Journal of Digital Media & Policy
Volume 12 Number 1
 https://doi.org/10.1386/jdmp_00047_1
Received 3 September 2020; Accepted 9 November 2020

ELENA SHERSTOBOEVA
City University of Hong Kong

VALENTINA PAVLENKO
National Research University Higher School of Economics

Trends in East Asian policies on digital surveillance tools during the COVID-19 pandemic

ABSTRACT

This article investigates how digital surveillance tools used by East Asian governments against COVID-19 affect privacy and personal data protection. It applies doctrinal legal analysis and case study to compare national regulations of these tools as well as their implementation in China, Hong Kong, Macau, Taiwan, Japan and South Korea. The approaches range considerably from total (China) to selective surveillance, which, however, seems overly excessive towards privacy of certain social groups, exacerbating social stratification and business disruptions in East Asia. The article argues that selective surveillance models vary across the region from voluntary selective (Japan) to compulsory selective surveillance (Hong Kong, Macau, Taiwan, South Korea) and differ in terms of privacy and related rights. Yet, the increased risks of data misuse and leakages in all the East Asian states and territories need effective legal mechanisms for privacy and data protection that pay sufficient attention to public scrutiny and independent regulators.

KEYWORDS

East Asia
COVID-19
digital surveillance
pandemic
personal data
privacy

INTRODUCTION

The governmental use of digital surveillance tools against COVID-19 has globally challenged privacy and personal data protection on an unprecedented scale (Mações 2020; Gershgorn 2020). While such tools have often been viewed as effective and necessary to fight the virus, they have posed an increasing threat of digital authoritarianism (Donahoe 2020), especially due to the rapid cross-borrowing of surveillance strategies around the world (McKinsey and Company 2020b). For instance, Asian digital surveillance tools have already been investigated for further integration in several countries within the region as well as outside it (Small 2020; Catania et al. 2020; Kelly 2020; Kabir 2020),[1] substantiating the viewpoint that considers the pandemic as 'the tipping point when the Asian Century truly began' (McKinsey and Company 2020a). Studying these tools and their effects on individual rights and freedoms is urgent and crucial.

Being the first region to face the pandemic, East Asia is often considered emblematic of active and effective exploitation of digital surveillance tools for these times (Cha 2020). Having experienced several disease outbreaks and natural disasters before COVID-19, this region seems to have promptly and effectively adapted and evolved its advanced digital surveillance measures to respond to the COVID-19 outbreak. Despite their considerable diversity in legal systems, traditions, political regimes, and challenges, the East Asian jurisdictions share a long legal and social tradition of caring greatly about protecting social welfare and public order (Dixon and Ginsburg 2014) and of ensuring healthy and safe life conditions. Furthermore, the overall regional population has reportedly supported these measures (Huang et al. 2020; Hui 2020). However, the extent of invasiveness affecting privacy and personal data protection is largely unknown.

These rights are guaranteed in international standards and in many national constitutional and other statutes across the globe, being important for individuals to have control over own lives, for social and political activities, as well as for the digital economy. Privacy is enshrined in the key United Nations (UN) documents, such as the 1948 Universal Declaration of Human Rights (UDHR) and the 1966 International Covenant on Civil and Political Rights (ICCPR). In its resolution 68/167, the UN General Assembly emphasized that unlawful or arbitrary surveillance and collection of personal data violate the rights to privacy and to freedom of expression. Still, privacy and data protection may be limited in times of crisis more than in normality (UN 2020). For an international perspective, the limitations on the right to privacy must match the three-part test established in key international human rights treaties. The criteria of legality and legitimacy mean that any limitations should be provided in law in a clear and precise manner and should pursue legitimate goals, such as protection of public order or health. The third criterion requires that interferences with an individual's right to privacy be necessary and proportionate. Limitations on the right to personal data protection must meet similar criteria (The Electronic Frontier Foundation and ARTICLE 19 2014; European Union Agency for Fundamental Rights and Council of Europe 2018). In particular, any interference must be conducted in the least invasive manner (Pierucci and Walter 2020a). Any tools used to tackle the pandemic must be 'limited in use, both in terms of purpose and time', and individual rights to privacy, non-discrimination and other freedoms should be 'rigorously protected' (OHCHR 2020a).

1. New Zealand was investigating the Singaporean government's Bluetooth-based app TraceTogether; the Australian government launched its own contact-tracing app, COVIDSafe, based on Singapore's TraceTogether software; China's social credit system was cited as a model for Israel's COVID-19 infection ranking system.

This article aims at exploring the extent to which digital surveillance tools used in East Asia in the pandemic times have intervened with the rights to privacy and other related rights, such as data protection. Sample states and territories include China, HKSAR, Macau SAR, Taiwan, Japan and South Korea, but exclude Mongolia and North Korea for methodology reasons.[2] Despite the diversity of East Asian jurisdictions, this article seeks to encapsulate the regional approach to digital surveillance invasiveness amidst COVID-19, while comparing national visions to the issue. Addressing the issue from a comparative doctrinal legal perspective, this article studies national digital surveillance tools through legally binding regulations and policies along with case study. The regulations and policies include the instructions provided by executive bodies, such as governments, health ministries, and embassies. They also cover English-language versions of the tools' terms of services. Case study has been applied to study the implementation strategies.

Methodologically, East Asian national regulations and policies are evaluated in light of a particular set of the criteria (see Table 1) that we have identified as a result of our study of scholarly, expert and international legal visions on privacy and data protection in the COVID-19 times.

The article bears in mind the differences between the international status of East Asian jurisdictions, some of which do not represent states. It uses international standards for methodological purposes to assess the degree of invasiveness of digital surveillance tools. International vision mainly refers to the UN standards, particularly the standards of the UN High Commissioner for Human Rights (OHCHR 2014; OHCHR 2020b) and the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Kaye 2020). The article also uses the standards developed by European organizations, such as the Council of Europe (CoE)[3] and the European Union (EU),[4] since Europe has modern rules to ensure data protection for the digital environment, such as the General Data Protection Regulation (GDPR).

Useful research projects that helped us to form the set of criteria include the studies and reports on privacy and related rights in the times of COVID-19 prepared by several NPOs, such as Access Now and Chaos Computer Club e. V. (CCC), Europe's largest association of hackers. More recent research by Cha (2020), Ponce (2020), Bradford and others (Bradford et al. 2020) has been useful to investigate the implications of anti-COVID-19 measures for privacy and data protection in some jurisdictions and worldwide. The study of Donahoe (2020) has aided to explore the impact of policy responses to COVID-19 in terms of civil liberties and political regimes. The articles of Miyashita (2011); Madsen (1992); Greenleaf (2014); Dixon and Ginsburg (2014); Aho and Duffield (2020); and Ko and others (Ko et al. 2017) have benefited our understanding of the East Asian context related to the protection of privacy and personal data.

The article does not question the need for these measures to fight the Coronavirus, nor does it aim at providing a comprehensive analysis of digital surveillance measures in East Asia. Instead, it focuses on the evaluation of the degree of their invasiveness for privacy and personal data protection in the region while pointing out the similarities and differences among East Asian states and territories.

This study argues that East Asian approaches intervening with the right to privacy and personal data protection are very diverse and vary among the jurisdictions from total to selective surveillance. Except for China, the latter approach is used in all other jurisdictions, although it varies substantially

2. Mongolia, being less technologically advanced than its peers, has focused on traditional methods of dealing with COVID-19, such as early and strict social distancing measures, that have been found to be successful in controlling the outbreak. See https://news.un.org/en/story/2020/07/1068821; https://www.thelancet.com/journals/langlo/article/PIIS2214-109X(20)30295-3/fulltext. Although Mongolia has reportedly used the surveillance app during the COVID-19 outbreak, there is very little available information about it. The study also excludes North Korea due to the lack of data.

3. The Council of Europe is the continent's leading human rights organization.

4. The European Union is a political and economic union made up of 27 member states.

No.	Criteria	Description
1.	Scope	Total vs. selective surveillance. Total surveillance means that digital surveillance tools target the entire population regardless of risk factors, such as health status, contacts and travel history, that could justify an invasion of privacy. Selective surveillance implies targeting certain categories of the population based on risk factors, e.g. patients, contacts, suspected patients, and suspected contacts
2.	Voluntariness	The presence or absence of mechanisms of coercion and punishment for the non-use of digital surveillance tools, including the users' ability to deactivate or delete corona app (CCC 2020)
3.	Minimization of data collection	Restrictions on time, territory, volume and use of data should be clearly stated and proportionate to the purpose of data collection (OHCHR 2014; Kaye 2020; EDPB 2020; Pierucci and Walter 2020b; Access Now 2020)
4.	Depersonalization	Data anonymization or pseudonymization should be guaranteed (WHO 2016; Kaye 2020; CCC 2020)
5.	Transparency	Clarity for the public about what personal data are collected and who has access to the collected data (Kaye 2020; Pierucci and Walter 2020b; Access Now 2020)
6.	Public scrutiny	Nations should establish or maintain independent oversight bodies in order to protect the rights of personal data subjects (OHCHR 2014; Pierucci and Walter 2020b; CCC 2020)
7.	Decentralized data storage	A dependence of the users' privacy on the trustworthiness and competence of the central infrastructure operator is considered technically unnecessary and undesirable (CCC 2020)
8.	Guarantees of data protection	Strong guarantees of data protection from leaks, breaches and unauthorized use must be established (OHCHR 2014; OHCHR 2020b; Kaye 2020; Access Now 2020)

Table 1: Criteria for the evaluation of the regulation of East Asian digital surveillance tools.

among them from voluntary selective surveillance (Japan) to compulsory selective surveillance (Hong Kong, Macau, Taiwan and South Korea). Nonetheless, the article has observed common signs of digital authoritarianism in all states and territories to control the spread of the virus, especially with regard to certain categories of individuals, e.g. patients and contacts, including suspected ones, curtailing their privacy and right to data protection as well as business opportunities. These signs include the forced use of digital surveillance tools,

insufficiently informed consent to data collection and processing, the redundancy of data collected, the lack of independent regulators, and insufficient guarantees for data security and depersonalization.

The article consists of two parts. The first considers background information on the right to privacy and data protection in East Asia. The second part starts with an overview of digital surveillance tools in East Asia used by governments during the pandemic. Then, it proceeds to evaluate their regulations and policies and to contemplate the prospects for privacy and data protection after the pandemic. In conclusion, the article provides a summary and critique of the results.

Asian background

The pre-pandemic experience of counteracting various disease outbreaks and natural disasters in East Asia has predetermined the existence in some jurisdictions of laws, policies and technologies that could help them to counter COVID-19 (Ariadne Labs 2020; Kim 2020; Wang 2020; Hartley and Jarvis 2020). Before the outbreak, East Asian states and territories have been affected by the 2002–04 SARS outbreak (WHO n.d. b) and the MERS outbreak (WHO n.d. a). As a technologically advanced region, East Asia also used some previous developments related to digital surveillance to fight the Coronavirus (Bradford et al. 2020). In general, the jurisdictions have been developing their digital infrastructure aggressively (McKinsey and Company 2020b). Japan, South Korea, and Hong Kong are among global trendsetters in terms of digital technology adoption (Sedik 2018). Hong Kong ranks 8th in the 2019 World Digital Competitiveness Ranking provided by Swiss business school, IMD. Hong Kong is followed by South Korea at 10th place; Taiwan at 13th; China at 22nd; Japan at 23rd (IMD 2019). Asian companies also invest actively in artificial intelligence (AI), robotics, cryptography and big data (Sedik 2018). Furthermore, AI advance is a part of national strategies in China, Japan and South Korea (Baker McKenzie 2020).

Despite some arguments suggesting that the right to privacy does not represent a real social value in Asian contexts at all, this approach largely negates the recent rapid growth of laws and technologies in the region (Privacy International 2012). East Asian jurisdictions, such as China, Hong Kong, and Japan, 'defend privacy rights, at least initially, in terms of data privacy protection that is instrumentally necessary for the development of e-commerce' (Ess 2005). The value of personal information protection is acknowledged in the region as being crucial for the banking system and other business areas that are important for East Asian economies. Although in different wordings, all East Asian constitutions guarantee privacy, including privacy of family life[5] and privacy of correspondence/communication.[6] Furthermore, East Asian privacy and data protection regimes have been open to global and Western legal standards (Miyashita 2011; Ko et al. 2017; Kirby and Greenleaf 2017).

All the sample jurisdictions provide statutory guarantees for the protection of personal information.[7] South Korea, a member of the Organisation for Economic Co-operation and Development (OECD), the 37-member intergovernmental economic organization, is viewed as 'one of the toughest jurisdictions' for data protection in the world (Hogan Lovells 2019). Japan, another member of OECD, has also made significant efforts to modernize its data protection legislation in line with the 1980 OECD Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data, and Japan's

5. Article 30 of the Basic Law of the Macao SAR.

6. Article 40 of the Constitution of the People's Republic of China; Article 30 of the Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China; Article 32 of the Basic Law of the Macao SAR; Article 12 of the Constitution of the Republic of China (Taiwan); Articles 17–18 of the Constitution of the Republic of Korea.

7. China's Cyber Security Law; Hong Kong's Personal Data (Privacy) Ordinance; Macau Personal Data Protection Act; Taiwan's Personal Data Protection Act; Japan's Act on the Protection of Personal Information; South Korean Personal Information Protection Act.

progress towards an Economic Partnership Agreement with the European Union has also played a role (Hogan Lovells 2019). Hong Kong has one of the best developed data protection laws in the region (Hogan Lovells 2019), with an awareness of the need for personal data protection stemming from its economic interests (Madsen 1992). Although the Chinese legal vision of cybersecurity is associated mostly with the concept of digital sovereignty and speech control, even China provides several important measures for data protection in its 2017 Cyber Security Law.

Still, social attitudes towards privacy vary across the region where democracies (Japan, South Korea, Taiwan) coexist with semi-democracies (Hong Kong, Macau) and authoritarian regimes (China) (Greenleaf 2014). The Chinese social credit system that combines 'surveillance architectures and AI technologies for purposes of statecraft' (Aho and Duffield 2020) has repeatedly raised grave concerns about data protection and invasion of privacy (Lee 2020). Being the only country in the 'extensive surveillance' category, China has scored just 1.8 out of 5.0 points in a study of privacy protection and government surveillance in 47 countries, provided by the UK-based technology website Comparitech (Bischoff 2019). Japan and Taiwan (both 2.8) are in the 'some safeguards but weakened protection' category.

Digital surveillance tools in East Asia in the COVID-19 times

To combat and prevent the spread of COVID-19, East Asian national authorities have relied heavily on technological tools and innovations, especially track-and-trace systems and mobile applications (Bradford et al. 2020). However, the use of similar surveillance technologies by East Asian jurisdictions does not necessarily accompany similar regulatory approaches.

The Chinese regulatory approach can be qualified as *total surveillance* as it targets the entire population regardless of risk factors, such as health status, contacts and travel history, that could justify an invasion of individuals' privacy. Based on recent developments in mobile technologies and big data, as well as the capacities of two Chinese internet giants, Alibaba and Tencent,[8] the country has established a pervasive 'health code' system. Alibaba's and Tencent's popular smartphone apps host a system that generates coloured QR-codes (red, yellow and green) to indicate the status of citizen health and to determine the degree of freedom of movement for a person. People with a red code must undergo quarantine for 14-days; those with a yellow code should be quarantined for seven days; and anyone with the green code can move freely. People without the 'health code' app may not leave their residential compounds or enter most public venues in many cities (Gan and Culver 2020). The functionality of the system is overly broad. Because QR-codes are scanned when citizens visit public places, the system also allows the tracking of user movements and contacts. The system lacks clarity and transparency, as it not only implies the use of several tools, but it also has local versions of the health code, for example, in Beijing (Gan and Culver 2020) and Shanghai (Borak 2020). Chinese authorities reportedly put pressure on private companies to hand over sensitive data for anti-epidemic purposes (Yang et al. 2020). This can have far-reaching implications, given that private companies in China, such as Alibaba and Tencent, have a huge amount of user data at their disposal.

Other East Asian jurisdictions use *compulsory selective surveillance* (Hong Kong, Macau, Taiwan, South Korea) or *voluntary selective surveillance* (Japan).

8. Alibaba's mobile payment app Alipay and Tencent's messaging app WeChat are used by hundreds of millions of people, ensuring mass implementation of the 'health code' system.

Representing a more targeted strategy, selective surveillance assumes categorizing the population to define the degree of the intrusion to their privacy and personal data protection. This approach implies a vision of the threat in certain categories of people, mostly patients with confirmed or suspected COVID-19, as well as people who are suspected of being in contact with patients. Most jurisdictions have established particular excessive surveillance over the entrants, regardless of their citizenship and health status.

Hong Kong authorities have made it mandatory to use the 'StayHomeSafe' mobile app and electronic wristbands for people arriving from abroad who are subject to compulsory quarantine (HKSAR Government 2020). After a user downloads the app and scans the QR code from the wristband, the application starts analysing Bluetooth, Wi-Fi, and geospatial communication signals. A change in signals shows that the user has left his or her home, and the user is obligated to keep running the app with the Bluetooth, Wi-Fi, and location service functions engaged.

Macau has also launched a colour QR-code system, the 'Macao Health Code', but it is less invasive than in China. Although voluntary for entering premises within Macao, unlike in China, the use of the 'Macao Health Code' is a mandatory declaration of health condition at the port of Macau's entry (Macau Government n.d.). Non-residents with the red code are denied entry into Macau, while residents are immediately transferred to a public hospital for medical tests and possible hospitalization. People with red code cannot visit public administration premises, casinos or other private premises (Anon. 2020d).

The selective surveillance in Taiwan is slightly different. Its 'digital fence' system aimed at quarantine enforcement is mandatory for anyone arriving from overseas, with a few exceptions for some groups such as business travellers (Eigen et al. 2020). It does not require the receipt of consent or any confirmatory actions (such as downloading an application) from people. This system monitors cellular signals from the phones to track the location and to alert police and local officials if those who must stay in home quarantine move away from the dwelling place or turn off the phone. So, the intrusion with the privacy of quarantined individuals is nearly automatic. They just must keep the phone turned on for the system to track their location. Officials also call people twice a day to ensure they don't violate quarantine requirements by leaving their phones at home (Lee 2020).

South Korea, which has not implemented a full lockdown, has greatly relied on digital surveillance in the fight against the pandemic. South Korea has instituted mandatory location tracking using cell phone location information, with Article 76-2 of Infectious Disease Prevention Act authorizes the location check of not just patients and suspected patients but also those who are suspected of being in contact with patients (Park 2020), which significantly increases the scale of mandatory location tracking. All citizens[9] and long-stay foreigners who have been ordered to undergo quarantine must install the 'Self-quarantine Safety Protection App' aimed at quarantine enforcement. In case of refusal or leaving the quarantine area without permission, foreigners could be immediately deported (MOHW 2020). In addition, people arriving in the country are required to use the 'Self-diagnosis Mobile App' to monitor and record daily their health status for two weeks (Kim 2020). If a person does not download the app or record health status, he or she may receive a call from health officials, and if that person fails to receive the call, measures may be taken to identify his or her location (Korean Embassy in Sri Lanka 2020).

9. According to guidelines from the Korean Centers for Disease Control and Prevention, anyone who has come into contact with a confirmed COVID-19 carrier is subject to a mandatory 14-day self-quarantine.

A very different approach to selective surveillance is practiced in Japan, which has been using the 'COCOA - COVID-19 Contact App' since June, 2020. With Bluetooth signals, the application alerts users when they may have been in close proximity to someone infected with the COVID-19. The effectiveness of the Japanese approach has been questioned, as its contact-tracing app relies on voluntary registration by those who test positive for COVID-19. Although the authorities urge users to download the COCOA, downloads of the contact-tracing app have slowed since its debut (Anon. 2020b). The least invasive tools can also be illustrated by corona maps with anonymized data used in Hong Kong and South Korea to help people to avoid contagious areas if they wish to do so.[10] Still, in these jurisdictions such tools coexist with the compulsory ones.

10. See Hong Kong's map https://chp-dashboard.geodata.gov.hk/covid-19/en.html; South Korean Corona Map http://coronamap.site, Corona Nearby https://corona-nearby.com.

Data redundancy and non-depersonalization

Compulsory selective surveillance may match the criterion of a legitimate purpose to protect public health during a pandemic and represents an attempt to be more sensitive to people who are not affected by the Coronavirus in any way. However, it mostly does not meet the *minimization of data collection* and *depersonalization* criteria for those people who are subject to such surveillance. During the COVID-19 pandemic, the previously established collaborations with private companies on the development and use of the tools (McKinsey and Company 2020b) have not only helped authorities to provide extensive coverage but also to integrate several databases created and used for different purposes.

In South Korea, the COVID-19 Smart Management System extracts and uses various personal data, including credit card transactions and mobile phone location, from 28 organizations, such as the National Police Agency, the Credit Finance Association, three smartphone companies, and 22 credit card companies to trace the movements of people with COVID-19 (Choon 2020). Taiwan has implemented its 'digital fence' system in collaboration with the nation's five major telecom companies. Apart from the collaboration between the government and companies, the Taiwanese system implies a massive data exchange between government agencies and police. The police control the situation through access to several databases, including a database of individuals under quarantine orders, and they visit popular gathering places, like bars and karaoke parlours, to check for any quarantined individuals (Hui 2020).

Despite the collaborations however, the storage and use of the tools in East Asia is fully controlled by governments, which does not meet the *decentralized data storage* criterion. Overall, the East Asian approach implies a very high degree of confidence in governments to deal with the crisis, reflecting East Asian legal and cultural traditions. The pandemic has given rise to a significant increase in the state powers in the region, although it is partly smoothed by the selective surveillance strategy limiting the amount of data that state holders have at their disposal in the jurisdictions that adhere to this strategy. Although decentralized data storage is considered more secure, in all the East Asian states and territories, the main data holders are government agencies. This approach might be justifiable under the crisis conditions, but it needs to match more criteria of compliance of the regulations with privacy and data protection standards.

However, only a few East Asian regulations have any guarantees regarding data depersonalization and narrowing the scope of collected data. The

Japanese app 'COCOA' tracks contacts, however, details on time and place of contacts, as well as patients' identities, cannot be known by the government and other users, according to the Ministry of Health, Labor and Welfare, which operates the programme (Anon. 2020c). Hong Kong authorities claim that the 'StayHomeSafe' app analyses changes in environmental signals to detect possible location changes but does not collect personal data (Anon. 2020a). At the same time, Taiwan's 'digital fence' system that allows the collection of subscriber location data seems to provide no guarantees for their anonymization. The electronic tracking system logs data, such as names of quarantine evaders and of those who have their phones turned off (Tzu-ti 2020).

Users of the South Korean 'Self-Diagnosis Mobile App' must also report personal details, such as phone number and more sensitive data about health condition, as they must record whether they have developed any symptoms every day for fourteen days after entering South Korea (Korean Embassy in Sri Lanka 2020). Their 'Self-quarantine Safety Protection App' collects 'personal information, including name, date of birth, gender, nationality, mobile phone number, mobile phone number of a family member, and address where the quarantine is taking place' (Ponce 2020). The COVID-19 Smart Management System allows the South Korean authorities to monitor not only mobile phone location records but also a variety of other data, like information about credit card transactions (Choon 2020), which provides a glimpse of person's daily routine. This amount of data raises questions about proportionality in relation to the legitimate purpose of data collection.

In China, which has been viewed as a 'surveillance state' even before the pandemic (Mitchell and Diamond 2018), the model is even more invasive. To get a code, citizens must specify their name, national identity number or passport number, phone number, travel history, and whether they have come into contact with any confirmed or suspected COVID-19 patients in the past two weeks. They also need to report information about symptoms they have (Gan and Culver 2020). Scanning QR-codes at the entrance to public venues means that the state can track user movements and contacts. Beijing's version of the system, launched in March, 2020, requires users to not only provide name and ID number, but also to register with facial recognition to obtain a personal colour code (Gan and Culver 2020). Collecting such a large amount of non-depersonalized data about users not only goes beyond the legitimate purpose but actually makes it possible to create digital projections of personalities. On a national scale, this means creating a kind of digital herbarium, or digital cast of the population. The question is how this digital herbarium will be used. Access to it allows both the improvement of people's lives by promoting technologies and solutions based on better understanding of human needs and behavioural patterns but also the introduction of Orwellian control and surveillance of the population.

Social stigmatization and alienation

Although in general, the fear of infection during the pandemic has increased social tensions in some jurisdictions, including hostility towards expats in Hong Kong (Hale and Shepherd 2020), some anti-COVID digital surveillance tools in East Asia could exacerbate these tensions. As some of them do not imply health data anonymization, they pose a threat of stigmatization and intolerance towards particular persons and their families because of their health status. This threat is significantly increasing in China, where the owners

of yellow and especially red QR-codes are exposed to a serious threat of social alienation and displacement from public life. A similar risk has emerged in Macau; however, the use of colour codes there is not mandatory for all people, so it does not pose quite the total threat as it does in China.

Digital alienation is another problem that may be aggravated with the use of anti-pandemic digital tools in several East Asian jurisdictions due to insufficient considerations of media literacy. The increased use of digital surveillance tools during the pandemic has led to the emergence of new human and civil responsibilities – *stay in touch* and *stay digital*. This manifests itself as a requirement to those subject to the obligation to maintain mobile and internet connectivity for the purpose of contact tracing and quarantine enforcement via corona apps or phone signal tracking. In China, elderly people, who lack digital literacy skills to confirm their health status, have been banned from entering restaurants and supermarkets (Sheng and He 2020). Apart from the elderly population, such new 'digital aliens' may include the poor, illegal migrants, anyone with disabilities, and other vulnerable groups who need additional protection amidst the outbreak in East Asian laws.

Data leakage threat

The leakage of data accumulated by digital surveillance tools has become another common central problem in the region during the pandemic. Existing legal *guarantees and measures of data protection* have been insufficient to protect personal data, which represents a vital asset in a digital, data-driven economy (Baker McKenzie 2020), particularly in the health sector. Several nations have already experienced data leaks.

While China has rolled out consumer privacy standards after the implementation of the 2017 Cyber Security Law, the country continues to face the problem of personal data leaks, including medical data (Gkritsi 2020). During the pandemic, the personal data of Chinese citizens who visited the city of Wuhan, the epicentre of the COVID-19 outbreak, was reportedly leaked (Yang et al. 2020). Some of the victims of such leaks claim they have been harassed since the data disclosure.

In Hong Kong, two mobile phones with the private information of 122 people under quarantine, including their names, locations, photographs and other personal data, went missing from a government building (Lo 2020). This demonstrates that government agencies are not always able to provide sufficient data protection, even in large and digitally advanced financial hubs, such as Hong Kong. Leakage from Taiwan's government database containing personal information on more than twenty million citizens (Chen 2020) also showed that government databases are not immune from leaks.

All this presents a challenge to the high level of credibility that populations are willing to place in their governments in search of protection from the virus. A common problem is the lack of *transparency, public scrutiny and independent oversight mechanisms*, which threatens both individual rights and business opportunities, as strong and reliable data protection is key for businesses, including banking and e-commerce.

Data leaks may also worsen the issues of social stigmatization, xenophobia and homophobia. In May, 2020, South Korean media linked a COVID-19 outbreak to gay people in Seoul and specified the age, district, type and location of work of the patient believed to be in the cluster of COVID-19 cases (Kwon and Rahim 2020).

After COVID-19?

It is imperative that, as the epidemiological situation improves, crisis measures should be scaled back. Almost all East Asian jurisdictions show the acknowledgement of the need for time limits for digital surveillance measures, regulating through limiting the period for data storage or the tools' usage.

As for the Japanese COCOA app, the data is deleted after fourteen days, which corresponds to the COVID-19 incubation period (App Store n.d.). Similarly, under the South Korean QR-code system, user data is logged in a database for four weeks before it is automatically deleted, according to South Korea's Ministry of Health and Welfare (Kim and Mah 2020).

According to the Hong Kong authorities, users may uninstall the 'StayHomeSafe' app from their smartphones after the quarantine period (HKSAR Government 2020). As stated, the South Korean 'Self-quarantine Safety Protection App' would be removed from Google Play Store and the iOS App Store when the situation returns to normal (Kim 2020). The Taiwanese authorities have also claimed that the tracking system would be discontinued after the COVID-19 pandemic passes (Hui 2020).

Nonetheless, almost all East Asian jurisdictions lack clear guarantees of a return to normalcy after the pandemic. They provide no concrete mechanisms to ensure that the data already collected will be destroyed after the tracking stops.

Meanwhile, in China, there are proposals to upgrade and continue using the 'health code' system after the pandemic (Horwitz and Goh 2020; Borak 2020). The prospects of the system are noted not only by officials but also by businesses. The president of Tencent Cloud, who also serves as the vice president at Tencent Group, said that 'the paperless, mobile, and traceable nature of the health code app can provide an innovative solution to future social governance' (Sheng and He 2020). China also reportedly links the prospects for the development of smart cities with the capabilities of the 'health code' system (Sheng and He 2020; Akiyama 2020). However, the collection and use of data, that most people recognize as necessary to protect public health during the pandemic, can pose a long-term threat to privacy in post-crisis times (Bacchi 2020), as it would go beyond legitimate goals.

CONCLUSION

During the pandemic, all East Asian governments have been using a vast array of digital surveillance tools, including 'Corona apps', 'QR codes' and 'Corona maps', along with electronic wristbands. While the national strategies have been mostly diverse across the region, varying from total to compulsory selective and voluntary selective surveillance, there is a common regional trend towards a more centralized and invasive model that does not look sufficiently justifiable for the protection of public health during the COVID-19 times.

For people who have the virus or are suspected of having it just because of their contacts or travelling history, insufficient informed consent has transformed access to digital technologies from a human right into a requirement, from an opportunity into a tool of restriction and sometimes, even of criminal sanction and deportation. All this may increase social tension in the region during the COVID-19 pandemic, reinforcing social disruptions and posing the risk of alienation and hostility towards certain social groups, particularly, patients, suspected patients, or visitors. The risks related to excessive digital surveillance should not be underestimated by populations, who must be made

sufficiently aware of the ramifications of their governments' strategies through the media and media literacy programmes.

East Asian government agencies often accumulate a significant amount of data gaining a glimpse of the daily routines of people subject to digital surveillance. In a number of nations, especially in China and South Korea, the amount of data collected fails the proportionality criterion. The pandemic has justified and stimulated a more active and large-scale use of digital surveillance tools, which significantly increases threat of digital authoritarianism in the region, especially in China, which adheres to a total surveillance strategy. Creating digital projections of individuals allows the state to amass a sort of digital herbarium or digital cast of the national population and its visitors, producing even more favourable ground for the growing state control over human lives. The trend is likely to increase with further development of digital technologies and augmented reality, while the legal tradition generally prioritizes the protection of public order and health over individual rights such as privacy and data protection. Although the selective surveillance strategy can help ensure the privacy of healthy persons who do not contact with the patients or suspected patients and do not travel during the outbreak, it leads to a substantial disbalance between the rights of people in these categories and of others. Ranging from sensitively invasive in Japan to deliberately invasive in South Korea, this strategy still reflects common regulatory problems in the region.

Cases of data leaks in East Asia have shown that existing legal guarantees and mechanisms of data protection are insufficient. As hacking technologies improve, stronger data protection mechanisms are needed – both at the legal and technological levels. Since digital surveillance tools involve, among other things, data exchange among government agencies, NGOs and companies, it is important to ensure the protection of data during the transfer, as well as transparency as to who has access to the data and on what conditions.

East Asian governments should consider decentralized data storage to be the preferred and more secure option, as suggested in international standards and many legal studies. The protection of privacy and personal data is essential both for individual rights and for business. It makes sense for the East Asian region to benefit from the experience of Western democracies. The existence of independent regulators that monitor respect for the rights of data subjects, following the example of Europe,[11] as well as the clarity and transparency of digital surveillance measures, could significantly ease tensions for both individuals and the business community.

Current regulations show that the pandemic context can contribute to even stronger cross-border dissemination of data and information about people, their health, and their contacts. Legal measures for cross-border protection of privacy, personal data, and other individual freedoms in line with global human rights standards should be reinforced. In this regard, the role of international players, in particular human rights organizations, is growing. The UN may play the most important role in the absence of Asian instruments, but European organizations should also contribute to strengthening global privacy and data protection.

Almost none of the East Asian jurisdictions, except for Japan, have clear guarantees for the destruction of data collected as part of the fight against COVID-19 after the pandemic. Society faces the question – what awaits us after the pandemic: a return to normalcy or a new normal? Much will depend

11. The European Data Protection Board (EDPB), established by the General Data Protection Regulation (GDPR), is an independent European body which aims to ensure the consistent application of data protection rules in the European Union. See https://edpb.europa.eu/about-edpb/about-edpb_en. Accessed 12 August 2020.

on the success of efforts to combat the pandemic. Continued spread of COVID-19 could motivate governments to step up their digital surveillance strategies.

ACKNOWLEDGEMENTS

The work described in this article was fully supported by a grant from City University of Hong Kong (Project No. 7200690).

REFERENCES

Access Now (2020), 'Recommendations on privacy and data protection in the fight against COVID-19', March, https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf. Accessed 12 August 2020.

Aho, Brett and Duffield, Roberta (2020), 'Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China', *Economy and Society*, 49:2, pp. 187–212.

Akiyama, Hiroyuki (2020), 'Japan grows wary of China's smart-city global standards', Nikkei Asian Review, 11 August, https://asia.nikkei.com/Politics/International-relations/Japan-grows-wary-of-China-s-smart-city-global-standards. Accessed 2 September 2020.

Anon. (2020a), 'Bracelets for all as new quarantine takes effect', RTHK News, 18 March, https://news.rthk.hk/rthk/en/component/k2/1515386-20200318.htm. Accessed 30 August 2020.

Anon. (2020b), 'Downloads of Japan's COVID-19 app reach 7.7 million in slowing pace since debut', Reuters, 21 July, https://www.reuters.com/article/us-health-coronavirus-japan-apps/downloads-of-japans-covid-19-app-reach-7-7-million-in-slowing-pace-since-debut-idUSKCN-24M0GB. Accessed 29 August 2020.

Anon. (2020c), 'Japan's Coronavirus contact-tracing app launched amid privacy concerns', *The Japan Times*, 19 June, https://www.japantimes.co.jp/news/2020/06/19/national/japan-contact-tracing-app-launched/#.XwY1nSgzZPY. Accessed 29 August 2020.

Anon. (2020d), 'Macau launches colour code to fight COVID-19', *Macau News*, 1 May, https://macaunews.mo/macau-launches-colour-code-to-fight-covid-19. Accessed 28 August 2020.

App Store (n.d.), 'COCOA: COVID-19 contact app', https://apps.apple.com/gb/app/cocoa-covid-19-contact-app/id1516764458. Accessed 1 September 2020.

Ariadne Labs (2020), 'Emerging COVID-19 success story: South Korea learned the lessons of MERS', Our World in Data, 30 June, https://ourworldindata.org/covid-exemplar-south-korea. Accessed 16 August 2020.

Bacchi, Umberto (2020), 'Coronavirus surveillance poses long-term privacy threat, UN expert warns', Reuters, 31 March, https://www.reuters.com/article/us-health-coronavirus-privacy/coronavirus-surveillance-poses-long-term-privacy-threat-un-expert-warns-idUSKBN21I1XG. Accessed 1 September 2020.

Baker McKenzie (2020), 'TMT looking ahead', https://www.bakermckenzie.com/-/media/files/insight/publications/2020/03/tmtlookingahead2020_final_doc.pdf?la=en. Accessed 14 August 2020.

Bischoff, Paul (2019), 'Data privacy laws & government surveillance by country: Which countries best protect their citizens?', Comparitech, 15 October,

https://www.comparitech.com/blog/vpn-privacy/surveillance-states. Accessed 26 August 2020.

Borak, Masha (2020), 'China wants to keep health codes after the pandemic but users aren't so sure', *South China Morning Post*, 3 June, https://www.scmp.com/abacus/tech/article/3087437/china-wants-keep-health-codes-after-pandemic-users-arent-so-sure. Accessed 25 August 2020.

Bradford, Laura, Aboy, Mateo and Liddell, Kathleen (2020), 'COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes', *Journal of Law and the Biosciences*, 7:1, https://doi.org/10.1093/jlb/lsaa034. Accessed 26 August 2020.

Catania, Philip, Clarke, Helen and Do Rozario, Michael (2020), 'COVIDSafe: Australian data-inspired path to containing the spread of COVID-19', Mondaq, 11 May, https://www.mondaq.com/australia/reporting-and-compliance/931896/covidsafe-australian-data-inspired-path-to-containing-the-spread-of-covid-19. Accessed 4 August 2020.

Cha, Victor (2020), 'Asia's COVID-19 lessons for the West: Public goods, privacy, and social tagging', *The Washington Quarterly*, 43:2, pp. 1–18.

Chaos Computer Club e.V. (CCC) (2020), '10 requirements for the evaluation of "contact tracing" apps', 6 April, https://www.ccc.de/en/updates/2020/contact-tracing-requirements. Accessed 11 August 2020.

Chen, Kelvin (2020), 'Taiwan government database leaked on dark web', *Taiwan News*, 30 May, https://www.taiwannews.com.tw/en/news/3942167. Accessed 31 August 2020.

Choon, Chang May (2020), 'How South Korea used tech to track down Coronavirus and curb spread', *The Straits Times*, 1 May, https://www.straitstimes.com/asia/east-asia/how-south-korea-used-tech-to-track-down-virus-and-curb-spread. Accessed 29 August 2020.

Dixon, Rosalind and Ginsburg, Tom (eds) (2014), 'Introduction', in *Comparative Constitutional Law in Asia*, Cheltenham, UK: Edward Elgar Publishing, pp. 1–20, https://doi.org/10.4337/9781781002704.00006. Accessed 26 August 2020.

Donahoe, Eileen (2020), 'The COVID-19 test of democratic governance', *The American Interest*, 14 May, https://www.the-american-interest.com/2020/05/14/the-covid-19-test-of-democratic-governance. Accessed 2 August 2020.

Eigen, Melyssa, Wang, Flora and Gasser, Urs (2020), 'Country spotlight: Taiwan's digital quarantine system', Berkman Klein Center for Internet & Society, 31 July, https://cyber.harvard.edu/story/2020-07/country-spotlight-taiwans-digital-quarantine-system. Accessed 2 November 2020.

The Electronic Frontier Foundation and Article 19 (2014), 'Background and supporting international legal analysis to the international principles on the application of human rights law to communication surveillance', OHCHR, https://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf. Accessed 10 August 2020.

Embassy of the Republic of Korea in the Democratic Socialist Republic of Sri Lanka (Korean Embassy in Sri Lanka) (2020), 'Self-diagnosis mobile app installation instructions for all passengers entering Korea', 24 March, http://overseas.mofa.go.kr/lk-en/brd/m_2309/view.do?seq=759798&srchFr=&srchTo=&srchWord=&srchTp=&multi_itm_seq=0&itm_seq_1=0&itm_seq_2=0&company_cd=&company_nm=&page=1. Accessed 28 August 2020.

Ess, C. (2005), '"Lost in translation?": Intercultural dialogues on privacy and information ethics', *Ethics and Information Technology*, Special Issue: 'Privacy and Data Protection in Asia', 7:1, pp. 1–6, https://doi.org/10.1007/s10676-005-0454-0. Accessed 28 August 2020.

The European Data Protection Board (EDPB) (2020), 'Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak', 20 April, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf. Accessed 12 August 2020.

European Union Agency for Fundamental Rights and Council of Europe (2018), *Handbook on European Data Protection Law*, Luxembourg: Publications Office of the European Union, https://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf. Accessed 10 August 2020.

Gan, Nectar and Culver, David (2020), 'China is fighting the Coronavirus with a digital QR code: Here's how it works', CNN Business, 16 April, https://edition.cnn.com/2020/04/15/asia/china-coronavirus-qr-code-intl-hnk/index.html. Accessed 25 August 2020.

Gershgorn, Dave (2020), 'We mapped how the Coronavirus is driving new surveillance programs around the world', OneZero, 9 April, https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9. Accessed 2 August 2020.

Gkritsi, Eliza (2020), 'Chinese tech companies still can't stop medical data leaks', TechNode, 9 January, https://technode.com/2020/01/09/chinese-tech-companies-still-cant-stop-medical-data-leaks. Accessed 31 August 2020.

The Government of the Hong Kong Special Administrative Region (HKSAR Government) (2020), '"StayHomeSafe" mobile app user guide', https://www.coronavirus.gov.hk/eng/stay-home-safe.html. Accessed 27 August 2020.

The Government of the Macau Special Administrative Region (Macau Government) (n.d.), 'Macao health code', https://app.ssm.gov.mo/healthPHD/page/index.html. Accessed 27 August 2020.

Greenleaf, Graham (2014), *Asian Data Privacy Laws: Trade and Human Rights Perspectives*, Oxford: Oxford University Press.

Hale, Thomas and Shepherd, Christian (2020), 'Expats face hostility after second wave of virus cases hits China and Hong Kong', *Financial Times*, 31 March, https://www.ft.com/content/35c8fb72-ab36-4df7-8d38-68aa02b767e4. Accessed 31 August 2020.

Hartley, Kris and Jarvis, Darryl S. L. (2020), 'Policymaking in a low-trust state: Legitimacy, state capacity, and responses to COVID-19 in Hong Kong', *Policy and Society*, 39:3, pp. 403–23.

Hogan Lovells (2019), 'Asia Pacific data protection and cyber security guide 2019', IAPP, https://iapp.org/media/pdf/resource_center/Hogan_Lovells_Alert_Asia_Pacific_Data_Protection_Guide_2019.pdf. Accessed 24 August 2020.

Horwitz, Josh and Goh, Brenda (2020), 'As Chinese authorities expand use of health tracking apps, privacy concerns grow', Reuters, 26 May, https://www.reuters.com/article/us-health-coronavirus-china-tech/as-chinese-authorities-expand-use-of-health-tracking-apps-privacy-concerns-grow-idUSKBN23212V. Accessed 1 September 2020.

Huang, Yasheng, Sun, Meicen and Sui, Yuze (2020), 'How digital contact tracing slowed Covid-19 in East Asia', *Harvard Business Review,* 15 April, https://hbr.org/2020/04/how-digital-contact-tracing-slowed-covid-19-in-east-asia. Accessed 7 August 2020.

Hui, Mary (2020), 'How Taiwan is tracking 55,000 people under home quarantine in real time', Quartz, 1 April, https://qz.com/1825997/taiwan-phone-tracking-system-monitors-55000-under-coronavirus-quarantine. Accessed 7 August 2020.

IMD (2019), 'The IMD world digital competitiveness ranking 2019 results', https://www.imd.org/wcc/world-competitiveness-center-rankings/world-digital-competitiveness-rankings-2019. Accessed 4 August 2020.

International Covenant on Civil and Political Rights (1966), '999 UNTS 171', https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx. Accessed 25 August 2020.

Kabir, Omer (2020), 'New Israeli Covid-19 infection ranking app reminiscent of China's citizen ranking system, experts say', CTech, 1 April, https://www.calcalistech.com/ctech/articles/0,7340,L-3805426,00.html. Accessed 4 August 2020.

Kaye, David (2020), 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on disease pandemics and the freedom of opinion and expression A/HRC/44/49', https://freedex.org/wp-content/blogs.dir/2015/files/2020/04/A_HRC_44_49_AdvanceEditedVersion.pdf. Accessed 11 August 2020.

Kelly, Lidia (2020), 'Australia launches controversial COVID-19 tracking app as some states start easing rules', Reuters, 26 April, https://www.reuters.com/article/us-health-coronavirus-australia/australia-launches-controversial-covid-19-tracking-app-as-some-states-start-easing-rules-idUSKCN22806F. Accessed 4 August 2020.

Kim, Daewoung and Mah, Soohyun (2020), 'South Korea mandates QR codes to log customers after nightclub Coronavirus outbreak', Reuters, 2 June, https://www.reuters.com/article/us-health-coronavirus-southkorea-qr-code/south-korea-mandates-qr-codes-to-log-customers-after-nightclub-coronavirus-outbreak-idUSKBN23907E. Accessed 1 September 2020.

Kim, HyunJung (2020), 'South Korea learned its successful Covid-19 strategy from a previous Coronavirus outbreak: MERS', Bulletin of the Atomic Scientists, 20 March, https://thebulletin.org/2020/03/south-korea-learned-its-successful-covid-19-strategy-from-a-previous-coronavirus-outbreak-mers. Accessed 16 August 2020.

Kim, Samuel (2020), 'Safely connected: Public health apps and websites', Korean Culture and Information Service, http://www.kocis.go.kr/eng/webzine/202006/sub04.html. Accessed 28 August 2020.

Kirby, Michael and Greenleaf, Graham (2017), 'Asian data privacy laws: Trade and human rights perspectives', *International Data Privacy Law*, 7:1, pp. 70–71.

Ko, Haksoo, Leitner, John, Kim, Eunsoo and Jeong, Jonggu (2017), 'Structure and enforcement of data privacy law in South Korea', *International Data Privacy Law*, 7:2, pp. 100–14.

Kwon, Jake and Rahim, Zamira (2020), 'South Korea issues privacy warning after local reports link gay people to Coronavirus outbreak', CNN, 12 May, https://edition.cnn.com/2020/05/11/asia/south-korea-coronavirus-lgbt-intl/index.html. Accessed 31 August 2020.

Lee, Amanda (2020), 'What is China's social credit system and why is it controversial?', *South China Morning Post*, 9 August, https://www.scmp.com/economy/china-economy/article/3096090/what-chinas-social-credit-system-and-why-it-controversial. Accessed 26 August 2020.

Lee, Yimou (2020), 'Taiwan's new "electronic fence" for quarantines leads wave of virus monitoring', Reuters, 20 March, https://www.reuters.com/article/us-health-coronavirus-taiwan-surveillanc/taiwans-new-electronic-fence-for-quarantines-leads-wave-of-virus-monitoring-idUSKBN2170SK. Accessed 28 August 2020.

Lo, Clifford (2020), 'Coronavirus: Hong Kong police investigate suspected theft of two mobiles storing private details of quarantined residents', *South China Morning Post*, 19 February, https://www.scmp.com/news/hong-kong/health-environment/article/3051461/coronavirus-hong-kong-police-investigate. Accessed 31 August 2020.

Maçães, Bruno (2020), 'Only surveillance can save us from Coronavirus', Foreign Policy, 10 April, https://foreignpolicy.com/2020/04/10/coronavirus-pandemic-surveillance-privacy-big-data. Accessed 2 August 2020.

Madsen, W. (1992), 'Data protection in Japan and Hong Kong', in *Handbook of Personal Data Protection*, London: Palgrave Macmillan, https://doi.org/10.1007/978-1-349-12806-8_7. Accessed 31 August 2020.

McKinsey & Company (2020a), 'Could the next normal emerge from Asia?', https://www.mckinsey.com/featured-insights/asia-pacific/could-the-next-normal-emerge-from-asia. Accessed 6 August 2020.

McKinsey & Company (2020b), 'How technology is safeguarding health and livelihoods in Asia', https://www.mckinsey.com/featured-insights/asia-pacific/how-technology-is-safeguarding-health-and-livelihoods-in-asia. Accessed 6 August 2020.

Ministry of Health and Welfare of South Korea (MOHW) (2020), 'Guide on the installation of "self-quarantine safety protection app"', http://ncov.mohw.go.kr/upload/ncov/file/202004/1585732793827_20200401181953.pdf. Accessed 28 August 2020.

Mitchell, Anna and Diamond, Larry (2018), 'China's surveillance state should scare everyone', The Atlantic, 2 February, https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203. Accessed 6 November 2020.

Miyashita, Hiroshi (2011), 'The evolving concept of data privacy in Japanese law', *International Data Privacy Law*, 1:4, pp. 229–38.

The Office of the UN High Commissioner for Human Rights (OHCHR) (2014), 'Report of the Office of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age A/HRC/27/37', Geneva: OHCHR, https://digitallibrary.un.org/record/777869. Accessed 27 January 2021.

The Office of the High Commissioner for Human Rights (OHCHR) (2020a), 'COVID-19: Governments must promote and protect access to and free flow of information during pandemic – International experts', https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25729&LangID=E. Accessed 10 August 2020.

The Office of the High Commissioner for Human Rights (OHCHR) (2020b), 'COVID-19 guidance', https://www.ohchr.org/Documents/Events/COVID-19_Guidance.pdf. Accessed 11 August 2020.

Park, Kyung Sin (2020), 'Korea's COVID-19 success and mandatory phone tracking', Open Net Korea, 20 October, http://opennetkorea.org/en/wp/3142. Accessed 2 November 2020.

Pierucci, Alessandra and Walter, Jean-Philippe (2020a), *Joint Statement on the Right to Data Protection in the Context of the COVID-19 Pandemic*, Strasbourg: Council of Europe, https://rm.coe.int/covid19-joint-statement/16809e09f4. Accessed 10 August 2020.

Pierucci, Alessandra and Walter, Jean-Philippe (2020b), *Joint Statement on Digital Contact Tracing*, Strasbourg: Council of Europe, https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7. Accessed 12 August 2020.

Ponce, Aida (2020), 'COVID-19 contact-tracing apps: How to prevent privacy from becoming the next victim', *ETUI Research Paper: Policy Brief 5/2020*, May, https://ssrn.com/abstract=3593405. Accessed 15 August 2020.

Privacy International (2012), 'A new dawn: Privacy in Asia', https://privacyinternational.org/sites/default/files/2017-12/A%20New%20Dawn_Privacy%20in%20Asia.pdf. Accessed 14 August 2020.

Sedik, Tahsin Saadi (2018), 'Asia's digital revolution', Washington, DC: Finance & Development (IMF), September, https://www.imf.org/external/pubs/ft/fandd/2018/09/asia-digital-revolution-sedik.htm. Accessed 22 August 2020.

Sheng, Chuyi and He, Zijia (2020), 'Is China's "health code" here to stay?', *The Diplomat*, 18 July, https://thediplomat.com/2020/07/is-chinas-health-code-here-to-stay. Accessed 31 August 2020.

Small, Zane (2020), 'Singapore's COVID-19 contact tracing tech TraceTogether catches Jacinda Ardern's eye to fight Coronavirus', Newshub, 9 April, https://www.newshub.co.nz/home/politics/2020/04/singapore-s-covid-19-contact-tracing-tech-tracetogether-catches-jacinda-ardern-s-eye-to-fight-coronavirus.html. Accessed 4 August 2020.

Tzu-ti, Huang (2020), 'Taiwan's digital fence technologies draw international attention', *Taiwan News*, 8 April, https://www.taiwannews.com.tw/en/news/3912429. Accessed 30 August 2020.

United Nations (UN) (1948), ' Universal Declaration of Human Rights 1948, GA Res 217A (III), A/810 at 71', http://hrlibrary.umn.edu/instree/b1udhr.htm. Accessed 10 August 2020.

United Nations (UN) (2014), 'GA Res 68/167, UN Doc A/RES/68/167', 21 January, http://undocs.org/A/RES/68/167. Accessed 10 August 2020.

United Nations (UN) (2020), 'COVID-19 and human rights: We are all in this together', https://www.un.org/victimsofterrorism/sites/www.un.org.victimsofterrorism/files/un_-_human_rights_and_covid_april_2020.pdf. Accessed 10 August 2020.

Wang, Zhiqiong June (2020), 'Law in crisis: A critical analysis of the role of law in China's fight against COVID-19', *Griffith Law Review,* https://doi.org/10.1080/10383441.2020.1790332. Accessed 27 January 2021.

World Health Organization (WHO) (2016), *International Health Regulations (2005)*, 3rd Ed., Geneva: WHO, https://www.who.int/ihr/publications/9789241580496/en/. Accessed 13 August 2020.

World Health Organization (WHO) (2020a), 'Middle East respiratory syndrome Coronavirus surveillance archive', https://www.who.int/westernpacific/emergencies/surveillance/archives/mers. Accessed 20 August 2020.

World Health Organization (WHO) (n.d.), 'SARS (severe acute respiratory syndrome)', https://www.who.int/ith/diseases/sars/en/. Accessed 20 August 2020.

Yang, Yuan, Liu, Nian, Wong, Sue-Lin and Liu, Qianer (2020), 'China, coronavirus and surveillance: The messy reality of personal data', *Financial Times*, 2 April, https://www.ft.com/content/760142e6-740e-11ea-95fe-fcd274e920ca. Accessed 27 August 2020.

SUGGESTED CITATION

Sherstoboeva, Elena and Pavlenko, Valentina (2021), 'Trends in East Asian policies on digital surveillance tools during the COVID-19 pandemic', *Journal of Digital Media & Policy*, 12:1, pp. 47–65, doi: https://doi.org/10.1386/jdmp_00047_1

CONTRIBUTOR DETAILS

Elena Sherstoboeva is an assistant professor at the School of Creative Media and School of Law, City University of Hong Kong. She worked at the National Research University Higher School of Economics and Moscow State University (MSU) in Russia. Elena earned two Ph.D. degrees with distinctions in journalism (MSU) and in communication (Ramon Llull University, Spain). She has diverse experience in interdisciplinary research and providing expert reviews in media, communication and entertainment law and policies for academia, industry and international organizations, including the Council of Europe, OSCE Representative on Freedom of the Media and UNESCO.

Contact: School of Creative Media, City University of Hong Kong, Run Run Shaw Creative Media Centre, Level 7, 18 Tat Hong Avenue, Kowloon Tong, 999077, Hong Kong.
E-mail: eshersto@cityu.edu.hk

http://orcid.org/0000-0003-1528-0300

Valentina Pavlenko is a senior lecturer in the School of Communications, Media and Design at National Research University Higher School of Economics, Moscow, Russia. Her research interests include media regulation and policies in the context of international legal standards.

Contact: National Research University Higher School of Economics, 20 Myasnitskaya Ulitsa, Moscow 101000, Russia.
E-mail: vpavlenko@hse.ru

https://orcid.org/0000-0002-5287-6210