TRACING. TESTING. TWEAKING.
Approaches to data-driven Covid-19 management in China

Kai von Carnap, Katja Drinhausen and Kristin Shi-Kupfer

MERICS
Mercator Institute for China Studies

MERICS

Mercator Institute for China Studies

**Vodafone Institute
for Society and
Communications**

TRACING. TESTING. TWEAKING.

Approaches to data-driven Covid-19 management in China

Kai von Carnap, Katja Drinhausen and Kristin Shi-Kupfer

MAIN FINDINGS AND CONCLUSIONS

- China deployed data-driven solutions fast and early in the Covid-19 epidemic. Responses included upgrading and expanding components of the existing digital technology ecosystem, most notably facial recognition and "super apps" like WeChat. Well-established links between government and business enabled Beijing to draw on large amounts of user data, often in real-time.

- Macro and micro tools generated from mobile phone tracking data are at the core of China's approach to Epidemic Prevention and Control (EPC). They have provided inputs to develop the QR-code health apps that enabled quarantine restrictions to be lifted relatively swiftly.

- To identify potentially infected people, China's government deployed refined facial recognition technology with added temperature sensors and infrared identification solutions. Hospitals and doctors used digital platform solutions for disease monitoring, diagnostics and resource management systems based on big data and AI, and free online health consultations.

- Beijing's epidemic management prioritizes security over privacy. Laws and regulation focus on facilitating data aggregation and sharing between stakeholders, rather than privacy rights. Despite the integration of personal data protection into the newly established Civil Code, legislation is still fragmented and mainly addresses the private sector. Government departments have greater legal scope to collect and share data.

- Developers of new contact tracing and health apps have been able to build on existing user agreements and standard privacy policies that permit them to share, transfer and disclose personal information without additional consent in the interest of public safety and public health.

- China's data-driven management of Covid-19 has shown key benefits, i.e. reviving public life in a strictly controlled form based on rapidly deployed solutions to trace people's movements, contacts and health status. Digital platform solutions have improved medical research, patient treatment and resource management within the health sector.

- However, the swift roll out of data-driven solutions to manage public health also highlighted several kinds of risks. Technological solutions like the QR health codes proved only partially functional or serviceable. Personal data has been misused by companies to collect data for their own commercial interest. Local cadres have also abused personal data in the drive to detect infected people and reduce new cases.

- Data leaks have resulted in discrimination and stigma against some social groups, e.g., people from severely affected areas. Data breaches led to publicly voiced concerns about personal data protection. Overall, Covid-19 has triggered new debates on privacy in China which, as in Europe, increasingly evolve around the dilemma of balancing public safety and privacy interests.

- Only some of China's data-driven solutions for managing Covid-19 are appropriate for use in a European context. Solutions for diagnostics and treatment should be further assessed and could be relatively easily applied in Europe. Others, like contact tracing based on excessive data collection and opaque algorithms, are incompatible with European data protection values and norms.

Freedom or quarantine – China's digital health control in times of Covid-19

Complex and often opaque algorithms evaluate individual parameters

Identification

Travel History

Location

Self-assessed health status

Close contact to infected

Centralized data storage and sharing with authorities is standard practice in China

Dynamic QR code delivers up-to-date information on individual infection probability

Big Data analysis

Individual health assessment

Scan result options:
- Red: 14-day quarantine
- Yellow: 7-day quarantine
- Green: free to move

14d

7d

Housing complexes

Airports/ public transportation

Theaters/ event locatios

Restaurants

The Hangzhou Health Code:
In the first days, out of 7.25 million QR-verdicts, 316,000 were red and 200,000 were yellow → 4.4% of users were high and 2.8% medium risk. In contrast, approximately three months after launch of the app, the official case number for Hangzhou was at **only** 169.

?

How good is app-based health control?
There are several caveats:
- Self-assessed health status is unrealiable input
- Regionally fragmented use of apps reduces efficacy
- Questionable accuracy of geo-sat navigation

© MERICS

1. Introduction: Using data to fight the virus

In the global Covid-19 crisis, European governments find themselves struggling to decide on how to use digital technologies appropriately. They hope that using contact tracing apps can rekindle the economy while curbing the "R rate" – the rate of new infections – and keep the outbreak at bay. At the same time, they have to strike a difficult balance between personal data protection on one hand and effective data collection and analysis on the other.

So far, European countries have generally acted in a slow and uncoordinated manner concerning the deployment of data-driven solutions to fight Covid-19. The various technical solutions being discussed or rolled out by national governments differ on what data can be collected, where data should be stored, and the transparency of data-sharing agreements.

By contrast, China's government and companies did deploy data-driven solutions early on to battle the virus. They swiftly turned to AI-based and Big Data solutions for crisis management, enforcing their use across multiple departments. Therefore, looking at China can offer a valuable window into the future for Europe. But it is also important to recognize at least three specific features of China's approach that limit its relevance and applicability for other countries.

■ **First,** the People's Republic of China (PRC) has a relatively weak legal and institutional framework for personal data protection, favoring protection of party-state interests over individual civil rights. In cases of broadly defined public security and health issues, the state has direct access to data collected by bureaucracies and companies. Faced with the Covid-19 epidemic, this provided Chinese authorities with speedy access to sensitive information for individual contact tracing and monitoring.

■ **Second,** China's government started fighting the pandemic relying on an extensive pre-existing digital infrastructure that was already producing massive amounts of data. The Chinese government could readily transform the existing infrastructure and turn it into an integral part of its anti-coronavirus strategy, notably employing facial recognition solutions and so-called "super apps" like WeChat developed by commercial companies that routinely integrate user data and various services.

■ **Third,** the close ties between government and business enabled China's government to draw on large amounts of user data, often in real-time. China's major internet and communication technology (ICT) companies are privately owned. However, they are linked to the government by internal party cells, granted protection and favors or through public private partnerships.

The Chinese government itself – as well as some political actors and journalists in liberal democracies – has been quick to declare its approach provides a model for others to follow.[1] However, China's data-driven Covid-19 management is not as effective as it is often claimed or supposed in Western media reports or among politicians.

This study will examine three issues:

1) The various data-driven digital solutions that China employed.

2) China's personal data protection framework and how it has been implemented in the context of Covid-19 containment measures.

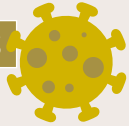**3)** The observed benefits and risks of the deployed data-driven solutions and how to evaluate them.

China's government and companies deployed data-driven solutions early on to battle the virus

Exhibit 1

Swift roll-out: Data-driven solutions supported China's anti-Corona fight

Timeline of outbreak and related app development

OUTBREAK EVENTS

December 8
First cases of 'Wuhan Pneumonia' reported

December 31
Wuhan Municipal Health Commission publicly acknowledges 27 cases

January 12
WHO announces official name of novel Coronavirus (2019-nCov)

January 20
Xi Jinping calls for fighting the epidemic. Confirmation of human-to-human transmission

January 23
Wuhan under lock-down, 13 cities follow next day; 639 confirmed cases in China

January 31
11,791 cases confirmed

February 12
Hubei reports 14,840 new cases in a single day

March 11
WHO declares Covid-19 outbreak a global pandemic

March 19
China reports no new locally spread infections

April 8
Wuhan lockdown lifted; China declares victory over Covid-19

April 17
Wuhan authorities adjust death toll; national total pushed to 4,632 deaths

December 2019 | January 2020 | February 2020 | March 2020 | April 2020

January 20
First special big-data working group coordinates with National Health Commission and relevant institutions across the country

January 30
Baidu Research launches LinearFold, an AI algorithm to speed up analysis of coronavirus RNA

February 2
Hospital staff and resource management platform goes live

February 8
Launch of tracking app „Close Contact"

February 9
Launch of Hangzhou Health Code

February 14
Company Dilusense launches "Body temperature detection guard"

February 15
FRT company Hanwang first to claim ability to identify masked faces

February 29
China's three major telecoms launch „Information Big Data Itinerary Pass"

March 20
Tencent launches „Study Resumption Code"

April 21
"Information Big Data Itinerary Pass" upgraded to include international travel, renamed "Anti-epidemic Health Information Code"

June 12
New Covid-19 outbreak in Beijing prompts mass testings and lockdowns

TECH DEVELOPMENT

Source: MERICS

© MERICS

2. How the state and firms deployed apps and data infrastructure
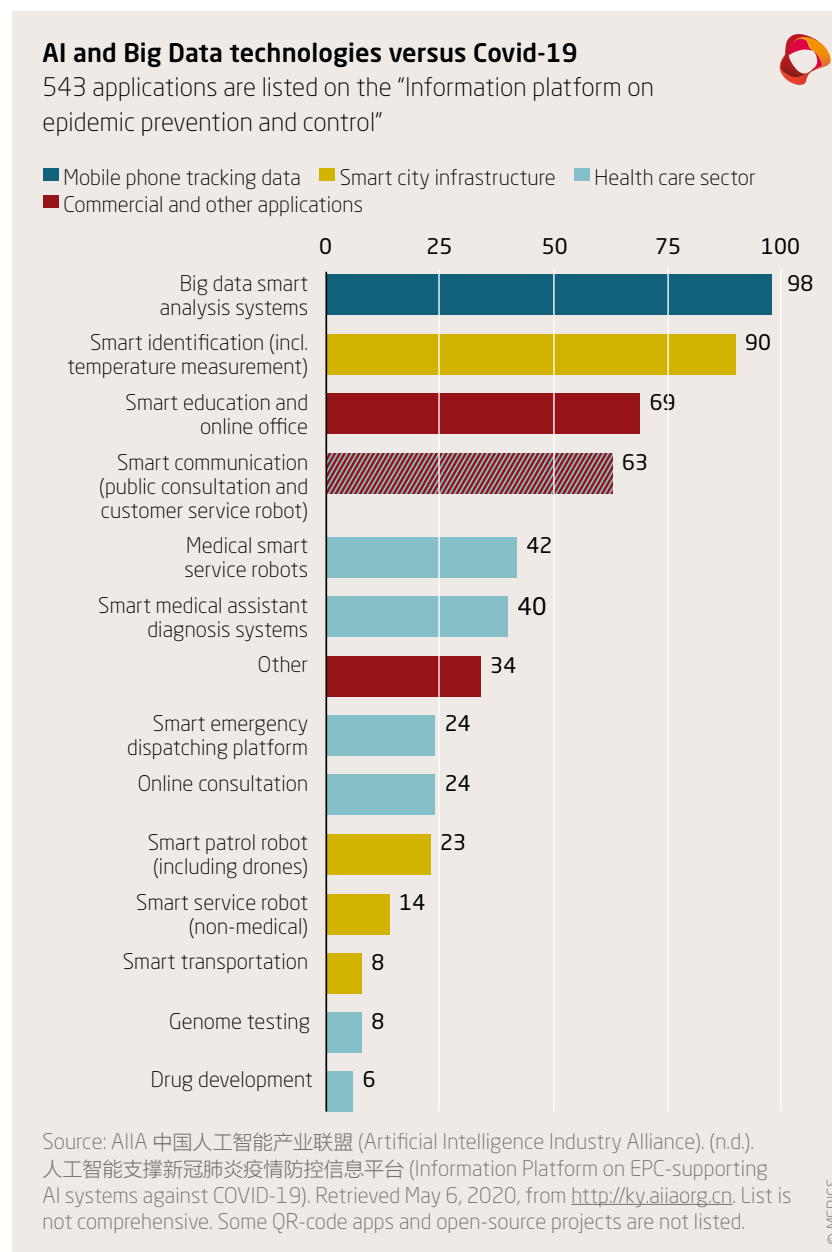
Exhibit 2

A wide range of AI and Big Data applications have been deployed in China to fight the spread of the novel coronavirus following its emergence in Wuhan in December 2019. There are three broad categories of tools and applications supporting the government's data-driven management of Covid-19.

1) Movement tracing tools

2) Recognition and identification technologies

3) Digital health sector applications

The outbreak of Covid-19 has also spurred innovation and development in other digital commercial markets not directly connected to the government's data-driven epidemic management strategies, such as online education, e-commerce plat-forms, or gaming. "The virus outbreak has fast-forwarded the development of the remote working (market) by five years," according to platform provider Tencent. However, an examination of these commercial aspects lies beyond the scope of this analysis (see Exhibit 2).

2.1. MACRO AND MICRO MOVEMENT TRACING TOOLS

Mobile phone tracking is at the heart of China's approach to Epidemic Prevention and Control (EPC). At the macro level, tracking has helped to monitor and visualize large-scale population movement. It has also enabled screening and monitoring of high-risk groups. Such tools have been developed either by telecom providers tracking registered phone numbers or by private companies who drew on data collected through multifunctional apps (including online payment, satellite local-ization, etc.). By mid-February, 40 percent of all Covid-19-related data harvesting was directed towards visualization and monitoring efforts to analyze the spread of the virus, according the China Academy of Telecommunication Planning Research (CAICT), an institution affiliated with the Ministry of Industry and Information Technology (MIIT).[2]

AI and Big Data technologies versus Covid-19
543 applications are listed on the "Information platform on epidemic prevention and control"

■ Mobile phone tracking data ■ Smart city infrastructure ■ Health care sector
■ Commercial and other applications

Big data smart analysis systems	98
Smart identification (incl. temperature measurement)	90
Smart education and online office	69
Smart communication (public consultation and customer service robot)	63
Medical smart service robots	42
Smart medical assistant diagnosis systems	40
Other	34
Smart emergency dispatching platform	24
Online consultation	24
Smart patrol robot (including drones)	23
Smart service robot (non-medical)	14
Smart transportation	8
Genome testing	8
Drug development	6

Source: AIIA 中国人工智能产业联盟 (Artificial Intelligence Industry Alliance). (n.d.). 人工智能支撑新冠肺炎疫情防控信息平台 (Information Platform on EPC-supporting AI systems against COVID-19). Retrieved May 6, 2020, from http://ky.aiiaorg.cn. List is not comprehensive. Some QR-code apps and open-source projects are not listed.

© MERICS

Box 1

HOW QR HEALTH CODES WORK

At the core of most apps are algorithms that gauge the probability of an individual having the virus, based on the phone owner's travel history over the previous 14 days, geographic location and personal identification. User-submitted information can include contact with an infected person and a self-assessment of their health status. These individualized digital health assessment certificates are stored in QR codes. When scanned, these return one of three results. Green for "allowed to move freely," orange for "recommended for seven-day quarantine," or red for "recommended for 14-day quarantine". Most public transport, supermarkets, and housing complexes now request individuals to show a QR code instead of the previously issued paper certificates.[8] Most QR apps are designed to produce dynamic codes that once scanned retrieve individual information from a central database. Information in static QR codes, in contrast, is permanently built into the code.

Mobile tracking data was among the inputs used to develop QR-code health apps for individual use, which became central to China's ability to lift quarantine restrictions. Co-operation between tech firms and local authorities played a major role: Alibaba assembled a team of engineers the day after Hangzhou – the internet giant's home city – went into lockdown on February 3rd. Working with Hangzhou city government, Alibaba conducted the first public trials of the QR "Health Code" (健康码) just three days later. Within a week, the Hangzhou government began rolling out the QR "Health Code" (健康码) onto phones city-wide. The QR code was adopted by the rest of Zhejiang province, the nearby metropolis of Shanghai, and the western powerhouse province of Sichuan on February 12th.

However, the Hangzhou city hotline received more than 50,000 complaints within the first week about inexplicable QR results, and several cities recorded QR app crashes in the following weeks. Alibaba and various project partners have subsequently made similar versions of the "Health Code" available in over 200 Chinese cities and on multiple platforms. The app is currently used by almost all of China's 900 million internet users.[3]

At least 100 similar QR-based health assessment apps have been launched by other developers apart from Alibaba. Many provinces introduced regional health codes,[4] and private companies started offering similar products, for instance the "Daily Health Check-in", a new feature in DingTalk (Alibaba's company communication platform), and the "Study Resumption Code" by Tencent, started in the southern province of Guizhou. China's three telecom providers (China Mobile, China Unicom, China Telecom) jointly launched the "Information Big Data Itinerary Pass" (通信大数据行程卡) on February 29th, pooling data on China's 1.6 billion registered phone numbers and the geographic movement of their customers.

However, these new QR apps lack mutual recognition standards and interoperability features, which undermines their usefulness. This has caused confusion and even tensions at provincial borders: citizens were not allowed to cross into other administrative districts when they were not using the same app.[5] Some provinces have started signing cooperation agreements on joint health code recognition, e.g., between Zhejiang, Hainan, Hubei, Sichuan and Hubei.[6] This fragmentation of applications is problematic because, according to studies, effective use of tracing apps for containment requires a relatively high amount of the overall population with smartphones to run the same app, or apps that collect and process data based on the same standards (see Box 1).[7]

2.2 RECOGNITION AND IDENTIFICATION TECHNOLOGIES

Surveillance tech has advanced significantly in response to the needs of emergency management. In the early stage, Chinese experts had called the recognition and identification infrastructure of smart cities almost "useless".[9] For example, after the government mandated facemasks, facial recognition technology (FRT) proved able to recognize only 50 percent of masked faces. However, after engineers trained the AI recognition systems, using, amongst others, a police identification database of some 1.2 billion people,[10] individuals wearing facemasks could be recognized with accuracies of above 90 percent.[11] Additionally, Hanwang, MegVii, and other private companies have now added temperature sensors to their facial recognition devices that – after individual identification – measure individuals' temperature with an error rate of ±0.3° Celsius.

Infrared identification solutions have been developed for commercial use as an alternative to facial recognition systems. Dilusense, a Beijing based FRT company with cameras in multiple regions, including the Hong Kong-Macao-Zhuhai bridge and cities in Zhejiang province, launched the "body temperature detection guard" (体温检测门卫机). It is a gate-like machine for use at entry and exit points

<div style="color:#e8613c">Surveillance tech has advanced significantly in response to the needs of emergency management</div>

to buildings, e.g., housing complexes. People's body temperatures are taken with infrared thermal imaging and announced by a voice system. A summary is sent to the company.[12] Dilusense developed its technologies partly by supplying the Public Security Bureau of Yiwu County in the Xinjiang region,[13] for surveillance of the Muslim Uighur population.

Dilusense also provided its facial recognition infrastructure to the city of Wenzhou to enforce measures that required every household to appoint one family member who was allowed on shopping trips every two days.[14] Recognition and identification technologies beyond facial recognition have also been vital to China's epidemic prevention control. Drone maker DJI, for example, has provided the city of Shenzhen and 1,000 counties with disinfectant-spraying drones.[15]

2.3 DIGITAL HEALTH SECTOR APPS FOR RESEARCH, CONSULTATION AND RESOURCE MANAGEMENT

Due to recent digitalization efforts, China's health sector has been well prepared to use data-driven tools. A national drive led since 2018 by the State Council and the National Health Commission has pushed ahead the digitalization of information channels. These include medical records, lab evaluations, and image archiving, areas where individual data and diagnostic tools overlap. This initiative has stimulated the use of big data and AI to implement platform-based early warning systems, disease monitoring, and resource management systems. Areas to benefit include research and development (R&D) in public health and medicine.

For instance, a prediction model developed by PingAn Technology is helping official health care bodies in the cities of Chongqing and Shenzhen to predict outbreaks with accuracy rates of more than 90 percent.[16] The National Supercomputing Center in Shenzhen, in collaboration with companies like Sensetime, provides high-performance computing support to researchers conducting large-scale screening of potential drugs, and working on predicting virus mutations. Similar efforts have already succeeded in drastically reducing the time needed to evaluate CT scans or analyze the genetic RNA structure of SARS-CoV-2.

Online platforms have been an essential support for many medical institutions to develop efficient responses to Covid-19-related challenges. Government data from MIIT shows more than 190 public medical institutions and nearly 100 corporate internet hospitals across the country currently provide free online consultations that partially alleviate the pressure on conventional public hospitals. Good Doctor Online, Chunyu Doctor, Ping An Good Doctor, and other enterprises have pooled the resources of over 10,000 medical experts in the fields of respiratory, infectious diseases and internal medicine to provide free consultations for patients.[17] These platforms have also helped improve resource management; for instance, "Huoshaoyun Health Management Platform" (火烧云健康管理平台) now provides the Fujian local government with a database of 60,000 employees from 4,500 enterprises in the health sector to coordinate the deployment of resources and to relieve hospital staff.

2.4. SOCIAL CREDIT SYSTEM HAS BEEN USED TO ENFORCE COMPLIANCE

Digital tools have played an important role in monitoring compliance and supporting extensive analog EPC measures. To enforce lockdown measures, travel bans, centralized quarantine, and home isolation as well as strict hygiene requirements for employers and building managers, the government has been able to make use of the Social Credit System. The system is a framework of interconnected databases and rating mechanisms that tracks compliance with laws and regulations – and a key project of the government to use digitization and pooling of data sources for social governance. Serious offenders are blacklisted and face coordinated punishments and restrictions across government departments.

To boost compliance with pandemic containment regulations, people and companies who hid infections, broke mandatory quarantine and other preventive measures found themselves blacklisted and sanctioned.[18] At the same time, to avoid excessive burdens for individuals and companies suffering income losses due to the pandemic, the government offered temporary exemptions from sanctions, when they failed to repay debts or pay social insurance fees.[19]

3. Beijing's epidemic management prioritizes security over privacy

China's data-driven approach to combatting the pandemic rests on digitalization and informatization policies reaching back more than a decade. Most recently, the 2016 National Informatization Development Strategy[20] and the "Internet+" strategy in the current five-year plan (2016–2020), promote the use of ICT in all policy areas, including public health.[21] As part of the "Internet+" strategy, the "Internet+Health Care" initiative has focused on the expansion of e-services such as online consultation, and establishing a national information system. The initiative also explicitly seeks to use big data analysis for epidemic prevention and management.

China's health sector has been well prepared to use data-driven tools

Exhibit 3

China's authorities have long treated data-driven solutions and digital infrastructures as essential for effective governance. New epidemic control measures and policies during the Covid-19 crisis also benefited from the rapid build-out of monitoring and surveillance technology across China in past years.

One key goal of the Social Credit System, a comprehensive monitoring and tracking system currently developed under the auspices of the central government, and efforts to promote "smart city" development since 2016 has been to integrate data sources across government departments.[22] Under the rubric of "safe cities" policies, public spaces from schools to streets and transport hubs are now fully monitored by digital security technologies like facial recognition systems.[23] Experience gained in these efforts enabled companies such as Hanwang, Dilusense, and Sensetime to adapt their algorithms quickly when the coronavirus outbreak required swift solutions for epidemic control.

3.1 CHINA'S DATA PROTECTION LEGISLATION IS FRAGMENTED

China's legal and regulatory framework reflects the party-state's view of data as a freely accessible governance resource and a commodity aiding economic development. Laws and regulations focus on facilitating data aggregation and on sharing between stakeholders rather than privacy rights. Regarding personal data, there is no comprehensive framework comparable to the European Union's *General Data Protection Regulation* (GDPR). The *Cybersecurity Law* (CSL), in force since 2017, features a section on data privacy, defining, for instance, principles of legality, proportionality and necessity for the collection and use of personal data.[24] But the law also requires network and service providers to verify user identities and share data with supervisory and public security organs.

The new *Civil Code* adopted in May 2020 has strengthened privacy protection by more clearly defining under what circumstances personal information can be gathered and used and by expanding civil liability for infringement of privacy rights.[25] However, the main definitions and benchmarks for personal data protection in China are found in non-binding standards like the *Personal Information Security Specifications* (PIS) issued by the *National Information Security Standardization Technical Committee*.[26] According to these standards, explicit consent and encryption are generally needed to collect sensitive information like biometric data, travel history or health information. The *Basic Healthcare* and *Health Promotion Law* of 2019 only broadly prohibits illegal collection, use and sale and it stops short of clearly defining personal health data.[27]

To share or not to share
Chinese and European approaches to data

Comparison of key data protection standards:
🔴 Absent 🟠 Partially adressed 🟢 Adressed

Assessment: Strength of the general legal framework for personal data protection	China	European Union
Privacy protected by constitution	⚪⚪🟢	⚪⚪🟢
Definition of personal data	⚪⚪🟢	⚪⚪🟢
Legal framework for personal data protection and coherence	⚪🟠⚪	⚪⚪🟢
Independent data protection agency	🔴⚪⚪	⚪⚪🟢
Civil society participating in regulations and oversight	🔴⚪⚪	⚪⚪🟢
Possibility of consumer lawsuit	⚪⚪🟢	⚪⚪🟢

Assessment: Emphasis of best practices by relevant agencies during Covid-19	China	European Union
Data minimization	⚪⚪🟢	⚪⚪🟢
Purpose limitation & voluntary nature	⚪🟠⚪	⚪⚪🟢
Temporary nature and review of continued necessity	⚪🟠⚪	⚪⚪🟢
Transparency	⚪🟠⚪	⚪⚪🟢
Security	⚪🟠⚪	⚪⚪🟢
Restriction of data sharing with authorities	🔴⚪⚪	⚪🟠⚪

Source: Based on relevant personal data protection legislation, CAC Notice (Feb 4, 2020) and recommendations by the APP Working Group (Feb 27, 2020) and on Common EU-Toolbox for Member States (April 15, 2020).

© MERICS

3.2 THE GOVERNMENT CAN ACCESS PERSONAL DATA ON 'PUBLIC EMERGENCY' GROUNDS

In a public emergency such as a pandemic, the *CSL* and *PIS* permit derogation from existing data protection norms. Authorities are obliged by these laws to limit data collection to what is required to address the emergency, but the exemption permits them to access, for instance, personal data collected via mobile devices. Retention of personal data by telecoms and online service providers is the norm, not the exception.

In early February, the *Cyberspace Administration of China (CAC)*, a cross-ministerial coordination agency in charge of internet oversight, called on government departments to actively cooperate with "capable firms" and allowed the publication of desensitized data for epidemic protection without consent. Publication of raw data remains prohibited (see Exhibit 3).[28]

Laws and regulations governing the collection and use of personal data primarily address the private sector. Government departments have greater legal scope to collect and share data. Central or local governments can, if they wish, give companies broad and rapid access to personal data by entering into agreements for them to receive and process the data. This has allowed the merging of public and private corporate data pools for crisis response work.

Facial recognition technology companies were even provided with a police database to train their algorithms to recognize individuals wearing facemasks. Public security organs play a key role in the drafting and implementation of regulations and have a keen interest in the collection of a wide array of personal data.

3.3 CRISIS HIGHLIGHTS WEAK PROTECTION OF PRIVACY RIGHTS

The government push for data-driven containment of Covid-19 has laid bare weak spots in personal data protection. Regulations are focused on providing government organs with enforcement information, rather than on anonymizing data or other protective measures. According to a note issued by the *Cyberspace Administration of China* (CAC) that laid the groundwork for the implementation of digital solutions in the epidemic, citizens are not obliged to use them. But the note also fails to establish additional safeguards for data protection to address the increased usage, analysis, and transfer of personal data during the crisis, which has created more potential for its misuse.[29]

Many apps are integrated into bigger online communication and payment ecosystems pooling vast amounts of personal data. Developers of new contact tracing and health apps tend to build on existing user agreements and standard privacy policy allowing them to share, transfer and disclose personal information to authorities for public safety or public health matters without additional consent.[30]

In light of the vast growth of data use and low transparency, the oversight of data protection is insufficient. The sheer amount of new public-private partnerships using different data sets and algorithms limits the possibility of efficient oversight of user agreements or actual practices. To remedy this problem, the *App Governance Working Group* was set up in 2019 as a watchdog. However, this is not an independent inspection agency but part of another committee that answers directly to the CAC and only addresses case-based violations (see Box 2).

The government is aware of the practical challenges stemming from fragmentation of contact tracing apps. New directives formulated since early April 2020 are aimed at standardizing data sets and algorithms so that one code can be used nationwide (一码通用).[31]

Box 2

<div style="background: #eceae6; padding: 1em;">

KEY AGENCIES BEHIND STANDARDS AND GUIDELINES

The **Cyberspace Administration of China (CAC)** was founded in 2014 as a super-agency in charge of cyberspace governance, from drafting regulations to inter-ministerial coordination and policy implementation. The CAC answers directly to the Central Cyberspace Affairs Commission, which is led by Xi Jinping.

The **National Information Security Standardization Technical Committee (TC260)** established in 2002 is subordinated to CAC and led by representatives from key government organs. Also represented are state-owned and private ICT companies such as ZTE, Huawei, Baidu, Alibaba, and Tencent.

The **App Governance Working Group** was established in late 2019 as a lower-level working group of the TC260. It is tasked with monitoring the protection of personal data in applications and coordinating different state-affiliated consumer and ICT associations.

</div>

Government departments in China have greater legal scope to collect and share data

Exhibit 4

While improvements are on the horizon with a *Personal Data Protection Law* and *Data Security Law* on the legislative agenda,[32] constraints on government organs will remain limited. On an institutional level, the newly established public-private partnerships and procedures for data exchange in their agreements are likely to become put on a permanent basis and to be adapted for uses beyond epidemic management.

4. Assessing China's data-driven approach to crisis management

As the analysis above has shown, China's data-driven management approach is inherently loaded with tension: China's government, in alliance with national ICT companies, has rapidly employed and upgraded a wide range of digital technologies to track, monitor, and treat the virus among its citizens. It has, however, prioritized quick and massive data collection and sharing, without equal attention to adequate safeguards for personal data protection.

Consequently, an assessment of the efficacy of China's data-driven management needs to reflect on benefits and risks (see Exhibit 4). The deployed solutions have enabled the Chinese government to quickly monitor, display and publicize the spread of the virus. Consequently, the leadership has been able to nurture a sense of safety and convenience in the population which has helped to restart societal and economic life. Especially within the health care sector, digital solutions helped to alleviate pressure on hospitals struggling with increased patient throughput.

However, the technical specifications of personal health apps are opaque, some apparently lack security in terms of data protection. Many accounts of false individual health status assessments have called into question the accuracy of data-driven solutions. In addition, officials on the local level have used gathered data to an extent that not permitted by Chinese law. As a result, data has been leaked, both accidentally and deliberately, and appeared on social media. This has fostered widespread discrimination and stigmatization of specific groups, such as people from areas with high Covid-19 infection rates. The following sections will look at these aspects in more detail.

Benefits for the party-state, risks for the people
Assessing the efficacy of China's data-driven Covid-19 management

Benefits			Distortion of pandemic assessment	Risks
	Restarting economy and society	**Boosting technological capabilities**	**Distortion of pandemic assessment**	**Privacy infringement**
Personal data governance	Quick data collection and aggregation	High acceptance of apps among population	Opaque and potentially flawed algorithms	Non-enforcement and misuse on local level
Mobile phone tracking	Real-time monitoring of mobility and health status	Quick go-market and test opportunities for private companies	False health status assessments due to inaccurate coding and user input	Lack of high encryption and verification standards
Smart City infrastructure	Comprehensive tracking and monitoring; identification of potential infections	More accurate facial recognition	Overreliance on facial recognition accuracy	Non-consented expanded use of personal data even after pandemic
Health sector infrastructure	Alleviation of pressure on hospital management and increased patient throughput	Improved AI-based diagnostics and patient record management	Delayed or inadequate data transmission	Data silos can hamper joint research
Public response	Sense of job security, convenience and safety	Increased public acceptance of digital monitoring and surveillance	Complaints over intransparent and false health assessments	Mistrust and societal stigmatization

Source: MERICS

© MERICS

4.1 USAGE OF TECHNOLOGICAL SOLUTIONS

China's authorities were quickly able to employ data-driven solutions to trace people's movements, contacts and health status by adapting and upgrading the existing digital technology ecosystem, which enabled them to revive public life in a strictly controlled form. The benefits and risks vary between the three different categories of solutions analyzed.

MOBILE TRACING TOOLS

On a national level, ready-to-use mobile phone tracking solutions have helped to monitor, display and publicize the spread of the virus. It provided the government and the public with easy access to interactive services. For instance, people could enter their train or flight number to check if there had been an infection reported related to their journey and assess hospital ICU capacity or the density of people at a given location.[33]

For ICT companies and app developers, Covid-19 has been a unique opportunity to quickly launch, test and refine new solutions based on massive user data and feedback. After the first individual health QR code launched in Hangzhou, other private companies quickly rushed to market with their own app versions. Alibaba claims to have powered some 200 regional variations while Tencent states that 300 cities implemented its QR code.[34]

The technical specifications of personal apps are opaque and offer questionable accuracy and poor security. Few makers of the widely adopted QR-code health apps have disclosed details of how probabilities are computed. Predicting viral outbreaks by relying on user input, such as self-assessed health status, has proved to be misleading. Furthermore, technical boundaries, such as a limited geographic accuracy when locating mobile phones, will leave a certain error margin and is likely to lead to false positives and false negatives (i.e., falsely identified infected and uninfected).[35]

No app maker has disclosed their algorithm, which has sparked debates among analysts and tech bloggers. Numbers from the first iteration of the Hangzhou Health Code QR-code app suggest that it was not designed to red flag the actually infected but to issue overly cautious quarantine requests.

Out of 7.25 million QR verdicts in the first few days, 316,000 were red and 200,000 were yellow, suggesting that 4.4 percent of the related persons were at high risk and 2.8 percent at medium risk.[36] However, approximately three months later, the city authorities have only acknowledged a total of 169 officially diagnosed cases of Covid-19.

Limited geographic accuracy when locating mobile phones may have produced false health status assessments: users have reported sudden, inexplicable changes to their health status or been denied access to their own apartments.[37]

The dynamic QR codes in use (as opposed to static codes) allow data retrieval relating to the scanned phone and its user from a central database that contains the individual information.[38] High standards in encryption, verification, and access control are therefore required – but currently absent – to prevent health code information being accessed by unauthorized scanning clients.

RECOGNITION AND IDENTIFICATION TECHNOLOGIES

Satellites in China's home-grown Beidou navigation system have enabled the Chinese government to enhance infrastructure setup and resource deployment. For example, Wuhan University was able to collect and analyze multiple data streams to find the best spots for huge makeshift hospitals. High-resolution earth observation satellites then monitored their construction. E-commerce company JD also delivered medical equipment to Wuhan's outlying hospitals with drones and robots operating on Beidou.[39]

Companies have refined their facial recognition technologies rapidly to provide comprehensive monitoring of individual behavior. A key innovation has been body temperature testing, in addition to monitoring travel history, quarantine and mask wearing compliance (via drones), The developers claim accuracy levels of more than 99 percent for temperature monitoring[40], (citing an error rate of ±0.3° Celsius) and more than 90 percent for facial recognition of people wearing masks.[41] However, accuracies may be lower than claimed. One survey from December 2019 found that around 60 percent of Chinese respondents had encountered issues with facial recognition technology (FRT) in situations that included housing complexes and public transport.[42]

Companies have refined their facial recognition technologies rapidly to provide comprehensive monitoring of individual behavior

Big data and AI-based solutions have supported resource management and patient treatment in the health care sector. Solutions include hospital-wide management of staff and beds, and between hospitals and extend to AI-based remote online consultations, on-site diagnosis, and patient care.[43] For example, a health platform built for the Jiangsu Health Commission to allow online consultation and standardize medical diagnostic forms (ERM) has been adopted by 68 hospitals and linked to 20 other health care platforms in the outbreak.

Poor quality data collection may introduce risks into these efforts. Misleading data could arise from an unfortunate combination of a backward collection method (in most hospitals patients are identified by handwritten form-filling) and a flawed classification system. For example. the option "unknown pneumonia" (potentially Covid-19) on CDC infectious disease reports brings so much extra bureaucratic burden that doctors may be discouraged from ticking this box.[44]

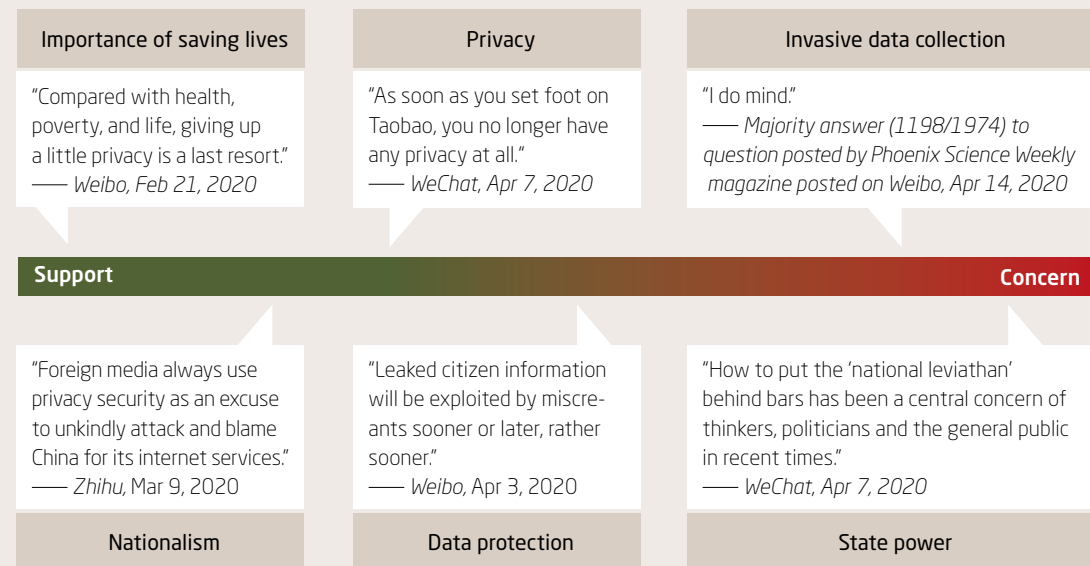## 4.2 IMPLEMENTATION OF PERSONAL DATA PROTECTION

The central government has endorsed quick and massive data collection and sharing to monitor and mitigate the spread of the virus. On a local level, QR code-based health apps have quickly become *de facto* mandatory, playing a gatekeeper role for access to residential and commercial buildings. Consequently, a high percentage of China's urban population is presumed to have installed such apps.

However, the ad hoc emergency EPC actions of local authorities have counter-acted some of the potential EPC benefits by introducing wider structural risks. Local governments have permitted companies and app developers to collect additional user data in pursuit of their own commercial interests. They have granted options for sharing data in public emergencies with scant restrictions on seeking user consent for data sharing with third parties. Developers have relied on already-granted user consent, as many apps have been integrated into existing platforms belonging to China's leading ICT companies.[45] Sensitive personal information has also been transferred to public security bodies without explicit user consent or knowledge.[46]

Grassroots public officials and party members have made use of gathered data beyond the constraints of the law. Local cadres were faced with the political priority of detecting infected individuals quickly and the rapid reduction of new cases at all costs. They had no professional incentives and also no training to build awareness of personal data protection or development of specific guidelines for it.

Sacrificing privacy over collective safety is no sure thing for Chinese citizens
Spectrum of opinions on social media platforms billboard

Importance of saving lives	Privacy	Invasive data collection
"Compared with health, poverty, and life, giving up a little privacy is a last resort." —— *Weibo, Feb 21, 2020*	"As soon as you set foot on Taobao, you no longer have any privacy at all." —— *WeChat, Apr 7, 2020*	"I do mind." —— *Majority answer (1198/1974) to question posted by Phoenix Science Weekly magazine posted on Weibo, Apr 14, 2020*

Support ———————————————————————— **Concern**

"Foreign media always use privacy security as an excuse to unkindly attack and blame China for its internet services." —— *Zhihu, Mar 9, 2020*	"Leaked citizen information will be exploited by miscreants sooner or later, rather sooner." —— *Weibo, Apr 3, 2020*	"How to put the 'national leviathan' behind bars has been a central concern of thinkers, politicians and the general public in recent times." —— *WeChat, Apr 7, 2020*
Nationalism	Data protection	State power

Source: Manual search for keywords related to data protection, privacy and surveillance on China Weibo, Douban, WeChat and Zhihu from February to mid-April 2020; no quantitative data analysis)

© MERICS

As a result, personal data has been – both accidentally and deliberately – leaked and appeared on social media. This has fostered widespread discrimination and stigmatization of specific groups, such as people from highly infected areas. The government has announced its intention to introduce stricter regulations for personal data use by corporates. However, China's party-state government is unlikely to shift its core approach in order to address personal data misuse, especially where party-state interests are involved.

4.3 PUBLIC RESPONSE

Within the official party-state media, China's government has portrayed the usage of data-driven solutions on a macro level as "precise management and control of the disease." Moreover, Beijing emphasizes societal benefits, e.g., restricted access to residential buildings by "outsiders", as well as economic incentives to secure one's workplace with the help of permits to enter office buildings.[47]

The gatekeeper function of health control apps has offered Chinese citizens a sense of security. Large parts of China's urban society have seemingly embraced the new apps and readily installed them to gain individualized risk/health assessments. Installation and usage of apps is not mandatory in a legal sense. But they offer healthy citizens a less restricted, more normal everyday life. Moreover, most personal health QR codes operate on widely used "super apps" like Alipay or WeChat. This convenience very likely contributes to Chinese people being more willing to support them.

Chinese citizens have also voiced criticism of recurring error reports and data leakages. Between January and February 2020, the official "App Governance Working Group" received 300 complaints about COVID-19 -related apps that collect personal data.[48] Complaints were made against a variety of apps and platform solutions, not only contact tracing. In its report, the working group merely responded by advising people to read user agreements carefully.

Incidents reported in China's media and reactions published in social media reflect the spectrum of public anxieties about personal data protection (see Exhibit 5).

Covid-19 has stimulated a new round of privacy debates in China, which have evolved around the difficult balance of addressing public safety concerns and providing privacy protection. A proponent of the former position is Liu Deliang, professor at Beijing Normal University's Law School. He argues that data leaks should be strictly punished, but that further "unnecessary" limitations would undermine the state´s capacity to handle data.[49] Objectors include law professor Yang Jian from Nanjing Normal University, who argues that facial recognition technologies greatly intrude on personal rights and that personal data protection rights should always be maximized and prioritized.[50]

These public voices are a strong signal that the party-state's data-driven approach is not uncontested within China. To what extent Chinese expert voices calling for privacy protection modeled according to the GDPR will continue to exist or even gain influence within the PRC will depend partly on how effectively European actors design and implement technological solutions for Covid-19 management.

5. Recommendations: Assessing the efficacy of China's data-driven crisis management

Our assessment of the efficacy of China's data-driven management approach to Covid-19 has revealed a mixed picture. The speed and scope of technological adaptation and adoption has shown Beijing's ability to promote technical solutions to meet urgent political needs, and to some extent public needs too. The digital measures have contributed to an enhanced perception of public security among China's citizens. However, this has come at the expense of personal data protection. It has also exposed weaknesses in technical functionality and limitations on the central and local authorities' ability to secure full public support without greatly improving personal data protection.

China is ahead of Europe on the pandemic curve, so there is much that European actors can learn from an assessment of China's data-driven crisis management:

LESSONS FOR EUROPE

- **Assess data-driven digital solutions in greater detail and specificity:** As China's experience has shown, mobile phone tracing data and smart city infrastructure applications come with high risks of inaccuracy and misuse. Digital solutions in the health care sector, i.e. in hospital management or diagnostics have proven to be mainly beneficial.

- **Initiate a holistic debate about app infrastructure:** Emphasize transparency and user consent on data sharing beyond the current focus on data storage. Evidence from China suggests that obsessive data sharing is one key source of data breaches/leakages. This endangers public support for contract tracing applications.

- **Learn from best practices in other countries that have done well in fighting the pandemic so far.** Taiwan, Hongkong and Singapore have managed to maximize the benefits of data-driven solutions even better than the PRC. In those countries, app usage was often mandatory. However, clear legal restrictions applied, and on- and offline measures were communicated actively and transparently.

European actors can learn much from an assessment of China's data-driven crisis management

- Strengthen civil society participation and public transparency and media engagement to prevent rent seeking from vested interests during the adoption of digital solutions. An existing framework for personal data protection is not enough to prevent infringement of privacy, especially in countries that lack powerful actors to enforce the implementation of privacy rights.

DEALING WITH CHINA

- Mitigate against privacy and data security risks stemming from China's increasing efforts to export digital health products/apps under its Digital Silk Road strategy. Companies like Huawei or Alibaba have started to offer communication and diagnostics work with hospitals and health authorities in Italy and France. European government should ensure that personal health data of European citizens are stored in EU-based data centers. Otherwise, if Chinese companies transfer personal data to China, i.e. under the EU's standard contractual clauses, privacy protection up to the GDPR level can't be ensured.

- Track the evolving integration of different digital applications and models. New data collection methods established through epidemic prevention efforts may serve as a model and feed into other monitoring initiatives such as the Social Credit System. Hangzhou has sought to introduce an integrated health score including individual behavior such as smoking or exercise. A pilot project in Tiantai, Zhejiang, uses the grading and health code model for discipline inspection and monitoring work of the Communist Party. Understanding this is relevant in the broader context of Chinese governance.

- Leverage ongoing privacy debates within China to advocate for European interests. Domestic public voices put pressure on China's government to refine and unify personal data protection. European politicians can link their own reasoning to legal and economic arguments from Chinese experts when engaging with the Chinese government.

- Track open source initiatives to explore potential for corporate-led cooperation: Corporates have announced plans to make open-source platforms available for tackling various aspects of the pandemic. For example, Baidu has made its RNA folding prediction algorithm LinearFold publicly available.

1 | E.g. Wu Xifeng, Xu Xiaolin andWang Xuchang (2020). "6 Lessons from China's Zhejiang Province and Hangzhou on How Countries Can Prevent And Rebound From an Epidemic Like COVID-19." World Economic Forum, March 12, 2020. https://www.weforum.org/agenda/2020/03/coronavirus-covid-19-hangzhou-zhejiang-government-response/. Accessed: June 11, 2020; AFP (2020). "COVID-19 | Can China's model work for the West?" The Hindu, March 22., 2020. https://www.thehindu.com/news/international/covid-19-can-chinas-model-work-for-the-west/article31136788.ece. Accessed: June 11,2020.

2 | CAICT (China Academy of Telecommunication Planning Research of Ministry of Industry and Information Technology) (2020). "Research Report on Data and Smart Applications for Epidemic Prevention and Control (Version 1.0)." http://www.caict.ac.cn/english/yjcg/qwsj/202003/P020200325657818669882.pdf. Accessed: June 12.2020.

3 | Sina News (2020). "Almost 900 million people nationwide use Tencent's Health Code, data queries have skyrocketed to 6 billion (全国近9亿人都在用腾讯健康码访问量破60亿)." https://tech.sina.com.cn/roll/2020-03-10/doc-iimxxstf7793469.shtml. Accessed: April 22, 2020.

4 | While some local governments publicly provide regularly updated datasets regarding on confirmed infected, suspected, and released cases, intervals and data formats are often fragmented and differ across regions and cities, some do not provide such geospatial data at all CAICT (China Academy of Telecommunication Planning Research of Ministry of Industry and Information Technology) (2020). "Research Report on Data and Smart Applications for Epidemic Prevention and Control (Version 1.0)." http://www.caict.ac.cn/eng_2020/lb/202004/t20200408_278749.html.

5 | Wang Yang 王阳, and Zhang Shoukun 张守坤 (2020). "健康码何时实现全国互通互认 (When Will the Health Code Be Recognized Nationwide?)." Xinhua, March 30, 2020. http://www.xinhuanet.com/2020-03/30/c_1125785795.htm. Accessed: April 10, 2020.

6 | Han Dandong 韩丹东, and Qi Zhengbei 祁增蓓 (2020). "多地实现防疫健康码互通互认 专家提醒：严防健康码数据泄露或被滥用 (Mutual Recognition of Epidemic Prevention Health Codes Has Been Achieved in Many Places Experts Caution: Guard against Health Code Data Leakage or Abuse)." Xinhua, March 18, 2020. http://www.xinhuanet.com/politics/2020-03/18/c_1125727318.htm. Accessed: April 5, 2020.

7 | Patrick Howell O'Neill, Patrick Howell (2020). "No, Coronavirus Apps Don't Need 60% Adoption to be Effective".MIT Technology Review, June5,2020. https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/. Accessed: June 12,2020.
Kelion, Leo (2020). "Coronavirus: NHS contact tracing app to target 80% of smartphone users." BBC, April 16, 2020. https://www.bbc.com/news/technology-52294896. Accessed: June 11, 2020.

8 | Xia Xiaohua 夏小华 (2020). "你绿了吗? 中国推健康码引发防疫与监控争论 (Are You Green? China's Push for Health Codes Sparks Debate on Epidemic Prevention and Surveillance)." Radio Free Asia, 2020. https://www.rfa.org/mandarin/yataibaodao/huanjing/hx2-03042020111216.html. Accessed: May 5, 2020.

9 | Li Bin 李斌, Yang Na 阳娜, and Guo Yujing 郭宇靖 (2020). "战'疫'中，中国人工智能开启'快进键' (Fighting the 'Epidemic', Chinese AI Pushes the 'fast Forward' Button)." Xinhua. http://www.xinhuanet.com/2020-04/22/c_1125887785.htm. Accessed: April 24, 2020.

10 | Bondade, Navin (2020). "How China built facial recognition for people wearing masks." Techgrabyte, March 21, 2020. https://techgrabyte.com/hanwang-china-facial-recognition-people-masks/. Accessed: March 14, 2020.

11 | AIIA 中国人工智能产业联盟 (Artificial Intelligence Industry Alliance) (2020). "人工智能助." BBC, 力新冠疫情防控 调研报告 (Research Report: How Artificial Intelligence Helps Epidemic Prevention and Control against COVID-19)." http://aiiaorg.cn/uploadfile/2020/0324/20200324060228591.pdf.

12 | Security Knowledge Network 安防知识网 (2020). "人脸识别技术在疫情防控当中有什么作用 (What Role Does Facial Recognition Technology Play in Epidemic Prevention and Control)." 电子发烧友网 (Elecfans). http://www.elecfans.com/consume/1167543.html. Accessed: April 17, 2020.

13 | Dilusense 卢深视 (n.d.). "City of Piece 平安城市." http://www.dilusense.com/public/index.php/index/index/yingyong/53. Accessed: May 8, 2020.

14 | Dilusense 卢深视 (2020). "3D战'疫' | 3D视觉技术助力温州疫情防控 赋能国内首个智能感管系统示范基地 (A 3D War against the 'Epidemic' | 3D Vision Technology to Help Wenzhou Epidemic Prevention and Control, Enabling the Country's First Demonstration Base for Intelligent Sensor System)." February 14, 2020. https://mp.weixin.qq.com/s/IE_GBLKv6uCV-L9WxTYGLIw. Accessed: April 29, 2020.

15 | DJI (2020). "DJI Helps Fight Coronavirus With Drones - DJI ViewPoints." DJI Articles. February 12, 2020. https://content.dji.com/dji-helps-fight-coronavirus-with-drones/. Accessed: April 29, 2020.

16 | Dai, Sarah (2020). "How China's Investment in Health Care AI Helps It Deal with the Coronavirus Crisis." South China Morning Post, March 9, 2020. https://www.scmp.com/tech/policy/article/3073929/how-chinas-investment-health-care-ai-helps-it-deal-coronavirus-crisis?. Accessed: April 11, 2020.

17 | CAICT (China Academy of Telecommunication Planning Research of Ministry of Industry and Information Technology) (2020). "Research Report on Data and Smart Applications for Epidemic Prevention and Control (Version 1.0)." http://www.caict.ac.cn/eng_2020/lb/202004/t20200408_278749.html. Accessed: June 12,2020.

18 | Xinhua (2020): "China blacklists individuals for concealing symptoms, violating quarantine". http://en.people.cn/n3/2020/0213/c90000-9657352.html. Accessed: April 22, 2020.

19 | Rödl&Partner (2020): "China's Social Credit System in the light of Covid-19." https://www.roedl.com/insights/covid-19/coronavirus-china-social-credit-system. Accessed: April 25, 2020.

20 | Central Committee General Office, State Council General Office (2016). "Outline of the National Informatization Development Strategy [Rogier Creemers; trans.]." https://chinacopyrightandmedia.wordpress.com/2016/07/27/outline-of-the-national-informatization-development-strategy/. Accessed: May 6, 2020.

21 | General Office of the State Council (2018). "Opinions of the General Office of the State Council on Promoting the Development of "Internet plus Health Care." http://en.pkulaw.cn/display.aspx?cgid=37395b41f6f018e4bdfb&lib=law; Godement, François (2019). "Digital Privacy: How Can We Win the Battle?" https://www.institutmontaigne.org/ressources/pdfs/publications/digital-privacy-how-can-we-win-battle-study.pdf. Institut Montaigne, pp. 130-134.

22 | Different localities have updated their regulations on the scope of security technology in public spaces pushing for increased usage of video surveillance. See also Mozur, Paul and Krolik, Aaron (2019). "A Surveillance Net Blankets China's Cities, Giving Police Vast Powers." December 17. https://www.nytimes.com/2019/12/17/technology/china-surveillance.html. Accessed: May 5, 2020.

23 | Fan Yang (2018). "China's Big Brother smart cities - can the law protect the privacy of Chinese citizens?". July 26. https://www.policyforum.net/chinas-big-brother-smart-cities/. Asia & the Pacific Policy Studies. Accessed: April 26, 2020.

24 | Cybersecurity Law of the PRC; in effect since June 1, 2017 (2016) [transl. Creemers, R., Triolo, P., and Webster, G.]. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

25 | Fang, Sammy et al (2020): „New Chinese Civil Code Introduces Greater Protection of Privacy Rights and Personal Information." https://www.dlapiper.com/en/uk/insights/publications/2020/06/new-chinese-civil-code-introduces-greater-protection-of-privacy-rights-and-personal-information/. Accessed: June 11, 2020.

26 | An updated version of the specifications was released in March and will come into effect in October. Beckett, Nick and Ge, Amanda: „China publishes new specification on personal data security." https://www.lexology.com/library/detail.aspx?g=47c9f-fa9-7f9f-4cb8-80cd-b218da78fa39. Accessed: June 10, 2020.

27 | Basic Healthcare and Health Promotion Law [in effect since effective June 1, 2020] (2019). NPC Observer. https://npcobserver.com/legislation/basic-healthcare-and-health-promotion-law/. Accessed: May 12, 2020.

28 | CAC (2020). "Notice on Protecting Personal Information and Using Big Data to Support Joint Prevention and Joint Control Work [trans. Zhong, R., Creemers, R., and Webster, G.]". Issued Feb 4. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-authorities-emphasize-data-privacy-and-big-data-analysis-coronavirus-response/.

29 | The GDPR lays out a whole range of additional criteria for consent. Consent is only one way to obtain data under GDPR. See Wolford, Ben (n.d.). "What are the GDPR consent requirements?" GDPR EU. h ttps://gdpr.eu/gdpr-consent-requirements/. Accessed: May 3, 2020

30 | See e.g. template statement in Alipay privacy agreement, allowing them to share, transfer, and publicly disclose personal information without consent when directly related matters of public health and safety.
支付宝隐私权政策. https://cshall.alipay.com/lab/help_detail.htm?help_id=201602172661. Accessed: May 7, 2020.

31 | People's Daily (2020): "一"码"平川，健康码有了国家标准." (A "code" for everywhere - Health code gets national standard). http://health.people.com.cn/n1/2020/0515/c14739-31710066.html. Accessed: May 20, 2020.

32 | Wei, Sheng (2020): „Lawmakers urge proper handling of personal data collected during pandemic." https://technode.com/2020/05/22/lawmakers-urge-proper-handling-of-personal-data-collected-during-pandemic/. Accessed: June 11, 2020

33 | Zhongguozhengfuwang (2020). 返程速查! 官方同乘查询来了，可查飞机火车患者前后三排 ("Return trip check! The official paratransit check is here. Three rows of patients in front of and behind the plane and train)." February 13, 2020, http://www.gov.cn/fuwu/2020-02/13/content_5477983.htm. Accessed: June 12,2020.

34 | Kuaikeji (2020)."腾讯健康码累计访问量43亿次：老外也能用 (Tencent Health Code accumulated 4.3 billion visits: even foreigners can use it)." March 5, 2020. https://news.mydrivers.com/1/676/676135.htm. Accessed: June 11, 2020.

35 | Xia Xiaohua 夏小华 (2020). "你绿了吗? 中国推健康码引发防疫与监控争论 (Are You Green? China's Push for Health Codes Sparks Debate on Epidemic Prevention and Surveillance)." Radio Free Asia., 2020. https://www.rfa.org/mandarin/yataibaodao/huanjing/hx2-03042020111216.html. Accessed: April 20, 2020.

36 | Ye, Josh (2020). "China's QR health code system brings relief for some... and new problems". Abacusnews. February 18. https://www.abacusnews.com/tech/chinas-qr-health-code-system-brings-relief-some-and-new-problems/article/3051020. Accessed: April 2, 2020.

37 | Zhihu (2020). „各地健康码算法是什么? 除了自觉填报，有什么实际用处? (What is the

health code algorithm for each location? What practical use is there for it, other than to fill it out consciously?)". https://www.zhihu.com/question/374819655/answer/1041498699; Zhihu (2020). „健康出行码为什么我昨天是绿色今天就变成红色了? (Health Travel Code Why was I green yesterday and am red today?)". https://www.zhihu.com/question/371511448/answer/1014240812; Zhihu (2020). 疫情期间，被禁止进入小区怎么办? (What if you are banned from the community during an outbreak?)". https://www.zhihu.com/question/369390434. All accessed: June 12, 2020.

38 | App 个人信息举报 (App personal information reporting) (2020). "观察丨使用'健康码'能平衡个人信息保护和使用吗? (Analysis: Can the Use of 'Health Codes' Balance the Protection and Use of Personal Information?)." Weixin. March 19, 2020. https://mp.weixin.qq.com/s/Dpxl8MqYGWsu6aRo3SZrcQ. Accessed: June 12,2020.

39 | Lee, Emma (2020). JD completes first unmanned delivery for coronavirus aid in Wuhan. Technode, February 7. https://technode.com/2020/02/07/jd-completes-first-unmanned-delivery-for-coronavirus-aid-in-wuhan/. Accessed: June 12, 2020.

40 | AI Report (AI-报告) (2017). "2017年中国人脸识别行业报告: 即将出现大量倒闭 (China Face Recognition Industry Report 2017: A Mass Collapse Imminent)." 豆瓣. 2017. https://www.douban.com/note/638962904/.

41 | AIIA 中国人工智能产业联盟 (Artificial Intelligence Industry Alliance) (2020). "人工智能助力新冠疫情防控 调研报告 (Research Report: How Artificial Intelligence Helps Epidemic Prevention and Control against COVID-19)." http://aiiaorg.cn/uploadfile/2020/0324/20200324060228591.pdf. Accessed: June 12, 2020.

42 | Yuan Yang, Yuan and Nian Liu (2020). China survey shows high concern over facial recognition abuse. Financial Times. https://www.ft.com/content/7c32c7a8-172e-11ea-9ee4-11f260415385. Accessed: May 12, 2020.

43 | International Data Corporation (IDC) (2020). IDC Identifies China's Emerging Healthcare AI Trends in New CIO Perspective Report. April 22. https://www.idc.com/getdoc.jsp?containerId=prCHC46215920. Accessed: April 28, 2020.

44 | Chen Peng 陈鹏 (2020). "让大数据为疫情预警——大数据在疾控应用中的方方面面_新浪医药新闻 (Let Big Data Be the Early Warning of Epidemic Situation -- Every Aspect of the Applications of Big Data in Disease Control)." Medical News 医药新闻. March 13, 2020. https://med.sina.cn/article_detail_103_2_79056.html. Accessed: May 2, 2020.

45 | CAC (2020). "Notice on Protecting Personal Information and Using Big Data to Support Joint Prevention and Joint Control Work [trans. Zhong, Rui, Creemers, Rogier and Webster, Graham.]". Issued Feb 4. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-authorities-emphasize-data-privacy-and-big-data-analysis-coronavirus-response/.

46 | Mozur, P., Zhong, R., and Krolik, A. (2020). "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags." New York Times. March 1. https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html. Accessed: May 5, 2020.

47 | Xinhua (2020). "健康码与社会智能治理" (Health code and AI societal management). Xinhua. April 22. http://www.xinhuanet.com/globe/2020-04/22/c_138971800.htm. Accessed May 6, 2020; Shanghai Release 上城发布 (2020). „人工智能+大数据"推广健康码，上城推出全市首个基层治理人工智能系.统!" ("Artificial intelligence + big data" to promote health code, uptown launched the city's first grassroots governance artificial intelligence system!). Sohu. February 25. https://www.sohu.com/a/375775906_349139. Accessed: May 6, 2020.

48 | Baijiahao - Xinhua (2020). "见过凌晨四点的杭州，只为早日'无码'——'健康码'背后的复工记" (Saw the QR-code at 4 am in the morning and there was no code; the recovery code behind the 'health code'). February 21. https://baijiahao.baidu.com/s?id=1659147516916399925&wfr=spider&for=pc. Accessed: May 5, 2020.

49 | Liu, Deliang (2020). "Is facial recognition a step too far in combating COVID-19?".

49 | Liu, Deliang (2020). "Is facial recognition a step too far in combating COVID-19?".
     February 19. China Global Television Network. https://news.cgtn.com/news/2020-02-19/
     Is-facial-recognition-a-step-too-far-in-combating-COVID-19--OcDlezcrRK/index.html?-
     from=timeline. Accessed: May 6, 2020.
50 | Xinhua (2020). "新知 | "刷脸"时代来临，人脸识别应用"边界"何在 (The era of "face swipe" is
     approaching, where is the "boundary" of facial recognition applications?)". November 26, 2019.
     http://news.xhby.net/js/kj/201911/t20191126_6420266.shtml. Accessed: June 11, 2020.