTON Brett, SRIDHAR Devi, ARIYOSHI Koya, VON SEIDLEIN Lorenz, MÜLLER Olaf, 2021, "COVID-19 in Germany and China: mitigation versus elimination strategy", *Global Health Action*, Vol. 14, Issue 1, Article N. 1875601, pp. 2-3.
[278] YANG Fang, HEEMSBERGEN Luke, FORDYCE Robbie, 2021, "Comparative analysis of China's Health Code, Australia's COVIDSafe and New Zealand's COVID Tracer Surveillance Apps: a new corona of public health governmentality?", *Media International Australia*, Vol. 178, Issue 1, p. 186.

the discovery of the new virus.[279] During this first wave, the majority of confirmed cases have been registered in Hubei, and especially in Wuhan.[280]

The Chinese Government has not only thoroughly mobilized its surveillance apparatus and implemented strict lockdown measures such as mandatory use of surgical masks and social distancing, travel and mobility restrictions, mandatory quarantine, large-scale population testing, but also deployed extensively digital technologies such as big data, artificial intelligence, cloud computing and newly-developed contact-tracing mobile applications to effectively trace virus clusters, prevent, monitor and control pandemic trends and their evolution, and to better allocate resources.[281] In the most hard-hit areas, community-based control measures, such as the so-called "grid closed management" (网格化管理, *wǎnggéhuà guǎnlǐ*) system have been deployed alongside the integration of CCTV systems with facial recognition and thermal sensor technologies in order to both restrict the movements of citizens and to monitor their health status.[282]

The collaboration with Chinese private digital platforms in elaborating contact-tracing applications, such as Alipay Health Code and WeChat Health Code, has been deemed crucial in both technically implementing such measures and in contributing to its vast popular application and public acceptance.[283] Such broad application of privacy-intrusive digital means developed by Chinese private enterprises to tackle the pandemic raises however many questions of data accountability, data security and fair processing of personal information collected through these technological means, even so in a country where the privacy and data protection

[279] World Health Organization, "China: WHO Coronavirus Disease (COVID-19) Dashboard", https://covid19.who.int/region/wpro/country/cn, accessed 29-01-2022; ZANIN Mark, XIAO Cheng, LIANG Tingting, LING Shiman, ZHAO Fengming, HUANG Zhenting, LIN Fangmei, LIN Xia, JIANG Zhanpeng, WONG Sook-San, 2020, "The public health response to the COVID-19 outbreak in mainland China: a narrative review", *Journal of Thoracic Disease*, Vol. 12, Issue 8, p. 4435.

[280] Between December 31, 2019, and March 22, 2020, there were 67,707 confirmed cases in Hubei Province, of which Wuhan alone recorded 49,912 cases. ZANIN Mark, XIAO Cheng, LIANG Tingting, LING Shiman, ZHAO Fengming, HUANG Zhenting, LIN Fangmei, LIN Xia, JIANG Zhanpeng, WONG Sook-San, 2020, "The public health response to the COVID-19 outbreak in mainland China: a narrative review", *Journal of Thoracic Disease*, Vol. 12, Issue 8, p. 4435.

[281] WU Jun, WANG Jian, NICHOLAS Stephen, MAITLAND Elizabeth, FAN Qiuyan, 2020, "Application of Big Data Technology for COVID-19 Prevention and Control in China: Lessons and Recommendations", *Journal of Medical Internet Research*, Vol. 22, Issue 10, pp. 2-3.

[282] KHALIL Lydia, "Digital Authoritarianism, China and Covid", *Lowy Institute*, https://www.lowyinstitute.org/publications/digital-authoritarianism-china-and-covid, accessed 10-02-2021; ; "Grid-based community workers power up China's grassroots coronavirus fight", *Xinhua*, http://www.xinhuanet.com/english/2020-03/01/c_138832911.htm, accessed 29-01-2022.

[283] CONG Wanshu, 2021, "From Pandemic Control to Data-Driven Governance: The Case of China's Health Code", *Frontiers in Political Science*, Vol. 3, p. 7.

framework enables, more than hinders, the vast collection and processing powers of the Chinese Government and its broad access to private sector digital data.[284]

Thanks to these strict measures however, while the WHO declared the Covid-19 outbreak "a global pandemic" on 11 March 2020,[285] which represents the highest level of emergency in the six-level warning system devised by the organization, China already contained its major clusters and gradually proceeded to lift lockdown restrictions in affected provinces and cities, with Wuhan being eased from travel restrictions on 8 April 2020.[286] After this initial phase, other sporadic local outbreaks of the virus have been equally treated with massive lockdown measures and outspread population testing, supported by the wide application of these contact-tracing technological tools.

3.2. PRC Regulatory Aspects of Prevention and Control of Major Infectious Diseases

Since the outbreak of SARS (Severe Acute Respiratory Syndrome) in 2003, the PRC has drawn up many legislative instruments whose main aim is to establish an emergency response mechanism whenever the country is faced with public health crisis. The Law on Prevention and Treatment of Infectious Diseases (中华人民共和国传染病防治法, *Zhōnghuá rénmín gònghéguó chuánrǎn bìng fángzhì fǎ*) issued in 1989 and revised in 2013, and the Emergency Response Law (中华人民共和国突发事件应对法, *Zhōnghuá rénmín gònghéguó tú fā shìjiàn yìngduì fǎ*) issued in 2007 are the two major laws that served as the legal basis for China's response to the Covid-19 crisis.

These laws prescribe four levels of emergency alert, with Level I being the maximal level of emergency, which gives local governments, under the coordination of the central government, extensive powers to mitigate the emergency, for example allocating resources, closing premises, restricting freedom of movement, implementing compulsory control measures,

[284] *Ibidem*, pp. 10-11.
[285] World Health Organization, "WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020", https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020, accessed 27-01-2022.
[286] Bloomberg, "China to Lift Lockdown Over Virus Epicenter Wuhan on April 8", https://www.bloomberg.com/news/articles/2020-03-24/china-to-lift-lockdown-over-virus-epicenter-wuhan-on-april-8, accessed 27-01-2022.

conducting investigations etc. (Article 45 of Emergency Response Law).[287] By 29 January 2020, all Chinese provinces had launched a Level I emergency alert, and as a consequence many restrictive measures above described were implemented.

These two laws provide some additional requirements for personal data collection and processing during health emergencies, although very general. Article 12 of the Law on Prevention and Treatment of Infectious Diseases for example sets out a general requirement for all individuals and entities to provide truthful information about the diseases to disease prevention and control institutions and medical agencies, which in turn have the obligation to not disclose any information or materials relating to personal privacy.[288] Article 33 of the same law provides that "disease prevention and control institutions shall take the initiative to collect, analyse, investigate and verity information on epidemic situation of infectious diseases"[289], and provide such reports to relevant health administration departments. Reports are also mandated by the Regulation on Responses to Public Health Emergencies revised in 2011 (突发公共卫生事件应急条例, *Túfā gōnggòng wèishēng shìjiàn yìngjí tiáolì*). The reports usually contain both personal information and sensitive information of patients, such as name, ID number, age, occupation, residential address, date of disease onset, date of diagnosis, type of infectious disease, and route of transmission.[290]

These specific requirements for prevention and control institutions and medical agencies seem to be supplemented by the more general obligation of all companies to report the condition of any employee confirmed or suspected of having an infectious disease. In order to do so, during the Covid-19 pandemic companies have been required to collect health and travel information of their employees, which is not collected under normal conditions as a company is required to collect only employee's information related to the fulfilment of their contract under Labour

[287] "中华人民共和国突发事件应对法", Zhōnghuá rénmín gònghéguó tú fā shìjiàn yìngduì fǎ, https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E7%AA%81%E5%8F%91%E4%BA%8B%E4%BB%B6%E5%BA%94%E5%AF%B9%E6%B3%95, accessed 27-01-2022. English Translation: "Emergency Response Law of the People's Republic of China", http://english.mee.gov.cn/Resources/laws/envir_elatedlaws/201705/t20170514_414040.shtml, accessed 27-01-2022.

[288] "中华人民共和国传染病防治法", Zhōnghuá rénmín gònghéguó chuánrǎn bìng fángzhì fǎ, https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E4%BC%A0%E6%9F%93%E7%97%85%E9%98%B2%E6%B2%BB%E6%B3%95, accessed 27-01-2022. English Translation: "Law Of The People's Republic Of China On Prevention And Treatment Of Infectious Diseases (2013 Amendment), June 29, 2013", https://china.usc.edu/law-peoples-republic-china-prevention-and-treatment-infectious-diseases-2013-amendment-june-29-2013, accessed 27-01-2022.

[289] *Ibidem*.

[290] WU Jun, WANG Jian, NICHOLAS Stephen, MAITLAND Elizabeth, FAN Qiuyan, 2020, "Application of Big Data Technology for COVID-19 Prevention and Control in China: Lessons and Recommendations", *Journal of Medical Internet Research,* Vol. 22, Issue 10, p. 2.

Contract Law.[291] The breadth and scope of collection of such information have been mandated differently at the provincial and local level, for example the Shanghai government issued a Notice requesting companies to monitor the everyday health status and body temperature, while Beijing and Guangdong also required companies to collect the travel history of employees.[292]

3.2.1 Specific Legal Instruments for Personal Data Protection during Covid-19

The eagerness of containing the virus spread combined with the increased amount of data of confirmed and suspected carriers of the disease that were collected and processed lead to many personal information data leakage incidents that sparked public concern. For example, only in January 2020, Hunan, Jiangxi, Inner Mongolia and Shanxi reported cases of leakage of personal information related to the epidemic.[293] This prompted the Cyberspace Administration of China to issue the "Notice on the Protection of Personal Information and the Use of Big Data to Support Joint Prevention and Control" (关于做好个人信息保护利用大数据支撑联防联控工作的通知, *Guānyú zuò hǎo gèrén xìnxī bǎohù lìyòng dà shùjù zhīchēng liánfáng lián kòng gōngzuò de tōngzhī*) on 4 February 2020.[294]

The Notice dictates that entities and individuals shall not collect and use personal information related to the prevention and control of the Covid-19 disease without previous obtaining consent of the person, except for institutions authorized by the health department of the State Council in accordance with the Cybersecurity Law, the Law on the Prevention and Control of Infectious Diseases, and Regulations on Responses to Public Health Emergencies (Article 1).[295] Moreover, the collection and process of personal information related to the pandemic shall refer to the PI Security Specification of 2017 (Article 2). Despite it being a non-mandatory national standard, the Specification provided for the most advanced and stringent provisions for

[291] "Client Advisory Regarding COVID-19 Legal Issues in China", *Squire Patton Boggs*, https://www.squirepattonboggs.com/-/media/files/insights/publications/2020/03/client-advisory-regarding-covid-19-legal-issues-in-china/client-advisory-regarding-covid19-legal-issues-in-china.pdf, accessed 09-03-2021.
[292] *Ibidem*.
[293] MENG Qingwei, 孟庆伟, "*Hǎiliàng shè yìqíng gèrén xìnxī xièlòu liǎng de gōng'ān zuò chū xíngzhèng jūliú chǔfá*" 海量涉疫情个人信息泄露 两地公安做出行政拘留处罚 (public security issued administrative detention penalties following massive leakage of personal information related to the epidemic), https://news.sina.com.cn/o/2020-02-05/doc-iimxyqvz0398976.shtml, accessed 27-01-2022.
[294] "关于做好个人信息保护利用大数据支撑联防联控工作的通知", *Guānyú zuò hǎo gèrén xìnxī bǎohù lìyòng dà shùjù zhīchēng liánfáng lián kòng gōngzuò de tōngzhī*, http://www.cac.gov.cn/2020-02/09/c_1582791585580220.htm, accessed 28-01-2022.
[295] *Ibidem*.

collection and processing of personal information if compared with other legally binding laws and regulations in the PRC. This national standard was specifically revised in March 2020, with effect from October, with even more stringent obligations for data processors, limitations to user profiling, an expanded definition of sensitive information, and exceptions to consent.

The Notice also expressively provides for minimal collection and processing strictly connected to the purpose of preventing and controlling the spread of Covid-19. While the Notice encourages the active use of big data in order to analyse and predict the spread of the virus (Article 5), the collection of personal information has to be limited to key groups: confirmed patients, suspected patients, close contacts. There is a general prohibition of disclosing information such as name, age, ID number, phone number, home address, etc. without consent of the person or without desensitizing the personal information (Article 3).[296] Management and technical protection measures to prevent theft and leakage of such information are also mandated by the Notice (Article 4). Any illegal collection, processing or disclosure of such information shall be reported to informatization and public security departments (Article 6).[297]

Except for this rather general governmental decree, privacy and personal data issues concerning the digital response of the PRC in the fight against the spread of the virus have been rather side-lined, especially if we compare it with the attention that personal information protection has sparked in the implementation of digital monitoring measures in most liberal democracies. As a consequence, only industrial and non-mandatory national standards have been published in order to address privacy and personal information protection in the newly developed contact-tracing applications that have been widely accepted by the Chinese population.[298]

The role of two major Chinese tech giants, namely Tencent and Alibaba, in the drafting of these standards along with the respective local governments where the two companies are based (Shenzhen for Tencent and Hangzhou for Alibaba), have been pivotal but has further "blurred the boundary between private and public", as Cong suggests.[299] The two companies have also participated in the elaboration of the three national standards on health code published by the

[296] "关于做好个人信息保护利用大数据支撑联防联控工作的通知", *Guānyú zuò hǎo gèrén xìnxī bǎohù lìyòng dà shùjù zhīchēng liánfáng lián kòng gōngzuò de tōngzhī*, http://www.cac.gov.cn/2020-02/09/c_1582791585580220.htm, accessed 28-01-2022.
[297] *Ibidem*.
[298] CONG Wanshu, 2021, "From Pandemic Control to Data-Driven Governance: The Case of China's Health Code", *Frontiers in Political Science*, Vol. 3, p. 7.
[299] *Ibidem*. The two standards in question are the "Reference Architecture and Technology Guide of Anti-Epidemic Pass Code" published by Shenzhen Standards Promotion Council and the "Guide to Management and Service of Hangzhou Health Code" published by Hangzhou Market Regulation Administration.

Chinese National Standardization Administration in April, which specify the reference model, data format and application interface of Health Codes.[300]

These three national standards deal with the protection of personal information collected and processed through health code applications, which have to obtain express or authorized consent from citizens and must enact encryption measures and storage through specific algorithms that have to be in line with requirements for national password management.[301]

3.3. Contact-Tracing Mobile Applications

The tracking and monitoring of the spread of the Novel Coronavirus disease posed significant challenges as the virus not only has a longer incubation period but also features a higher rate of transmission compared to previous outbreaks of other respiratory syndromes such as SARS and MERS (Middle East Respiratory Syndrome), complicated even more by the existence of asymptomatic patients.[302] Traditional control and monitoring measures such as social distancing, quarantine and travel and mobility restrictions, even if supported by modern technological surveillance tools such as CCTVs and thermal sensors, soon proved to be unsatisfactory to curb the pandemic spread in China. This in turn created the opportunity for digital tech giants such as Alibaba and Tencent to expand their influence with the integration of mini-programs dedicated to contact-tracing in their mobile applications Alipay and WeChat.

Data extracted from mobile phones can be leveraged and fed into algorithms to calculate the mobility and interactions of individuals, and this in turn can be decisive to detect new clusters, to predict Covid-19 trends and to assess the impact of implementation measures.[303] The Global Positioning System (GPS) is a key feature integrated in mobile phones that can collect very

[300] CONG Wanshu, 2021, "From Pandemic Control to Data-Driven Governance: The Case of China's Health Code", *Frontiers in Political Science*, Vol. 3, p. 7.
[301] "Regulating electronic means to fight the spread of COVID-19: Argentina, Australia, Brazil, China, England, European Union, France, Iceland, India, Iran, Israel, Italy, Japan, Mexico, Norway, Portugal, Russian Federation, South Africa, South Korea, Spain, Taiwan, Turkey, United Arab Emirates." *The Law Library of Congress, Global Research Directorate*, https://www.loc.gov/item/2020714995/, accessed 10-02-2021.
[302] BOEING Philipp, WANG Yihan, 2021, "Decoding China's COVID-19 'virus exceptionalism': Community-based digital contact Tracing in Wuhan", *R&D Management*, Vol. 51, Issue 4, pp. 339-340.
[303] OLIVER Nuria, LEPRI Bruno, STERLY Harald, LAMBIOTTE Renaud, DELETAILLE Sébastien, DA NADAI Marco, LETOUZÉ Emmanuel, ALI SALAH Albert, BENJAMINS Richard, CATTUTO Ciro, COLIZZA Vittoria, DE CORDES Nicolas, FRAIBERGER Samuel P., KOEBE Till, LEHMANN Sune, MURILLO Juan, PENTLAND Alex, PHAM Phuong N., PIVETTA Frédéric, SARAMAKI Jari, SCARPINO Samuel V., TIZZONI Michele, VERHULST Stefaan, VINCK Patrick, 2020, "Mobile phone data for informing public health actions across COVID-19 pandemic life cycle", *Science Advances*, Vol. 6, Issue 23, pp. 1-2.

precise location data; moreover, Bluetooth can sense proximity between two devices, helping in estimating the number of face-to-face interactions.[304] In a country like China, where smartphone users exceeded 970 million in 2020 according to Statista,[305] the development of contact-tracing applications was seen as a potential solution to time-consuming and economically infeasible traditional cluster management. China has not been the only country that has resorted to this kind of digital tool, as more than 50 countries in the world have implemented contact-tracing applications. Nonetheless, other than being one of the first applications to be developed and one of the most widely accepted by the public with a very high rate of diffusion between Chinese citizens, Chinese Health Codes bear many differences with the majority of the Bluetooth-based, decentralized applications developed in most of the other countries, especially in European countries and the United States where many specific privacy-preserving frameworks have been designed, such as the Pan-European Privacy-Preserving Proximity Tracing framework and the Apple and Google joint contact-tracing technology.[306]

3.3.1 Alipay and WeChat Health Codes

The first Health Code contact-tracing applications (健康码, *Jiànkāng mǎ*), originally called "Anti-Virus Code" (病毒码, *Bìngdú mǎ*), were issued on 9 February 2020 by both Alibaba and Tencent under the request of the municipal governments of Hangzhou and Shenzhen, where the two tech giants' headquarters are based.[307] Alibaba's Health Code is a mini software program

[304] BUDD Jobie, MILLER Benjamin S., MANNING Erin M., LAMPOS Vasileios, ZHUANG Mengdie, EDELSTEIN Michael, REES Geraint, EMERY Vincent C., STEVENS Molly M., KEEGAN Neil, SHORT Michael J., PILLAY Deenan, MANLEY Ed, COX Ingemar J., HEYMANN David, JOHNSON Anne M., MCKENDRY Rachel A., "Digital technologies in the public-health response to COVID-19", *Nature Medicine*, https://www.nature.com/articles/s41591-020-1011-4, accessed 24-02-2021.
[305] Statista, "Number of smartphone users in China from 2015 to 2020 with a forecast until 2026", https://www.statista.com/statistics/467160/forecast-of-smartphone-users-in-china/#:~:text=In%202020%2C%20the%20number%20of,exceeded%20six%20billion%20that%20year., accessed 31-01-2022.
[306] BUDD Jobie, MILLER Benjamin S., MANNING Erin M., LAMPOS Vasileios, ZHUANG Mengdie, EDELSTEIN Michael, REES Geraint, EMERY Vincent C., STEVENS Molly M., KEEGAN Neil, SHORT Michael J., PILLAY Deenan, MANLEY Ed, COX Ingemar J., HEYMANN David, JOHNSON Anne M., MCKENDRY Rachel A., "Digital technologies in the public-health response to COVID-19", *Nature Medicine*, https://www.nature.com/articles/s41591-020-1011-4, accessed 24-02-2021.
[307] YANG Fang, HEEMSBERGEN Luke, FORDYCE Robbie, 2021, "Comparative analysis of China's Health Code, Australia's COVIDSafe and New Zealand's COVID Tracer Surveillance Apps: a new corona of public health governmentality?", *Media International Australia*, Vol. 178, Issue 1, p. 186; CONG Wanshu, 2021, "From Pandemic Control to Data-Driven Governance: The Case of China's Health Code", *Frontiers in Political Science*, Vol. 3, pp. 3-4.

whose functions seem to be derived from DingTalk's monitoring of workers' health records, which was integrated into the leading mobile payment platform Alipay.[308] Similarly, Tencent's Health Code was implemented in instant-messaging and social media super-application WeChat. These two are the most popular applications in China, with 1,005 million monthly active users for WeChat and 845 million monthly active users of Alipay reported in 2021.[309] In the following months, many local governments implemented their own versions of the Health Code, which was nonetheless integrated either on WeChat or Alipay.

Health codes are small file size programs which have been automatically integrated in the Alipay and WeChat applications, leaving users unable to uninstall them without abandoning the two applications altogether.[310] Although there is very little official information relating to how these applications work and manage data, a number of articles report that these programs' location tracking feature is powered through GPS and information collected about an individual's location, city name and ID number is then sent to a central server.[311]

[312]

The three colors displayed by Alipay's Health Code implemented in the municipality of Hangzhou: green enables citizens to travel and access public places, yellow requests 7-day mandatory quarantine, and red requests 14-day mandatory quarantine.

[308] YANG Fang, HEEMSBERGEN Luke, FORDYCE Robbie, 2021, "Comparative analysis of China's Health Code, Australia's COVIDSafe and New Zealand's COVID Tracer Surveillance Apps: a new corona of public health governmentality?", *Media International Australia*, Vol. 178, Issue 1, p. 186
[309] CURRY David, "Most Popular Apps (2022)", *Business of Apps*, https://www.businessofapps.com/data/most-popular-apps/, accessed 01-02-2022.
[310] YANG Fang, HEEMSBERGEN Luke, FORDYCE Robbie, 2021, "Comparative analysis of China's Health Code, Australia's COVIDSafe and New Zealand's COVID Tracer Surveillance Apps: a new corona of public health governmentality?", *Media International Australia*, Vol. 178, Issue 1, p. 186
[311] MOZUR Paul, ZHONG Raymond, KROLIK Aaron, "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags", *The New York Times*, https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html, accessed 10-03-2021; LIANG Fan, 2020, "COVID-19 and Health Code: How Digital Platforms Tackle the Pandemic in China", *Social Media + Society*, Vol. 6, Issue 3, pp. 1-4.
[312] "全国版健康码，来了！", *Quánguó bǎn jiànkāng mǎ, láile!,* https://mp.weixin.qq.com/s/amB7fBxLw8KSR9DcUsbTWg, accessed 01-02-2022.

These applications generate a Quick-Response (QR) Code to every user that determines the risk exposure to the virus and assigns a color which dictates its freedom of movement: a green code enables a user to move freely through public areas, while yellow and red require self-isolation and quarantine from 7 up to 14 days, either at home or at a designated facility.[313] The Health Codes pool different data sources together in order to extrapolate the risk level of contracting the virus and converting it into a colored QR code:

1. Self-reported personal and health information from the user: the user is requested to enter its personal information upon registration, comprising name, gender, cellphone number, national ID number, home address, and travel history (usually of the last 14 days).[314] Additionally, users have to complete a health survey with their physical condition (if they experienced symptoms like tiredness, fever, dry cough) and if they have come into contact with Covid-19 confirmed patients.[315] Health status surveys have to be updated every day, if not, a green code will turn yellow after a few days, and for people with yellow and red codes, consecutive reporting of a healthy status has to be provided for 7 up to 14 days in order for the code to turn green;[316]

2. Location and travel data: precise location data is collected through GPS receivers present in mobile phones which transmit a signal to GPS satellites, which provide the exact longitude and latitude coordinates of an individual's location and consequent movements.[317] Population mobility is also assessed through the scanning of QR Codes in public avenues such as public transport, public institutions, schools, airports, restaurants, hotels, and grocery stores; and in high-risk areas, QR Codes are scanned even when leaving the grid-based residential compound.[318] This permits the collection of the so called "Origin-Destination matrices", which can assess not only population

[313] LIANG Fan, 2020, "COVID-19 and Health Code: How Digital Platforms Tackle the Pandemic in China", *Social Media + Society*, Vol. 6, Issue 3, pp. 1-2.
[314] "Regulating electronic means to fight the spread of COVID-19: Argentina, Australia, Brazil, China, England, European Union, France, Iceland, India, Iran, Israel, Italy, Japan, Mexico, Norway, Portugal, Russian Federation, South Africa, South Korea, Spain, Taiwan, Turkey, United Arab Emirates." *The Law Library of Congress, Global Research Directorate*, https://www.loc.gov/item/2020714995/, accessed 10-02-2021.
[315] *Ibidem*; LIANG Fan, 2020, "COVID-19 and Health Code: How Digital Platforms Tackle the Pandemic in China", *Social Media + Society*, Vol. 6, Issue 3, pp. 1-2.
[316] CONG Wanshu, 2021, "From Pandemic Control to Data-Driven Governance: The Case of China's Health Code", *Frontiers in Political Science*, Vol. 3, p. 4.
[317] CHOWDHURY Mohammad Jabed Morshed, FERDOUS Md Sadek, BISWAS Kamanashish, CHOWDHURY Niaz, MUTHUKKUMARASAMY Vallipuram, 2020, "COVID-19 Contact Tracing: Challenges and Future Directions", *IEEE Access*, Vol. 8, pp. 225704-225705.
[318] LIANG Fan, 2020, "COVID-19 and Health Code: How Digital Platforms Tackle the Pandemic in China", *Social Media + Society*, Vol. 6, Issue 3, p. 2.

mobility but also the efficacy and impact of travel restrictions implemented in certain areas;[319]

3. Externally pooled data: multiple data sources are collected from the public transportation system, telecommunication operators and from banking and financial firms, even though there hasn't been any official declaration about the exact data sources.

The Health Code system has not been officially deemed as mandatory by governmental authorities, however due to the fact that Chinese citizens are required to scan the code to access most public places, and in some cases even to leave their residential compounds, it has become indispensable for day-to-day necessities.[320] That certainly contributes to its wide adoption rate and public acceptance: Health Codes implemented by local and provincial governments of more than 200 Chinese cities were developed in collaboration with Tencent and Alibaba and third-parties ICT firms.[321]

Another factor that contributed to the success and expansion of Health Code programs during the most sever phases of the pandemic in China is its successful integration with the community-based "grid closed management system". In Wuhan for example, the population was divided into grids and each Health QR Code assigned a user to a community grid for monitoring, with designated community correspondents which were empowered to conduct door-to-door health surveys, check QR Codes at the entrance and exit of community grids, coordinating essential goods supply and arranging transport to hospitals and quarantine centers.[322] Moreover, Health Codes have been linked to the provision of other public health services: for example, by providing the service of booking doctor appointments and psychological assistance through the app.[323]

---

[319] OLIVER Nuria, LEPRI Bruno, STERLY Harald, LAMBIOTTE Renaud, DELETAILLE Sébastien, DA NADAI Marco, LETOUZÉ Emmanuel, ALI SALAH Albert, BENJAMINS Richard, CATTUTO Ciro, COLIZZA Vittoria, DE CORDES Nicolas, FRAIBERGER Samuel P., KOEBE Till, LEHMANN Sune, MURILLO Juan, PENTLAND Alex, PHAM Phuong N., PIVETTA Frédéric, SARAMAKI Jari, SCARPINO Samuel V., TIZZONI Michele, VERHULST Stefaan, VINCK Patrick, 2020, "Mobile phone data for informing public health actions across COVID-19 pandemic life cycle", *Science Advances*, Vol. 6, Issue 23, p. 3.
[320] "Regulating electronic means to fight the spread of COVID-19: Argentina, Australia, Brazil, China, England, European Union, France, Iceland, India, Iran, Israel, Italy, Japan, Mexico, Norway, Portugal, Russian Federation, South Africa, South Korea, Spain, Taiwan, Turkey, United Arab Emirates." *The Law Library of Congress, Global Research Directorate*, https://www.loc.gov/item/2020714995/, accessed 10-02-2021.
[321] CONG Wanshu, 2021, "From Pandemic Control to Data-Driven Governance: The Case of China's Health Code", *Frontiers in Political Science*, Vol. 3, p. 4.
[322] BOEING Philipp, WANG Yihan, 2021, "Decoding China's COVID-19 'virus exceptionalism': Community-based digital contact Tracing in Wuhan", *R&D Management,* Vol. 51, Issue 4, pp. 344-345.
[323] CONG Wanshu, 2021, "From Pandemic Control to Data-Driven Governance: The Case of China's Health

These Chinese contact-tracing applications do present major shortcomings, especially due to the lack of transparency on which data and how it is collected, who owns the data and under which conditions data is retained or transferred. Chinese citizens are not explicitly notified how the system works to assign the colors, and the color changes without any explanation from the app. Since Health Codes relied on local and provincial implementation when they first were issued, this led to a lack of standardization, with Health Codes issued in a province or city not working in another, and with each Health Code having different parameters and data sources to assess the risk level of an individual, so that individuals who were assigned a green code in an area turned to yellow or red in another.[324] The inconsistencies between different Health Codes were even more evident as there was lack of coordination between Alibaba and Tencent, which in turn led a fiery competition for the diffusion of their own systems, causing technical problems to users when switching from one application to another.[325]

A first national Health Code system was embedded in WeChat in February 2020, nonetheless as of today there is still no single Health Code program consistently adopted throughout China.[326] After three national standard were issued in April 2020, rules for standardization were set. For example, even though many Health Codes are developed and run by different third-parties ICT firms, WeChat has currently integrated them in a single platform contained in the mini-program of Tencent Healthcare (腾讯健康, *Téngxùn jiànkāng*).

Interface of Tencent Healthcare mini program that can be found in WeChat. In red the Epidemic Prevention Health Code.[327]

Code", *Frontiers in Political Science*, Vol. 3, p. 6.
[324] *Ibidem*, pp. 7-8.
[325] TAN Shining, "China's Novel Health Tracker: Green on Public Health, Red on Data Surveillance", *Center for Strategic & International Studies*, https://www.csis.org/blogs/trustee-china-hand/chinas-novel-health-tracker-green-public-health-red-data-surveillance, accessed 01-02-2022.
[326] CONG Wanshu, 2021, "From Pandemic Control to Data-Driven Governance: The Case of China's Health Code", *Frontiers in Political Science*, Vol. 3, p. 7.
[327] Image source: screenshot taken on 02-02-2022 in WeChat personal account.

This program enables individuals to access many public health services, such as booking medical appointments, physical examinations, booking vaccines and nucleic acid testing by registering electronically their health and social security cards. By accessing this program, it is also possible to register for the Epidemic Prevention Health Code, which lets the person choose the province and city and consequently leads to the provincial or municipal Health Code issued there.

Interface of the registration page of the Epidemic Prevention Health Code. Example of the Shenzhen Health Code.[328]

3.3.1. Communication Big Data Itinerary Card App

On the same day the World Health Organization declared the Covid-19 emergency a "global pandemic" (11 March 2020), the Ministry of Industry and Information Technology, alongside the China Academy of Information and Communications Technology (CAICT) and China

[328] Image source: screenshot taken on 02-02-2022 in WeChat personal account.

Telecom, China Unicom, and China Mobile launched the "Communication Big Data Itinerary Card" (通信大数据行程卡, *Tōngxìn dà shùjù xíngchéng kǎ*).[329]

When this application was first issued, it had similar functionality to the Health Codes, as it displayed a green, yellow, or red symbol (not a QR Code) according to the provinces and cities visited in the last 14 days for more than 4 hours. Accessing the application only requires however the phone number of the user and a verification code, and to consent to access the travel history of the user and does not claim to collect the ID card number, home address or other personal information of the user, configuring itself as a more privacy-preserving contact tracing application. [330]

[331]

The application was not only released on WeChat but also on Android and iOS app stores.[332] A Bluetooth-based close contact reminder function was added in an updated version of the app, so that if an individual who has been in close contact with a user is diagnosed as a confirmed or suspected patient of new coronary pneumonia virus, a reminder on the application will inform the user to observe isolation or quarantine.[333] The Itinerary Card App has been mainly used to help users who have returned to work to prove the areas they have visited recently, and has been used in combination with Health Code applications than as an alternative to them.

[329] "How can I prove that I have not been to any epidemic-stricken region or country in the past 14 days? Check this!", http://english.www.gov.cn/news/topnews/202003/11/content_WS5e685fefc6d0c201c2cbe087.html, accessed 03-02-2022.
[330] *Ibidem*.
[331] *Ibidem*.
[332] YANG Fang, HEEMSBERGEN Luke, FORDYCE Robbie, 2021, "Comparative analysis of China's Health Code, Australia's COVIDSafe and New Zealand's COVID Tracer Surveillance Apps: a new corona of public health governmentality?", *Media International Australia,* Vol. 178, Issue 1, pp. 187-188.
[333] "通信大数据行程卡使用指南", *Tōngxìn dà shùjù xíngchéng kǎ shǐyòng zhǐnán*, https://xc.caict.ac.cn/help.html, accessed 03-02-2022.

3.4. Data Privacy Concerns of Digital Contact-Tracing in China

Digital Contact-Tracing Applications in China have been widely accepted and utilized by the public, despite the privacy concerns that the implementation of such applications has raised in the international community.

In this section, three main issues related to privacy and data privacy of the Health Code Applications are analyzed:

1. Digital technologies used to develop the Health Code: the way Health Codes are constructed is different from the majority of contact-tracing applications developed in other countries, which are based on privacy-preserving frameworks that utilize Bluetooth and decentralized servers. The use of GPS and the collection of personal information in a central server by Health Codes, on the other hand, constitute a major threat to the privacy of Chinese citizens as it gives the Chinese Government much leeway to expand its surveillance powers and control on the population and at the same time grants private tech companies the opportunity to grasp even more in-depth sensitive personal information of its users, especially in face of the real-name registration system.

2. Data privacy principles behind Health Codes: these programs have been criticized for the lack of transparency and standardization between different provinces and cities, that have led to many data leakage incidents. Questions on the efficiency of digital contact tracing, on data security and data ownership, and issues on data retention, storage and data sharing with government and third parties have also been raised.

3. Possible expansion and normalization of Health Codes after the pandemic: there have been proposals of integration of Health Code systems in public governance even after the end of the Covid-19 emergency, especially related to the expansion of smart city campaigns and the Social Credit System.

3.4.1 Data-driven Approach of Chinese Contact-Tracing Applications

According to Fahey, two different approaches have surfaced in the development of Digital Contact-Tracing Applications around the world: a data-driven approach and a privacy-preserving approach.[334] The majority of the contact tracing applications today lean towards this second approach, which allows individuals to be notified if they come in contact with confirmed patients while not storing their movements and contact logs into a central server, but directly onto their mobile phones.[335] Many privacy-preserving protocols have been devised at the international level, such as the Decentralized Privacy-Preserving Proximity Tracing (DP3T), the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) and Google-Apple's Exposure Notification (GAEN), all based on Bluetooth proximity tracing.[336]

Bluetooth and decentralized servers are the preferred technology when developing digital contact-tracing tools not only because of their efficiency, but also because they are considered less privacy-intrusive. Bluetooth Low Energy (BLE) only tracks the proximity between two devices and does not capture the absolute location of an individual, so when an individual comes into contact with one another, an identifier (usually anonymous) is exchanged between devices. However, the place where the interaction has happened is not revealed, so it's not possible for government departments and health agencies to reconstruct precise location and movements.[337] The identifiers exchanged are encrypted in the user's phone and cannot be either viewed or transmitted to anybody and are automatically deleted when epidemiologically unimportant.[338] If a person is diagnosed with Covid-19, decentralized applications upload only the information of this specific user on a backend server, while the proximity history of the user remains stored in its phone, so the server does not collect information about the individuals the confirmed patient has come in contact with. The server will then send a notification to all individuals that have the confirmed patient's identifier stored in their phones, allowing them to know they have come in contact with an infected individual.[339]

---

[334] FAHEY Robert A., HINO Airo, 2020, "Covid-19, digital privacy, and the social limits on data-focused public health responses", *International Journal of Information Management*, Vol 55, Special Issue, p. 2.
[335] *Ibidem*.
[336] CHOWDHURY Mohammad Jabed Morshed, FERDOUS Md Sadek, BISWAS Kamanashish, CHOWDHURY Niaz, MUTHUKKUMARASAMY Vallipuram, 2020, "COVID-19 Contact Tracing: Challenges and Future Directions", IEEE Access, Vol. 8, pp. 225709-225710.
[337] *Ibidem*, p. 225705.
[338] "National COVID-19 contact tracing apps", *Policy Department for Economic, Scientific and Quality of Life Policies – European Parliament*, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652711/IPOL_BRI(2020)652711_EN.pdf, accessed 04-02-2022.
[339] *Ibidem*.

Chinese Health Codes on the other hand, despite their opaqueness as the protocols they are based on have not been shared with the public, lean towards a more data-driven approach as they harness and store precise location and movement data collected through GPS, as well as self-reported health data and data mined and extracted from other sources into a central server.

GPS is able to record the absolute location (longitudinal and latitudinal coordinates) of an individual and its consequent interaction and proximity with other devices, even though its effectiveness is reduced indoors.[340] This enables authorities not only to assess general population movements but also to track specific infection clusters. GPS location data is usually combined with temporal data to assess if a user has entered a risky area and duration of its permanence. Health Codes pool precise location data and combine it with health information both reported from the user and data stored from "authoritative data owners" (权威数据拥有方，*Quánwēi shùjù yǒngyǒu fang*), such as health, transportation, mobile communications and financial institutions.[341] An enormous quantity of data is collected by the Health Codes in order to assess the risk exposure of each user, as the key to the effectiveness of these applications lies in data comparison and big data analysis.

When someone tests positive for Covid-19, all this data, including the user's contact history (basically, the information of all of the other users he came into contact with) is sent to a central server. According to an analysis of the New York Times on Alipay's Health Code, the application also alerts the authorities and share the data of infected, suspected patients and close contacts to relevant law enforcement agencies.[342] Moreover, each time the Health QR Code is scanned, information on the location is sent to the server, in order to better assess population movement. For example, if all the people on a bus scan their Health Code, and after that a confirmed case of a passenger on the bus occurs, other passengers on the bus will be able to be identified and found in time.[343] The collection and processing of such large amount of personal information not only raises questions related to data privacy protection and security, but also to

[340] CHOWDHURY Mohammad Jabed Morshed, FERDOUS Md Sadek, BISWAS Kamanashish, CHOWDHURY Niaz, MUTHUKKUMARASAMY Vallipuram, 2020, "COVID-19 Contact Tracing: Challenges and Future Directions", IEEE Access, Vol. 8, pp. 225704-225705.
[341] "《个人健康信息码》系列国家标准问答（FAQ）", *"Gèrén jiànkāng xìnxī mǎ" xìliè guójiā biāozhǔn wèndá (FAQ)*, http://www.cesi.cn/202005/6411.html, accessed 04-02-2022.
[342] MOZUR Paul, ZHONG Raymond, KROLIK Aaron, "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags", *The New York Times*, https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html, accessed 10-03-2021.
[343] 胡晓萌 HU Xiaomeng, 文贤庆 WEN Xianqing, 孙保学 SUN Baoxue, "*Jiànkāng mǎ de yǐnsī zhèngcè, hái yǒu nǎxiē gǎijìn kōngjiān*?", 健康码的隐私政策，还有哪些改进空间？, "What is the room for improvement in the privacy policy of the health code?", https://tech.sina.com.cn/roll/2020-03-16/doc-iimxyqwa0896942.shtml, accessed 05-02-2022.

what extent the application is used for prevention and control of the pandemic and not for the direct control of the population and the expansion of human surveillance network.

The epidemic has created huge potential for the Chinese digital tech companies to embed themselves even more into its citizens' private life. Chinese citizens need to register to social media and communication platforms whit their real name and ID, and digital platforms have at the same time the legal obligation to share data and technically support government agencies in safeguarding national and public security (Article 28 of Cybersecurity Law). The close collaboration between digital companies and the Chinese government is nothing new, but the Covid-19 emergency and the development of Health Code applications have further blurred the boundary between the two, to the extent that Cong argues that more than being a contact-tracing tool for epidemic control, Health Code is a technology of population and social control.[344]

3.4.2 Data Privacy Principles of Health Codes

Although the PRC Government has not established that Health Codes are mandatory in nature, they *de facto* are if considered that they are requested to access most public places and even to leave residential compounds in certain areas. This is a contrasting feature if we compare Health Codes with the majority of digital contact-tracing tools developed in other countries. Studies from both European Parliament's Department for Economic, Scientific and Quality of Life Policies and the Massachusetts Institute of Technology's Technology Review consider the Health Code programs to be obligatory.[345]

Health Codes have been criticized for their lack of transparency and standardization, that also make it difficult to assess the efficacy and efficiency of these applications. Neither Alibaba and Tencent nor other third-party ICT firms that developed the Health Codes have made their algorithms and protocols available to the public.[346] Technical problems, glitches, inaccuracies,

[344] CONG Wanshu, 2021, "From Pandemic Control to Data-Driven Governance: The Case of China's Health Code", *Frontiers in Political Science*, Vol. 3, pp. 1-2.
[345] "National COVID-19 contact tracing apps", *Policy Department for Economic, Scientific and Quality of Life Policies – European Parliament*, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652711/IPOL_BRI(2020)652711_EN.pdf, accessed 04-02-2022; JOHNSON Bobbie, "The Covid Tracing Tracker: What's happening in coronavirus apps around the world", *MIT Technology Review*, https://www.technologyreview.com/2020/12/16/1014878/covid-tracing-tracker#international-data, accessed 05-02-2022.
[346] VON CARNAP Kai, DRINHAUSEN Katja, SHI-KUPFER Kristin, "Tracing. Testing. Tweaking. Approaches to data-driven Covid-19 management in China", *Mercator Institute for China Studies (MERICS)*, https://merics.org/en/report/tracing-testing-tweaking, accessed 01-02-2022.

combined with the inability to access and correct their own personal information have led to public grievances and complaints about the Code in the first weeks of its implementation. Apart from the questionable accuracy of GPS location tracking, different Health Codes often lack mutual recognition and interoperability due to the fact that they are based on local algorithms and local data sources, some of which are also considered unreliable as they are self-reported by the user, and this ultimately undermines the applications' usefulness and efficacy.[347]

As a consequence, many personal data leaks have been reported since the implementation of Health Code applications, one of the most known has been the "Beijing Healthbao" (北京健康宝, *Běijīng jiànkāng bǎo*) incident occurred in December 2020, during which the photos, ID and nucleic acid tests of many celebrities collected through the app were leaked and sold on the Internet.[348]

Compared with the European Union's and United States' approach to the development of contact tracing applications, by which specific frameworks for protection of privacy and personal information have been devised prior to the implementation of such digital tools, the Chinese Central Government has given much leeway to provincial and municipal governments to implement their own digital tools for the prevention and control of the pandemic, which ultimately led to the development of Health Codes. Since the development and implementation of such digital tools started from the local level and was not mandated at the national level, privacy and personal information protection provisions have varied among the different Health Codes, notwithstanding the Notice issued by the CAC in February 2020. Only once Health Code applications gained traction through the country, the national government began the drafting of national standards for mutual recognition between different Health Codes and specific provisions for the protection of personal information, which nonetheless are recommendatory and not mandatory.[349]

According to researchers from the Shanghai Mana Data Technology Development Foundation, almost all of the Health Codes implemented in WeChat and Alipay did not have specific privacy

---

[347] *Ibidem*.

[348] "明星「健康寶」信息被泄露網上售賣　1元售1000藝人身分證號碼", *Míngxīng `jiànkāng bǎo'xìnxī bèi xièlòu wǎng shàng shòumài 1 yuán shòu 1000 yìrén shēnfèn zhèng hàomǎ*, https://news.mingpao.com/ins/%E5%85%A9%E5%B2%B8/article/20201228/s00004/1609148631862/%E6%98%8E%E6%98%9F%E3%80%8C%E5%81%A5%E5%BA%B7%E5%AF%B6%E3%80%8D%E4%BF%A1%E6%81%AF%E8%A2%AB%E6%B3%84%E9%9C%B2%E7%B6%B2%E4%B8%8A%E5%94%AE%E8%B3%A3-1%E5%85%83%E5%94%AE1000%E8%97%9D%E4%BA%BA%E8%BA%AB%E5%88%86%E8%AD%89%E8%99%9F%E7%A2%BC, accessed 05-02-2022.

[349] CONG Wanshu, 2021, "From Pandemic Control to Data-Driven Governance: The Case of China's Health Code", *Frontiers in Political Science*, Vol. 3, p. 8.

policies or user agreements upon registration.[350] Many of them were developed and implemented by relying on existing user agreements and standard privacy policy of the two super-applications.[351] Though the policies of both Alipay and WeChat are fully disclosed to the public, a user must navigate a variety of agreements across all Alibaba affiliates, such as Ant Financial and Alipay, or WeChat and Tencent, in order to be able to fully understand privacy obligations and user's rights related to the collection and processing of its personal information. The connection between WeChat and Alipay in order to mutually recognize different Health Codes implemented on their platforms additionally adds a degree to opacity on how data is managed and shared between the two.[352] Alipay additionally has no clear prohibition on secondary data usage, as Alipay's data are openly shared between Alibaba affiliates.[353]

The three recommendatory standards published in April 2020 partially provided clarifications on the data privacy principles that Health Code applications should be following. The recommendatory standards refer to the PI Security Specification of 2020 for the protection of personal data in Health Code applications, by requiring expressed informed consent and purpose limitation to the collection and processing of pandemic-related information (which nonetheless comprise a wide variety of personal information, location and travel information, health biometric information and even payment information).[354] The standards also require encryption and storage of such data with the establishment of a data security protection system and the implementation of relevant data security technical measures.[355]

Comparative studies of digital contact-tracing applications of multiple countries have however highlighted the problems of personal data protection that Health Codes raise. The MIT Technology Review's Covid Tracing Tracker, which assesses contact-tracing applications on the basis of their voluntary nature, limited collection, data destruction, data minimization and

[350] 胡晓萌 HU Xiaomeng, 文贤庆 WEN Xianqing, 孙保学 SUN Baoxue, "*Jiànkāng mǎ de yǐnsī zhèngcè, hái yǒu nǎxiē gǎijìn kōngjiān?",* 健康码的隐私政策，还有哪些改进空间？, "What is the room for improvement in the privacy policy of the health code?", https://tech.sina.com.cn/roll/2020-03-16/doc-iimxyqwa0896942.shtml, accessed 05-02-2022.
[351] VON CARNAP Kai, DRINHAUSEN Katja, SHI-KUPFER Kristin, "Tracing. Testing. Tweaking. Approaches to data-driven Covid-19 management in China", *Mercator Institute for China Studies (MERICS)*, https://merics.org/en/report/tracing-testing-tweaking, accessed 01-02-2022.
[352] BOUDREAUX Benjamin, DENARDO Matthew A., DENTON Sarah W., SANCHEZ Ricardo, FEISTEL Katie, DAYALANI Hardika, 2020, *Data Privacy During Pandemics - A Scorecard Approach for Evaluating the Privacy Implications of COVID-19 Mobile Phone Surveillance Programs*, RAND Corporation, Santa Monica, Calif, pp. 117-118.
[353] *Ibidem*.
[354] "《个人健康信息码》系列国家标准问答（FAQ）", *Gèrén jiànkāng xìnxī mǎ" xìliè guójiā biāozhǔn wèndá (FAQ)*, http://www.cesi.cn/202005/6411.html, accessed 04-02-2022.
[355] *Ibidem*.

transparency provisions, rated China's Health Codes 0 stars out of 5, even if it's not clear if this is because of the lack of official information published on the Code, as the article states.[356]

However, on the basis of both the CAC Notice on personal information protection issued in February 2020 and recommendations from the App Governance Working Group (which is part of the Cyberspace Administration of China), Von Carnap et al. argue that although data minimization of Health Codes is required, other provisions such as purpose limitation, temporary storage, transparency and security provisions are still only partially addressed, while there is no relevant restriction of data sharing with authorities and other departments.[357] Moreover, a specific study on Alipay's Health Codes show that the application "openly shares data with law enforcement, insurers, government authorities, banks, and a variety of other recipients".[358] What is most concerning is that the application clearly states that data will be retained as long as necessary, and there is no clear provision on deletion of such information even after the individual stops using the service.[359]

3.4.3 Possible Future Expansion of Health Code Applications in Post-Covid China

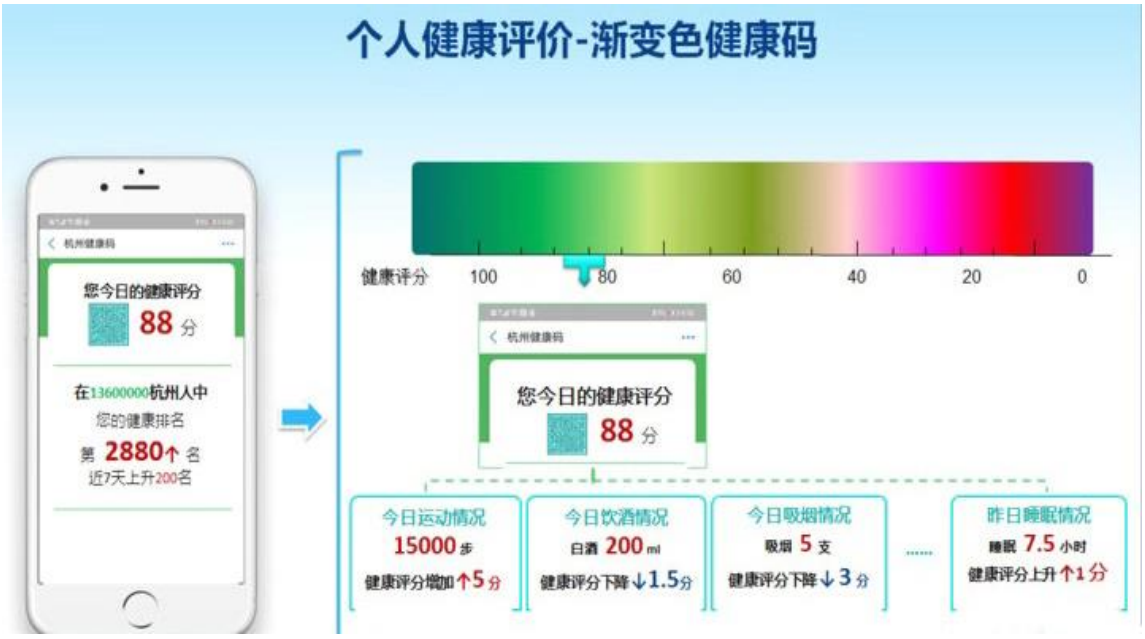
While many contact-tracing applications have automated the process of deleting personal information and data after a certain period of time, China not only notoriously lacks precise provisions on Health Codes data storage limitations and retention, but many local governments have begun exploring possible integration and expansion of the Health Code functionalities in other realms.

One of the most controversial proposals has been advanced by the Hangzhou municipal government on May 22, 2020. The Hangzhou Health Code application had already been

[356] JOHNSON Bobbie, "The Covid Tracing Tracker: What's happening in coronavirus apps around the world", *MIT Technology Review*, https://www.technologyreview.com/2020/12/16/1014878/covid-tracing-tracker#international-data, accessed 05-02-2022.
[357] VON CARNAP Kai, DRINHAUSEN Katja, SHI-KUPFER Kristin, "Tracing. Testing. Tweaking. Approaches to data-driven Covid-19 management in China", *Mercator Institute for China Studies (MERICS)*, https://merics.org/en/report/tracing-testing-tweaking, accessed 01-02-2022.
[358] BOUDREAUX Benjamin, DENARDO Matthew A., DENTON Sarah W., SANCHEZ Ricardo, FEISTEL Katie, DAYALANI Hardika, 2020, *Data Privacy During Pandemics - A Scorecard Approach for Evaluating the Privacy Implications of COVID-19 Mobile Phone Surveillance Programs*, RAND Corporation, Santa Monica, Calif, pp. 117-118.
[359] *Ibidem*.

included in its eHealth management platform integrated in WeChat, which connected citizens' health and social security cards and provided multiple services such as medical appointment registration and psychological assistance.[360]

The Hangzhou officials advanced the proposal to further expand the Health Code application with the creation of a "personal health index" (个人健康指数, *Gèrén jiànkāng zhǐshù*), suggesting replacing the three stoplight-like based coloring system with gradient coloring and a ranking system based on individuals' habits such as their level of exercise, drinking, smoking and even average sleeping hours.[361]



[362]

Example of the gradient color system devised by the Hangzhou administration and possible integration of the ranking system.

The possible normalization and expansion of Health Codes, and in particular the Hangzhou proposal has sparked controversy among the public and scholars, as this would further enhance the already broad collection and processing of its citizens' personal data.

Other local governments have also started to explore possible applications of Health Codes after the end of the pandemic. In a recent Q&A from Shanghai Government, it was announced that its "Suishen Health Code" (随申码, *Suí shēn mǎ*) would eventually "become the personal identification and service assistant of Shanghai citizens, as more data and application

[360] 姚佳莹 YAO Jiaying, "*Yìqíng hòu, jiànkāng mǎ kěfǒu shēngjí "quánnéng mǎ"?*", 疫情后，健康码可否升级"全能码"？, "After the epidemic, can the health code be upgraded to the "universal code"?", https://m.caijing.com.cn/api/show?contentid=4757152, accessed 06-02-2022.
[361] *Ibidem*.
[362] Image source: https://mp.weixin.qq.com/s/pKIM2f_FuEakp6LVctoS2g

services will be launched in the future".[363] In Guangzhou, a new "Suikang Health Code" (穗康码, *Suì kāng mǎ*) has been used as a real-name electronic identity certificate, and many other local government are exploring the potential use of Health Codes for hospital registration, traffic violation, business and personal situation declarations.[364]

There is still much controversy on the possible future of the Health Codes after the end of the pandemic. Many are in favor of a complete deletion of the personal information and usage of Health Codes after the end of the pandemic period. Notably, Robin Li, the CEO of Baidu, has raised its voice in favor of "creating a mechanism for deleting personal information collected during the pandemic".[365]

Even though the implementation of Health Code applications has opened new discussions in the realm of privacy and personal data protection, its possible normalization and integration in Chinese' citizens daily life still sparks the fear of social control and public surveillance. Furthermore, it provides digital companies with opportunities to further institutionalize their collaboration with the Chinese government, blurring the already thin line separating the two in regard to the collection and sharing of user's personal data. Digital and ICT companies, and especially Alibaba and Tencent, not only had a central role in technically implementing these technological tools, but also had active participation in establishing the regulatory standards both at the local level (in collaboration with Shenzhen and Hangzhou government) and at the national level, enhancing their bargaining power in influencing policy and law-making regarding the digital realm and collection and processing of information collected through these applications.

[363] 胡晓萌 HU Xiaomeng, 文贤庆 WEN Xianqing, 孙保学 SUN Baoxue, "*Jiànkāng mǎ de yǐnsī zhèngcè, hái yǒu nǎxiē gǎijìn kōngjiān?*", 健康码的隐私政策，还有哪些改进空间？, "What is the room for improvement in the privacy policy of the health code?", https://tech.sina.com.cn/roll/2020-03-16/doc-iimxyqwa0896942.shtml, accessed 05-02-2022.

[364] 姚佳莹 YAO Jiaying, "*Yìqíng hòu, jiànkāng mǎ kěfǒu shēngjí "quánnéng mǎ"?*", 疫情后，健康码可否升级"全能码"？, "After the epidemic, can the health code be upgraded to the "universal code"?", https://m.caijing.com.cn/api/show?contentid=4757152, accessed 06-02-2022.

[365] ZHONG Raymond, "China's Virus Apps May Outlast the Outbreak, Stirring Privacy Fears", *New York Times*, https://www.nytimes.com/2020/05/26/technology/china-coronavirus-surveillance.html, accessed 06-02-2022.

Conclusions

The development and implementation of digital contact-tracing applications in response to the Covid-19 pandemic has created new opportunities for digital and ICT private companies to further expand the collection and processing of sensitive biometric and geospatial information of Chinese citizens, and at the same time it has opened a new level of collaboration with local governments in preventing and monitoring pandemic trends with the sharing of user's data through these digital tools.

The integration of the so-called "Health Codes" (健康码, *Jiànkāng mǎ*) mini programs in Alibaba's and Tencent's super-applications Alipay and WeChat raised a number of issues related to privacy and personal information collection and processing and data sharing between private companies and the Chinese Government. Although the exact algorithms and protocols used to create the Health Codes remain unknown to the public, the collection of precise location and travel information through the use of GPS and the scanning of the generated QR codes in different public avenues, combined with user's self-reported personal and health information and data pooled and extracted from other sources, and the storage of such information of confirmed, suspected patients and their closed contacts into a central server renders the functionality of Health Codes very different from most of the contact-tracing applications developed in other foreign countries, which are mostly based on specific privacy-preserving protocols which utilize Bluetooth proximity tracing and prevents the storage of users' movements and contact logs into a central server, but store it directly onto users' mobile phones. The collection and processing of information gathered through Health Codes not only permits contact-tracing but is also used in order to assess the risk exposure of users and to automate the enforcement of quarantine measures on users deemed to be high-risk; moreover, as GPS pinpoints the exact location and movements of users, it is possible to use this information to track infection patterns and specific local clusters.

As the efficacy and accuracy of Health Codes applications not only relies on the quality of the data analysis and algorithms implemented but also on the quality of the information collected, this has in turn justified the collection and processing of information from "authoritative data

owners" such as health, transportation, mobile communications and even users' credit information from financial institutions, in order to verify the data declared by individuals.[366]

The development of Health Code applications started in February 2020 as a local initiative from Hangzhou and Shenzhen Governments, which have respectively collaborated with Alibaba and Tencent both in technically developing and implementing the applications and in devising specific local standards for collection and processing of personal information through these applications. Health Codes soon gained traction and expanded in other provinces and in other cities, where they were requested to enter almost all public places and even to leave residential compounds, becoming *de facto* mandatory. Only in April 2020, the national government issued three non-mandatory national standards that were developed in collaboration with many local governments, Alibaba, Tencent and other third-party ICT firms. These standards also provide for the collection and processing of personal information in Health Codes. Apart from these standards, the only specific legal instrument devised during the pandemic for the protection of personal information is a Notice issued by the Cyberspace Administration of China (CAC).

Compared to the attention given abroad to personal data collection and processing during the pandemic through the use of contact-tracing applications, especially in Europe and USA, in which specific protocols have been devised before developing and implementing these applications in order to protect the privacy of citizens and to ensure data minimization, limited collection, transparency and data destruction, the PRC has only issued non-mandatory legal instruments for the protection of personal information processed and collected during the pandemic. This has led to many Health Codes not having specific privacy policies but relying on the already existing policies and user agreements of Alipay and WeChat.

The many proposals of expanding the functionalities and usage of Health Codes even after the end of the Covid-19 emergency did not only raise questions on privacy and personal data protection and fear of public surveillance and social control but could also envisage a new level of collaboration between private digital technologies and governments in the realm of personal data collection, processing and sharing.

The creation and adoption of data-driven digital contact-tracing tools in combination with private digital firms in China has been possible also thanks to the special legal background on personal information protection that the PRC has been devising in these last decades. Personal information protection has been legislated as part of the protection of the right to privacy, which

[366] "《个人健康信息码》系列国家标准问答（FAQ）", *"Gèrén jiànkāng xìnxī mǎ" xìliè guójiā biāozhǔn wèndá (FAQ)*, http://www.cesi.cn/202005/6411.html, accessed 04-02-2022.

has been formally separated in the law from other personality rights at the beginning of the 21st century. Different laws, administrative and sectorial regulations have devised a general framework and principles for personal information protection that has generally covered the private sector, while partly leaving out and not extending the same provisions to public institutions. Moreover, the personal information protection framework in China has mainly evolved within a security context, making the safety of persons and property the main criterion, which led many laws and regulations focusing on devising the obligations of private sector entities instead of focusing on building a fundamental rights protection framework (as it happens for example in the European GDPR).[367] More recently, and especially after the update of the National People's Congress' five-year legislative plan in 2018, China has been shifting its view on privacy and personal data, by further distinguishing the two into separate legal regimes provided in the new Chinese Civil Code approved in 2020, and by leaning towards a more comprehensive approach on personal data protection with the issuing of the Personal Information Protection Law and the Data Security Law at the end of 2021.

Obligations and requirements for personal data protection devised in the private sector do present some specificities, that in turn allow the sharing of personal data with Chinese authorities under certain circumstances. Not only digital and ICT companies are required to technically assist authorities in order to safeguard national security and investigate criminal acts (Article 28 of Cybersecurity Law), but also have to put in place a real-name registration system by which users that access the Internet shall register with their real identity (by providing their ID). The last years have also seen new stringent requirements for data localization devised in the Cybersecurity Law and in the newly issued Personal Information Protection Law and Data Security Law, meaning that certain industries cannot transfer personal information collected within Chinese borders outside the Mainland without previous passing a security assessment by PRC authorities. All of these provisions, combined with the less stringent obligations and requirements devised for the public sector, facilitate more than hinder the access of the Chinese Government to private sector data. Health Codes represent both an opportunity for the Chinese Government to establish enhance and institutionalize the access to private sector data held by digital firms and at the same time represents an opportunity for these enterprises to embed themselves even more into the private life of Chinese citizens, as Health Codes, although implemented on private applications, share personal information of confirmed, suspected patients and close contacts to Chinese authorities.

[367] GELLER Anja, 2020, "How Comprehensive is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective", *GRUR International*, Vol. 69, Issue 12, p. 1195.

Acknowledgements

I would like to take this opportunity to express my gratitude to all people who supported and assisted me in the development of this paper, but also contributed to the incredible experiences that I had during my academic journey at Ca' Foscari University.

First and foremost, I would like to thank Professor Cavalieri, my thesis supervisor, for the patience and professionalism shown in advising me during every step of reviewing this paper.

I would have never had the possibility to reach this important objective without the precious support and advice of my parents, Elisabetta and Massimo. A special thanks to them that have been encouraging me to push through during the most tough times.

I wish to extend my special thanks to Luca, the love of my life, for always believing in me and pushing me to do more. For giving me a future, I could believe in and strive for. For always inspiring me and finding solutions to my problems. You are a work of art and truly are the person I admire the most. I could never thank you enough for the happiness you have given me in these eight years together.

This thesis couldn't have been possible without the support of Luca's family, which have welcomed me like a daughter. Thanks to Patrizia, who has always said nothing but kind words to me, and to Stefano, who is the most hardworking person I know, thanks for showing me that hard work pays off. I'd like to thank Alessandro, Luca's little brother, for always being a ray of sunshine and making everybody laugh even in the most tough situations. I extend my gratitude to Luca's uncles, aunts, cousins and grandparents, which always made me feel like home.

I would like to thank my grandparents, who I know are looking after me from up there.

Last but not least, a special thanks to all my precious friends, which I could not live without. Thanks to Ilaria, for all the laughter and joy you brought in my life, for all the pain and misfortune we have gone through together and made us stronger. Thanks to Alessia, who has been and always will be my friend of a lifetime. Thanks to Elena, a brave and kind-hearted soul, which showed me how to be strong in these tough times even though the pandemic hurt you more than anyone. Thanks to Elisa, for all the conversations and laugh and anime memes. A special thanks to Maria, Simone, Silvia, Luca and Simone, for all our nights out and joy you brought me. Thanks to all the friends I've met at 'Ca Foscari, which have made my experience

in Venice unforgettable: Paola, Laura, Giulia, Giorgia etc. Finally, I would like to thank my cat Mulan, for trying to contribute to this paper by leaving numbers and exclamation points whenever the laptop was left unattended.

Bibliography

BOEING Philipp, WANG Yihan, 2021, "Decoding China's COVID-19 'virus exceptionalism': Community-based digital contact Tracing in Wuhan", *R&D Management*, Vol. 51, Issue 4, pp. 339-351.

BOUDREAUX Benjamin, DENARDO Matthew A., DENTON Sarah W., SANCHEZ Ricardo, FEISTEL Katie, DAYALANI Hardika, 2020, *Data Privacy During Pandemics - A Scorecard Approach for Evaluating the Privacy Implications of COVID-19 Mobile Phone Surveillance Programs*, RAND Corporation, Santa Monica, Calif.

CHANDER Anupam, LÊ Uyên, 2015, "Data Nationalism", *Emory Law Journal*, Vol. 64, Issue 3, pp. 667-739.

CHEN Dingding, 2005, "Explaining China's Changing Discourse on Human Rights, 1978-2004", *Asian Perspective*, Vol. 29, No. 3, pp. 155-182.

CHOWDHURY Mohammad Jabed Morshed, FERDOUS Md Sadek, BISWAS Kamanashish, CHOWDHURY Niaz, MUTHUKKUMARASAMY Vallipuram, 2020, "COVID-19 Contact Tracing: Challenges and Future Directions", *IEEE Access*, Vol. 8, pp. 225703-225729.

CONG Wanshu, 2021, "From Pandemic Control to Data-Driven Governance: The Case of China's Health Code", *Frontiers in Political Science*, Vol. 3, pp. 1-14.

CUI Shujie, QI Peng, 2021, "The legal construction of personal information protection and privacy under the Chinese Civil Code", *Computer Law & Security Review*, Vol. 41, Art. 105560, pp. 1-17.

FAHEY Robert A., HINO Airo, 2020, "Covid-19, digital privacy, and the social limits on data-focused public health responses", *International Journal of Information Management*, Vol 55, Special Issue, pp. 1-5.

FENG Yang 2019, "The future of China's Personal Data Protection Law: challenges and prospects", *Asia Pacific Law Review*, Vol. 27, Issue 1, pp. 62-82.

FU Tao, 2019, "China's personal information protection in a data-driven economy: A privacy policy study of Alibaba, Baidu and Tencent", *Global Media and Communication*, Vol. 15, Issue 2, pp. 195-213.

GELLER Anja, 2020, "How Comprehensive is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective", *GRUR International*, Vol. 69, Issue 12, pp. 1191-1203.

GELLERT Raphaël, GUTWIRTH Serge, 2013, "The legal construction of privacy and data protection", *Computer Law & Security Review*, Vol. 29, Issue 5, pp. 522-530.

GREENLEAF Graham, 2012, “China’s Internet Data Privacy Regulations 2012: 80% of a Great Leap Forward?”, *Privacy Laws & Business International Report*, Issue 116, pp. 1-5.

GREENLEAF Graham, 2013, “Data Protection Widened by China’s Consumer Law Changes”, *Privacy Laws & Business International Report*, Vol. 126, pp. 127-128.

GREENLEAF Graham, 2014, *Asian Data Privacy Laws*, New York, Oxford University Press.

GREENLEAF Graham, LIVINGSTON Scott, 2016, “China's New Cybersecurity Law – Also a Data Privacy Law?”, *Privacy Laws & Business International*, Issue 144, pp. 1-11.

HSU Kimberly, MURRAY Craig, 2014, “China and International Law in Cyberspace”, *U.S.-China Economic and Security Review Commission Staff Report*, pp. 1-11.

KOKOTT Juliane, SOBOTTA Christoph, 2013, “The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR”, *International Data Privacy Law*, Vol. 3, No.4, pp. 222-228.

LEE Jyh-An, 2018, “Hacking into China’s Cybersecurity Law”, *Wake Forest Law Review*, Vol. 53, No. 1, pp. 57-104.

LEE Jyh-An, LIU Ching-Yi, 2016, “Real-Name Registration Rules and the Fading Digital Anonymity in China”, *Washington International Law Journal*, Vol. 25, No. 1, pp. 1-34.

LI Yuxiao, XU Lu, 2015, “China’s Cybersecurity Situation and the Potential for International Cooperation”. In LINDSAY Jon R., CHEUNG Tai Ming, REVERON Derek S., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, New York: Oxford University Press, pp. 225-240.

LI Tiffany, BRONFMAN Jill, ZHOU Zhou, 2017, “Saving Face: Unfolding the Screen of Chinese Privacy Law”, *Journal of Law, Information, and Science (Forthcoming)*, pp. 1-33.

LI Yongjun 李永军, 2017, “*Lùn “mínfǎ zǒngzé” zhōng gèrén yǐnsī yǔ xìnxī de “èr yuán zhì” bǎohù jí qǐngqiú quán jīchǔ*”, 论《民法总则》中个人隐私与信息的 “二元制” 保护及请求权基础（The Research on the “Dual System” Protection and Claim Basis of the Personal Privacy and Information in The General Principles of Civil Law), 浙 江 工 商 大 学 学 报 *Journal of Zhejiang Gongshang University*, Vol. 31 (3), pp. 10-21.

LIANG Fan, 2020, “COVID-19 and Health Code: How Digital Platforms Tackle the Pandemic in China”, *Social Media + Society*, Vol. 6, Issue 3, pp. 1-4.

LU Guangyu, RAZUM Oliver, JAHN Albrecht, ZHANG Yuying, SUTTON Brett, SRIDHAR Devi, ARIYOSHI Koya, VON SEIDLEIN Lorenz, MÜLLER Olaf, 2021, “COVID-19 in Germany and China: mitigation versus elimination strategy”, *Global Health Action*, Vol. 14, Issue 1, Article N. 1875601, pp. 1-11.

MCDOUGALL Bonnie S., 2004, "Privacy in Modern China", *History Compass*, Vol. 2, Issue 1, pp. 1-8.

OLIVER Nuria, LEPRI Bruno, STERLY Harald, LAMBIOTTE Renaud, DELETAILLE Sébastien, DA NADAI Marco, LETOUZÉ Emmanuel, ALI SALAH Albert, BENJAMINS Richard, CATTUTO Ciro, COLIZZA Vittoria, DE CORDES Nicolas, FRAIBERGER Samuel P., KOEBE Till, LEHMANN Sune, MURILLO Juan, PENTLAND Alex, PHAM Phuong N., PIVETTA Frédéric, SARAMAKI Jari, SCARPINO Samuel V., TIZZONI Michele, VERHULST Stefaan, VINCK Patrick, 2020, "Mobile phone data for informing public health actions across COVID-19 pandemic life cycle", *Science Advances*, Vol. 6, Issue 23, pp. 1-6.

ONG Rebecca, 2012, "Online vigilante justice Chinese style and privacy in China", *Information & Communications Technology Law*, Vol. 21, Issue 2, pp. 127-145.

POLLPETER Kevin, 2015, "Chinese Writings on Cyberwarfare and Coercion". In LINDSAY Jon R., CHEUNG Tai Ming, REVERON Derek S., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, New York: Oxford University Press, pp. 138-157.

SOLOVE Daniel J., 2008, *Understanding Privacy*, Cambridge, Harvard University Press.

TIMOTEO Marina, 2019, "China Codifies. The First Book of the Civil Code between Western Models to Chinese Characteristics", *Opinio Juris in Comparatione*, Vol.1, Issue 1, pp. 51-72.

WANG Faye Fangfei, 2014, *Law of Electronic Commercial Transactions – Contemporary Issues in the EU, US, and China*, London, Routledge.

WANG Hao, 2011, *Protecting Privacy in China, A Research on China's Privacy Standards and the Possibility of Establishing the Right to Privacy and the Information Privacy Protection Legislation in Modern China*, Springer-Verlag Berlin Heidelberg.

WANG Liming, 2019, "The modernization of Chinese civil law over four decades", *Frontiers of Law in China*, Vol. 14, Issue 1, 39-72.

WANG Zhizheng, 2017, "Systematic Government Access to Private-Sector Data in China". In CATE Fred H., DEMPSEY James X., *Bulk Collection: Systematic Government Access to Private-Sector Data*, New York: Oxford University Press, pp. 241-258.

WEBER Philip Andreas, ZHANG Nan, WU Haiming, 2020, "A comparative analysis of personal data protection regulations between the EU and China", *Electronic Commerce Research*, Issue 20, pp. 565-587.

WU Jun, WANG Jian, NICHOLAS Stephen, MAITLAND Elizabeth, FAN Qiuyan, 2020, "Application of Big Data Technology for COVID-19 Prevention and Control in China: Lessons and Recommendations", *Journal of Medical Internet Research*, Vol. 22, Issue 10, pp. 1-16.

XU Jinghong, 2015, “Evolving Legal Frameworks for Protecting the Right to Internet Privacy in China”. In LINDSAY Jon R., CHEUNG Tai Ming, REVERON Derek S., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, New York: Oxford University Press, pp. 242-260.

YAO-HUAI Lü, 2005, “Privacy and data privacy issues in contemporary China”, *Ethics and Information Technology*, Issue 7, pp. 7-15.

YANG Fan, XU Jian, 2018, “Privacy concerns in China's smart city campaign: The deficit of China's Cybersecurity Law”, *Asia and the Pacific Policy Studies*, Vol. 5, Issue 3, pp. 533-543.

YANG Fang, HEEMSBERGEN Luke, FORDYCE Robbie, 2021, “Comparative analysis of China’s Health Code, Australia’s COVIDSafe and New Zealand’s COVID Tracer Surveillance Apps: a new corona of public health governmentality?”, *Media International Australia,* Vol. 178, Issue 1, pp. 182-197.

ZANIN Mark, XIAO Cheng, LIANG Tingting, LING Shiman, ZHAO Fengming, HUANG Zhenting, LIN Fangmei, LIN Xia, JIANG Zhanpeng, WONG Sook-San, 2020, “The public health response to the COVID-19 outbreak in mainland China: a narrative review”, *Journal of Thoracic Disease*, Vol. 12, Issue 8, pp. 4434–4449.

ZHAO Bo, FENG Yang, 2021, “Mapping the development of China’s data protection law: Major actors, core values, and shifting power relations”, *Computer Law & Security Review*, Vol. 40, pp. 1-16.

ZHANG Lu, 2021, “Personal information of privacy nature under Chinese Civil Code”, *Computer Law & Security Review*, Vol. 43, pp. 1-13.

Webliography

“中华人民共和国宪法”, *Zhōnghuá rénmín gònghéguó xiànfǎ*, http://www.gov.cn/guoqing/2018-03/22/content_5276318.htm, accessed 01-10-2021. English Official Translation: http://www.npc.gov.cn/englishnpc/constitution2019/201911/1f65146fb6104dd3a2793875d19b5b29.shtml, accessed 01-10-2021.

“中华人民共和国民法通则-1986”, *Zhōnghuá rénmín gònghéguó mínfǎ tōngzé*, https://www.pkulaw.com/chl/4202520b3be0ae24bdfb.html?keyword=%E6%B0%91%E6%B3%95%E9%80%9A%E5%88%99, accessed 15-10-2021. English Translation: “General Principles of the Civil Law of the People's Republic of China - 1986”, https://www.pkulaw.com/en_law/4202520b3be0ae24bdfb.html, accessed 15-10-2021.

“中华人民共和国民法总则- 2017”, *Zhōnghuá rénmín gònghéguó mínfǎ zǒngzé*, https://www.pkulaw.com/chl/c6f2d80ee8c0c709bdfb.html, accessed 16-10-2021. English Translation: “General Provisions of the Civil Law of the People's Republic of China - 2017”, https://www.pkulaw.com/en_law/c6f2d80ee8c0c709bdfb.html, accessed 16-10-2021.

“中华人民共和国刑法(1997修订)”, *Zhōnghuá rénmín gònghéguó xíngfǎ (1997 xiūdìng)*, https://www.pkulaw.com/chl/9ec4004a183a7d8cbdfb.html, accessed 18-10-2021. English Translation: “Criminal Law of the People's Republic of China (1997 Revision)”, https://www.pkulaw.com/en_law/9ec4004a183a7d8cbdfb.html?keyword=criminal%20law%201997, accessed 18-10-2021.

“中华人民共和国刑法修正案(七)”, *Zhōnghuá rénmín gònghéguó xíngfǎ xiūzhèng àn (qī)*, https://www.pkulaw.com/chl/e9381f0afa80a487bdfb.html, accessed 19-10-2021. English Official Translation: “Amendment VII to the Criminal Law of the People's Republic of China”, http://www.npc.gov.cn/zgrdw/englishnpc/Law/2011-02/15/content_1620636.htm, accessed 19-10-2021.

“中华人民共和国刑法修正案(九)”, *Zhōnghuá rénmín gònghéguó xíngfǎ xiūzhèng àn (jiǔ)*, https://www.pkulaw.com/chl/6c18c6f3a93ad220bdfb.html, accessed 19-10-2021. English translation: “Amendment (IX) to the Criminal Law of the People's Republic of China”, https://www.pkulaw.com/en_law/6c18c6f3a93ad220bdfb.html, accessed 19-10-2021.

“最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释”, *Zuìgāo rénmín fǎyuàn, zuìgāo rénmín jiǎncháyuàn guānyú bànlǐ qīnfàn gōngmín gèrén xìnxī xíngshì ànjiàn shìyòng fǎlǜ ruògān wèntí de jiěshì*, https://www.pkulaw.com/chl/88d3a698daf58033bdfb.html, accessed 19-10-2021.

“全国人大常委会关于加强网络信息保护的决定”, *Quánguó réndà chángwěi huì guānyú jiāqiáng wǎngluò xìnxī bǎohù de juédìng*, http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm, accessed 23-10-2021. English Translation: WANG Ted, 2016, “The NPC Standing Committee Decision on Strengthening the Network Information Protection”, *Chinese Law and Government, Taylor & Francis Group*, Vol. 48, No. 1, 13–14.

“中华人民共和国消费者权益保护法”，*Zhōnghuá rénmín gònghéguó xiāofèi zhě quányì bǎohù fǎ*, https://www.pkulaw.com/chl/f9d6438c22a2f335bdfb.html, accessed 25-10-2021. English Translation: “Law of the People's Republic of China on Protection of Consumer Rights and Interests”, https://www.pkulaw.com/en_law/f9d6438c22a2f335bdfb.html?keyword=consumer, accessed 25-10-2021.

“中华人民共和国消费者权益保护法(2013修正)”, *Zhōnghuá rénmín gònghéguó xiāofèi zhě quányì bǎohù fǎ (2013 xiūzhèng)*, https://www.pkulaw.com/chl/a347c82e6a7d13aabdfb.html, accessed 26-10-2021.

“侵害消费者权益行为处罚办法”, *Qīnhài xiāofèi zhě quányì xíngwéi chǔfá bànfǎ*, http://www.saic.gov.cn/fgs/lflg/fgfb/201504/t20150403_154911.html, accessed 26-10-2021.

“规范互联网信息服务市场秩序若干规定”，*Guīfàn hùliánwǎng xìnxī fúwù shìchǎng zhìxù ruògān guiding*, https://www.pkulaw.com/chl/c513bd8a91c45ac4bdfb.html, accessed 28-10-2021. English Translation: “Several Provisions on Regulating the Market Order of Internet Information Services”, https://www.pkulaw.com/en_law/c513bd8a91c45ac4bdfb.html?keyword=Internet%20Information%20Services, accessed 28-10-2021.

“电信和互联网用户个人信息保护规定”，*Diànxìn hé hùliánwǎng yònghù gèrén xìnxī bǎohù guiding*, https://www.pkulaw.com/chl/f0f7c6124531c3bebdfb.html?keyword=%E7%94%B5%E4%BF%A1%E5%92%8C%E4%BA%92%E8%81%94%E7%BD%91%E7%94%A8%E6%88%B7%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A4%E8%A7%84%E5%AE%9A, accessed 28-10-2021. English Translation: “Provisions on Protecting the Personal Information of Telecommunications and Internet Users”, https://www.pkulaw.com/en_law/f0f7c6124531c3bebdfb.html, accessed 28-10-2021.

“中华人民共和国网络安全法”, *Zhōnghuá rénmín gònghéguó wǎngluò ānquán fǎ*, https://www.pkulaw.com/chl/4dce14765f4265f1bdfb.html, accessed 03-11-2021. English Translation: “Cybersecurity Law of the People's Republic of China”, http://www.lawinfochina.com/Display.aspx?LookType=3&Lib=law&Id=22826&SearchKeyword=&SearchCKeyword=&paycode=, accessed 03-11-2021; https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/, accessed 03-11-2021.

“中华人民共和国电子商务法”, *Zhōnghuá rénmín gònghéguó diànzǐ shāngwù fǎ*, https://www.pkulaw.com/chl/3f020f79c1e5316ebdfb.html, accessed 07-11-2021. English Translation: “E-Commerce Law of the People’s Republic of China”, https://ipkey.eu/sites/default/files/documents/resources/PRC_E-Commerce_Law.pdf, accessed 07-11-2021.

“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”, *Xìnxī ānquán jìshù gōnggòng jí shāngyòng fúwù xìnxī xìtǒng gèrén xìnxī bǎohù zhǐnán*, https://www.pkulaw.com/chl/0ff5bc705d989a1abdfb.html?keyword=%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8%E6%8A%80%E6%9C%AF%E5%85%AC%E5%85%B1%E5%8F%8A%E5%95%86%E7%94%A8%E6%9C%8D%E5%8A%A1%E4%BF%A1%E6

%81%AF%E7%B3%BB%E7%BB%9F%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A4%E6%8C%87%E5%8D%97, accessed 08-11-2021. English Translation: "Information Security Technology – Guidelines for the Protection of Personal Information in Public and Commercial Service Information Systems", https://www.pkulaw.com/en_law/0ff5bc705d989a1abdfb.html, accessed 08-11-2021.

"中华人民共和国民法典", *Zhōnghuá rénmín gònghéguó mínfǎ diǎn*, https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E6%B0%91%E6%B3%95%E5%85%B8, accessed 30-12-2021. English Translation: "Civil Code of the People's Republic of China", https://npcobserver.com/wp-content/uploads/2020/11/Civil-Code_Eng_July-2021-version.pdf, accessed 31-12-2021.

"最高人民法院印发《关于修改＜民事案件案由规定＞的决定》的通知（2020)", *Zuìgāo rénmín fǎyuàn yìnfā "guānyú xiūgǎi <mínshì ànjiàn ànyóu guīdìng >de juédìng" de tōngzhī (2020)*, http://lawinfochina.com/display.aspx?id=34794&lib=law, accessed 02-01-2022. English Translation: "Notice by the Supreme People's Court of Issuing the Decision to Amend the Provisions on the Causes of Action of Civil Cases (2020)", http://lawinfochina.com/display.aspx?id=34794&lib=law, accessed 01-01-2022.

"中华人民共和国个人信息保护法"， *Zhōnghuá rénmín gònghéguó gèrén xìnxī bǎohù fǎ*, https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A4%E6%B3%95, accessed 04-01-2022. English Translation: "Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021", https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/, accessed 04-01-2022.

"中华人民共和国数据安全法"， *Zhōnghuá rénmín gònghéguó shùjù ānquán fǎ*, https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E6%95%B0%E6%8D%AE%E5%AE%89%E5%85%A8%E6%B3%95, accessed 06-01-2022. English Translation: "Data Security Law of the People's Republic of China", https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/, accessed 06-01-2022.

"中华人民共和国突发事件应对法"， *Zhōnghuá rénmín gònghéguó tú fā shìjiàn yìngduì fǎ*, https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E7%AA%81%E5%8F%91%E4%BA%8B%E4%BB%B6%E5%BA%94%E5%AF%B9%E6%B3%95, accessed 27-01-2022. English Translation: "Emergency Response Law of the People's Republic of China", http://english.mee.gov.cn/Resources/laws/envir_elatedlaws/201705/t20170514_414040.shtml, accessed 27-01-2022.

"中华人民共和国传染病防治法"，*Zhōnghuá rénmín gònghéguó chuánrǎn bìng fángzhì fǎ*, https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E4%BC%A0%E6%9F%93%E7%97%85%E9%98%B2%E6%B2%BB%E6%B3%95, accessed 27-01-2022. English Translation: "Law Of The People's Republic Of China On Prevention And Treatment Of Infectious Diseases (2013 Amendment), June 29, 2013", https://china.usc.edu/law-peoples-republic-china-prevention-

and-treatment-infectious-diseases-2013-amendment-june-29-2013, accessed 27-01-2022.

“关于做好个人信息保护利用大数据支撑联防联控工作的通知”, *Guānyú zuò hǎo gèrén xìnxī bǎohù lìyòng dà shùjù zhīchēng liánfáng lián kòng gōngzuò de tōngzhī*, http://www.cac.gov.cn/2020-02/09/c_1582791585580220.htm, accessed 28-01-2022.

“全国版健康码，来了！”, *Quánguó bǎn jiànkāng mǎ, láile!*, https://mp.weixin.qq.com/s/amB7fBxLw8KSR9DcUsbTWg, accessed 01-02-2022.

“通信大数据行程卡使用指南”, *Tōngxìn dà shùjù xíngchéng kǎ shǐyòng zhǐnán*, https://xc.caict.ac.cn/help.html, accessed 03-02-2022.

“《个人健康信息码》系列国家标准问答（FAQ）”, *“Gèrén jiànkāng xìnxī mǎ” xìliè guójiā biāozhǔn wèndá (FAQ)*, http://www.cesi.cn/202005/6411.html, accessed 04-02-2022.

“明星「健康寶」信息被泄露網上售賣　1元售1000藝人身分證號碼”, *Míngxīng `jiànkāng bǎo'xìnxī bèi xièlòu wǎng shàng shòumài 1 yuán shòu 1000 yìrén shēnfèn zhèng hàomǎ*, https://news.mingpao.com/ins/%E5%85%A9%E5%B2%B8/article/20201228/s00004/1609148631862/%E6%98%8E%E6%98%9F%E3%80%8C%E5%81%A5%E5%BA%B7%E5%AF%B6%E3%80%8D%E4%BF%A1%E6%81%AF%E8%A2%AB%E6%B3%84%E9%9C%B2%E7%B6%B2%E4%B8%8A%E5%94%AE%E8%B3%A3-1%E5%85%83%E5%94%AE1000%E8%97%9D%E4%BA%BA%E8%BA%AB%E5%88%86%E8%AD%89%E8%99%9F%E7%A2%BC, accessed 05-02-2022.

Alibaba Group, “*Yèwù fànchóu*”, 业务范畴, https://www.alibabagroup.com/cn/about/businesses, accessed 19-01-2022.

“Article 8 - Protection of personal data”, *EU Charter of Fundamental Rights*, https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data, accessed 20-09-2021.

Baidu, “Company Overview”, https://ir.baidu.com/company-overview/, accessed 19-01-2022.

Baidu Privacy Policy, “*Bǎidù yǐnsī zhèngcè zǒngzé*”, 百度隐私政策总则, http://privacy.baidu.com/policy, accessed 20-01-2022.

Bloomberg, “China to Lift Lockdown Over Virus Epicenter Wuhan on April 8”, https://www.bloomberg.com/news/articles/2020-03-24/china-to-lift-lockdown-over-virus-epicenter-wuhan-on-april-8, accessed 27-01-2022.

BUDD Jobie, MILLER Benjamin S., MANNING Erin M., LAMPOS Vasileios, ZHUANG Mengdie, EDELSTEIN Michael, REES Geraint, EMERY Vincent C., STEVENS Molly M., KEEGAN Neil, SHORT Michael J., PILLAY Deenan, MANLEY Ed, COX Ingemar J., HEYMANN David, JOHNSON Anne M., MCKENDRY Rachel A., “Digital technologies in the public-health response to COVID-19”, *Nature Medicine*, https://www.nature.com/articles/s41591-020-1011-4, accessed 24-02-2021.

CHOUDHURY Sahely Roy, “Jack Ma’s Alibaba is doubling down on its supermarket strategy”, https://www.cnbc.com/2017/07/18/alibaba-hema-stores-blend-online-and-offline-

retail.html, *CNBC News*, accessed 19-01-2022.

"Client Advisory Regarding COVID-19 Legal Issues in China", *Squire Patton Boggs*, https://www.squirepattonboggs.com/-/media/files/insights/publications/2020/03/client-advisory-regarding-covid-19-legal-issues-in-china/client-advisory-regarding-covid19-legal-issues-in-china.pdf, accessed 09-03-2021.

CURRY David, "Most Popular Apps (2022)", *Business of Apps*, https://www.businessofapps.com/data/most-popular-apps/, accessed 01-02-2022.

"Grid-based community workers power up China's grassroots coronavirus fight", *Xinhua*, http://www.xinhuanet.com/english/2020-03/01/c_138832911.htm, accessed 29-01-2022.

"How can I prove that I have not been to any epidemic-stricken region or country in the past 14 days? Check this!", http://english.www.gov.cn/news/topnews/202003/11/content_WS5e685fefc6d0c201c2cbe087.html, accessed 03-02-2022.

胡晓萌 HU Xiaomeng, 文贤庆 WEN Xianqing, 孙保学 SUN Baoxue, "*Jiànkāng mǎ de yǐnsī zhèngcè, hái yǒu nǎxiē gǎijìn kōngjiān?*", 健康码的隐私政策，还有哪些改进空间？, "What is the room for improvement in the privacy policy of the health code?", https://tech.sina.com.cn/roll/2020-03-16/doc-iimxyqwa0896942.shtml, accessed 05-02-2022.

"International Covenant on Civil and Political Rights", https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx, accessed 07-10-2021.

JOHNSON Bobbie, "The Covid Tracing Tracker: What's happening in coronavirus apps around the world", *MIT Technology Review*, https://www.technologyreview.com/2020/12/16/1014878/covid-tracing-tracker#international-data, accessed 05-02-2022.

KHALIL Lydia, "Digital Authoritarianism, China and Covid", *Lowy Institute*, https://www.lowyinstitute.org/publications/digital-authoritarianism-china-and-covid, accessed 10-02-2021.

KHARPAL Arjun, "Tencent launches new online shopping feature in WeChat app, in a challenge to rivals Alibaba and JD", *CNBC News*, https://www.cnbc.com/2020/07/16/china-tech-giant-tencent-launches-new-online-shopping-feature-in-wechat-app.html, accessed 06-11-2021.

LAU Nanda, GUO Gavin, GONG James, "China Cybersecurity and Data Protection: China's Civil Code lays foundation for data protection", *China Investments E-Bulletin - Herbert Smith Freehills*, https://www.lexology.com/library/detail.aspx?g=89f22cb9-ff6c-41c1-9c55-3f94c6ef5faa, accessed 16-10-2021.

LUO Duoqun, WANG Yanchen, "China - Data Protection Overview", https://www.dataguidance.com/notes/china-data-protection-overview, accessed 18-01-2022.

MENG Qingwei, 孟庆伟, *"Hǎiliàng shè yìqíng gèrén xìnxī xièlòu liǎng de gōng'ān zuò chū xíngzhèng jūliú chǔfá"* 海量涉疫情个人信息泄露 两地公安做出行政拘留处罚 (public

security issued administrative detention penalties following massive leakage of personal information related to the epidemic), https://news.sina.com.cn/o/2020-02-05/doc-iimxyqvz0398976.shtml, accessed 27-01-2022.

MOZUR Paul, ZHONG Raymond, KROLIK Aaron, "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags", *The New York Times*, https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html, accessed 10-03-2021.

"National COVID-19 contact tracing apps", *Policy Department for Economic, Scientific and Quality of Life Policies – European Parliament*, https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652711/IPOL_BRI(2020)652711_EN.pdf, accessed 04-02-2022.

"OECD Privacy Guidelines", *Organisation for Economic Co-operation and Development*, https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm, accessed 18-09-2021.

QuestMobile, 2018, "QuestMobile: 2017 China mobile Internet report", https://www.questmobile.com.cn/blog/en/blog_130.html, accessed 03-11-2021.

"Regulating electronic means to fight the spread of COVID-19: Argentina, Australia, Brazil, China, England, European Union, France, Iceland, India, Iran, Israel, Italy, Japan, Mexico, Norway, Portugal, Russian Federation, South Africa, South Korea, Spain, Taiwan, Turkey, United Arab Emirates." *The Law Library of Congress, Global Research Directorate*, https://www.loc.gov/item/2020714995/, accessed 10-02-2021.

"Regulation (EU) 2016/679 of the European Parliament and of the Council", *Official Journal of the European Union*, https://eur-lex.europa.eu/eli/reg/2016/679/oj, accessed 04-01-2022.

ROBINSON Mark, LAU Nanda, GONG James, "China cybersecurity and data protection: Review of 2020 and outlook for 2021", *Herbert Smith Freehills*, https://sites-herbertsmithfreehills.vuturevx.com/95/24431/compose-email/china-cybersecurity-and-data-protection--review-of-2020-and-outlook-for-2021.asp?sid=3e6b986b-17d9-4d66-a1ff-bb17e5da30f7, accessed 15-02-2021.

Statista, "Number of smartphone users in China from 2015 to 2020 with a forecast until 2026", https://www.statista.com/statistics/467160/forecast-of-smartphone-users-in-china/#:~:text=In%202020%2C%20the%20number%20of,exceeded%20six%20billion%20that%20year., accessed 31-01-2022.

TAN Shining, "China's Novel Health Tracker: Green on Public Health, Red on Data Surveillance", *Center for Strategic & International Studies*, https://www.csis.org/blogs/trustee-china-hand/chinas-novel-health-tracker-green-public-health-red-data-surveillance, accessed 01-02-2022.

Tencent Privacy Policy. "*Téngxùn gōngsī wǎngyè jí wèn xún tíjiāo yǐnsī zhèngcè*", 腾讯公司网页及问询提交隐私政策，https://www.tencent.com/zh-cn/privacy-policy.html, accessed 20-01-2022.

"The data protection regime in China – In-depth Analysis for the LIBE Committee",

Directorate-General for Internal Policies of the Union (European Parliament), https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf, accessed 17-03-2021.

"Tort Liability Law of the People's Republic of China", http://www.npc.gov.cn/zgrdw/englishnpc/Law/2011-02/16/content_1620761.htm, accessed 16-10-2021.

VON CARNAP Kai, DRINHAUSEN Katja, SHI-KUPFER Kristin, "Tracing. Testing. Tweaking. Approaches to data-driven Covid-19 management in China", *Mercator Institute for China Studies (MERICS)*, https://merics.org/en/report/tracing-testing-tweaking, accessed 01-02-2022.

WAGNER Jack, "China's Cybersecurity Law: What You Need to Know", *The Diplomat*, https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/, accessed 04-11-2021.

WANG Shengjun, "Report concerning the Inspection of the Implementation of the 'Cybersecurity Law of the People's Republic of China' and the 'National People's Congress Standing Committee Decisions concerning strengthening Online Information Protection'", https://digichina.stanford.edu/work/report-concerning-the-inspection-of-the-implementation-of-the-cybersecurity-law-of-the-peoples-republic-of-china-and-the-national-peoples-congress-standing/, accessed 03-11-2021.

WEI Changhao, "2020 NPC Session: A Guide to China's Civil Code (Updated)", https://npcobserver.com/2020/05/21/2020-npc-session-a-guide-to-chinas-civil-code/, *NPC Observer*, accessed 31-12-2021.

"What is freedom and privacy of correspondence?", https://www.chinadaily.com.cn/m/chinalic/2017-06/16/content_29774939.htm, *China Legal Information Center*, accessed 11-10-2021.

World Health Organization, "Statement on the second meeting of the International Health Regulations (2005) Emergency Committee regarding the outbreak of novel coronavirus (2019-nCoV)", https://www.who.int/news/item/30-01-2020-statement-on-the-second-meeting-of-the-international-health-regulations-(2005)-emergency-committee-regarding-the-outbreak-of-novel-coronavirus-(2019-ncov), accessed 26-01-2022.

World Health Organization, "WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020", https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020, accessed 27-01-2022.

World Health Organization, "China: WHO Coronavirus Disease (COVID-19) Dashboard", https://covid19.who.int/region/wpro/country/cn, accessed 29-01-2022.

XIAO Tangfei 肖腾飞, SHEN Yanru 申燕茹, "*Gèrén xìnxī bǎohù fǎ zhìdù liàngdiǎn jiěxī*" 《个人信息保护法》制度亮点解析, *Deloitte* https://www2.deloitte.com/cn/zh/pages/risk/articles/personal-information-protection-law-analysis.html, accessed 05-01-2022.

XU Hui, DONOVAN Kieran, LEE Bianca, “China Introduces First Comprehensive Legislation on Personal Information Protection”, https://www.lw.com/thoughtLeadership/china-introduces-first-comprehensive-legislation-on-personal-information-protection#:~:text=On%20August%2020%2C%202021%2C%20the,effect%20on%20November%201%2C%202021., *Latham & Watkins Data Privacy & Security Practice*, accessed 02-01-2022.

XU Hui, DONOVAN Kieran, “China’s New Data Security Law: What to Know”, https://www.lw.com/thoughtLeadership/china-new-data-security-law-what-to-know, *Latham & Watkins Data Privacy & Security Practice*, accessed 06-01-2022.

姚佳莹 YAO Jiaying, “*Yìqíng hòu, jiànkāng mǎ kěfǒu shēngjí “quánnéng mǎ”?”*, 疫情后，健康码可否升级“全能码”？, “After the epidemic, can the health code be upgraded to the "universal code"?”, https://m.caijing.com.cn/api/show?contentid=4757152, accessed 06-02-2022.

ZHANG Laney, 2013, “China: NPC Decision on Network Information Protection”, https://www.loc.gov/item/global-legal-monitor/2013-01-04/china-npc-decision-on-network-information-protection/, *Library of Congress*, accessed 22-10-2021.

ZHONG Raymond, “China’s Virus Apps May Outlast the Outbreak, Stirring Privacy Fears”, *New York Times*, https://www.nytimes.com/2020/05/26/technology/china-coronavirus-surveillance.html, accessed 06-02-2022.