

CHINA'S NEW LEGISLATION ON PERSONAL INFORMATION PROTECTION IN LIGHT OF THE COVID-19 PANDEMIC

Chao Wang* and Taixia Shen**

Abstract: During the COVID-19 pandemic period, China used a data-based approach to protect public health. Although this approach has supported the containment of the COVID-19 virus, it risks infringing the right to privacy. This article considers how this data-based approach, including data collection, sharing, storage and disclosure could affect the right to privacy and shows that the data collection process in China may involve the collection of irrelevant personal data from too many broad categories and sometimes without consent of the data subject. The results show that the main challenges to the right to privacy are (1) a lack of effective information control and storage safeguards, (2) the improper use and disposal of information and (3) the disclosure of non-desensitised information. This article examines PRC's newly passed legislation, including the Cybersecurity Law, Data Security Law and the Personal Information Protection Law, which constitute China's first systematic and comprehensive regulatory framework to protect personal information. This regulatory framework requires that any restrictions on the right to protect personal information and privacy rights must be in the public interest such as public health and security. This article examines whether and to what extent this regulatory framework is capable of addressing challenges of big data applications to individual rights to privacy and proposes some further improvements.

Keywords: *Big data technology; China; data privacy; pandemic prevention and control; personal data; right to privacy*

I. Introduction: Application of Big Data Technology for Pandemic Prevention and Control in China

Big data technology has been used to some extent in preventing and controlling the spread of COVID-19, especially in Peoples' Republic of China (PRC). The Chinese government considers it necessary to collect personal information for research, decision-making in relation to the prevention and control of the COVID-19 pandemic and other public health emergencies, by reference to their experience with

* Associate Professor, Faculty of Law, University of Macau, Macao SAR. chaowang@um.edu.mo.

** Associate Professor, the Law School and Intellectual Property School at Jinan University, Guangzhou, China. sunbird726@hotmail.com, taixiashen@jnu.edu.cn. This manuscript is supported by the "Fundamental Research Funds for the Central Universities."

H1N1, to effectively apply big data technology to prevent and control the spread of COVID-19.¹

Use of technology for these purposes includes collection, analysis and disclosure of personal data on location, travel, health status, medical records, personal consumption expenditure, telecommunication records, Internet records, electronic medical records, hospital information systems, government information systems, epidemic prevention systems, smart devices, questionnaire results, flow maps (showing the movement of people) and appointment registration dates. These data are used for personal tracking via descriptive, diagnostic, predictive and prescriptive analytics. The results can be used for epidemic surveillance and early warning, tracking of virus sources, drug screening, medical treatment, resource allocation and production recovery.² However, such data collection, storage, control and disclosure processes risk invasion of right to privacy.³

It is understandable that the onset of COVID-19 disaster inevitably and justifiably occasioned some non-compliance with law: but it is necessary that any such non-compliance with law is kept within reasonable limits so as not to unduly infringe fundamental personal freedoms and rights. In order to strike a right balance between personal freedoms and the wider interests of the society, as this article will argue, two principles must be kept in sight: proportionality of restrictions on rights and transparency of regulatory measures that tend to compromise rights of the individual.

The promulgation in 2021 of PRC Data Security Law and the PRC Personal Information Protection Law supplemented a number of PRC laws and regulations that set out a regulatory framework for the protection of the rights to privacy and personal information in relation to disease control and prevention. Article 38 of the PRC Emergency Response Law of 2007,⁴ art.40 of the PRC Emergency Regulations

-
- 1 Gang Li *et al.*, "Application of Big Data Technology in Precise Prevention and Control of Epidemic Situation" (2021) 7(1) *Big Data Research* 124, available at <http://www.infocomm-journal.com/bdr/CN/10.11959/j.issn.2096-0271.2021009> (visited 1 August 2022) (in Chinese).
 - 2 Jun Wu *et al.*, "Application of Big Data Technology for COVID-19 Prevention and Control in China: Lessons and Recommendations" (2020) 22(10) *Journal of Medical Internet Research* e21980, available at <https://www.jmir.org/2020/10/e21980/> (visited 1 August 2022).
 - 3 Taixia Shen and Chao Wang, "Big Data Technology Applications and the Right to Health in China during the COVID-19 Pandemic" (2021) 18(14) *International Journal of Environmental Research and Public Health* 7325, available at <https://doi.org/10.3390/ijerph18147325> (visited 1 August 2022). See also, Xixuan Zhou and Yawen Xu, "The Restriction and Protection of Personal Information Right in Public Health Events" (2020) 5 *Technology and Law* 58, available at <https://www.cnki.com.cn/Article/CJFDTotal-KJFL202005009.htm> (visited 1 August 2022) (in Chinese).
 - 4 Article 38 of the PRC Emergency Response Law provides that "the people's governments at the county level shall establish a full-time or part-time information reporter system in the resident's committees, the villagers' committees and the units concerned. The citizens, legal persons and other organizations that get information on emergencies shall immediately report to the local people's governments, the relevant competent departments or the designated specialized institutions". The Law is available at http://www.npc.gov.cn/zgrdw/englishnpc/Law/2009-02/20/content_1471589.htm (visited 1 August 2022).

on Public Health Emergencies (adopted in 2003 and revised in 2011)⁵ and art.33 of the PRC Law on the Prevention and Treatment of Infectious Diseases (adopted in 1989 and revised in 2013) set forth the parameters for collecting and disclosing such information.⁶ These regulations also provide legal guidelines for government agencies, companies and village and community resident committees involved in epidemic prevention.

The Prevention and Treatment of Infectious Diseases Law states that privacy should be protected during information collection (art.12);⁷ the Resident Identity Card Law (adopted in 2003 and revised in 2011) stipulates that public security agencies and the police should protect personal information as part of their work (art.6);⁸ the E-Commerce Law of 2018 mainly addresses how business entities use the Internet with a focus on the commercial use of personal information rather

5 Article 40 PRC Emergency Regulations on Public Health Emergencies provides as follows: "In case of the outbreak and epidemic of any infectious disease, subdistrict offices, people's governments of towns (townships), residents' committees and villagers' committees shall, by following the principles of solidarity and cooperation and of community-based disease prevention and control, organize their strength to assist the competent health administrative departments, other relevant departments and medical and health institutions in collecting and reporting the information of epidemic situations, evacuating and isolating persons, and implementing public health measures, and popularize the knowledge on the prevention and control of infectious diseases among residents or villagers". This Law is available at http://en.nhc.gov.cn/2014-06/18/c_46454.htm (visited 1 August 2022) (Official translation).

6 Article 33 of the Law of the PRC on the Prevention and Treatment of Infectious Diseases provides as follows: "Disease prevention and control institutions shall take the initiative to collect, analyse, investigate and verify information on epidemic situation of infectious diseases. . . . Disease prevention and control institutions shall set up or assign special departments and persons the task of controlling information on the epidemic situation of infectious diseases and making timely verification and analysis of reports on epidemic situation". The English translation of this Law is available at <https://china.usc.edu/law-peoples-republic-china-prevention-and-treatment-infectious-diseases-2013-amendment-june-29-2013> (visited 1 August 2022).

7 Article 12 of the Law of the PRC on the Prevention and Treatment of Infectious Diseases provides that "all units and individuals within the territory of China shall accept the preventive and control measures taken by disease prevention and control institutions and medical agencies for investigation, testing, collection of samples of infectious diseases and for isolated treatment of such diseases, and they shall provide truthful information about the diseases. Disease prevention and control institutions and medical agencies shall not divulge any information or materials relating to personal privacy". It goes on to say: "Where health administration departments and other relevant departments, or disease prevention and control institutions and medical agencies infringe upon the lawful rights and interests of any units or individuals when exercising administrative control or taking preventive and control measures in violation of law, the units or individuals concerned may apply for administrative reconsideration or initiate legal proceedings according to law".

8 Article 6 of the Law of the People's Republic of China on Resident Identity Cards provides that "public security organs and people's police department" shall keep confidential citizen's personal information gained through making, issuing, examining or seizing resident identity cards. Moreover, art.19 provides that public and private entities other than the public security department have similar obligation to keep confidential any personal information they acquire in the course of performing their duties or rendering services and stipulates the criminal responsibility of public servants (art.19) and police officers (art.20) who "divulg[e] citizens' personal information recorded on their resident identity card". This Law is available at <http://www.lawinfochina.com/display.aspx?lib=law&id=9228&EncodingName=big5> (visited 1 August 2022).

than protecting personal information (arts.23, 25, 32, 79 and 87);⁹ the Civil Code of 2020 provides a legal remedy when personal information is leaked but is only applicable in the field of civil law matters and does not regulate public power;¹⁰ and the PRC Cybersecurity Law of 2021 mainly addresses the national and public security of the network infrastructure, including the security issues of enterprises and other public and private sectors.¹¹ Although the Cybersecurity Law also involves the protection of personal information, it distinguishes between infringement of personal information and infringement of personal interests.¹² The provisions of the Cybersecurity Law impose administrative and criminal liabilities on network operators and service providers for abuse and unauthorised release of personal information.¹³ Therefore, it is difficult for individuals to obtain an effective remedy if the government accesses and uses personal information.

In spite of these existing laws and regulations, large-scale information collection, comprehensive tracking, surveillance and information disclosure during the COVID-19 pandemic compromised individuals' right to privacy and the protection of their personal information.¹⁴ For example, information on location and whereabouts of individuals is always collected by the government for the purpose

9 Articles 23 and 32 of the PRC's E-Commerce Law regulate the e-commerce platform and their employees in collecting personal information. Article 23 provides as follows: "When collecting and using the personal data of users, an e-commerce operator shall abide by the provisions regarding the protection of personal data as stipulated in laws and administrative regulations" and art.32 provides: "An operator of an e-commerce platform shall conform to the principles of openness, fairness and justice, draw up a platform service agreement and design transaction rules, in order to specify rights and obligations with respect to the entry into and exit from the platform, guarantee the quality of commodities and services, protection of consumers' rights and interests, and protection of personal data, etc.". Article 79 provides as follows: "Where an e-commerce operator violates provisions in respect of the protection of personal information, according to laws and administrative regulations, or fails to fulfil obligations of ensuring cyber security, set out in Article 30 hereof and in applicable laws and administrative regulations, it shall be punished according to such laws and administrative regulations as the Cyberspace Security Law of the People's Republic of China". Articles 25 and 87 deal with the responsibility and liability of supervisory authorities in the protection of personal information. Article 87 states: "Where an authority that is responsible for e-commerce supervision and administration under the law neglects his or her duties, abuses his or her power or plays favoritism or commits any irregularity, or divulges, sells or illegally provides others with personal information or privacy or trade secrets he or she has accessed during the performance of his or her duties, his or her legal liability shall be investigated and pursued". An English translation of this Law is available at https://gain.fas.usda.gov/Recent%20GAIN%20Publications/China%20Passes%20E-Commerce%20Law_Shanghai%20ATO_China%20-%20Peoples%20Republic%20of_China_10-19-2018.pdf (visited 1 August 2022) (English translation).

10 Civil Code of China, Book Four, Chapter VI (arts.1032–1039). This is available at <http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf> (visited 1 August 2022).

11 Cybersecurity Law of PRC, Chapter IV: Network Information Security, arts.40–45.

12 Xianzhong Sun, "Why Do We Need the Personal Information Protection Law" *People Weekly* (23 March 2021), available at https://www.peopleweekly.cn/html/2021/kexue_0323/64732.html (visited 1 August 2022) (in Chinese).

13 Cybersecurity Law of PRC, art.64.

14 Yuan Ning, "Regulations on the Personal Information Protection in the Use of COVID-tracking Code" (2020) 38(6) *Law Review* 111, available at <https://www.cnki.com.cn/Article/CJFDTotal-FXPL202006012.htm> (visited 1 August 2022) (in Chinese); Jun Wu *et al.*, "Application of Big Data Technology for COVID-19 Prevention and Control in China" (n. 2).

of COVID-19 prevention. The central and local governments always use big data to improve their information infrastructure and their digital government and digital intelligence in public services and social governance.¹⁵ For example, the Guangzhou government launched a project called *Sibiao Sishi* (Four Standards and Four Realities)¹⁶ in 2017 that built a unified digital basic application platform.¹⁷ Through this project, the government gathered information on residents from 35 public sectors, including public security, housing construction, urban planning, land, transport, civil affairs, water affairs and environmental protection. The information collected included residents' basic status, home address and personal information related to personal relationships, population mobility, business registration based on housing, social security, employment, medical care and daily travel.¹⁸

To deal with such privacy issues, the China's National People's Congress (NPC) adopted two new laws to enhance protection of personal information and data security: PRC Data Security Law and PRC Personal Information Protection Law.

The first Law, the Data Security Law, was passed on 10 June 2021 and the Personal Information Protection Law was passed on 20 August 2021, at the height of the COVID-19 pandemic. The Data Security Law set up a regulatory framework broadly for national security aspects of data security through classification of different categories of data based on their potential impact on national security, and public and individual interests.¹⁹ As such, the Data Security Law is generally seen "as a response to the U.S. Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which gives U.S. law enforcement agencies the authority to compel companies falling under U.S. jurisdiction to produce requested data regardless of where the data is stored".²⁰ However, the adoption of the Data Security Law should also be considered as a response to the challenges to the "the lawful rights and interests of individuals and organizations",²¹ which are protected by the Data Security Law, posed by big data application in an informatics society against the backdrop of the COVID-19 pandemic. Article 6 of this law sets forth data collectors' responsibilities

15 China Academy of Information and Communications Technology (CAICT), *Digital Economy Development in China* (Report, CAICT, Beijing, July 2020), 23–24. This report is available at <http://www.caict.ac.cn/english/research/whitepapers/202007/P020200728343679920779.pdf> (visited 1 August 2022).

16 The Four Standards are standard work maps, standard address libraries, standard building codes and standard basic grids. The Four Realities are the actual population, houses, units and facilities.

17 Shumin Huang, "QR Code Will Be Set to Identify the Building Address" *Nanfang Daily News* (Guangdong, 25 July 2019), 9, available at <https://ishare.ifeng.com/c/s/7oadxxdXIQP> (visited 1 August 2022) (in Chinese); Xueyu Chen, "Grassroots Governance Innovation from the Perspective of Big Data: Taking Guangzhou's Four Standards and Four Realities as an Example" (2019) 31 *Technology Innovation and Application* 35, available at <https://www.cnki.com.cn/Article/CJFDTotal-CXY201931011.htm> (visited 1 August 2022) (in Chinese).

18 Shumin Huang, "QR Code Will Be Set to Identify the Building Address" (n. 17).

19 Data Security Law, arts.1 and 21.

20 Ryan D Junck *et al.*, "China's New Data Security and Personal Information Protection Laws: What They Mean for Multinational Companies" *Skadden, Arps, Slate, Meagher & Flom LLP* (3 November 2021), available at https://www.skadden.com/-/media/Files/Publications/2021/11/Chinas_New_Data_Security_and_Personal_Information_Protection_Laws_What_They_Mean.pdf (visited 1 August 2022).

21 Data Security Law, art.1.

regarding data security. According to arts.32 and 38 of this law, data collection and use should be done in a legal and proper way that protects privacy. While art.32 prohibits private organisation and individuals from acquiring data by theft or by other illegal means, art.38 provides that a state organ, when collecting data as required for the performance of its statutory duties, must preserve confidentiality of the data accessed and must not divulge such data or illegally provide them to others. Article 53 provides that legislative provisions relating to protection of state secrets apply to data processing that involves state secrets.

The second law, the PRC Personal Information Protection Law, deals with and regulates activities involving the collection and use of personal data. Its objectives are to protect personal information rights and interests, to regulate the processing of personal information and to promote reasonable use of personal information (art.1). The law also stipulates the principles of legality and proportionality.²² It prescribes stringent requirements on data transfer, security controls and data localisation and prescribes increased penalties and fines on organisations for violations.²³

This article will not attempt a comprehensive discussion of the legislation which deal with data processing and likely invasions of personal freedoms. Rather, this study investigates the privacy issues in the PRC's application of big data technology for epidemic prevention and control and examines whether the PRC's regulatory framework, especially the newly adopted Personal Information Protection Law, is able to accommodate the conflicting private and public interests.

This article is organised as follows. Sections II, III and IV examine how the use of big data technology challenges the right to privacy in China by identifying some key issues in relation to data collection, data control and storage, and the data disclosure process. It discusses whether the Personal Information Protection Law is able to address the challenges to personal information and privacy posed by big data applications. Section IV provides conclusions with suggested policy recommendations.

II. Privacy Issues in China Emerging from the Large-Scale Application of Big Data: Data Collection Process

According to arts.40 and 41 of the Cybersecurity Law, network operators have the following responsibility:(1) to ensure the confidentiality of user information they

22 Article 6 of the PRC Personal Information Protection Law stipulates that “personal information processing shall be based on explicit and reasonable purposes and directly related to those purposes and shall exert the minimum impacts on the rights and interests of individuals. The collection of personal information shall be limited to the minimum scope required by the purpose of processing, and personal information may not be collected excessively”. This Law is available at http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (visited 1 August 2022).

23 PRC Personal Information Protection Law Chapter VII, Legal Liability, arts.66–71. See Xiao Cheng, “Milestone in Legal Protection of Personal Information in Our Country” *Economic Information Daily* (24 August 2021), available at http://www.jjckb.cn/2021-08/24/c_1310144654.htm (visited 1 August 2022) (in Chinese).

collect, and establish complete user information protection systems; (2) to abide by the principles of legality, propriety and necessity and publish rules for collection and use, explicitly stating the purposes, means and scope for collecting or using information, and obtain the consent of the persons whose data are gathered; (3) to refrain from gathering personal information unrelated to the services they provide; (4) abide by the provisions of laws, administrative regulations or agreements between the parties to gather, use or process personal information.²⁴

Article 32 of the Data Security Law stipulates that any person or organisation authorised to collect information must act within their power and act lawfully.²⁵ Article 5 of the Personal Information Protection Law states that personal information shall be processed in accordance with the principles of legality, fairness, necessity and good faith. Article 6 reaffirms that processing of personal information must be for a definite and reasonable purpose, must be directly related to the purpose of processing and must be processed in a manner that has the least impact on individual rights and interests. However, studies show that governments collect as much information as possible to ensure precise and effective epidemic prevention and control, and that personal information is thus sometimes over-collected, including subjects' age, household registration, place of birth or origin and close contacts, which are irrelevant to epidemic control.²⁶

First, these laws lack clarity concerning the entities empowered to engage in information collection. Article 38 of the PRC Emergency Response Law provides that people's governments at or above the county level and their relevant departments and the specialised institutions shall collect information on emergencies through a variety of channels without explicitly enumerating what these "relevant departments and the specialized institutions" refer to,²⁷ whilst art.40 of the PRC Emergency Regulations on Public Health Emergencies states that "health departments and other relevant departments and medical and health institutions" are empowered to collect information on the pandemic outbreak. Except for the Emergency Regulations on Public Health Emergencies, so far there is no other administrative regulation to implement the national laws or to authorise government

24 Cybersecurity Law of the People's Republic of China, arts.40–41. This Law is available at <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/> (visited 1 August 2022).

25 The art.32 of the Data Privacy Law provides as follows: "An organization or individual shall collect data by lawful and proper means and shall not acquire data by theft or in other illegal manners. Where laws or administrative regulations have provisions on the purposes or scopes of data collection and use, data shall be collected and used for the purposes and within the scopes provided for by those laws and administrative regulations". This Law is available at www.npc.gov.cn/englishnpc/c23934/202112/1ab48829788946ecab270e469b13c39c.shtml 8/12 (visited 1 August 2022).

26 Kui Shen, "How to Balance the Pandemic Prevention and Personal Information Protection" *Economic Information Daily* (28 July 2020), available at http://www.jjckb.cn/2020-07/28/c_139245300.htm?from=groupmessage (visited 1 August 2022) (in Chinese). See also Xianzhong Sun, "Why We Need Personal Information Protection Law" (n. 12).

27 The PRC Emergency Response Law, art.38. This Law is available at http://www.npc.gov.cn/zgrdw/englishnpc/Law/2009-02/20/content_1471589.htm (visited 1 August 2022).

agencies to collect personal information. Although the Regulations on the Disclosure of Government Information regulate the disclosure of government information for the purpose of protecting the freedom of information and right of access to government information of individual citizens, it does not concern personal information.

Besides the Emergency Regulations on Public Health Emergencies, the Prevention and Treatment of Infectious Diseases Law also stipulates that disease prevention and control institutions at all levels are empowered to collect pandemic information. The Emergency Regulations on Public Health Emergencies and the Prevention and Treatment of Infectious Diseases Law do not directly authorise local community organisations, such as neighbourhood and village committees, or employers to collect emergency information; in practice, however, community organisations, employers, universities, app developers and other public service units such as hotels, theatres, restaurants and shopping malls are directly involved in information collection.²⁸ Thus, personal information is collected by many unqualified entities that lack the capability to engage in proper information collection, disclosure and disposal.

Second, the existing laws did not provide that the data subjects' consent must be obtained before collecting their personal data. According to art.41 of the Cybersecurity Law, network operators must inform the data subjects of the rules, purposes, methods and scope of use and obtain their consent.

Let us consider the requirement of consent in relation to the Health Code system introduced in March 2020 in response to the pandemic. The health code system uses mobile phone positioning data to generate a quick medical response code that indicates an individual's health status. To obtain a health code, without which one cannot enter any public place, an individual must sign up on the official webpage and provide their personal information, including their name, national identity number or passport number and phone number. An individual must also report their travel history and any possible contact with a confirmed or suspected COVID-19 patient in the previous 14 days, as well as whether they have a fever, fatigue, a dry cough, a stuffy nose, a runny nose, throat ache or diarrhoea. After the information is verified by the authorities, each user is assigned a quick-response code of red, amber or green. People with a green quick-response code can return to work or school and even travel between different areas and provinces. The system also incorporates civil aviation, railway, bus and other traffic data, telecommunication operator data and financial institution and payment data. Through data analysis, citizens' travel patterns and high-risk groups can be identified.²⁹

28 Xixuan Zhou and Yawen Xu, "The Restriction and Protection of Personal Information Right in Public Health Events" (n. 3).

29 See for example, Fan Yang *et al.*, "Comparative Analysis of China's Health Code, Australia's COVID Safe and New Zealand's COVID Tracer Surveillance Apps: A New Corona of Public Health Governmentality?" (2021) 178(1) *Media International Australia* 182.

While the requirement of obtaining data subject's consent, as stipulated in Cybersecurity Law, applies to the Health Code system, in reality, users do not give informed consent because when registering with the system, users must agree to the user service agreement and privacy policy. It is likely, however, that most users would sign the user service agreement without reading the small print which might state that the data subjects must give their consent to the use of their personal data. However, if a user refuses to consent to the use of their personal information, they will not be able to obtain a health code. During the pandemic, the health code has become necessary to enter public places such as parks, supermarkets and hospitals, and without the health code, it is difficult to travel. Thus, for all practical purposes, the principle of informed consent seems to have no significant part to play in the health code system.³⁰ Some provinces also introduced their own health code system in the early stages of the pandemic, which could be obtained through Alipay or WeChat mini-programs.³¹

There is no unified health code centrally administered by the central government; instead, every provincial government has their own health code system and disease control policy on COVID-19. For example, individuals must provide a medical quick response code or itinerary query information before entering public places. Such programs often collect location and consumption data, and it is difficult to establish that consent was given for the collection and processing of all data.³²

III. Privacy Issues in China Emerging from the Large-Scale Application of Big Data: The Data Control and Storage Process

Personal information collected by various organisations appear to have been stolen or leaked. Two main reasons for this may be identified: the first is that some of the hardware and software are not fully developed and therefore not capable of ensuring safe processing and storing data and the second reason is that not all personnel involved in data processing are fully competent and professionally trained.

The absence of an effective safety management of mechanism in information control and storage aggravates the problems created by technical deficiencies in data processing hardware and software. When information is disseminated through tools such as WeChat and QQ, it is stored by commercial companies rather than on

30 Fan Liang, "COVID-19 and Health Code: How Digital Platforms Tackle the Pandemic in China" (2020) 6(3) *Social Media & Society* 1.

31 Xiheng Jiang, "Health Code: What and How?" *China Daily* (10 April 2020), available at <https://covid-19.chinadaily.com.cn/a/202004/10/WS5e8fbb0a3105d50a3d15266.html> (visited 1 August 2022). See also P Mozur *et al.*, "In Coronavirus Fight, China Gives Citizens a Color Code, with Red Flags" *The New York Times* (1 March 2020), 1, available at <https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html?searchResultPosition=1> (visited 1 August 2022).

32 Fan Liang, "COVID-19 and Health Code" (n. 30).

government-specific databases, leading to breach of confidentiality and security. Information can flow rapidly, and when there are no identity restrictions for users to view information and the transfer of files between users is unrestricted, information is more likely to leak.³³

Many government agencies, community organisations and technology companies are involved in collecting and processing of personal information, such as disease control, health, public security, transportation, customs, market supervision, industrial information and Internet information agencies, as are various types of medical institutions, technology companies, employers, resident committees, village committees, community property service companies and other autonomous grassroots and economic organisations. With so many information collection entities involved, it is difficult to ensure that all staff have sufficient professional knowledge and training. There is hard evidence that epidemic prevention and control departments at all levels have had statistical personal privacy information unintentionally leaked and spread.³⁴

Information leakage can result in cyber violence,³⁵ which is defined by the Cyber Convention Committee as “the use of computer systems to cause, facilitate, or threaten violence against individuals that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual’s circumstances, characteristics or vulnerabilities”.³⁶ A webinar of the Council of Europe on “Introduction to Cyberviolence” goes on to say: “This definition, although still a work on progress, suggests an extreme breadth of topics that are covered by the concept of cyberviolence [including, for instance,] violence against women and girls, cyber-harassment, cyber-bullying and violations of privacy, as well as hate speech”.³⁷

No official guidance has been issued to regulate how data collected during the pandemic is to be handled in the future, and it is unknown whether the personal information so collected will be preserved or destroyed. Article 43 of the Cybersecurity Law, which applies only to network operators who are private entities, and art.38 of the Data Security Law, which applies to state organs, go some way towards addressing this situation. Article 43 of the Cybersecurity Law stipulates that a person may request a network operator to delete personal information if such

33 *Ibid.*

34 Yandong Gao, “To Prevent and Control the Epidemic, It Is More Important to Protect Personal Information” *Global Times* (16 May 2020), 7, available at <https://opinion.huanqiu.com/article/9CaKrnKqYGM> (visited 1 August 2022) (in Chinese).

35 Kui Shen, “How to Balance the Pandemic Prevention and Personal Information Protection” (n. 26).

36 Cybercrime Convention Committee (T-CY), Working Group on cyberbullying and other forms of online violence, especially against women and children, “Mapping Study on Cyberviolence”, available at <https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914> (visited 1 August 2022).

37 Council of Europe, “Introduction to Cyberviolence”, available at <https://www.coe.int/en/web/cyber-crime/introduction-to-cyberviolence> (visited 1 August 2022), citing Cybercrime Convention Committee (T-CY), Mapping Study on Cyberviolence, 2019: Working Group on cyberbullying and other forms of online violence, especially against women and children (n. 36).

personal information has been collected in violation of laws and regulations or the agreement between the individual and the network operator. An individual has a right to demand that any errors in personal information stored by a network operator be corrected. Article 38 of the Data Security Law provides that state organs must, in collecting and using data, act lawfully and ensure that they observe confidentiality of data so collected. There is, however, no provision for any enforcement mechanism to deal with breaches of this duty.

IV. Privacy Issues in China Emerging from the Large-Scale Application of Big Data: The Data Disclosure Process

Article 12 of the Prevention and Treatment of Infectious Diseases Law states that disease prevention and control institutions and medical institutions shall not divulge relevant information and materials involving personal privacy. Article 1032, para.1 of the PRC Civil Code reaffirms that “individuals have the right to privacy”, and para.2 defines the right to privacy as including “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”. According to art.15 of the Regulations on the Disclosure of Government Information, however, disclosure of personal information is justified if the data subject agrees to the disclosure of their private information or the data collecting administrative agency believes that non-disclosure would significantly harm the public.

No such provision exists in the Cybersecurity Law whose main concern is cybersecurity and the protection of the country's critical information infrastructure. The law lacks dedicated provisions regarding the protection of individuals' personal information.

Article 6 of the Personal Information Protection Law sets out in broad terms the confines within which personal information may be processed: “Processing of personal information shall be for a definite and reasonable purpose, shall be directly related to the purpose of processing, and shall be processed in a manner that has the least impact on individual rights and interests”. It also sets out the guiding principle for collecting personal information: “Collection of personal information shall be limited to the minimum scope for the purpose of processing and shall not be excessively collected”. While art.6 embodies a salutary principle, that principle will only be fully effective if detailed administrative regulations supplement it, clarifying for instance what could be regarded as the minimum scope for the purposed processing personal information.

Chapter II of the Law sets out rules for processing personal information (arts.13–37). Section I (arts.13–27) sets out the general provisions. Article 13 sets out situations where personal information processing would be justified. They include, for instance: where the person concerned consents to the processing or personal information or where the consent of the person concerned is not required; where personal information processing is necessary for the performance of statutory

duties and where it is necessary for coping with public health emergencies or for the protection of the life, health and property safety of a natural person. There are several provisions in Personal Information Protection Law which elaborate on the requirement of consent. For instance, the consent of the person concerned must be voluntary and given expressly and where the purpose for which the information was collected changes, consent for the use of personal information for the new purpose must be obtained (art.14); the person concerned is free to withdraw their consent and the personal information processor must provide convenient means to withdraw the consent (art.15); the personal information processor is not permitted to refuse to provide products or services if the person concerned refuses to consent to the processing of their personal information, unless the processing of information is necessary for the provision of products or services (art.16). Section 2: Rules for Processing Sensitive Personal Information (arts.28 to 33) makes similar provision as regards the consent requirement. Specific provision that regulates processing of personal information by state organs is set out in Section 3 of the Law (arts.33–37).

Chapter III of the Law deals with rules for cross-border provision of personal information (arts.38–43). Quite importantly, Chapter IV of the Law deals with rights of individuals in activities of processing personal information (arts.44–50) and Chapter V sets out the obligations of personal information processors (arts.51–59). Chapter VI deals with departments performing duties of personal information protection (arts.60–65). Article 62 provides for coordination of relevant departments by the state cyberspace administration for the protection of personal information by, for instance, formulating rules and standards for the protection of personal information.

These provisions of the Personal Information Protection Law, which reflect the provisions in General Data Protection Regulation of the EU, have introduced a welcome improvement of the law relating to collection, storage, processing and use of personal information. Much remains to be done to ensure full and effective implementation of the salutary principles and guidance in the Personal Information Protection Law. For instance, administrative measures must be taken to deal with a broad range of information collectors and controllers. As many data processing units do not have any personal information protection systems or their systems are incomplete, it will take time for the aforementioned measures to ensure that personal information processing activities comply with the laws and administrative regulations and to prevent unauthorised access to, disclosure or loss of, and tampering with personal information.

Article 10 of the Personal Information Protection Law stipulates that no organisation or individual may disclose personal information of other people.³⁸ Article 25

38 Article 10 of the Personal Information Protection Law provides as follows: “No organization or individual may illegally collect, use, process, or transmit the personal information of another person or illegally buy or sell, provide, or disclose the personal information of another person; or engage in personal information processing activities compromising national security or public interests”. This Law is available at http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559_3.htm (visited 1 August 2022).

states that entities processing personal information shall not disclose the personal information processed except with the individuals' consent. Article 27 stipulates that an entity processing personal information shall obtain consent from the individual in accordance with the provisions of the law if such processing has a major impact on the individual's rights and interests. These provisions provide further protection to personal information.

V. Policy Recommendations and Conclusion

The Personal Information Protection Law alone cannot overcome the challenges to both the right of personal information and the right to privacy caused by the widespread application of big data technology. Helpfully, this Law provides guidelines for personal information protection and establishes the principle of proportionality for collecting and processing personal information.³⁹ In the context of the COVID-19 pandemic, it is argued that the principle of proportionality should apply, for example, in the collection of data from affected people, which means as follows:

The data collection must (i) be proportional to the seriousness of the public-health threat, (ii) be limited to what is necessary to achieve a specific public health objective, and (iii) be scientifically justified. Gaining access to data from personal devices for contact tracing purposes, for example, can be justified if it occurs within specific bounds, has a clear purpose—e.g., warning and isolating people who may have been exposed to the virus, and no less-invasive alternative—e.g., using anonymized mobile positioning data—is suitable for that purpose.⁴⁰

In the meantime, it is also important to note that the principle of proportionality is closely associated with the requirement of transparency, meaning that “secrecy about data access and use should be avoided. Transparent public communication about data processing for the common good should be pursued. Data-processing agreements, for example, should disclose which data are transmitted to third parties and for which purpose”.⁴¹

In light of this principle of proportionality and transparency, the following suggestions may be made:

39 Article 6 of the Personal Information Protection Law of the PRC provides as follows: “Personal information processing shall be based on explicit and reasonable purposes and directly related to those purposes and shall exert the minimum impacts on the rights and interests of individuals. The collection of personal information shall be limited to the minimum scope required by the purpose of processing, and personal information may not be collected excessively”.

40 M Ienca and E Vayena, “On the Responsible Use of Digital Data to Tackle the COVID-19 Pandemic” (2020) 26 *Nature Medicine* 463–464, at 463. available at <https://doi.org/10.1038/s41591-020-0832-5> (visited 1 August 2022).

41 *Ibid.*

- (a) The Prevention and Treatment of Infectious Diseases Law and Emergency Regulations on Public Health Emergencies should be revised to balance the needs of public health and the right to privacy. In any such amendment, the State Council or the State Council's emergency command agency should be authorised to determine the purpose and scope of the personal information collected for epidemic prevention and control and to approve the collectors and users that match the purpose and scope of the exercise. The principles of personal information and privacy protection must be clearly stipulated in the amendments to the regulations. In addition, the entities collecting personal information should be specified by the Prevention and Treatment of Infectious Diseases Law, the Emergency Regulations on Public Health Emergencies and other laws and regulations, and the powers of the authority processing the information should be determined by law.
- (b) Personal information and privacy protection specifications must be integrated into the established Joint Prevention and Control Mechanism of the State Council. The Joint Prevention and Control Mechanism of the State Council is a joint task force that serves as the highest authority of the state in the prevention and control of the COVID-19 pandemic. It consists of officials and experts from many different government departments at the central level, with the secretariat based at the National Health Commission (NHC). All other central entities must follow the instructions on COVID-19 prevention and control from the Joint Prevention and Control Mechanism of the State Council.

Although every province also has their own joint force or working group for prevention and control of COVID-19, these local authorities must follow all the instructions from the Joint Prevention and Control Mechanism of the State Council.⁴² Entities involved in personal information collection, such as government agencies, medical institutions, technology companies, public space management, employers, residents' committees, villagers' committees and community properties, must carry out their functions and duties in accordance with the Personal Information Protection Law.

- (c) Personal information and privacy protection systems with security measures compatible with the Personal Information Protection Law should be established, and these protection mechanisms and measures should be transparent and accessible by the public.

Public security and other departments should have an effective system of oversight and regulation to prevent personal privacy infringements. Article 70 of the Personal Information Protection Law establishes a class action system through which the public procuratorate, the consumer organisations specified by law or the organisation determined by the Cyberspace Administration of

42 See Report: China's fight against COVID-19 (full text), at 24–27, China Daily, available at <http://www.chinadaily.com.cn/pdf/2020/Chinas.Fight.Against.COVID-19-0420-final-2.pdf> (visited 1 August 2022). See also, http://english.www.gov.cn/policies/latestreleases/202005/08/content_WS5eb54d41c6d0b3f0e9497377.html (visited 1 August 2022).

China may file a lawsuit.⁴³ Article 69 of the Personal Information Protection Law provides individuals with a tort remedy. It has been argued, however, that this tort remedy is insufficient. Individuals are always in a weak position to challenge government power and big private companies who abuse individuals' personal information, because it is difficult for individuals to obtain enough evidence to provide proof for an administrative or judicial remedy.⁴⁴ Therefore, as Xixin Wang suggested, a strong government protection model may be more desirable where the state should take the major responsibility to protect personal information of individuals and investigate and punish the misconduct of private companies for their abuse and misuse of personal information.⁴⁵

Although Xixin Wang's suggestion was made before the introduction of the Personal Protection Information Law, Wang's view is still valid because tort remedy is insufficient and ineffective. In other words, the tort remedy does not address the weakness in the system that Wang saw. As a matter of fact, from a national security perspective, the Chinese government does have a strong motivation to protect personal information for the sake of data security, as shown in the most recent case of Didi Global who was fined \$1.2 billion for violation of the Data Security Law, Cyberspace Security Law and the Personal Information Protection Law after a year-long probe.⁴⁶

In the meantime, individuals should be entitled not only to report the disclosure of personal information but also to initiate civil lawsuits for redress. Moreover, individuals whose personal information or privacy is violated by a public entity should be entitled to request that the entity take corrective action or request the same from its superior and can file an administrative lawsuit to hold the officials involved responsible.⁴⁷

The PRC's Data Security Law and Personal Information Protection Law are intended to strike a balance between public health and the right to privacy. To this end, these laws, just as other PRC laws on human rights protection, must also be consistent with the PRC's human rights discourse, which prioritises

43 Article 70 of the *PIPL* provides as follows: "Where a personal information processor processes personal information in violation of the provisions of this Law which infringes the rights and interests of a large number of individuals, the people's procuratorate, the consumer organizations specified by law, and the organization designated by the national cyberspace department may file a lawsuit with the people's court in accordance with the law". This Law is available at http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559_3.htm (visited 1 August 2022).

44 Xixin Wang, "Obligation of State Protection in Personal Information and Its Expansion" (2021) 1 *China Legal Science* 145, available at http://www.pkulaw.cn/fulltext_form.aspx?Gid=503aa9bd5779594e3bb1992795625c36bdfb (visited 1 August 2022) (in Chinese).

45 *Ibid.*

46 See, for example, "China Fines Didi \$1.2 Billion for Breaking Data-security Laws" *The Washington Post*, 21 July 2022, available at <https://www.washingtonpost.com/world/2022/07/21/china-didi-fine-data-security/> (visited 1 August 2022). An official declaration in Chinese by the Cyberspace Administration of China is available at http://www.cac.gov.cn/2022-07/21/c_1660021534364976.htm (visited 1 August 2022).

47 *Ibid.*

collectivism and economic and social rights.⁴⁸ According to the Personal Information Protection Law, the disposal of personal information does not require individual consent in cases of public health emergency, but this law does not specify the entities processing such information or the scope of their power. In addition, the Data Security Law mainly concerns data security from a public dimension rather than privacy. Because the provisions of these two new laws are relatively general, their implementation requires detailed implementation regulations.

China's new laws may not be as effective as expected in dealing with the challenges to privacy posed by big data applications emerging from pandemic prevention and control efforts, but they provide a sound foundation for a comprehensive, effective and fair regulatory framework.

48 Kui Shen, "How to Balance the Pandemic Prevention and Personal Information Protection" (n. 26).