



universität
wien

MASTER THESIS

Titel der Master Thesis / Title of the Master's Thesis

**“International data protection
in the fight against a global pandemic”**

verfasst von / submitted by

Dinara Aryspayeva

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of
Master of Laws (LL.M.)

Wien, 2021 / Vienna 2021

Studienkennzahl lt. Studienblatt /
Postgraduate programme code as it appears on
the student record sheet:

A 992 548

Universitätslehrgang lt. Studienblatt /
Postgraduate programme as it appears on
the student record sheet:

Europäisches und Internationales Wirtschaftsrecht /
European and International Business Law

Betreut von / Supervisor:

Univ.-Prof. Dr. Dr. h.c. Peter Fischer

Acknowledgements

I would like to express my sincere gratitude to my dissertation supervisor Univ.-Prof. Dr. Dr. h.c. Peter Fisher for giving me the opportunity to do this research under his supervision.

Furthermore, let me express my thanks to my sister, Dr. Elmira Lechat who made it possible for me to enroll in this master's course and for her love and understanding.

In addition, I would also like to acknowledge everyone who played a role in my academic accomplishments. Thank you all for your unwavering support.

Abstract

The sudden global outbreak of SARS-CoV-2, or better known as Covid-19 has heavily impacted people's day-to-day lives around the world. To address and conquer the threats posed of this virus, governments, the general public and private organizations alike have taken crucial steps such as the use of tracking apps and digital surveillance (face recognition technology and drones). Such measures taken often involve the processing of various types of personal data, including those related to health, and privacy and data protection, which in turn creates significant challenges. This dissertation aims to explore international data protection in the fight against a global pandemic. In this regard, it considers as an overview the legal basis of data protection on international, European and selected national legislations. More precisely, this dissertation focuses on three categories of measures that countries use in fighting a global pandemic: the collection and use of data related to health, tracking apps and digital surveillance. Moreover, in order to conduct the research, qualitative methods are applied, focusing particularly on the case study approach, during which data protection violations are identified. In brief, data should always be processed in a lawful, fair, and transparent manner and comply with all the necessary principles under the relevant data protection laws. This dissertation attempts to understand the possible necessity of the digital measures applied in the fight against a global pandemic based on recommendations which will ensure that people's rights to privacy and data protection are safeguarded through the current pandemic and those that we will inevitably have to face again in the future.

Keywords: pandemic, data protection, Covid-19, tracing apps, digital surveillance, GDPR, face recognition technology, personal data, health data

Deutscher Abstract

Der plötzliche weltweite Ausbruch von SARS-CoV-2 oder besser bekannt als Covid-19 hat das tägliche Leben der Menschen in der ganzen Welt stark beeinflusst. Um die durch diesen Virus verursachten Bedrohungen anzugehen und zu besiegen, haben Regierungen sowie allgemeine öffentliche bzw. private Organisationen bedeutende Schritte unternommen, wie die Verwendung von Tracking-Apps und die digitale Überwachung (Gesichtserkennungstechnologie und Drohnen). Solche Maßnahmen umfassen häufig die Verarbeitung verschiedener Arten personenbezogener Daten, einschließlich solcher im Zusammenhang mit Gesundheit, Datenschutz und Privatsphäre, was wiederum erhebliche Herausforderungen mit sich bringt. Ziel dieser Dissertation besteht darin, den internationalen Datenschutz im Kampf gegen eine globale Pandemie zu untersuchen. In dieser Hinsicht behandelt sie als Überblick die Rechtsgrundlage des Datenschutzes für internationale, europäische und ausgewählte nationale Rechtsvorschriften. Genauer gesagt konzentriert sich diese Dissertation auf drei Kategorien von Maßnahmen, die Länder zur Bekämpfung einer globalen Pandemie auf der ganzen Welt anwenden: die Ansammlung und Verwendung von Gesundheitsdaten, Tracking-Apps und digitale Überwachung. Darüber hinaus wurden qualitative Methoden für die Durchführung der Forschung angewendet, die sich insbesondere auf den Fallstudienansatz konzentrieren, bei dem Datenschutzverletzungen festgestellt wurden. Kurz gesagt, sollten Daten immer auf rechtmäßige, faire und transparente Weise verarbeitet werden und allen erforderlichen Grundsätzen und Anforderungen der einschlägigen Datenschutzgesetze entsprechen. Diese Dissertation versucht, die mögliche Notwendigkeit der digitalen Maßnahmen zur Bekämpfung einer globalen Pandemie zu begreifen, die auf Empfehlungen beruhen, die sicherstellen, dass die Menschenrechte auf Privatsphäre und Datenschutz durch die aktuelle Pandemie und diejenigen, denen wir uns in Zukunft zwangsläufig erneut stellen müssen, gewahrt bleiben.

Schlagwörter: Pandemie, Datenschutz, Covid-19, Tracking-Apps, digitale Überwachung, Gesichtserkennungstechnologie, DSGVO, personenbezogenen Daten, Gesundheitsdaten

Table of Contents

List of Abbreviations	6
Introduction.....	7
1. Global data protection.....	8
1.1 International data protection.....	8
1.1.1 The United Nations.....	9
1.1.2 Convention 108 and OECD Guidelines	10
1.1.3 The Global Privacy Assembly.....	10
1.2 European Data Protection.....	11
1.3. Selected national data protection.....	12
1.3.1 Data Protection in the United States of America.....	12
1.3.2 Data Protection in the People's Republic of China.....	13
1.3.4. Data Protection in the MENA and in the ASEAN.....	16
1.3.5. Implementing data protection legislation in the fight against a global pandemic.....	17
1.4. The released statements and guidelines on data privacy obligations during the COVID-19 pandemic.....	19
2. The use of digital surveillance.....	20
2.1 Collection and use of health data.....	20
2.1.1 Legal basis of health data protection.....	20
2.1.2 Incorrect collection and use of health data during the pandemic in some countries.....	21
2.1.3. Main measures protecting the processing of health data	23
2.2 The use of Contact Tracing Apps (CTA) in the fight against a global pandemic.....	25
2.2.1 Main advantages and concerns of using CTA.....	25
2.2.2 Decentralised and centralised technological approaches of CTA.....	27
2.2.3 Data protection in the use of the CTA.....	30
2.3. The Use of Face Recognition Technology and Drones.....	34
2.3.1 Facial recognition technology (FRT) in the context of the COVID-19 outbreak.....	35
2.3.2 Chinese approach to FRT.....	35
2.3.3 European approach to FRT.....	38
2.3.4 The US approach to FRT.....	41
2.3.5 Use of drones in the context of COVID-19.....	43
3. Recommendations on the use of the digital surveillance	45
3.1 Legal basis for data protection and creating an independent supervisory authority.....	46
3.2 Taking several steps for optimization.....	46
3.3 Respect international data protection standards.....	48
3.4 Additional amendments or laws in the Covid-19 outbreak.....	49
3.5 Technical privacy solutions.....	49
3.6 Public awareness.....	50
Conclusion.....	51
Bibliography	55

Abbreviations

AFR	the Automated facial recognition
ASEAN	the Association of Southeast Asian Nations
BIPA	the Biometric Information Privacy Act
CAC	the Central Cyberspace Administration of China
CCPA	the California Consumer Privacy Act
COVID-19	the Severe acute respiratory syndrome coronavirus 2 or SARS-CoV-2
CTA	the Contact Tracing App
DPIA	the Data Protection Impact Assessments
DDPA	the Danish Data Protection Agency
ECHR	the European Convention on Human Rights
EDPB	the European Board of Data Protection
GDPR	the General Data Protection Regulation
FRT	the Facial recognition technology
LED	the Law Enforcement Directive
EU	the European Union
MENA	the Middle East North Africa
PDPA	the Personal Data Protection Act 2012
PEPP-PT	the Pan-European Privacy-Preserving Proximity Tracing
PEA	the Privacy enforcement authority
PIPA	the Personal Information Protection Act
PII	the Personally Identifiable Information
PISS	the Personal Information Security Specification
OECD	the Organization for Economic Co-operation and Development
SWP	the South Wales Police
UAS	the unmanned aircraft system
UN	the United Nations
USA	the United States of America
WHO	the World Trade Organization

Introduction

Since the beginning of 2020, the world has been rocked by the discovery of COVID-19¹, which by the end of 2019 had infected and killed an unprecedented amount of people in China's Wuhan province². And although quarantine was a successful course of action from an epidemiological perspective in controlling transmission, it was also the cause of devastation to the economy and people's mental health. Thus, to control and alleviate the threats of COVID-19, governments, and public and private organizations alike have taken numerous steps accordingly.

In the era of digitalization, the main containment strategies such as social distancing, hygiene, and wearing masks have been supplemented by technological measures to slow the transmission and infection of COVID-19, including tracing apps for smartphones, face recognition cameras and drones.

As noted by the Director-General of the World Health Organization, Tedros Adhanom Ghebreyesus, the fight against COVID-19 is leveraging the same tools that conquered Ebola - these include disease surveillance, case finding, contact tracing, and mass communication campaigns to notify and educate affected populations.³ Moreover, other than mass and ring vaccination, history shows that contact tracing and case isolation have resolutely helped to eradicate smallpox around the world.⁴

Data are also critical to assessing and improving the capacity of healthcare systems and to assess the efficiency of containment and mitigation strategies that limits the mobility and

¹ WHO, 'Naming the coronavirus disease (COVID-19) and the virus that causes it' <[https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-\(covid-2019\)-and-the-virus-that-causes-it](https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it)> accessed 30 September 2020

² WHO, 'Coronavirus disease 2019 (Covid-19)' Situation Report 94 (2020) <https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200423-sitrep-94-covid-19.pdf?sfvrsn=b8304bf0_2#:~:text=Retrospective%20investigations%20by%20Chinese%20authorities,%2C%20some%20did%20not> accessed 1 October 2020

³ WHO, 'WHO Director-General's opening remarks at the media briefing on COVID-19 - 8 May 2020' (2020) <<https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---8-may-2020>> accessed 1 October 2020

⁴ Mirjam Kretzschmar, Susan van den Hof, Jan van Wijngaarden, 'Ring vaccination and smallpox control' (2004) Research, Emerg Infect Dis. <<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3323203/pdf/03-0419.pdf>> accessed 1 October 2020

movement of individuals.⁵ Despite the potential in using data in order to help the end of the pandemic, such methods can interfere with the protection of personal data and the right to private life. Accordingly, it raises question as to how such data can be used in such measures in compliance with data protection legislation?

To answer this question, this dissertation examines international, European and national legal frameworks that concern data protection, and more specifically legislation that has been adopted and implemented by countries around the world in the fight against COVID-19, as well as some laws that were already in place that assist in the protection and safeguarding of people's data.

The second chapter examines the collection and application of data related the people's health, the legal basis for doing so, and the main measures that can be used to safeguard such data. Furthermore, the usage of digital technology in the fight against a global pandemic helps demonstrate the advantages and concerns from a legal perspective associated with such measures. In addition, the chapter provides different cases that highlight violations of data protection in the given context.

The application of technology in the flight against COVID-19 has reintroduced a pre-prevailing global concern concerning the protection of data and users' privacy. In this unprecedented time, measures carried out in to the fight against the pandemic that requires the use of personal data, including those related to health, should thus be essential and proportionate. Therefore, the third chapter discusses different recommendations on the processing of personal data with regard to the measures taken to contain the spread of COVID-19, by data protection authorities around the world and in compliance with the relevant principles and laws.

1. Global data protection

1.1 International data protection

The increasing worldwide advancement of information technology raises the significance of data privacy law, the proper assessment of it, and its enforcement based on global norms. For

⁵ OECD, 'Ensuring data privacy as we battle COVID-19' (2020) 2 <https://read.oecd-ilibrary.org/view/?ref=128_128758-vfx2g82fn3&title=Ensuring-data-privacy-as-we-battle-COVID-19>, accessed 1 October 2020

instance, international human rights law offers a clear-cut and universal framework for the promotion and protection of the right to privacy.

1.1.1 The United Nations

The United Nations (UN) has long promoted the right to privacy via its numerous human rights treaties. The right to privacy is enshrined by the Universal Declaration on Human Rights⁶, International Covenant on Civil and Political Rights⁷, Convention on the Rights of the Children⁸, International Covenant on the Protection of All Migrant and Members of their Families⁹, and the International Covenant on Civil and Political Rights¹⁰. Moreover, the UN has further increased its role in privacy protection via the adoption of two well-known measures:

- the publication of a statement on digital rights;
- the appointment of a Special Rapporteur on the right to privacy.¹¹

The General Assembly implemented Resolution 68/167, which expressed serious misgivings about the negative impact that surveillance and the interception of communications may have on human rights.¹² As a result, the General Assembly recommended that countries around the world re-evaluate their procedures, norms and legislation associated with communications surveillance, and the interception and collection of personal data and stressed the requirements for countries to confirm the complete and effective implementation of their obligations under international human rights law.¹³ The resolution notes that international human rights law offers a universal framework against which any interference to the right of privacy of the individual must be evaluated.

⁶ The Universal Declaration on human Rights, Art. 12

⁷ The International Covenant on Civil and Political Rights, Art. 17

⁸ The Convention on the Rights of the Children, Art. 16

⁹ The International Covenant on the Protection of All Migrant and Members of their Families, Art. 14

¹⁰ The International Covenant on Civil and Political Rights, Art.17

¹¹ UNCTAD, 'Data protection regulations and international data flows: Implications for trade and development' (2016) 24 <https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf> accessed 3 October 2020

¹² Resolution of the General Assembly UN 'The right to privacy in the digital age' 18 December 2013, 68/167 <http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167> accessed 3 October 2020

¹³ UNCTAD, 'Data protection regulations and international data flows: Implications for trade and development' (n 11) 24

Due to the global spread of COVID-19, numerous additional privacy, data protection, security, and legal compliance questions have been generated. The UN Special Rapporteur released the preliminary evaluation of the privacy dimensions of COVID-19, which examines two particular aspects of its impact on the right to privacy: data protection and surveillance.¹⁴

1.1.2 Convention 108 and OECD Guidelines

Data protection is implicit in two of the original data protection frameworks with global influence, namely the Organization for Economic Co-operation and Development Privacy Guidelines in 1980¹⁵ (OECD Guidelines) and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data¹⁶, known as Convention 108¹⁷

Convention 108 is most robust, legally-enforceable international agreement on data protection. Moreover, it is distinct from other global initiatives in that it legally binds its signatories, unlike the OECD Guidelines which can be followed by any country, and not purely OECD members. Convention 108 offers full coverage; for instance, there is common acceptance of the principles contained within it; and it offers the chance for any country to join.¹⁸ Meanwhile, the OECD Guidelines include eight privacy principles that make up the spine of most related national privacy laws.¹⁹

1.1.3 The Global Privacy Assembly

The Global Privacy Assembly (hereon in referred to as “Assembly”) first met in 1979 as the International Conference of Data Protection and Privacy Commissioners. The Assembly intends to deliver global leadership in the spheres of data protection and privacy by bringing

¹⁴ Office of the High Commissioner United Nations Human Rights, ‘Preliminary evaluation of the privacy dimensions of the coronavirus disease (COVID-19) pandemic: report’, 2020, <<https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/COVID-19.aspx>>, accessed 3 October 2020

¹⁵ Recommendation of the Council concerning Guidelines governing the Protection of Privacy and transborder flows of personal data 23 September 1980

¹⁶ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 28 January 1981

¹⁷ Digital Rights Center, ‘Data protection history: emerged as GDPR’ (2018) <<https://habr.com/ru/company/digitalrightscenter/blog/431582/>> accessed 2 October 2020

¹⁸ UNCTRAD, ‘Data protection regulations and international data flows: Implications for trade and development’ (n 11) 25-26

¹⁹ Ibid 26

together the endeavours of 130 data protection and privacy authorities from across the world.²⁰ At its 2005 meeting, the International Data Protection Commissioners released a statement titled: The Protection of Personal Data and Privacy in a Globalised World: A Universal Right Respecting Diversities ("Montreux Declaration").²¹ The declaration encouraged the creation of an international convention on data protection, and to synchronize global data protection laws. On the 42nd closed session of the Assembly, a new temporary Working Group on COVID-19 related to privacy and data protection issues was established.²²

1.2 European Data Protection

This chapter discusses the main regional data protection agreements, which were developed by the European Union (EU).

The right to data protection comes from the right to privacy, which was defined by Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (1950), also known as the European Convention on Human Rights (ECHR).

Secondly, data protection in Europe cemented the adequacy approach, particularly by the EU's Data Protection Directive (1995)²³ and its successor, the General Data Protection Regulation (GDPR)²⁴. The GDPR advances a more robust and unified data protection regulation throughout the entire European Union.²⁵ EU countries have stringent laws and are permitted to levy massive fines in the event of a data breach. An organization that processes or keeps personal data on any living citizen, or any living individual residing in the EU must conform with the regulation.²⁶

²⁰ Global Privacy Assembly, < <https://globalprivacyassembly.org/>>, accessed 3 October 2020

²¹ The Protection of Personal Data and Privacy in a Globalized World: A Universal Right Respecting Diversities 2005 (Montreux-Declaration)

²² Resolution on the Privacy and Data Protection Challenges in the Context of the Covid-19 Pandemic, 42nd closed session of the Global Privacy Assembly October 2020

²³ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281 23/11/1995 P. 0031 – 0050)

²⁴ EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ 2016 L 119/1) (GDPR)

²⁵ Haug, Charlotte J, 'Turning the tables - the new european general data protection regulation' (2018) the New England Journal of Medicine 208

²⁶ Mark Foulsham, Brian Hitchen, Andrew Denley, 'GDPR: How to achieve and Maintain Compliance' (2019) London: Routledge 1st Edition 2

1.3. Selected national data protection

To date, 132 out of 194 countries have adopted legislation to ensure the protection of individuals' data and privacy.²⁷

In the fight against COVID-19, and with regard any pandemic in the future, when the accumulation and processing of large-scale personal data takes place, it is crucial that countries have in place robust data protection measures in order to avoid the mishap of data protection breaches. As mentioned in the report by the UN Special Rapporteur on the right to privacy: "If a State decides that technological surveillance is necessary as a response to the global COVID-19 pandemic, it must make sure that, after proving both the necessity and proportionality of the specific measure, it has a law that explicitly provides for such surveillance measures. The law must include safeguards, which, if not spelled out in sufficient detail, cannot be considered adequate under international law."²⁸ This subsection gives an outline of the legal basis of data protection of the selection countries, in particular legislation that has been made by countries around the world in the fight against a global pandemic.

1.3.1 Data Protection in the United States of America

At the federal level, the US lacks centralized, formal legislation to protect the electronic transmission and storage of individuals' data as that of the GDPR.²⁹ For example, the US state of California serves as a global centre for high technology and innovation and was the first US state to adopt its own privacy law.³⁰ The California Consumer Privacy Act (CCPA), which became effective on 1 January 2020, was created to strengthen privacy rights and consumer protection by offer the residents of California the right to apply the CCPA in order to control and be acknowledged as regards what personal data are being collected, how they are being used and to prohibit any use or sale of their personal data.³¹ The CCPA is not necessarily similar

²⁷ UNCTAD, 'Data Protection and Privacy Legislation Worldwide' <<https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>> accessed 2 October 2020

²⁸ Joseph A. Cannataci, 'Report of the Special Rapporteur on the right to privacy', (2020), Seventy-fifth session of General Assembly of the UN 27 July 2020 2

²⁹ Steven Chabinsky, Paul Pittman, 'USA: Data protection Laws and Regulations' (2020) <<https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa>> accessed 2 October 2020

³⁰ Jeeyn Baik, 'Data privacy against innovation or against discrimination? The case of the California Consumer Privacy Act (CCPA)' (2020) 1

³¹ Chabinsky, Pittman (n 29)

to GDPR, but both enjoy several common characteristics. For instance, the GDPR is comprehensive, while the CCPA is more limited.³²

Of particular note, a group of four US Republican senators aim to introduce a COVID-19 Consumer Data Protection Act that would control the data gathered by COVID-19 contact tracing apps in order to give all US citizens more transparency, choice, and control over the collection and use of their data related to their health, geolocation, and proximity.³³ The act would require organizations to get explicit permission from individuals to collect any data on their health, location or proximity to another person. Organizations would be obliged to reveal the use, retention and deletion period of the data and apply specific measures to guarantee that the identification of any individual would not be made possible based on anonymized data.³⁴ Under a state action doctrine, only government action is subject to scrutiny under constitutional law, but private conduct is not proscribed. Constitutional law does not provide a complete framework for considering many potential threats to digital privacy and consumer data. Instead, the most critical data protection standards come from statutory law.³⁵

1.3.2 Data Protection in the People's Republic of China

Privacy protection³⁶ is weak in China and the concepts of data protection and data privacy laws are relatively new.³⁷ However, the situation was changed in the fight against a global pandemic. To collect swathes of personal data, including tracking citizens' travel, health and people who had been in close proximity with those who had developed infection symptoms, it has been reported that China applied ubiquitous sensor data and health-check apps that also assisted in curbing the disease spread.³⁸ However, multiple data breach incidents have aroused concerns

³² California Consumer Privacy Act (CCPA), Compliance' <https://cpl.thalesgroup.com/compliance/americas/california-consumer-privacy-act-compliance-solutions-ccpa-compliance?_ga=2.99010590.1060482728.1601540838-1057165311.1601540838> accessed 2 October 2020

³³ Natalie Moreno, 'Coronavirus and contact tracing apps: Global privacy perspective' (2020) 6 <https://www.addleshawgoddard.com/globalassets/insights/data-protection/coronavirus-and-contact-tracing-apps-article_spreads.pdf> accessed 3 October

³⁴ Ibid 6

³⁵ Congressional Research Service, 'Data Protection Law: An Overview Congressional Research Service' 2019 7

³⁶ Bu Qingxiu 'Human flesh search' in china: The double-edged sword'. International Data Privacy Law. 2013 3(3)184

³⁷ Lothar Determann, 'Healthy Data Protection', Michigan Telecommunications and Technology Law Review Vol. 26 No. 229 UC Hastings Research Paper No. 349 (2020) 244

³⁸ The Economist, 'To curb covid-19, China is using its high-tech surveillance tools' (2020) <<https://www.economist.com/china/2020/02/29/to-curb-covid-19-china-is-using-its-high-tech-surveillance-tools>> accessed 3 October 2020

over privacy and potential discrimination against those namely from Wuhan and Hubei provinces.³⁹

On February 2020, the National Health Commission of China, regarding the aforementioned concerns, issued a Notice on Strengthening Informatization to Support the Prevention and Control of the Pneumonia Epidemic of New Coronavirus Infection which outlines the personal data protection requirements with regards to the prevention and control of COVID-19.⁴⁰ Moreover, on 4 February 2020, the Central Cyberspace Administration of China (CAC) issued the Circular on Ensuring Effective Personal Information Protection and Utilization of Big Data to Support Joint Efforts for Epidemic Prevention and Control (CAC Circular) that outlines clear guidance on protecting personal data under the current circumstances.⁴¹ It declares that parties permitted by the health department of the state council may collect personal data to prevent and control the epidemic⁴² whereby “personal data collected to prevent or treat epidemic diseases cannot be used for any other purpose...” and “cannot be disclose any personal information without the consent of the person being collected, unless it required for joint prevention and control work”.⁴³ Bodies and organizations gathering and possessing personal data are required to have robust data security measures in place to avoid data breaches.⁴⁴

Unless otherwise authorized under Chinese legislation, no person or organization may gather or use personal data without the express consent of the data subject. If such data are gathered and employed to thwart and control epidemic diseases, those that do so must abide by to the Personal Data Specifications, which are indeed mandatory industry standards for data protection. In other words, the principles of limitation and minimum collection should be adhered to. For example, data collected should be restricted to those confirmed or suspected of having COVID-19 and those who have shared close contact with confirmed or suspected COVID-19 carriers. Such personal information cannot be made public without the data

³⁹ Ibid

⁴⁰ General Office of the National Health Commission of China, “Notice of the General Office of the National Health Commission on Strengthening Informationization to Support the Prevention and Control of Pneumonia Epidemics Caused by the Novel Coronavirus Infection Issuing Authority” 2020 <http://www.gov.cn/zhengce/zhengceku/2020-02/05/content_5474692.htm> accessed 4 October 2020

⁴¹ Ibid

⁴² The Office of Cyberspace Affairs in China, ‘Notice on Doing a Good Job in Personal Information Protection and Using Big Data to Support Joint Prevention and Control Work’ (2020) <<https://perma.cc/6WUS-ZLQV>>, accessed 4 October 2020

⁴³ Ibid

⁴⁴ Ibid

subjects' consent unless it is necessary to do so with a target of prevention further spread of the virus. Moreover, the information must be redacted and or anonymized.⁴⁵

Furthermore, following the statement⁴⁶ by the National People's Congress, the Chinese government is mindful of the insistence for a centralized data protection law. On 2 July 2020, the Standing Committee of the 13th National People's Congress announced the draft of the "Data Security Law"⁴⁷, meaning that China's first legislative process for data security laws was officially launched. The draft defines data as the recording of information in electronic or non-electronic forms, and introduces the concept of "data activity", including the collection, storage, processing, use, provision, transaction and disclosure of data. Meanwhile, data security refers to the capacity to guarantee that data are efficiently safeguarded and employed in a legal manner by applying the necessary steps, and that they are stored at all times securely.⁴⁸

One of the central issues in the draft is the obtainment of personal consent with full notice in advance, where the individual has the right to withdraw consent; personal consent should also be re-obtained if essential matters are changed; while personal disagreement shall not be used as a reason to refuse to provide products or services.⁴⁹ Sun Xianzhong, a member of the Chinese Academy of Social Sciences, noted that the main link concerning information is notification.⁵⁰ This requires that the processor of personal information must to be honest and clear in notifying individuals.

In recent years, in China the trading of information such as flight whereabouts of public figures has formed a black industry chain, which has seriously violated personal privacy; citizens' personal information registered with relevant institutions has been frequently leaked, and has even been used in illegal and criminal activities such as telecommunications fraud.⁵¹ Taking

⁴⁵ Norton Rose Fulbright, 'Personal data protection amid coronavirus: Key takeaways for business operating in China' (2020) 1 <<https://www.nortonrosefulbright.com/ru-ru/knowledge/publications/d61ee6b6/personal-data-protection-in-the-time-of-coronavirus-covid-19>> accessed 4 October 2020

⁴⁶ Zhang Yesui, 'The formulation of a personal information protection law has been included in this legislative plan' (2019) <http://www.china.com.cn/lianghui/news/2019-03/04/content_74529251.shtml> accessed 4 October 2020

⁴⁷ Yan Luo, Zhijing Yu, 'China issued the Draft Data Security Law' (2020), <<https://www.insideprivacy.com/data-security/china-issued-the-draft-data-security-law/>> accessed 4 October 2020

⁴⁸ Ibid

⁴⁹ Bai Yang, Ren Qinqin, 'How does the first draft of the Personal Information Protection Law defend your information security?' (2020) <https://www.thepaper.cn/newsDetail_forward_9544106> accessed 4 October 2020

⁵⁰ Ibid

⁵¹ Ibid

into account today's surveillance in the fight against COVID-19, due to the obligation to use tracking apps in China, this is an even more vulnerable point. Thus, for this reason, it is vital that Chinese authorities implemented in the draft a special section to restrict the processing of sensitive personal information. According to the draft, sensitive personal information includes such as including nationality, physical condition and financial position. In this regard, China is inclined to follow the EU approach with some tailored modifications.⁵²

The draft is also aimed at responding to public health emergencies or at protecting the lives and health of natural persons in emergencies. Thus, it emphasizes that personal information protection obligations must also be fulfilled in the handling of personal information in the fight against a global pandemic.⁵³

1.3.4. Data Protection in the Middle East North Africa (MENA) and in the Association of Southeast Asian Nations (ASEAN)

In most jurisdictions across the MENA region, an individual's privacy and the protecting of personal data are given under general provisions of law rather than those particularly cantered on these issue per se.⁵⁴ For example, in Jordan, data protection is regulated by multiple constitutional provisions and some sectoral laws, which have not long ago been strengthened further by the new Data Privacy and Protection Bill, 2020, Draft Law.⁵⁵

A similar situation exists in the ASEAN region, where not all countries have comprehensive legislation covering the sphere of data protection. For instance, in Brunei Darussalam, no comprehensive law exists that focuses on data protection at the moment, but a data protection policy has guided the country since 2014.⁵⁶ In another example, the Personal Data Protection Act 2012 (PDPA) in Singapore establishes a data protection law that provides multiple rules

⁵² Ibid

⁵³ James Gong, Gavin Guo, Nanda Lau, 'China Cyber Security and Data Protection: China Issues Draft of "Data Security Law' (2020) <<https://www.lexology.com/library/detail.aspx?g=0b312359-b397-445e-b659-5a5bf19a4e62>> accessed 4 October 2020

⁵⁴ The GSMA, 'Data Privacy Frameworks in MENA. Emerging approaches and common principles', (2019), Executive Summary 5 <<https://www.gsma.com/mena/wp-content/uploads/2019/07/GSMA-Data-Privacy-in-MENA-Exec-Summary.pdf>> accessed 3 October 2020

⁵⁵ Alaelidin Alkhasawneh, 'The Future of Biometric Data Protection in Jordan in Light of the GDPR: Do we need to comply with the GDPR?' (2020) Vol. 23 Iss.2, 1

⁵⁶ Deloitte, 'Data and Privacy Protection in ASEAN. What does it mean for business in the region?' (2019) <<https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-data-privacy-in-asean.pdf>> 5 accessed 3 October 2020

concerning the collection, use, disclosure, and care of personal data acknowledging both the rights of individuals to protect their personal data, including the rights of access and correction, and the requirements of organizations to collect, use, or disclose personal data for genuine and reasonable objectives.⁵⁷ Meanwhile, Cambodian law contains no comprehensive legislation or regulations that specifically address privacy rights or protect personal information obtained from individuals. Although data privacy is regulated by various laws, Cambodian e-commerce law sets out, for the first time, data protection rules that are applicable to every sector of the country that electronically stores personal information obliging entities to set up all required measures to guarantee that the data are reasonably shielded from unallowed accession, use, alteration, outflow, or disclosures.⁵⁸

1.3.5. Implementing data protection legislation in the fight against a global pandemic

Very few countries have frameworks to sustain these extraordinary measures that are swift, secure, reliable, scalable and adhere to existing privacy and data protection regulations⁵⁹. Thus, several countries have recently adopted or are about to adopt laws detailing how data collection will be limited to a certain population, for what time, and for what purpose.

On 12 May 2020, the Privacy Amendment Act (Public Health Contact Information) was introduced into the Australian Federal Parliament. Even though 60% of Australians agreed that some concessions must be made to privacy protection to fight COVID-19, the Australian government still made additional steps to protect its citizens' right to privacy during this pandemic. Overall, privacy is a key worry for nearly three out of every four Australians while nearly nine out of 10 want more control and choice over the gathering and usage of their personal data.⁶⁰ According to the Commonwealth Attorney-General Mr. Porter, the legislation introduces strong privacy protections that apply to data collected through the COVIDSafe app and is intended to facilitate the COVID-19 contact tracing efforts of the state and territory

⁵⁷ Personal Data Protection Commission in Singapore, 'PDPA Overview' <<https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act>> accessed 3 October 2020

⁵⁸ Deloitte (n 56) 5

Pichrotanak Bunthan, Jay Cohen, "What Cambodia's New Law on Electronic Commerce Means for Business", 2020 14

⁵⁹ OECD, 'Ensuring data privacy as we battle COVID-19' (n 5) 2

⁶⁰ Office of the Australian Information Commissioner, 'Australians want more control over privacy, survey shows', 2020, <https://www.oaic.gov.au/updates/news-and-media/australians-want-more-control-over-privacy-survey-shows/> accessed 4 October 2020

health authorities.⁶¹ The Minister for Health, Greg Hunt, indicated: “This legislation clearly defines the very limited circumstances in which COVIDSafe data can be collected, used or disclosed, as well as prescribing significant criminal and civil penalties for any misuse... . That includes jail terms of up to five years, or a fine of \$63,000 per offence. It is also a criminal offence under the legislation for anyone to coerce a person to use the app, to store or transfer COVIDSafe data to a country outside Australia, and to decrypt app data.”⁶²

Similar to the act in Australia, Switzerland has Article 60a paragraph 7 of the Epidemics Act of 28 September 2012 Ordinance on the Proximity Tracing System for the Sars-CoV-2 coronavirus, which regulates the details of the organization, operation and data processing of the Proximity Tracing System for the Sars-CoV-2 coronavirus (the SwissCovid app)⁶³. The main idea in this ordinance is that the explicit consent of the infected individual is obliged before any announcement is sent to app users who have possibly been exposed to the virus⁶⁴, which highlights that the processing of data is provided with respect to international data protection standards.

In the United Kingdom, in addition to the Data Protection Act 2018, the government provided the Health Protection (Coronavirus) Regulations 2020 as a supplementary legal foundation for handling data relating to COVID-19.⁶⁵ Moreover, in response to the ongoing pandemic, the UK government adopted the Coronavirus Act 2020,⁶⁶ which has indirectly created space for new data processing, in particular regard to law enforcement.⁶⁷

⁶¹ Attorney-General for Australia and Minister for Industrial Relations, ‘Privacy protections for COVIDSafe App enshrined in law’ Media release (2020) <<https://www.attorneygeneral.gov.au/media/media-releases/privacy-protections-covidsafe-app-enshrined-law>> accessed 4 October 2020

⁶² Ibid

⁶³ Ordinance on the Proximity Tracing System for the Sars-CoV-2 coronavirus of the Swiss Confederation <<https://www.admin.ch/opc/de/classified-compilation/20201730/index.html>> accessed 5 October 2020

⁶⁴ Ibid Art. 3 (2)

⁶⁵ The Health Protection (Coronavirus) Regulations 2020 of the UK <<https://perma.cc/5GJU-XYQ8>> accessed 5 October 2020

⁶⁶ Coronavirus Act 2020 of the UK, <<https://www.legislation.gov.uk/ukpga/2020/7/contents>> accessed 5 October 2020

⁶⁷ Antony Kuhn, ‘South Korea's Drive-Through Testing For Coronavirus Is Fast — And Free’ (2020) <<https://www.npr.org/sections/goatsandsoda/2020/03/13/815441078/south-koreas-drive-through-testing-for-coronavirus-is-fast-and-free?t=1605650456898>> accessed 5 October 2020

1.4. The released statements and guidelines on data privacy obligations during the COVID-19 pandemic

On April 2020, the European Data Protection Board and the Council of Europe released similar announcements outlining that the GDPR and Convention 108 do not impede procedures taken in the fight against COVID-19 but they do necessitate that emergency restraints on freedoms be proportionate and limited to the crisis period.⁶⁸ Privacy enforcement authorities (PEAs) in Argentina, Australia, Canada, Finland, France, Germany, Ireland, New Zealand, Poland, Slovakia, Switzerland and the United Kingdom have all released published general guidance for data controllers and processors with regards the application of their privacy and data protection laws during the pandemic.⁶⁹ PEAs have in general favoured a rational and contextual approach, and applied enforcement discretion noting that respect for fundamental data protection and privacy principles do not impede essential and proportionate frontline responses to COVID-19.⁷⁰

Secondly, not all countries have suitable or specific data protection laws, where data protection is given under general provisions of sectoral laws rather than those particularly centred on the “data privacy” or “data protection”.

Thirdly, not only COVID-19, but other pandemics such as the Ebola crisis showed that for responding to such a contagious outbreak, a mass assemblage of mobile data from swathes of users can raise serious worries regarding topics of privacy and data protection. Some feel that “in the data-intensive world of 2020, ubiquitous data points and digital surveillance tools can easily exacerbate those concerns.”⁷¹ In this regard, based on international experience, it is essential in the fight against a global pandemic for states to focus more on the implementation and amendment to data protection at the legislative level.

⁶⁸ The European Data Protection Board, ‘Statement on the processing of personal data in the context of the COVID-19 outbreak’

Alessandra Pierucci and Jean-Philippe Walter, ‘Joint Statement on the right to data protection in the context of the COVID-19 pandemic by the Chair of the Committee of Convention 108 and Data Protection Commissioner of the Council of Europe’, 30 March 2020

⁶⁹ OECD, ‘Ensuring data privacy as we battle COVID-19’ (2020) (n 5) 2

⁷⁰ Ibid

⁷¹ Marcello Ienca, Effy Vayena, ‘On the responsible use of digital data to tackle the COVID-19 pandemic’ (2020) Nature Medicine <<http://europepmc.org/article/MED/32284619#CR6>> accessed 5 October 2020

Lastly, data protection frameworks, thoughtful and targeted legislative efforts, like amendments in Australia, Switzerland or the related bill in the US, addressing specific data protection in combating COVID-19, provide for citizens to have complete certainty that their private data are in trustworthy hands.

2. The use of digital surveillance

2.1 Collection and use of health data

2.1.1 Legal basis of health data protection

Health data have become more and more crucial and useful for scientists and health authorities alike in trying to find answers to the latest global pandemic. However, the protection of health data may also be regarded as the starting point of data protection rules and regulations. The Hippocratic Oath requires physicians to preserve the secrecy and confidentiality of their patients' medical information.⁷² In the present context, COVID-19-related data are health data and thus qualify for special levels of protection.

In cases concerning public health crises and regardless of whether countries have already adopted data protection and privacy laws, privacy and data rights should not be abandoned, because international human rights law gives a universal framework to data protection as individual privacy rights. Therefore, various specific provisions to ensure the deserved respect for the right to privacy are merited, in accordance with article 12 of the Universal Declaration of Human Rights.

The GDPR and Convention 108 recognize health data as a “special category of data”. In compliance with the GDPR, personal data concerning health ought to comprise all data relating to the health status of a person that discloses information concerning the past, current or future physical or mental health status of the person.⁷³ According to Convention 108, the handling of health data is permissible only in cases where proper precautions are protected in the law. The GDPR is comprehensive and outlines rules that are also applicable to the handling of personal data in contexts such as those concerning COVID-19. With regard the European Board of Data

⁷² Cannataci, ‘Report of the Special Rapporteur on the right to privacy’, (2020), (n 28) 2

⁷³ Recital 35 of the GDPR

Protection (EDBP), the GDPR permits competent public health authorities and employers to handle personal data in the fight against COVID-19⁷⁴. For instance, for the sake of public interest in the sphere of public health following the circumstances indicated in Article 9(2)(i) and Article 89 of the GDPR, there is no requirement to rely on an individual's consent. To put it differently, the lawfulness of processing information without collecting consent is reasonable, and derogations from the rule of receiving consent is necessary only under the circumstances well defined under the articles of the GDPR mentioned above. The Regulation permits EU member states to “maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.”

Cognizant of the increasing application of new technologies in the handling of health-related data Recommendation CM/Rec (2019)2 of the Committee of Ministers to Member States on the protection of health-related data was adopted in 2019.⁷⁵ Therein includes a set of principles to protect health-related data combining the aspects introduced in the updated Convention 108+. Moreover, this recommendation defined that for health-related data gathered during the course of this crisis, they should be subject to the same legal protections and principles of confidentiality appropriate to any other health-related data.

In addition, in October 2019, the UN Special Rapporteur formally presented to the General Assembly the Recommendation on the protection and use of health-related data. The recommendation recognizes the sensitivity of health-related data and provides a shared international standard for minimum standards of protection for health data.⁷⁶

2.1.2 Incorrect collection and use of health data during the pandemic in some countries

In combating COVID-19, more and better data collection and processing are needed in data security, law enforcement, and medical progress⁷⁷. Below is a selection of some cases where health data were collected and used in an incorrect manner during the fight against COVID-19.

⁷⁴ The European Data Protection Board, ‘Statement on the processing of personal data in the context of the COVID-19 outbreak’ (n 68)

⁷⁵ The Committee of Ministers, ‘Recommendation CM/Rec (2019) 2 of the Committee of Ministers to member States on the protection of health-related data’ <<https://edoc.coe.int/en/international-law/7969-protection-of-health-related-data-recommendation-cmrec20192.html>> accessed 6 October 2020

⁷⁶ Joseph A. Cannataci, ‘The Protection and Use of Health-Related Data: report’ 74th session of the General Assembly of the UN 5 August 2019

⁷⁷ Determann (n 37) 244

Around the world, government authorities and private organizations have published health data to varying extents.⁷⁸ For example, in Argentina, a local newspaper released the personal information of those infected with COVID-19, thus exposing personal data.⁷⁹ This, according to Argentina's data protection legislation required consent from those whose personal information was disseminated.⁸⁰ Meanwhile, the National Health Institute of Perú created a platform on which people could refer to the health reports of patients tested for COVID-19 by simply entering their national identity details. For a period of a couple of days, the information publicly accessible. However, in Peru, legislation protecting private data requires prior, express, and unequivocal consent, where access to sensitive data such as those related to health needs consent in writing. Logically, after being subject to censure, the state bodies established a another authenticator (an SMS-based code is now necessary).⁸¹ In India, PDF files were uploaded online with sensitive personal data such as the names, addresses, and travel records of those instructed into COVID-19 quarantine. The information was accessible by the general public.⁸² Based on the Indian Information Technology Act 2000 and Information Technology Rules 2011, sensitive personal data also include medical records and history, and biometric information.⁸³

In South Korea, when a person has a positive test for COVID-19, their city or district authority might alert those living nearby about the infected person's movements before being diagnosed.⁸⁴ These alert may include the infected person's personal data including which room of a building they were in and whether they wore a mask at that time. Meanwhile, countries such as Singapore, publicize data such as the age and gender of those diagnosed, but nothing as extensive as done in South Korea.⁸⁵

⁷⁸ Access now, 'Recommendations on privacy and data protection in the fight against COVID-19' (2020) 5 <<https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf>> accessed 5 October 2020

⁷⁹ La Nación, 'Quiénes son y de dónde vinieron los 21 infectados por coronavirus en la Argentina' (2020), <https://www.lanacion.com.ar/sociedad/quienes-son-17-infectados-coronavirus-argentina-nid2341456>> accessed 5 October 2020

⁸⁰ Personal Data Protection Act, Act No. 25.326 of 2000 of Argentina

⁸¹ Access now, 'Recommendations on privacy and data protection in the fight against COVID-19' (n 73) 5

⁸² Ibid 5

⁸³ Section 43A of the Information Technology Act 2000 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011

⁸⁴ Mark Zastrow, 'South Korea is reporting intimate details of COVID-19 cases: has it helped?' (2020) Journal "Nature" <<https://www.nature.com/articles/d41586-020-00740-y>> accessed 5 October 2020

⁸⁵ Ibid

But the specificity of the use and collection of health data has raised privacy concerns. The Chair of the National Human Rights Commission of Korea, Choi Young-ae, also voiced unease that the “excessive disclosure of private information” could encourage people showing symptoms to avoid testing.⁸⁶ The data might be useful for epidemiologists, and publishing them justifies the risk of subjecting people to social stigma says Maimuna Majumder, a computational epidemiologist at Boston Children’s Hospital in Massachusetts. This is likely to affect the quality of life of those affected and can also cause additional health conditions, such as a variety of psychosomatic symptoms.⁸⁷

Based on the aforementioned practice in various countries, accountability must be ensured via the scrutinizing of data processing activities by assigned authorities permitted to employ sanctions in cases of indiscretions.

2.1.3 Main measures protecting the processing of health data

Health-related privacy principles must be automatically respected,⁸⁸ which can be achieved using special measures. Around the world, healthcare providers and researchers rely primarily on the following three measures to protect patient privacy in the processing of health data:

- limitation of the use of health information to what is necessary to treat patients;
- obtainment of consent from the patient to secondary or unusual data usages;
- redact or aggregate information in order that the individual cannot be identified or associated with the data.⁸⁹

The collection, use, and other types of health processing of data should be restricted to what is absolutely necessary to combat COVID-19. In other words, a pandemic does not give free rein to gather extensive and unnecessary data. It should be done to identify the bare minimum of personal data that is required to fulfil a public good or public health purposes. This is one of the main principles concerning data standards (embedded in Convention 108+, OECD Guidelines, GDPR), along with accuracy and storage limitations. Data minimization

⁸⁶ Ibid

⁸⁷ Michael Koller et al., Symptom Reporting in Cancer Patients: The Role of Negative Affect and Experienced Social Stigma 77 CANCER 983, 994 (1996).

⁸⁸ Cannataci, ‘The Protection and Use of Health-Related Data: report’ (n 76)

⁸⁹ Determann (n 37) 244

Naya Sethi, Graeme T. Laurie, ‘Delivering Proportionate Governance in the Era of eHealth: Making Linkage and Privacy Work Together’ 13 MED. LAW INT. 168 (2013)

necessitates that personal data be sufficient, relevant, and restricted to what is required to achieve the given purpose.

Given that the GDPR is one of the main go-to documents for many countries when deciding upon data protection legislation, it is essential to mention that Articles 6(1)(a) and 7 of the GDPR set high standards in this regard and demands consent. The processing of health data is prohibited unless the data subject has given their express consent for one or more specified purposes.⁹⁰ It requires the consent to be narrow and specific even though Recital 33 of the GDPR acknowledges that this might not be possible in medical research and a broader form of consent may be required, creating uncertainty in practice.⁹¹ However, as recommended by the UN Special Rapporteur, everyone should to have right to retract their consent to the data processing at any time and be told that any such withdrawal will not affect the legality of any data processing already done on the basis of their consent prior to any withdrawal thereof.⁹²

As regards the third measure, the use of pseudonymization has been applied by the EU. The anonymization way to use data is by “remov[ing] identifying information from (something, such as computer data) so that the original source cannot be known.”⁹³ In the GDPR, the concept of “anonymization” is not used or defined. Article 4 of the GDPR only defines pseudonymization as “the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.”⁹⁴

Similarly, the CCPA in the US does not use the term “anonymization” but rather used the terms “deidentification” and “aggregation”.⁹⁵ Meanwhile, in South Korea, amendments, which were passed to the Personal Information Protection Act (PIPA) on 9 January 2020 by the Korean National Assembly and differentiate between ‘personal data’, ‘pseudonymised data’, and

⁹⁰ GDPR Art. 6 (1) (a) and Art. 9 (2) (a)

⁹¹ David Townend, ‘Conclusion: Harmonization in Genomic and Health Data Sharing for Research: An Impossible Dream?’ 137 Hum. Genetics, 657 661 (2018).

⁹² Cannataci, ‘The Protection and Use of Health-Related Data: report’ (n 76)

⁹³ Merriam-Webster Dictionary, Anonymize <<https://www.merriam-webster.com/dictionary/anonymize>> accessed 5 October

⁹⁴ Council Regulation 2016/679, Art. 4, 2016 O.J. (L 119/33-35)

⁹⁵ California Consumer Privacy Act (CCPA), CAL. CIV. CODE § 1798.140(o), (h) (West 2020)

‘anonymised data’ but eliminate ‘anonymised data’ from the range of personal data also highlight some of the challenges to personalizing anonymised data.⁹⁶

One of the amendments aims is to develop a ‘data economy’ by establishing the notion of ‘pseudonymised data’ and the legal foundation on which data may be applied in a more flexible manner to an extent satisfactorily associated with the original purposes of collection.⁹⁷ Pseudonymised data could also be processed without gaining consent if, on the whole, the intention of the usage concerns preparing statistics, research, and keeping public records.

The downsides of anonymization apply, to a lesser extent, to pseudonymization as it uses similar techniques, and because the goal is to somewhat loosen the link between the data and their subject. Pseudonymization should be considered as a data protection measure but it does not completely avoid restrictions under data protection or data privacy law.⁹⁸

The legitimacy of collecting, processing, sharing and using data relating to health is not gained from the access to the data, but rather from the faith in whomever possesses them, treats them, and operates with them within the boundaries of the law. From this perspective, the use of health data in the fight against the current and next pandemics must be governed by strict measures of protection, beginning with the collection of data, and expanding towards the processing of operations and the use of data.

2.2 The use of Contact Tracing Apps (CTA) in the fight against a global pandemic

2.2.1 Main advantages and concerns of using CTA

Digital surveillance has performed an important part in controlling the COVID-19 outbreak in China, Singapore, Israel, and South Korea.⁹⁹ The current COVID-19 pandemic has revealed that governments now turn to technological measures in times of crisis such as digital contact tracing, which pose challenges to data protection. Contact tracing is a well-established method

⁹⁶ Chris H. Kang, Sun Hee Kim, Doil Son, ‘Korea introduces major amendments to data privacy laws’, 2020, <<https://www.lexology.com/library/detail.aspx?g=223051e2-0346-4935-8fbb-6146e4424d94>>, 6 October 2020

⁹⁷ Ibid

⁹⁸ Determann (n 37) 251

⁹⁹ Euronews, ‘Coronavirus conundrum: COVID-19 tracking apps that don’t breach privacy’ television broadcast (2020) <<https://www.euronews.com/video/2020/04/10/coronavirus-conundrum-covid-19-tracking-apps-that-don-t-breach-privacy>> accessed 6 October 2020

of discovering who may have been exposed to a disease by asking someone diagnosed who else they may have had contact with recently. The digital and traditional approach work in essentially the same manner, but rather than health professionals asking questions, the person's mobile phone retains an anonymized record of those you have had any contact with¹⁰⁰ or by tracing your location, using a dedicated app. Many countries currently implement CTA to facilitate the fight against COVID-19. Using such measures brings advantages and thus governments to implement these digital technologies. First of all, it can help in the modelling of the spatial spread of viruses. More precise spread types of viruses could significantly improve the population-level outcomes of interventions implemented to combat the spread of infectious diseases.¹⁰¹ In other words, it can help to highlight the largest foci of possible infection.

Secondly, CTA can even help to focus on predictions and risks. Supported by the experiences of the spread of cholera, significant headway has been achieved in forecasting the geographical development of epidemics after outbreaks have grown beyond a tiny preliminary cluster of cases.¹⁰² The data obtained assist experts to make more differentiated predictions and short-term forecasts about the extent of the infection.¹⁰³ Furthermore, this is crucial for policymakers because it makes both current and future measures verifiable and improves the assessment of their effectiveness.¹⁰⁴

Thirdly, contact tracing is a system which monitors the movement of people location to decrease the further transmissions of viruses and traces back to those who may have been in contact with a person infected.¹⁰⁵ Overall, the aim of such apps is to limit the circulation of the virus quickly and efficiently.

¹⁰⁰ Katie Collins, 'The COVID-19 contact-tracing apps we were promised are finally here' 2020 <<https://www.cnet.com/news/the-covid-19-contact-tracing-apps-we-were-promised-are-finally-here/>> accessed 6 October 2020

¹⁰¹ Linus Bengtsson, Jean Gaudart, Xin Lu, Sandra Moore, Erik Wetter, Kankoe Sallah, Stanislas Rebaudet & Renaud Piarroux, 'Using Mobile Phone Data to Predict the Spatial Spread of Cholera' (2015) *Scientific Report* 1

¹⁰² *Ibid*

¹⁰³ Jason Chumtong, 'Phone tracking against COVID-19 Using digital technology against an analogue virus', Konrad Adenauer Stiftung (2020) *JSTOR* 5

¹⁰⁴ *Ibid*

¹⁰⁵ Emanuella Ventrella, 'Privacy in emergency circumstances: data protection and the COVID-19 pandemic' *ERA Forum* (2020) 383

However, the use of CTA has sparked some concerns. First of all, during a crisis, trust becomes particularly crucial. In the fight against COVID-19, people must have even higher levels of trust in institutions (e.g., federal government, technology companies) that work toward finding a way out from the pandemic. When considering CTA, this requires significant buy-in to be effective. For instance, if people's trust is low in the entity creating and distributing such an app then they are less likely to use it.¹⁰⁶ Secondly, CTA intends to assist in the reduction in the spread of COVID-19 in order for normalization life of population their everyday life. For example, in Australia, this notion hinges on how many Australians download and apply the app, as the lowest required uptake is projected at 40-60% of the population.¹⁰⁷

2.2.2 Decentralised and centralised technological approaches of CTA

Nowadays, there is a variety of CTA and technological methods used around the world to combat the COVID-19 crisis. For example, China, Singapore, and South Korea are now held up as good examples worldwide for their successes in controlling the spread of the virus,¹⁰⁸ while European CTA assert to centre users' privacy and security in their design.¹⁰⁹ Some CTA are developed based on geolocation, such as Coronamadrid and StopCovid19 in Spain, while others are premised on Bluetooth technology or better known as a "digital handshake", such as the Stop Corona app in Austria, StopCovid in France, and ProteGo in Poland.¹¹⁰ Today, digital contact tracing has the following two primary approaches¹¹¹:

¹⁰⁶ Eszter Hargittai, Ellissa Redmiles, Jessica Vitak, Mochaël Zimmer 'Americans' willingness to adopt a Covid-19 tracking app: The role of app distributor' (2020) <<https://firstmonday.org/ojs/index.php/fm/article/view/11095/9985>> accessed 8 October 2020

¹⁰⁷ Simon J Dennis, '70% of people surveyed said they'd download a coronavirus app. Only 44% did. Why the gap?' (2020) <<https://theconversation.com/70-of-people-surveyed-said-theyd-download-a-coronavirus-app-only-44-did-why-the-gap-138427>> accessed 8 October 2020

¹⁰⁸ Justin McCurry, 'Test, trace, contain: how South Korea flattened its coronavirus curve' the Guardian (2020) <<https://www.theguardian.com/world/2020/apr/23/test-trace-contain-how-south-korea-flattened-its-coronavirus-curve>> accessed 6 October 2020

Phillippe Mesmer, 'Endiguer le coronavirus : Singapour et la Corée du Sud, des exemples à suivre', L'Express (2020) <https://www.lexpress.fr/actualite/monde/asie/endiguer-le-coronavirus-singapour-et-la-coree-du-sud-des-exemples-a-suivre_2121024.html> accessed 6 October 2020

¹⁰⁹ Aida Ponce Del Castillo, 'COVID-19 contact-tracing apps: how to prevent privacy from becoming the next victim', (2020), European Economic Employment and Social Policy N°5/2020, 2 <<https://www.etui.org/sites/default/files/2020-06/Covid-19%2Bcontact-tracing%2Bapps%2BCorona%2BPonce%2BPolicy%2BBrief%2B2020.05.pdf>> accessed 7 October 2020

¹¹⁰ Laura R. Bradford, Aboy Mateo, Liddell Kathleen, 'COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR and Data Protection Regimes' Journal of Law and the Biosciences (2020) University of Cambridge Faculty of Law Research Paper No. 23/2020 2

¹¹¹ Patrick Howell O'Neill, Tate Ryan-Mosley, Bobbie Johnson, 'A flood of coronavirus apps are tracking us Now it's time to keep track of them' MIT Technology Review (2020) <<https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker>> accessed 7 October 2020

1. a centralized approach that works through cell-phone location data or Bluetooth-based data¹¹² and applies anonymized location data shared by telecommunications companies to examine crowd movements.
2. a decentralized approach that works through Bluetooth-based data¹¹³ through CTA to quicken the process of identifying those infected individuals.¹¹⁴

Decentralized CTA have been called “privacy-preserving”. In this regard, EU states and researchers have supported the Pan-European Privacy-Preserving Proximity Tracing (PEPPPT).¹¹⁵ The PEPP-PT system protects privacy by total anonymization and by performing without central data storage.¹¹⁶ PEPP-PT does not use sensitive location data, and shifts the responsibility for notification to the citizen, who can act anonymously.¹¹⁷ The alliance proposes the application of matching Bluetooth signals, premised on the TraceTogether app developed and applied in Singapore.¹¹⁸ These MCTA would then utilize “a record of anonymous principal codes exchanged between phones” to determine which other individuals, who had the app installed or active, had been in proximity with infected people during the contagious period.¹¹⁹ However, Singapore’s Trace Together collects all data from individual devices in a national-government database.¹²⁰ This means that the app also has a centralized approach. Centralized digital CTA diverge from decentralized apps in relying on a central database or central authority for the contact-tracing data and process.¹²¹ Thus, the privacy of users of centralized CTA depends on the trustworthiness of the central authority.

¹¹² Li Tiffany, ‘Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis’ (2020) Loyola University Chicago Law Journal Volume 52 Issue 3 61

¹¹³ Ibid 61

¹¹⁴ Kladia Klonowska, ‘The COVID-19 Pandemic: Two Waves of Technological Responses in the European Union’ (2020) The Hague Centre for Strategic Studies 2

¹¹⁵ Tiffany (n 112) 66

¹¹⁶ EU Commission Recommendation 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data, <<https://op.europa.eu/en/publication-detail/-/publication/1e8b1520-7e0c-11ea-aea8-01aa75ed71a1/language-en>>, accessed 7 October 2020

¹¹⁷ Chumtong (n 103)

¹¹⁸ Klonowska (n 114) 8

¹¹⁹ Kylie Foy, ‘Bluetooth signals from your smartphone could automate Covid-19 contact tracing while preserving privacy’ (2020) MIT News <<https://news.mit.edu/2020/bluetooth-covid-19-contact-tracing-0409>> accessed 7 October 2020

¹²⁰ Baobao Zhang et al., Americans’ Perceptions of Privacy and Surveillance in the COVID-19 Pandemic OSF PREPRINTS (2020) osf.io/9wz3y

¹²¹ Tiffany (n 112) 68

The EDPB notes that data on location taken from automated or electronic communication providers can solely be handled within the limits of articles 6, 9 of the ePrivacy Directive.¹²² Given that such data can be passed over to organizations or other third parties if the provider has anonymized them,¹²³ it has been reported that data on anonymized phone location are utilized by the governments of Belgium, Austria, Estonia, France, Germany, Latvia, Greece, Portugal, Italy, and Spain.¹²⁴ Telecom providers guarantee that shared location data are anonymized and aggregated.¹²⁵ Thus, the anonymization of telecom data means that their handling and sharing is considered lawful under EU law without the express consent of users.¹²⁶ However, at the same time, the EDPB has made it clear that location data had to be anonymized may, in fact, not be. Mobility traces of people are inherently highly correlated and individual. Therefore, they can be vulnerable to re-identification attempts under certain circumstances.¹²⁷ Moreover, research has recently shown that various techniques exist that can re-identify individuals using apparently anonymous information.¹²⁸ On top of that, as such new technologies are being developed on a daily basis means that users cannot feel fully confident that data shared ‘anonymously’ will not be linked back to them in the future.¹²⁹ Furthermore, a Bluetooth-based decentralized app would infer proximity through anonymous key exchange device-to-device; but a Bluetooth-based centralized CTA could infer proximity through keys stored on a central database, with data collected from each device and results pushed back to devices.¹³⁰ According to some critics, the main problem with this concept is that the data gathered are centrally kept and that anyone with authorization to the data could, with sufficient

¹²² Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

¹²³ Guidelines 03/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the COVID-19 Outbreak Adopted on 21 April 2020’ (European Data Protection Board 2020)

¹²⁴ Klonowska (n 114) 3

¹²⁵ ‘Vodafone Group’s Five-Point Plan to Help Counter the Impact of COVID-19’ <<https://www.vodafone.com/news-and-media/vodafone-group-releases/news/vodafone-launches-five-point-plan-to-help-counter-the-impacts-of-the-covid-19-outbreak>> accessed 8 October 2020

¹²⁶ Klonowska (n 114) 3

¹²⁷ Guidelines 03/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the COVID-19 Outbreak Adopted on 21 April 2020’ (n 120)

¹²⁸ Bradford (n 110) 6

Yves-Alexandre de Montjoye and others ‘Evaluating COVID-19 contact tracing apps? Here are 8 privacy questions we think you should ask’ Computational Privacy Group (2020) <<https://cpg.doc.ic.ac.uk/blog/evaluating-contact-tracing-apps-here-are-8-privacy-questions-we-think-you-should-ask/>> accessed 8 October 2020

¹²⁹ Bradford (n 110) 6

¹³⁰ Tiffany (n 112) 39

will and technical know-how, deanonymize the data.¹³¹ However, some have argued that centralized contact-tracing apps may be more secure or privacy-protective, in that one central source stores all private information, making it potentially easier to govern the flows of data.¹³² However, this brings up the question of trust.

2.2.3 Data protection in the use of CTA

As COVID-19 shows no immediate end in sight, there is continual and heightening pressure to adopt MCTA, and entrust the technology developers and government organizations to weigh individual privacy with the requirement to safeguard public health effectively.¹³³ Companies that design and make applications and services used to coping with or responding to the COVID-19 pandemic must offer users data protection rights and adhere to data protection principles. The 8 data protection principles derive primarily from international standards, concretely Convention 108+ and the OECD guidelines as outlined earlier. Six out of the eight protection principles outlined above are contained in the GDPR¹³⁴. The efficient systematization of these principles involves the evolution package rights of users, a legal foundation for data processing, data security measures, oversight mechanisms, obligations for entities processing data, and procedures allowing the send data to other countries. These data protection principles are regarded as “minimum standards” to protect basic rights by controllers that have signed up to worldwide data protection frameworks. The GDPR describes a data controller as a “natural and legal person, public authority, agency or other body which, alone or jointly, with others, determines the purposes and means of the processing of personal data”.¹³⁵ The concept of a 'data controller' is not utilised under the Singapore Personal Data Protection Act (PDPA). However, the broader term 'organisations' is used when defining entities that are subject to the obligations of the PDPA. 'Organisation' is defined in the PDPA as “any individual, company, association or body of persons, corporate or unincorporated, whether or not formed or recognised under the law of Singapore; or resident, or having an office or a location of business, in Singapore”.¹³⁶ In the context of MCTA, the controller can

¹³¹ Michael Baxter, ‘Centralised versus decentralised contact tracing solutions pit privacy academics against each other’ (2020) PrivSec Report <<https://gdpr.report/news/2020/04/22/centralised-versus-decentralised-contact-tracing-solutions-pit-privacy-academics-against-each-other/>> accessed 7 October 2020

¹³² Tiffany (n 112) 39

¹³³ Hargittai, Redmiles, Vitak, Zimmer (106)

¹³⁴ The GDPR, Art.5

¹³⁵ The GDPR, Art. 4(7).

¹³⁶ The Singapore Personal Data Protection Regulations 2014 Sections 2(1) 4

create a potential vulnerability. For example, location data can be highly informative and can reveal the user's home address, visited places, etc. In the growing COVID-data industry, those data can pass on people's health data to insurance companies, hospitals or marketing agencies. Thus, to increase enough trust to download such CTA, it is advisable to make the controller a national health authority for processing data, as was also preferred by the EDPB.¹³⁷ In any case, if the deployment of CTA consists of various actors, their roles must be plainly set out from the start and explained to the users accordingly. This can be seen from experience in Switzerland, where the Federal Office of Public Health was appointed as the controller by the relevant ordinance.¹³⁸ Though, in case of Singapore, the PDPA does not apply to any public agencies or organizations acting on behalf of a public agency,¹³⁹ as that can also cause risks in cases when there are "data leaks".

The main issue in the context of using CTA is the grave intrusion into people's privacy because such surveillance provides systematic and largescale monitoring of locations and contacts between natural persons. In order not to infringe upon the right to privacy as protected in the Universal Declaration of Human Rights,¹⁴⁰ trusting the voluntary implementation by users of CTA appears the only legitimate way. For example, in accordance with Article 6(1) of the GDPR if considering the EU, the processing shall be lawful if "the data subject has given consent to the processing of his or her personal data for one or more specific purposes." Another example is the latest Australian Privacy Amendment Act, which also requires consent to upload the COVIDSafe app. However, some countries around the world made downloading CTA mandatory for millions of people. For example, in India¹⁴¹ it was reported that those who failed to download the app were faced with a fine or imprisonment.¹⁴² Meanwhile, data privacy law in South Korea has developed swiftly, and now has exceedingly stringent consent requirements. However, PIPA¹⁴³ permits the reasonable use of personal data without consent

¹³⁷ Guidelines of the European Board Data Protection 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak adopted on 21 April 2020

¹³⁸ Ordinance on the Proximity Tracing System for the Sars-CoV-2 coronavirus of the Swiss Confederation <<https://www.admin.ch/opc/de/classified-compilation/20201730/index.html>> accessed 5 October 2020

¹³⁹ The Singapore Personal Data Protection Regulations 2014 Sections 2(1) 4

¹⁴⁰ The Universal Declaration on human Rights, Art. 12

¹⁴¹ Cannataci, 'Report of the Special Rapporteur on the right to privacy' (n 28) 16

¹⁴² Patrick Howell O'Neil, 'India is forcing people to use its covid app, unlike any other democracy' (2020), <https://www.technologyreview.com/2020/05/07/1001360/india-aarogya-setu-covid-app-mandatory/>> accessed 9 October 2020

¹⁴³ Press Release of Ministry of Public Administration and Security e-Government Bureau Privacy Policy Division of the South Korea, 'Personal information protection law amendment passed the National Assembly' (2020) <<https://eiec.kdi.re.kr/main.do4>> accessed 10 October 2020

that can be used “within a scope that is reasonably related to the original purpose of collection” and “after considering whether the data subject’s rights would be infringed upon and/or measures to secure the integrity of the personal information have been appropriately taken.” The revised PIPA relaxes the existing regulations so that the subject of personal information is reasonably associated to the objective of the collection. It is understood to present the possibility of the use of data without consent.¹⁴⁴

In spring 2020, China released a revised edition of the Information Security Technology – Personal Information Security Specification. In this document, the controller has to get the data subject’s express consent so as to gather and process their personal data for each specific purpose.¹⁴⁵ However, in practice, unlike in Europe which boasts some of the most protective privacy laws around the world relating to personal data, in China citizens are also mandated to use CTA otherwise they are not permitted to depart their residential compounds or spend time in public places.¹⁴⁶ Meaning that people in China are forced to install the app on their phones and disclose their personal information and location-related data via a smartphone app. Moreover, in some cities like Shanghai, facial data are also needed.¹⁴⁷ Users of CTA will then get direct feedback on whether they might have been in contact with infected people. In China, this is managed via the Chinese Health Code App, which was created and designed in collaboration with the country’s corporate powerhouse Alibaba.¹⁴⁸

In China’s case, such an approach is possible as large-scale data infrastructure already exists. What is curious is the role of Alibaba, China’s answer to Amazon, in China’s extensive digitization strategy.¹⁴⁹ In China, many have been concerned about the potential justifications used for privacy invasion, and the transferred accountability and responsibility from the state

¹⁴⁴ Lawtimes, ‘Personal information protection law amendment passed the National Assembly’ (2020) <<https://m.lawtimes.co.kr/Content/Article?serial=158894>>, accessed 6 October 2020

¹⁴⁵ Nick Beckett and Amanda Ge, ‘China publishes new specification on personal data security’ (2020) <https://www.cms-lawnow.com/ealerts/2020/03/china-publishes-new-specification-on-personal-data-security?cc_lang=en>, accessed 10 October 2020

¹⁴⁶ Nectar Gan, David Culver, ‘China is fighting the coronavirus with a digital QR code. Here’s how it works’ CNN Business (2020) <<https://edition.cnn.com/2020/04/15/asia/china-coronavirus-qr-code-intl-hnk/index.html>> accessed 11 October 2020

¹⁴⁷ Liu, Chuncheng, ‘Algorithms in Action: Reassembling Contact Tracing and Risk Assessment during the COVID-19 Pandemic in China’ (2020) 7

¹⁴⁸ Aaron Holmes, ‘China is reportedly making people download an Alibaba-backed app that decides whether they’ll be quarantined for coronavirus’ Business Insider, 2020 <<https://www.businessinsider.com/alibaba-coronavirus-chinese-app-quarantine-color-code-2020-3?r=DE&IR=T>> accessed 12 October 2020

¹⁴⁹ Ibid

to individuals.¹⁵⁰ While, in Europe, the debate mostly focused on the selection of approach (centralized or decentralized) for digital CTA, which concern questions of data transmission and the data recipient, in China questions have been raised about the consequences of technical issues and long-term societal implications of apps used to regulate movement for the sake of disease prevention. In support of this, Alipay and WeChat, both of which have accommodated the Health Code app to track COVID-19 exposure, have the right to keep the data once the crisis is over.¹⁵¹ This clearly breaches the principles of purpose limitation and data minimization of the data protection.

Data minimization is linked with storage limitation that defines a proportionate period data are kept. Different data and security guidelines around the world during COVID-19 loosely agree that this period should be as long as necessary to realize the underlying purpose.¹⁵² However, once the pandemic is over, personal data must be deleted.

Similarly, the GDPR clearly spells out that data should be gathered purely for specific, explicit and legitimate purposes¹⁵³ and kept for a period no longer than is required for the purposes for which the personal data are handled.¹⁵⁴ In other words, the purpose in the current situation is to curb or end the spread of COVID-19. Thus, data collection cannot continue to be processed in a fashion that is contradictory for this specific goal.

China is not the only country in which the principle of storage limitation has been violated. In Poland, the government has created a quarantine enforcement app with data retention of up to six years.¹⁵⁵ As it was recommended by the Special Rapporteur on the right to privacy, even when installing the application is “voluntary”, compulsory data entry varies and it is crucial to assess the extent of data protection by ensuring that only necessary information is captured by

¹⁵⁰ Liu (n 147)

¹⁵¹ Remarks of Ruipeng Lei, ‘Beyond the Exit Strategy: ethical uses of data-driven technology in the fight against COVID-19’ Huazhong University of Science and Technology, Wuhan, China, Nuffield Council on Bioethics and Ada Lovelace Institute webinar (2020) <<https://www.nuffieldbioethics.org/publications/covid-19/webinar-beyond-the-exit-strategy-ethical-uses-of-data-driven-technology-in-the-fight-against-covid-19>> accessed 12 October 2020

¹⁵² International Data Protection Guidelines on Coronavirus/COVID-19 <<https://www.jonesday.com/-/media/files/publications/2020/04/covid19-cybersecurity/global-dpas-guidelines-on-coronavirus.pdf?la=en&hash=CBD0BBF9DDA4C329A088037F4B6BE109>> accessed 13 October 2020

¹⁵³ GDPR, Art. 5(1)(b)

¹⁵⁴ GDPR, Art. 5(1)(e)

¹⁵⁵ Mark Scott, Zosia Wanat, ‘Poland’s coronavirus app offers playbook for other governments’ (2020) POLITICO <<https://www.politico.eu/article/poland-coronavirus-app-offers-playbook-for-other-governments/>> accessed 14 October 2020

the application, storage of the data respects international data protection standards, and such storage is limited in time and used only for the right reasons.¹⁵⁶

The fight against the pandemic and any assistance in decelerating the spread of COVID-19 is in the public interest. Article 6 of the GDPR allows for a total of six lawful bases to process personal data legally. In this case, the EDPB notes that “the mere fact that the use of the contact tracing takes place on a voluntary basis, does not mean that the processing of personal data by public authorities necessarily be based on the consent. When public authorities provide a service, supported a mandate assigned by and in line with requirements laid down in law, it appears that foremost relevant legal basis for the processing is the necessity for the performance of a task for public interest during this case besides consent we can resort to public interest”. Further, the GDPR specifies that the basis regarding public interest has to be formed by EU law or the law of its member state.¹⁵⁷

Though the data can be used for an altruistic purpose, and of course, there may be good reason to provide data (e.g., for medical research), an understanding is required to safeguard data in a manner that is achievable and advantageous to society as a whole. Nowadays, data protection breaches when using such platforms cause untrust to governments, institutions and organizations. Therefore, taking into account the general public’s heightened understanding of their data privacy rights, authorities should take greater care in clamping down on those who fail to adhere to data protection laws and regulations. It is thus essential that processors, controllers and developers regard compliance with the utmost care; and only then can it diminish regulatory risk and preserve general public trust in tracing apps.

2.3. The Use of Face Recognition Technology and Drones

As the current pandemic affects and alters societies across the world, governments and business turn to new applications of digital technology to reduce the spread of the virus and keep economic opportunities alive. Technologies that once may have appeared like those out of science fiction novels – such as facial recognition, thermal facial recognition, or the use of drones – are now not only possible but also already in use. While digital surveillance

¹⁵⁶ Cannataci, ‘Report of the Special Rapporteur on the right to privacy’, (n 28) 2

¹⁵⁷ GDPR, Art. 6(3)

technologies may prove valuable in decelerating the spread of COVID-19, crucial questions on the potential privacy implications of the pervasive gathering and application of such personal data are duly raised.¹⁵⁸

2.3.1 Facial recognition technology (FRT) in the context of COVID-19

Facial recognition technology (FRT) automatically identifies a person by pairing two or more faces from a vast collection of digital images. It does so by identifying and evaluating different facial characteristics, extracting them from the picture and assessing them with elements taken from other faces.¹⁵⁹

The use of facial recognition surveillance cameras once lockdown has been moderated has been used to determine whether citizens have adhered to social distancing rules and the wearing of masks.¹⁶⁰ This has triggered a passionate dispute of the issue which would be influence on fundamental rights and data protection. For example, it was no secret that the Chinese authorities used such surveillance techniques on a large scale before the pandemic, which had already aroused heated discussions and concerns about potential human rights breaches.¹⁶¹

2.3.2 Chinese approach to FRT

FRT was rolled out in China to identify high temperatures in a crowded place or to flag citizens who fail to adhere to wearing a face mask.¹⁶² As mentioned by Vice President of the Chinese company Hanwang Huang Lei, it can gauge body temperature while at the same time

¹⁵⁸ Meredith Van Natta, Paul Chen, Savannah Herbek, Rishabh Jain, Nicole Kastelic, Evan Katz, Micalyn Struble, Vineel Vanam, Niharika Vattikonda, 'The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic', *Journal of Law and the Biosciences* Volume 7 Issue 1 2020, 1

¹⁵⁹ The European Union Agency for Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (2019) 2 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf> accessed 13 October 2020

¹⁶⁰ Clare Sellars, 'The use of facial recognition technology to combat COVID-19' (2020), <<https://ropesgrayinsights.passle.net/post/102g6qx/the-use-of-facial-recognition-technology-to-combat-covid-19>> accessed 13 October 2020

¹⁶¹ Xinmei Shen, 'Facial recognition data leaks are rampant in China as Covid-19 pushes wider use of the technology' (2020) <<https://www.scmp.com/abacus/tech/article/3104512/facial-recognition-data-leaks-rampant-across-china-covid-19-pushes>>, accessed 13 October 2020

¹⁶² Lily Kuo, 'The new normal': China's excessive coronavirus public monitoring could be here to stay', (2020), *The Guardian* <<https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay>> accessed 12 October 2020

pinpointing the person's identity in a throng of up to 30 people "within a second"¹⁶³, after which the system processes the result if it discovers a temperature more than 38 degrees. Moreover, FRT recognizes people wearing a mask at an accuracy rate of about 95%, ensuring that the majority can be identified, and the success rate of recognition for those not wearing a mask is just over 99%.¹⁶⁴

Additionally, Chinese start-up company Rokid established a biotechnological system that contains special glasses which can recognise body temperature, which may be combined with facial recognition technology, and used as an infrared sensor to detect the temperatures of up to 200 people from a distance of about three meters. This software is already being used in China by national authorities in public places like parks and schools.¹⁶⁵

This not only underlines China's technological improvements in the fight against COVID-19, but it also intensifies the increasing fears of citizens¹⁶⁶ concerning the pervasive application of facial recognition that jeopardizes their privacy.¹⁶⁷ Personal data leaks concerning facial recognition are commonplace, and China has a poor record in protecting biometric data.¹⁶⁸ Technical staff have often lack of time or the education required to develop a viable system or to avoid careless lapses.¹⁶⁹ On the whole, legislative in China concerning FRT has pursued a pragmatic 'learn from doing' method¹⁷⁰. Thus, legal protections for personal data are limited in China.

A broader data protection framework concerning facial recognition in China is the Cybersecurity Law of the People's Republic of China. This law outlines legal obligations on network operators by listing needs for collecting, using, and protecting personally identifiable

¹⁶³ Martin Pollard, 'Even mask-wearers can be ID'd, China facial recognition firm says' (2020) <<https://uk.reuters.com/article/us-health-coronavirus-facial-recognition/even-mask-wearers-can-be-idd-china-facial-recognition-firm-says-idUKKBN20W0WL>> accessed 15 October 2020

¹⁶⁴ Ibid

¹⁶⁵ Van Natta and others (n 158) 5

¹⁶⁶ Laurie Chen, 'China wakes up to wide web of online data leaks and privacy concerns' (2020) South China Morning Post <<https://www.scmp.com/news/china/society/article/3047186/china-wakes-wide-web-online-data-leaks-and-privacy-concerns>> accessed 13 October 2020

¹⁶⁷ Seungha Lee, 'Coming into Focus: China's Facial Recognition Regulations' (2020), Centre for Strategic and International Studies <<https://www.csis.org/blogs/trustee-china-hand/coming-focus-chinas-facial-recognition-regulations>> accessed 6 October 2020

¹⁶⁸ Xinmei Shen, 'China ranks as the worst country at collecting, using and storing biometric data' (2020) <<https://www.scmp.com/abacus/tech/article/3040841/china-ranks-worst-country-collecting-using-and-storing-biometric-data>> accessed 14 October 2020

¹⁶⁹ Ibid

¹⁷⁰ Ibid

information (PII) that also incorporates biometric data.¹⁷¹ In addition, China has regulations on data processing and protection in place, namely Personal Information Security Specification (PISS). This guideline is dedicated to prevent PII from illegal collection, abuse, and access. However, at present China is without a standardized legal framework or a clear-cut definition of personal information.

In accordance with PISS, the processing of PII must be legal, justified, necessary, and for specific purposes, that often requires consent, and must be kept safe and protected.¹⁷² In March 2020, China issued the latest version of PISS. Notably, the updated version is aimed at strengthening privacy protection and modifies exceptions to seeking consent and refinements for personal biometric information.¹⁷³

Furthermore, a new regulation is expected in the Chinese city of Hangzhou, prohibiting mandatory facial recognition. The regulation has a draft status so far, however once adopted, it will be the first local regulation in China that clearly would forbid to force people to enter their residential address using biometric information such as face recognition or fingerprints.¹⁷⁴

The Director-General of the WHO has intimated that method in China to the COVID-19 pandemic could become the standard of care for pandemics around the world. However, as impressive as the Chinese approach might be to many, it is unlikely to be replicated across the board.¹⁷⁵ For instance, the EU has political, legal, and technological restrictions that prevent the application of similar measures. Such restrictions or limitations do not exist in China.¹⁷⁶

¹⁷¹ Translation ‘Cybersecurity Law of the People’s Republic of China’ “New America” <<https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/>> accessed 15 October 2020

¹⁷² Translation ‘The Personal Information Security Specification’ Art. 4(b), <<https://web.archive.org/web/20201124083428/https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf>> accessed 15 October 2020

¹⁷³ Lester Ross, Kenneth Zhou, Ting ting Liu, ‘China Issues New Personal Information Security Specification’ (2020) WilmerHale <<https://www.wilmerhale.com/en/insights/client-alerts/20200324-china-issues-new-personal-information-security-specification>> accessed 15 October 2020

¹⁷⁴ This new regulation was submitted to the 30th meeting of the Standing Committee of the 13th Hangzhou Municipal People’s Congress for deliberation on 26 October 2020 China Money Ai, ‘Hangzhou City Proposes Laws Prohibiting Mandatory Facial Recognition’ China Money Network <<https://www.chinamoneynetwork.com/2020/10/29/hangzhou-city-proposes-laws-prohibiting-mandatory-facial-recognition>> accessed 17 October 2020

¹⁷⁵ Vera Lúcia Raposo, ‘Can China’s ‘Standard of Care’ for COVID-19 be Replicated in Europe?’ (2020) Journal of Medical Ethics <<https://ssrn.com/abstract=3706028>>, accessed 10 October 2020

¹⁷⁶ Ibid

Meanwhile, FRT may be embraced more favourably in other areas of the world, such as in several Asian countries.¹⁷⁷

2.3.3 European approach to FRT

The legislative framework for the processing of facial recognition technologies in European Union is covered by the European Convention on Human Rights (ECHR), the Charter of Fundamental Rights (Charter), the GDPR and the Law Enforcement Directive (LED) 2016/680. People's facial images represent biometric data, which are specific and cannot be altered or easily concealed.¹⁷⁸ In May 2020, at least fifteen EU countries have exercised biometric technologies like automatic facial recognition in public areas for potentially mass surveillance purposes.¹⁷⁹

The LED specifically refers to facial images as 'biometric data' when applied in biometric matching practices in pursuit of discovering a unique identification or authentication of a natural person.¹⁸⁰ Biometric data are "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".¹⁸¹ Moreover, biometric data relate to special groups of personal data¹⁸², for which European Union data protection legislation gives enhanced protection, and additional safeguards, compared to other forms of personal data.¹⁸³ Thus, it is clear from the following case that the implementation of FRT is not just.

¹⁷⁷ Mark Rasdale, John Magee, Cezary Bicki, Eilís McDonald, Marlene Winther Plas, Emil Agerskov Thuesen, Carolyn Bigg, 'Facial recognition technology: Supporting a sustainable lockdown exit strategy?' <<https://www.dlapiper.com/en/us/insights/publications/2020/05/facial-recognition-technology/>> accessed 10 October 2020

¹⁷⁸ The European Union Agency for Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (2019) <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf> accessed 13 October 2020

¹⁷⁹ European Digital Rights, 'Ban Biometric Mass Surveillance' (2020) <<https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf>> accessed 15 October 2020

¹⁸⁰ Law Enforcement Directive, Art. 3 (13), GDPR, Art. 4 (14), Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No.1247/2002/EC (PE/31/2018/REV/1), OJ L 295, 21.11.2018, pp. 39-98, Art. 3 (18).

¹⁸¹ Law Enforcement Directive, Art. 3 (18); GDPR, Art. 4 (14)

¹⁸² Law Enforcement Directive, Art. 10(1); GDPR, Art. 9 (1) and Regulation (EU) 2018/1725, Art. 10 (1)

¹⁸³ The European Union Agency for Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (2019) <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf> accessed 13 October 2020

A selection of cases in the pre-COVID era will be discussed below, providing a general understanding of the logic of certain courts behind decisions held on facial recognition technologies. Before COVID, the use of AFR was examined in the Great Britain, reaching the High Court in September 2019, when a case was brought against South Wales Police (SWP) with regards its use of AFR. The court held in its considerations that South Wales Police was lawful in its actions when using AFR.¹⁸⁴

One of the grounds that contested the overall lawfulness of the application of AFR, and the competency of the legal framework concerning AFR by the claimant related to data protection. However, the court opined that SWP was obliged to follow the data protection principles because the data from the AFR constituted personal data which could be used to distinguish a person. Crucial to SWP's case was that the SWP applied the broad data protection principles in their work with AFR by using Data Protection Impact Assessments (DPIA) and a policy on the sensitive handling of data for law enforcement functions.¹⁸⁵ However, the Court of Appeal delivered a significant judgment finding that the use of automated AFR by the SWP was unlawful.¹⁸⁶ It found that no clear guidance on where and how AFR technology could be used or who would be put on the watchlist was actually generated. The conclusion was a violation of article 8(2) of the ECHR concerning the right not to have public authorities interfere with a person's right to privacy unless granted under the law.¹⁸⁷

The conclusion made means that public authorities and legal entities regulated by public law cannot successfully rely on the demonstration that the data were handled by an official authority with discretionary powers. This would include scenarios in which the police use FRT or AFR in crime prevention activities or as a states bodies introducing FRT authentication to use their services.

¹⁸⁴ R (Bridges) v Chief Constable of South Wales Police, [2019], EWHC 2341 [2019] EWHC 2341

¹⁸⁵ Mark Rasdale, John Magee, Cezary Bicki, Eilís McDonald, Marlene Winther Plas, Emil Agerskov Thuesen, Carolyn Bigg, 'Facial recognition technology: Supporting a sustainable lockdown exit strategy?' <<https://www.dlapiper.com/en/us/insights/publications/2020/05/facial-recognition-technology/>> accessed 10 October 2020

¹⁸⁶ The Queen v The Chief Constable of South Wales Police and others [2020], [2019] EWHC 2341, CO/4085/2018, <https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html>

¹⁸⁷ Ibid

In the case of Brøndby,¹⁸⁸ AFR was effectively applied in Denmark in 2019 by Brøndby IF, one of the country's most successful soccer teams. In adopting AFR, Brøndby communicated with the Danish Data Protection Agency (DDPA) that agreed on the handling of personal data as essential for reasons of public interest, as deemed necessary for private entities according to the DDPA while considering the rights and freedoms of natural persons based on a data protection assessment. Similar to the SWP case, the club did not use AFR before DPIA was approved. DPIA is compulsory under the GDPR in cases where data processing "is likely to result in a high risk to the rights and freedoms of natural persons"¹⁸⁹, or on occasions when new data processing technology is being rolled out.

Implementation of mass surveillance in public places profoundly prohibits people's ability to provide legitimate, informed, freely-given consent, thereby breaching their rights to data protection.¹⁹⁰

The very nature of identification FRT renders getting consent more difficult when in a specific area. The messages that FRT show are unlikely to be sufficient to meet the threshold of explicit consent, as people are already situated in view of FRT-enabled cameras when they become aware of it. A further practical concern is that the data subject must be able to withdraw their consent at any time.

Following Article 6 (1) of the GDPR, processing shall be lawful only if and to the extent that at least one of the legal basis applies. The EDPB advises that video surveillance measures should only be chosen if the purpose of the processing could not reasonably be fulfilled by other means that are less intrusive to the data subject's fundamental rights and freedoms.¹⁹¹

In Sweden, FRT was introduced in highschool. The main idea was to monitor its students' attendance in classes, and was subsequently fined. The Swedish Data Protection Authority have criticized the FRT's use, due to attendance of students could have been verified by less intrusive methods. Another reason of criticism was that students' consent did not freely give, as they

¹⁸⁸ Jesper Lund from EDRI and member IT-pool, 'Danish DPA approves Automated Facial Recognition' <<https://edri.org/our-work/danish-dpa-approves-automated-facial-recognition/>> accessed 18 October 2020

¹⁸⁹ The GDPR, Art. 35

¹⁹⁰ European Digital Rights, 'Ban Biometric Mass Surveillance' (n 179)

¹⁹¹ Guidelines 3/2019 on processing of personal data through video devices, adopted on 10 July 2019 <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf> accessed 19 October 2020

were dependent on the school board.¹⁹² Therefore, for COVID, as Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, mention “Large-scale personal data processing can only be performed when based on scientific evidence, that the potential public health benefits of such digital epidemic surveillance, including their accuracy, override the benefits of other alternative solutions which would be less intrusive”.¹⁹³

The rights to respect for private life and data protection are key to the utilization of FRT in public spaces. Using live FRT implies collecting, comparing and storing facial images in an IT system for the purposes of identification. Therefore, it represents an form of intrusion in the right to protect personal data as set out in the Charter,¹⁹⁴ under the ECHR.¹⁹⁵ Facial images constitute personal data, as declared by the Court of Justice of the EU¹⁹⁶ and the European Court of Human Rights.¹⁹⁷ As a result, both the initial biometric processing of facial images, any ensuing retaining of video footage, and comparing the data to a ‘watchlist’ – together with crowding the watchlist with facial images – represent interferences with the right to respect for private life and the protection of personal data. Taking into consideration that the processing of personal data represents a limitation of these rights, it should be subjected to a stringent necessity and proportionality test, which includes consideration of a clear-cut legal foundation on which to do so and a legitimate aim pursued. European Digital Rights (EDRi) recommend banning biometric mass surveillance because it is not compatible with fundamental rights and freedoms, data protection laws, democracy, and fundamental principles of the rule of law at the heart of the European Union.¹⁹⁸ Thus, in line with the European approach this leads to a conclusion that it is not easy to implement FRT in the fight against a global pandemic.

2.3.4 The US approach to FRT

In the US, 6 states have approved laws that govern the gathering and application of biometric information by commercial organizations—laws that might serve as a standard for regulating

¹⁹² European Data Protection Board, ‘Facial recognition in school renders Sweden’s first GDPR fine’, 2019, <https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en>, accessed 19 October 2020

¹⁹³ Pierucci and Walter (n 68)

¹⁹⁴ EU Charter of Fundamental Rights, Art. 8 and 7

¹⁹⁵ ECHR, Art. 8

¹⁹⁶ The Court of Justice of the EU, C-291/12, M. Schwarz v. Stadt Bochum, 17 October 2013, paras. 22, 48-49

¹⁹⁷ The European Court of Human Rights, Szabó and Vissy v. Hungary, No. 37138/14, 12 January 2016

¹⁹⁸ European Digital Rights, ‘Ban Biometric Mass Surveillance’ (n 179)

multimodal biometric technologies during and beyond the current struggle against COVID-19.¹⁹⁹ Among them, the leading and most comprehensive one is Illinois' Biometric Information Privacy Act (BIPA), which regulates the gathering, use, and sharing of biometric information by corporate organizations.²⁰⁰ BIPA obliges commercial entities to get consent from persons before scanning for biometric information and make publicly available a written policy of the procedure used to destroy the biometric information²⁰¹. The law also establishes a right of action for those whose biometric information was gathered or utilized in violation of the law, in spite of whether the violation caused such individuals harm²⁰². As biometric information is defined in the BIPA as including any information, irrespective of capture method, that relies on biometric identifiers like facial scans or eye scans, this legal text would regulate any technologies that apply facial recognition technology or perhaps so as to capture the temperature of a specific facial location.²⁰³

San Francisco became the primary city in the US to ban the application of FRT by any local agencies, including law enforcement. In October 2019, California introduced a state-wide prohibition on the application of FRT on police body-worn cameras.²⁰⁴ The most common concern of the average Californian in mass surveillance is the risk of the invasion of privacy and inherent systematic bias that could leave minority groups at a disadvantage. In March 2020, the Washington State Legislature passed a public sector facial recognition privacy bill that requires extensive restrictions and conditions on governmental application of FRT, which is expected to decelerate the use and operation of the technology in the state.²⁰⁵ In the US, people tend to believe that FRT solutions can deliver positive outcomes as well as proving an effective tool helping the likes of businesses recover in the post-COVID era. But the privacy implications are considerable, and a careful and measured approach when considering those implications and balancing the risks is required.

¹⁹⁹ Van Natta and others (n 158) 2

²⁰⁰ Biometric Information Privacy Act of 2010, 740 ILCS/14, Public Act 095-994

²⁰¹ Ibid Section 15 (3)

²⁰² Ibid Section 10

²⁰³ Van Natta and others (n 158) 9

²⁰⁴ Kate Conger, Richard Fausset and Serge F. Kovalski, 'San Francisco Bans Facial Recognition Technology' (2020) The New York Times, <<https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html>> accessed 19 October 2020

²⁰⁵ Mark Rasdale, John Magee, Cezary Bicki, Eilís McDonald, Marlene Winther Plas, Emil Agerskov Thuesen, Carolyn Bigg, 'Facial recognition technology: Supporting a sustainable lockdown exit strategy?' <<https://www.dlapiper.com/en/us/insights/publications/2020/05/facial-recognition-technology/>> accessed 10 October 2020

Overall, based on evidence and the above-mentioned cases, it is clear that without a high legal standard of data protection, a full comparison of the risks and benefits in the use of FRT in the COVID-19 era needs to be implemented before the technology is applied and, in the EU at least, this analysis should be underpinned by the DPIA.

2.3.5 Use of drones in the context of COVID-19

The unprecedented demand to reduce human interaction as a health precaution during the first spike of the COVID-19 outbreak led to the greater application of drones. The ability of drones to provide a bird's eye view and fly over areas inaccessible by the likes of police vehicles fills an essential need from a crowd management perspective.²⁰⁶

In the COVID-19 era, robust advance in the use of drones with installed thermal cameras was made in China to identify potentially infected citizens by their body temperature.²⁰⁷ Looking beyond Asia, Australia not long ago made an agreement with the drone manufacturer Draganfly to build 'pandemic drones' fitted out with thermal recognition technology that can observe temperatures, sneezing and coughing in coronavirus hotspots, as well as heart rates and respiratory patterns.²⁰⁸ Meanwhile, in France, in order to examine the compliance with physical distancing measures in public areas such as parks and beaches, the police deployed drones.²⁰⁹ In India, police in Hyderabad city used drones to identify sensitive areas where people did not follow lockdown measures. This information is then used for the targeted deployment of law enforcement officials.²¹⁰ In Italy, local police were permitted to use drones to monitor citizens' movements during the coronavirus pandemic.

²⁰⁶ International Transport Forum, 'Covid-19 Transport Brief: Drones in the Era of Coronavirus' <<https://www.itf-oecd.org/sites/default/files/drones-covid-19.pdf>> accessed 20 October 2020

²⁰⁷ Daily Mail, 'China uses drones with THERMAL CAMERAS to check quarantined residents' temperatures and drop face masks in bid to control coronavirus outbreak' (2020) <<https://www.dailymail.co.uk/news/article-7974935/China-uses-drones-THERMAL-CAMERAS-check-quarantined-residents-temperatures.html>>, accessed 20 October 2020

²⁰⁸ Van Natta and others (n 158) 6

²⁰⁹ Trevor Mogg, 'French police the latest to use speaker drones to enforce coronavirus lockdown' (2020) <<https://www.digitaltrends.com/cool-tech/french-cops-use-speaker-drones-to-enforce-coronavirus-lockdown/>> accessed 20 October 2020

²¹⁰ Mahashreveta Choudhary, 'Hyderabad is using drones for implementing COVID-19 lockdown' (2020), Geospatial World <<https://www.geospatialworld.net/blogs/hyderabad-is-using-drones-for-implementing-covid-19-lockdown/>> accessed 23 October 2020

The processing of any images or other personal data (for example, health-related data) taken by drones necessitates the use of data protection safeguards.²¹¹ For example, the control of individuals' temperatures of individuals may expose previously private health information based on body temperature variances over time (e.g. pregnancy, menstrual cycles or menopause) which may connect back to identification documents. This is specifically challenging given the emerging nature of fever-based biometric technologies.

The Spanish Data Protection Agency (AEPD) expressed concern about temperature screening, taking into consideration that it involves the handling of protected personal data, which is prohibited by the GDPR, specifically in public places, which can inadvertently expose and reveal a person's protected health information.²¹² The risk of regulatory violation is exceptionally high with devices that also capture biometrics to spot individuals being screened for fever. For instance, one NGO in Greece stressed that legislation on drone surveillance does not include any accurate data protection assurances, while also not explicitly referring to data protection legislation.²¹³ Moreover, due to the present pandemic, the European Commission postponed the Commission Implementing Regulation (EU) 2019/947 on the rules and procedures of operating an unmanned aircraft. In other words, all UAS types can still operate under the existing conditions for an extra six months.

Mass data protection concerns might put an end to drone surveillance in some cases. In 2020, the constitutional court in France banned the employment of camera-equipped police drones to help contain COVID-19. It ruled that such use constituted "a serious and manifestly unlawful infringement of privacy rights".²¹⁴ In the US, regulation requires operators to prove that drones are necessary to respond to an emergency.²¹⁵

²¹¹ European Union Agency for Fundamental Rights, 'Coronavirus Pandemic in the EU – Fundamental Rights implications: with a focus on contact-tracing apps' <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf> accessed 6 October 2020

²¹² The Spanish Data Protection Agency <<https://www.aepd.es/es/documento/2020-0036.pdf>> accessed 20 October 2020

²¹³ Greece, Homo Digitalis 'Ανοιχτή Επιστολή: Υποβολή προτάσεων και σχολίων για την Πολιτική Προστασίας Προσωπικών Δεδομένων της Γενικής Γραμματείας Πολιτικής Προστασίας σχετικά με την αποστολή μηνυμάτων SMS στο 13033 προς λήψη βεβαίωσης μετακίνησης' 30 March 2020, p. 22. <https://www.homodigitalis.gr/wp-content/uploads/2020/04/Επιστολή_ΠολΠΔ_13033_HD_30.03.2020.pdf> accessed 20 October 2020

²¹⁴ Helena Fouquet, Gaspard Sebag, 'French Covid-19 Drones Grounded After Privacy Complaint', (2020), Bloomberg, <<https://www.bloomberg.com/news/articles/2020-05-18/paris-police-drones-banned-from-spying-on-virus-violators>> accessed 25 October 2020

²¹⁵ Jed Pressgrove, 'Do Drones Have a Realistic Place in the COVID-19 Fight?' (2020) <<https://www.govtech.com/products/Do-Drones-Have-a-Realistic-Place-in-the-COVID-19-Fight.html>> accessed 25 October 2020

Cameras placed on drones are hard to avoid. In Europe, mass surveillance is not permissible under the Charter, and so the use of biometric processing in public areas that leads to mass surveillance is by definition already illegal. Mass surveillance by its nature could be a violation of fundamental rights and encroaches on the very spirit of privacy, data protection and other rights. Any kind of application of biometric processing which intrudes into the right to privacy without proper justification and thereby contributes to mass surveillance – even unintended – is unlawful, in spite of whether the use is by law enforcement, public authorities, or commercial actors.²¹⁶

In the COVID-19 era, drone usage has been limited to restore safety, security, and privacy.²¹⁷ It appears that whether or not countries prefer a cautious approach to drones, establishing a regulatory framework for drones that takes into consideration concerns beyond safety may help improve emergency responses in the future.²¹⁸ Indeed, in Hong Kong and in public areas in Singapore, this type of data collection might not represent personal data collection if the aim is not to spot data subjects.²¹⁹ In the short term, the growth of digital surveillance may be partly tolerated as an essential technological aid to safeguard a populace's health and safety by strengthening the capability to handle infection and the next possible pandemics. Nevertheless, the granting of the use of such sensitive data, including personal information suggests the necessity for legislation on the application of digital surveillance at this particular time, and in the future.

3. Recommendations on the use of digital surveillance

Digital technologies are now being equipped to assist the public-health response to the global fight against COVID-19, including CTA, FRT, and drones. Here, the protection of personal data is of vital significance in an increasingly digitalized society. Therefore, this chapter provides ethical as well as legal recommendations in order to use such digital surveillance.

²¹⁶ European Digital Rights, 'Ban Biometric Mass Surveillance' (n 179) 22

²¹⁷ International Transport Forum, 'Covid-19 Transport Brief: Drones in the Era of Coronavirus' <<https://www.itf-oecd.org/sites/default/files/drones-covid-19.pdf>> accessed 20 October 2020

²¹⁸ Ibid

²¹⁹ Mark Rasdale, John Magee, Cezary Bicki, Eilís McDonald, Marlene Winther Plas, Emil Agerskov Thuesen Carolyn Bigg, 'Facial recognition technology: Supporting a sustainable lockdown exit strategy?' <<https://www.dlapiper.com/en/us/insights/publications/2020/05/facial-recognition-technology/>> accessed 10 October 2020

3.1 Legal basis for data protection and creating an independent supervisory authority

Protecting personal data or PII means creating clear-cut regulations that any organization processing personal data must adhere to. This is not a novel idea because data protection laws have been in place in many countries worldwide for some time; however, such laws are becoming increasingly crucial as people are forced to share more and more data in response to the fight against COVID-19.²²⁰ The Special Rapporteur of the Human Rights Council on the right to privacy has recommended that individuals be protected from any interference with their right to privacy, and that their governments should be subject to regulatory procedures provided for by national laws.²²¹

Therefore, as mentioned above, governments must have a law in place that explicitly provides data protection in a framework taking into account such digital measures. Furthermore, no data protection framework is complete without a strong enforcement mechanism which consist of an independent supervisory authority (for example, such in the EU - data protection authority)²²². Even the most dependable data protection law would be as good as worthless without an authority having the abilities and resources to control implementation, conduct investigations, and sanction entities in case of repeated, neglected, or wilful data protection violations.²²³ Moreover, in the COVID-19 era, a review procedure will likely be required, which is an excellent chance to revise the law, address any potential issues with compliance, and provide additional lucidity and legal certainty where needed.

3.2 Taking several steps for optimization

Several steps should be considered to optimize the potential of public health while at the same time limiting the impact on individuals' privacy, when considering whether, when, and how to use digital technology like thermal facial or tracking recognition or the use of drones. The first question is to ask here is whether the use of digital surveillance is a precise and efficient method of limiting viral spread and, if so, how it should be done in the handling of personal data. It

²²⁰ Accessnow, 'Creating a data protection framework: a do's and don'ts guide for lawmakers' Lessons from EU General Data Protection Regulation (2018) 3 <<https://www.accessnow.org/cms/assets/uploads/2019/11/Data-Protection-Guide-for-Lawmakers-Access-Now.pdf>> accessed 21 October 2020

²²¹ Cannataci, 'Report of the Special Rapporteur on the right to privacy' (n 28) 10

²²² GDPR, Art. 51

²²³ Accessnow, 'Creating a data protection framework: a do's and don'ts guide for lawmakers' (n 220) 12

may be required to define the objective of personal and health data collection and the particular use of the gathered data, and then to show how the technology design honours data protection parameters. The UN's Special Rapporteur has recommended that: "States should include in their laws precautionary measures designed to ensure that surveillance cannot be initiated until, or unless, it is proven to an independent and competent authority that such surveillance is legal, necessary and proportionate to the objective pursued..."²²⁴ Moreover, a further question is whether such data are to be employed solely on a one-off basis to identify the presence of symptoms? Moreover, will the practice remain after the pandemic has subsided, and how will the general public be assured that this is the case? If data are stored, how will this be done, by whom, and for how long?²²⁵ Firstly, those who design these emerging technologies should explain to the general society and to those organizations using their technology how they have engineered the machines to avoid causing harm to users' privacy first and foremost.²²⁶ When considering such questions during the current outbreak, existing recommendations and guidelines can be built upon to develop policies that can best govern digital surveillance technology for the context of infection.

Such designers should also show the extent to which privacy safeguards are required to be engineered into the design of the technology itself. Transparency and the "explainability" of analytics or artificial intelligence solutions, a precautionary method and a risk management approach (including the risk of re-identification in the case of anonymised data), an emphasis on data quality and the role of human oversight are only a few of the main points to consider in the developing of innovative solutions to fight the global pandemic.²²⁷ Additionally, those organization designing apps and services to address the COVID-19 outbreak must supply users with data protection rights, and adhere to the data protection principles. The successful codification of these principles necessitates the advancement of a set of users' rights, a legal basis for data processing, data security mechanisms, control measures, obligations for entities processing data, and procedures allowing the transfer of data to another countries. The 8 data protection principles are taken largely from international standards, in particular the OECD guidelines and Convention 108.²²⁸

²²⁴ Cannataci, 'Report of the Special Rapporteur on the right to privacy' (n 28) 10

²²⁵ Van Natta and others (n 158) 14

²²⁶ Ibid

²²⁷ Pierucci and Walter (n 68)

²²⁸ Accessnow, 'Creating a data protection framework: a do's and don'ts guide for lawmakers' (n 220) 5

3.3 Respect international data protection standards

It is clear, that the handling of personal data should be done on a volunteer basis and with consent. Though some nations have rolled out voluntary apps, others like India,²²⁹ have manoeuvred around this by mandating citizens to download and use a given app. Even when installing the application is “voluntary”, compulsory data entry varies and it is crucial to assess the level of data protection by ensuring that only necessary information is captured by the application, that the storage of the data respects international data protection standards, and that such storage is limited in time and used only for the right reasons.²³⁰

The processed data should be minimized to the lowest extent possible thus unrelated or unnecessary information should not be gathered. In the fight against COVID-19, the only data required are those relating to a person’s health. Thus, as recommended by the EBDP in scientific research, data minimization can be achieved by stating the research questions and evaluating the type and quantity of data required to answer these research questions correctly. What data are required depend on the aim of the research even when it has an explorative nature and must adhere to the purpose limitation principle pursuant to Article 5 (1) (b) GDPR. The data must be anonymised whenever possible.²³¹ Moreover, proportionate storage periods must be agreed upon. As stipulated by Article 5 (1) (e) GDPR “personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving, for example scientific purposes [...] in accordance with Article 89 (1), but with subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject”.²³² Organizations gathering biometric data should be transparent about the length of time in which they intend to store sensitive data (e.g., during an officially recognized pandemic, subsequent flu seasons, etc.).

In addition, it is recommended that companies inform consumers when the FRT is in use. For instance, entranceways should have simple language which guide people that data are being

²²⁹ Patrick Howell O’Neill, India Is Forcing People to Use Its Covid App, Unlike Any Other Democracy MIT TECH. REV. May 7 2020 <<https://www.technologyreview.com/2020/05/07/1001360/india-aarogya-setu-covid-appmandatory>> accessed 26 October 2020

²³⁰ Cannataci, ‘Report of the Special Rapporteur on the right to privacy’ (n 28) 10

²³¹ Guidelines 03/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the COVID-19 Outbreak Adopted on 21 April 2020’ (European Data Protection Board 2020) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf> accessed 7 October 2020

²³² GDPR, Art. 5(1) and Art. 89(1)

gathered, with specific directives of what will be stored and for how much time it will take for retaining.

3.4 Additional amendments or implementation of laws in the COVID-19 outbreak

Besides the European individual notice-and-consent model of privacy protection and data minimization, the focus should be shifted from preventing data leaks to the public, to protecting privacy values when data are already accessible in the public domain. Nowadays, location data are already being tracked by different devices, apps, and cell phone providers. A change to existing laws is needed that better reflect new definitions of privacy. The experience of Australia may be taken into account, which has been developed under the Biosecurity Act 2015 (Cth) (the Act) within the legal framework for the COVIDSafe app.²³³ COVID Determination (in conjunction with the Act) is designed to establish a legal framework for the operation of the COVIDSafe app and to govern the flows of personal information it establishes and enables.²³⁴

3.5 Technical privacy solutions

Apart from the simple minimization of data collection, focus should also shift towards endorsing other aspects that will safeguard privacy: security of data, transfer of data, exercise individual rights (right to access, right to object, right to erasure, right to rectification, right to information, right to explanation empowers, and right to portability. And although this list is inexhaustive, these rights must be protected by law, and not left to the discretion of organizing using the data²³⁵), and recourse when data are used against people and aspects concerning the responsibility of the use of such data. For instance, the Kerala government made an agreement with the US-based data analysis company Sprinklr to process and evaluate patient data. This caused several concerns such as the lack in the agreement of proper protections against the commercial and unauthorised misuse of data entrusted to Sprinklr. This meant that in case of any breach by Sprinklr, the Kerala government would have no legal recourse when comes to the Indian courts since the agreement gives sole jurisdiction to the New York courts. This lead

²³³ Privacy Amendment (Public Health Contact Information) Act 2020 <<https://www.legislation.gov.au/Details/C2020A00044>> accessed 26 October 2020

²³⁴ Watts, David, 'COVIDSafe, Australia's Digital Contact Tracing App: The Legal Issues' (2020) <<https://ssrn.com/abstract=3591622>> accessed 28 October 2020

²³⁵ Accessnow, 'Creating a data protection framework: a do's and don'ts guide for lawmakers' (n 220)

the Kerala High Court to communicate its concerns regarding the appropriate protection of data. It directed the Kerala government to provide only anonymised data to Sprinklr and apprise and obtain specific consent from citizens to the effect that their collected data would likely be accessed by Sprinklr or any other third party.²³⁶

3.6 Public awareness

In addition, companies should also offer recourse procedures for suspected false positives.²³⁷ For example, this may occur when having a high temperature after running. Article 16 of the GDPR outlines a right to rectification, whereby subjects of multimodal biometric collection should be confident that inaccurate or incomplete personal data will be expeditiously rectified and/or completed.²³⁸ Moreover, the development of digital surveillance has been accompanied by concerns about increased state surveillance and associated threats to data protection. For example, these include the application of centralised and de-centralised electronic architectures where individuals' location details and personal interactions, together with other personal data are made available, or are available to governments and their agencies in real time, or close to real time. Risks include instances whereby such information is used by law enforcement and national security agencies for unrelated aims, i.e., unconnected to managing pandemic risks. National authorities ought to be aware that exactly because personal data may include significant information about public interplay and recent movements of people who were infected, need be treated in responsible way. Disregarding consent and privacy rights for the sake of disease surveillance can increase levels of distrust which may in the long term turn out to be disadvantageous. Therefore, every time access to these data sources is requested or required and is deemed proportional, the public need be sufficiently told. Secrecy about data access and the use thereof should be avoided. For the common good should be pursued opened public communication on data processing. For instance, data-processing agreements should disclose data which will be transmitted to third parties and for which purposes.²³⁹ Furthermore,

²³⁶ Vasudha Luniya, 'COVID-19 and data protection and privacy' (2020) <<https://www.internationallawoffice.com/Newsletters/Tech-Data-Telecoms-Media/India/Clasis-Law/COVID-19-and-data-protection-and-privacy>> accessed 29 October 2020

²³⁷ Van Natta and others (n 158) 16

²³⁸ GDPR, Art. 16

²³⁹ Marcello Ienca, Effy Vayena, 'On the responsible use of digital data to tackle the COVID-19 pandemic' *Nature Medicine* 26, 463–464 (2020) <<https://doi.org/10.1038/s41591-020-0832-5>> accessed 30 October 2020

awareness-raising efforts should be made so as to avoid instances where companies are not aware of the existence and relevance of data protection laws.²⁴⁰

In a recent report by the University of Oxford's Nuffield Department of Medicine it was found that if 60% of a population uses a tracing app, it could end the epidemic²⁴¹. In other words, it is clear that to defeat the global pandemic, the use of surveillance is needed, which increases risks associated with data processing. Therefore, the authorities and companies should follow the recommendations and data protection legislation to avoid any such data protection breaches.

Conclusion

COVID-19 has changed the way we work, socialise, and think, affecting almost every aspect of our economy, society and well-being. Under the particular conditions of a pandemic, the handling of personal data is paramount so as to take suitable measures to limit the spread of the virus and subsequently alleviate its effects. However, digitalizing these measures in combating COVID-19 has raised concerns about data protection.

Questions relating to the legal basis of data protection in the fight against a global pandemic have been raised across the world. It is clear, that although most countries around the world have no specific data protection legislation or one that is under development, personal data and privacy are protected to an extent in other sectoral laws, particularly in the context of technology and electronic communications. The GDPR has without a doubt been a catalyst and harbinger of change in setting the standard of personal data privacy the world over. Furthermore, the use of personal data in the framework of the accepted measures to slow the expansion and infection of SARS-CoV-2 by countries around the world has caused an urgent need for the development of laws in the field of data protection. Governments must make sure that, concerning the collection and processing of personal data, a law that explicitly provides for such surveillance measures is required.

²⁴⁰ Accessnow, 'Creating a data protection framework: a do's and don'ts guide for lawmakers' (n 220)

²⁴¹ University of Oxford, 'Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown' (2020) <<https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown>> accessed 27 October 2020

This dissertation has provided an overview of cases in which a breach of the collection and use of health data in the COVID-19 crisis has occurred, which challenges the protection of privacy and personal data. Three measures are known to protect patient privacy in the processing of health data: the minimum amount of personal data, consent from the patient, anonymization and pseudonymization. Potential privacy risks justify a reflexive call for stricter prohibitions of data collection and use. However, more and better data collection and processing is needed in the interest of data security, law enforcement, and medical progress, especially during the current pandemic. Thus, data collection and processing could be governed by transparency, verification and accountability, starting with the gathering of data and extending onwards towards processing operations and the purported use of data, as well as by whom and for how long.

As a response to concerns about data protection, this dissertation considers the use of technological measures such as CTA, FRT and drones. First of all, this dissertation has provided an overview of two primary forms of digital CTA. Some advantages and concerns thereof were also highlighted. As a response to the concerns about data protection, the dissertation has elaborated on the legal landscape, in particular the GDPR and the legislation of other countries with regard to breaches of data protection in the use of tracing apps. Secondly, this dissertation has provided an overview of the use of thermal face recognition technology and drones. It has indicated the legal framework of the processing of facial recognition technologies across Europe, with the consideration of cases using such technology in the pre-pandemic period and their applicability in the EU. The rights to respect for private life and data protection are key to the implementation of facial recognition technology in public places. Thus, the processing of personal data in the use of FRT represents a constraint of these rights, and should be a subject to a rigorous necessity and proportionality test, which includes a clear legal basis and legitimate target in doing so.

Moreover, this dissertation has considered cases of the use of drones to monitor compliance with physical distancing measures through thermal recognition in public areas. Data protection concerns have put an end to drone surveillance in Europe and the US. Mass surveillance by its very essence is a fundamental breach of fundamental rights: it encroaches on the core spirit of privacy, data protection and other rights. It is important to keep in mind that the use of any processing of biometrical data which interfere with the right to privacy without proper

justification and so contributes to mass observation— even unintended – have not permission despite of whether the use is by legislation enforcement, states authorities, or business.

Though there are positive uses for data, and indeed, there may be ethical obligations to donate data (e.g., for medical research), the understanding of data protection needs to be shifted to keep pace with the modern world, so as to continue to protect data in a way that is practicable and beneficial to society as a whole.

This dissertation asserts that countries that have decided that technological surveillance is necessary as a answer to the global COVID-19 pandemic must make sure that it has measured both the necessity and proportionality of the specific measures accordingly. Thus, all countries and organizations should take into account various legal, as well as ethical recommendations mentioned in this dissertation.

First and foremost, governments should have a law that explicitly provides data protection taking into account the measures mentioned above. to the balance is to enhance the public health while limiting any influence on individuals' privacy, when considering whether, when, and how to use such digital technology. Depending on the answers, it can be also necessary to define the purpose of processing and data related the people's health and the specific use(s) to which they will be put and demonstrate how the technology design honours data protection parameters. Inventors of these technologies have also to show the degree to which they have engineered privacy safeguards into the design of the technology itself. Additionally, entities create apps and services used to dealing with or responding to the COVID-19 outbreak should give opportunity to individuals to exercise data protection rights and always follow the principles of data protection (refer to the right “standard principles”).

Furthermore, countries should ensure the European individual notice-and-consent model of privacy protection and data minimization and shift focus away from preventing data leaks, to preserving privacy values when data are already out in the public view. Nowadays, location data are already being tracked by different devices, apps, and cell phone providers. Existing laws need amended to reflect new definitions of privacy.

This dissertation notes that adequate legislation to protect human rights is inadequate in some countries, where cases of data protection violations have taken place during the flight against

COVID-19. Moreover, states authorities need aware that personal data may include vulnerable information about the social interplays and also infected people's movements, and thus they should be controled conscientiously. Authorities and companies are required to follow these recommendations and relevant data protection legislation to avoid such breaches of data protection, especially in the COVID-19 era.

Bibliography

Legislation

1. Biometric Information Privacy Act of 2010, 740 ILCS/14, Public Act 095-994
2. California Consumer Privacy Act 2018
3. Charter of Fundamental Rights of the European Union
4. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 28 January 1981
5. Coronavirus Act 2020 of the United Kingdom
6. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281 23/11/1995 P. 0031 – 0050)
7. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
8. Ordinance on the Proximity Tracing System for the Sars-CoV-2 coronavirus of the Swiss Confederation
9. Personal Data Protection Act, Act No. 25.326 of 2000 of Argentina
10. Privacy Amendment (Public Health Contact Information) Act 2020 of Australia
11. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ 2016 L 119/1) (GDPR)
12. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data
13. Resolution of the General Assembly UN ‘The right to privacy in the digital age’ 18 December 2013, 68/167
14. The Convention on the Rights of the Children
15. The European Convention on Human Rights
16. The Health Protection (Coronavirus) Regulations 2020 of the United Kingdom
17. The Information Technology Act 2000 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011
18. The International Covenant on Civil and Political Rights, 16 December 1966

19. The International Covenant on the Protection of All Migrant and Members of their Families, 18 December 1990
20. The Singapore Personal Data Protection Regulations 2014
21. The Universal Declaration on Human Rights 1948
22. Translation ‘Cybersecurity Law of the People’s Republic of China’ “New America” <<https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/>> accessed 15 October 2020
23. Translation ‘The Personal Information Security Specification of the People’s Republic of China’ <<https://web.archive.org/web/20201124083428/https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf>> accessed 15 October 2020

Court’s Decisions

1. R (Bridges) v Chief Constable of South Wales Police, [2019], EWHC 2341
2. The Court of Justice of the EU, C-291/12, M. Schwarz v. Stadt Bochum, 17 October 2013
3. The European Court of Human Rights, Szabó and Vissy v. Hungary, No. 37138/14, 12 January 2016
4. The Queen v The Chief Constable of South Wales Police and others [2020], [2019] EWHC 2341, CO/4085/2018

Recommendation and Guidelines

1. International Data Protection Guidelines on Coronavirus/COVID-19 <<https://webcache.googleusercontent.com/search?q=cache:XoZYdqJ6N5wJ:https://www.jonesday.com/-/media/files/publications/2020/04/covid19-cybersecurity/global-dpas-guidelines-on-coronavirus.pdf+&cd=1&hl=en&ct=clnk&gl=at>>
2. ‘Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe’, 30 March 2020
3. ‘Recommendation CM/Rec (2019) 2 of the Committee of Ministers to member States on the protection of health-related data’, adopted by the Committee of Ministers of the Council of Europe 27 March 2019
4. European Union Commission Recommendation 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility

data, <<https://op.europa.eu/en/publication-detail/-/publication/1e8b1520-7e0c-11ea-aea8-01aa75ed71a1/language-en>>, accessed 7 October 2020

5. Recommendation of the Council concerning Guidelines governing the Protection of Privacy and transborder flows of personal data 23 September 1980
6. Resolution on the Privacy and Data Protection Challenges in the Context of the Covid-19 Pandemic, 42nd closed session of the Global Privacy Assembly October 2020
7. The protection of personal data and privacy in a globalized world: a universal right respecting diversity 2005 (Montreux-Declaration)
8. The United Nations Special Rapporteur on the right to privacy J.A. Cannataci, 'Report of the Special Rapporteur on the right to privacy', 75th session of General Assembly of the UN 27 July 2020
9. The United Nations Special Rapporteur on the right to privacy J.A. Cannataci 'The Protection and Use of Health-Related Data: report', 74th session of the General Assembly of the UN 5 August 2019

European Data Protection Board Documents

1. Guidelines of the European Board Data Protection 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak adopted on 21 April 2020
2. Guidelines of the European Board Data Protection 3/2019 on processing of personal data through video devices, adopted on 10 July 2019
3. Guidelines of the European Board Data Protection 03/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the COVID-19 Outbreak adopted on 21 April 2020'
4. 'Statement on the processing of personal data in the context of the COVID-19 outbreak', adopted on 19 March 2020
5. 'Facial recognition in school renders Sweden's first GDPR fine', 2019, <https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en>, accessed 19 October 2020

Academic Sources

1. Alkhasawneh A, 'The Future of Biometric Data Protection in Jordan in Light of the GDPR: Do we need to comply with the GDPR?' (2020) Vol. 23 Iss.2, 1
2. Baik J, 'Data privacy against innovation or against discrimination? The case of the California Consumer Privacy Act (CCPA)' (2020)

3. Bengtsson L, Gaudart J, Lu X, Moore S, Wetter E, Sallah K, Rebaudet S, Piarroux R, 'Using Mobile Phone Data to Predict the Spatial Spread of Cholera' (2015) Scientific Report 1
4. Bradford L, Mateo A, Kathleen L, 'COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR and Data Protection Regimes' Journal of Law and the Biosciences (2020) University of Cambridge Faculty of Law Research Paper No. 23/2020
5. Chuncheng L, 'Algorithms in Action: Reassembling Contact Tracing and Risk Assessment during the COVID-19 Pandemic in China' (2020)
6. Chumtong J, 'Phone tracking against COVID-19 Using digital technology against an analogue virus', Konrad Adenauer Stiftung (2020) JSTOR
7. Determann L, 'Healthy Data Protection', Michigan Telecommunications and Technology Law Review Vol. 26 No. 229 UC Hastings Research Paper No. 349 (2020)
8. Foulsham M, Hitchen B, Denley A, 'GDPR: How to achieve and Maintain Compliance' (2019) London: Routledge 1st Edition 2
9. Greece, Homo Digitalis 'Ανοιχτή Επιστολή: Υποβολή προτάσεων και σχολίων για την Πολιτική Προστασίας Προσωπικών Δεδομένων της Γενικής Γραμματείας Πολιτικής Προστασίας σχετικά με την αποστολή μηνυμάτων SMS στο 13033 προς λήψη βεβαίωσης μετακίνησης' 30 March 2020, < https://www.homodigitalis.gr/wp-content/uploads/2020/04/Επιστολή_ΠολΠΔ_13033_HD_30.03.2020.pdf> accessed 20 October 2020
10. Haug C J, 'Turning the tables - the new european general data protection regulation' (2018) the New England Journal of Medicine 208
11. Hargittai E, Redmiles E, Vitak J, Zimmer M 'Americans' willingness to adopt a Covid-19tracking app: The role of app distributor' (2020) <<https://firstmonday.org/ojs/index.php/fm/article/view/11095/9985>> accessed 8 October 2020
12. Ienca M, Vayena E, 'On the responsible use of digital data to tackle the COVID-19 pandemic' Nature Medicine 26, 463–464 (2020) <<https://doi.org/10.1038/s41591-020-0832-5>> accessed 30 October 2020
13. Klonowska K, 'The COVID-19 Pandemic: Two Waves of Technological Responses in the European Union' (2020) the Hague Centre for Strategic Studies
14. Koller M et al., Symptom Reporting in Cancer Patients: The Role of Negative Affect and Experienced Social Stigma 77 CANCER 983, 994 (1996).

15. Kretzschmar M, Susan H, Wijngaarden J, 'Ring vaccination and smallpox control' (2004) Research, Emerg Infect Dis.
16. OECD, 'Ensuring data privacy as we battle COVID-19' (2020) 2 <https://read.oecd-ilibrary.org/view/?ref=128_128758-vfx2g82fn3&title=Ensuring-data-privacy-as-we-battle-COVID-19>, accessed 1 October 2020
17. Pichrotanak Bunthan, Jay Cohen, "What Cambodia's New Law on Electronic Commerce Means for Business", 2020
18. Raposo V L, 'Can China's 'Standard of Care' for COVID-19 be Replicated in Europe?' (2020) Journal of Medical Ethics <<https://ssrn.com/abstract=3706028>>, accessed 10 October 2020
19. Rasdale M, Magee J, Bicki C, McDonald E, Winther Plas M, Agerskov Thuesen E, Bigg C, 'Facial recognition technology: Supporting a sustainable lockdown exit strategy?' <https://www.dlapiper.com/en/us/insights/publications/2020/05/facial-recognition-technology/>>
20. Sethi N, Laurie G T, 'Delivering Proportionate Governance in the Era of eHealth: Making Linkage and Privacy Work Together' 13 MED. LAW INT. 168 (2013)
21. Tiffany L, 'Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis' (2020) Loyola University Chicago Law Journal Volume 52 Issue
22. The European Union Agency for Fundamental Rights, 'Coronavirus Pandemic in the EU – Fundamental Rights implications: with a focus on contact-tracing apps' <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-may_en.pdf> accessed 6 October 2020
23. The European Union Agency for Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (2019) 2 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf> accessed 13 October 2020
24. Van Natta M, Chen P, Herbek S, Jain R, Kastelic N, Katz E, Struble M, V Vanam, Vattikonda N, 'The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic', *Journal of Law and the Biosciences* Volume 7 Issue 1 2020
25. Ventrella E, 'Privacy in emergency circumstances: data protection and the COVID-19 pandemic' ERA Forum (2020) 383
26. Zhang B et al., Americans' Perceptions of Privacy and Surveillance in the COVID-19 Pandemic OSF PREPRINTS (2020)

Other Documents and Web Sources

1. Ai M, 'Hangzhou City Proposes Laws Prohibiting Mandatory Facial Recognition' China Money Network <<https://www.chinamoneynetwork.com/2020/10/29/hangzhou-city-proposes-laws-prohibiting-mandatory-facial-recognition>> accessed 17 October 2020
2. Accessnow, 'Creating a data protection framework: a do's and don'ts guide for lawmakers', Lessons from EU General Data Protection Regulation (2018) 14 <<https://www.accessnow.org/cms/assets/uploads/2019/11/Data-Protection-Guide-for-Lawmakers-Access-Now.pdf>> accessed 21 October 2020
3. Accessnow, 'Recommendations on privacy and data protection in the fight against COVID-19' (2020) <<https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf>> accessed 5 October 2020
4. Attorney-General for Australia and Minister for Industrial Relations, 'Privacy protections for COVIDSafe App enshrined in law' Media release (2020) <<https://www.attorneygeneral.gov.au/media/media-releases/privacy-protections-covidsafe-app-enshrined-law>> accessed 4 October 2020
5. Antony Kuhn, 'South Korea's Drive-Through Testing For Coronavirus Is Fast — And Free' (2020) <<https://www.npr.org/sections/goatsandsoda/2020/03/13/815441078/south-koreas-drive-through-testing-for-coronavirus-is-fast-and-free?t=1605650456898>> accessed 5 October 2020
6. Bai Yang, Ren Qinqin, 'How does the first draft of the Personal Information Protection Law defend your information security?' (2020) <https://www.thepaper.cn/newsDetail_forward_9544106> accessed 4 October 2020
7. Baxter M, 'Centralised versus decentralised contact tracing solutions pit privacy academics against each other' (2020) PrivSec Report <<https://gdpr.report/news/2020/04/22/centralised-versus-decentralised-contact-tracing-solutions-pit-privacy-academics-against-each-other/>> accessed 7 October 2020
8. Beckett N and Ge A, 'China publishes new specification on personal data security' (2020) <https://www.cms-lawnow.com/ealerts/2020/03/china-publishes-new-specification-on-personal-data-security?cc_lang=en>, accessed 10 October 2020
9. 'California Consumer Privacy Act (CCPA), Compliance' <<https://cpl.thalesgroup.com/compliance/americas/california-consumer-privacy-act->

- compliance-solutions-ccpa-compliance?_ga=2.99010590.1060482728.1601540838-1057165311.1601540838> accessed 2 October 2020
10. Chen L, 'China wakes up to wide web of online data leaks and privacy concerns' (2020) South China Morning Post <<https://www.scmp.com/news/china/society/article/3047186/china-wakes-wide-web-online-data-leaks-and-privacy-concerns>> accessed 13 October 2020
 11. Choudhary M, 'Hyderabad is using drones for implementing COVID-19 lockdown' (2020), Geospatial World <<https://www.geospatialworld.net/blogs/hyderabad-is-using-drones-for-implementing-covid-19-lockdown/>> accessed 23 October 2020
 12. Chris H. Kang, Sun Hee Kim, Doil Son, 'Korea introduces major amendments to data privacy laws', 2020, <<https://www.lexology.com/library/detail.aspx?g=223051e2-0346-4935-8fbb-6146e4424d94>>, 6 October 2020
 13. Collins K, 'The COVID-19 contact-tracing apps we were promised are finally here' 2020 <<https://www.cnet.com/news/the-covid-19-contact-tracing-apps-we-were-promised-are-finally-here/>> accessed 6 October 2020
 14. Conger K, Fausset R and Kovalski S F, 'San Francisco Bans Facial Recognition Technology' (2020) The New York Times, <<https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html>> accessed 19 October 2020
 15. Congressional Research Service, 'Data Protection Law: An Overview Congressional Research Service' 2019
 16. Daily Mail, 'China uses drones with THERMAL CAMERAS to check quarantined residents' temperatures and drop face masks in bid to control coronavirus outbreak' (2020) <<https://www.dailymail.co.uk/news/article-7974935/China-uses-drones-THERMAL-CAMERAS-check-quarantined-residents-temperatures.html>>, accessed 20 October 2020
 17. Deloitte, 'Data and Privacy Protection in ASEAN. What does it mean for business in the region?' (2019) <<https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-data-privacy-in-asean.pdf>> 5 accessed 3 October 2020
 18. Del Castillo A D, 'COVID-19 contact-tracing apps: how to prevent privacy from becoming the next victim', (2020), European Economic Employment and Social Policy N°5/2020, 2 <<https://www.etui.org/sites/default/files/2020-06/Covid-19%2Bcontact-tracing%2Bapps%2BCorona%2BPonce%2BPolicy%2BBrief%2B2020.05.pdf>> accessed 7 October 2020

19. Dennis S J, '70% of people surveyed said they'd download a coronavirus app. Only 44% did. Why the gap?' (2020) <<https://theconversation.com/70-of-people-surveyed-said-theyd-download-a-coronavirus-app-only-44-did-why-the-gap-138427>> accessed 8 October 2020
20. Digital Rights Center, 'Data protection history: emerged as GDPR' (2018) <<https://habr.com/ru/company/digitalrightscenter/blog/431582/>> accessed 2 October 2020
21. Euronews, 'Coronavirus conundrum: COVID-19 tracking apps that don't breach privacy' television broadcast (2020) <<https://www.euronews.com/video/2020/04/10/coronavirus-conundrum-covid-19-tracking-apps-that-don-t-breach-privacy>> accessed 6 October 2020
22. European Digital Rights, 'Ban Biometric Mass Surveillance' (2020) <<https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf>> accessed 15 October 2020
23. Foy K, 'Bluetooth signals from your smartphone could automate Covid-19 contact tracing while preserving privacy' (2020) MIT News <<https://news.mit.edu/2020/bluetooth-covid-19-contact-tracing-0409>> accessed 7 October 2020
24. Fouquet H, Sebag G, 'French Covid-19 Drones Grounded After Privacy Complaint', (2020), Bloomberg, <<https://www.bloomberg.com/news/articles/2020-05-18/paris-police-drones-banned-from-spying-on-virus-violators>> accessed 25 October 2020
25. Fulbright N R, 'Personal data protection amid coronavirus: Key takeaways for business operating in China' (2020) 1 <<https://www.nortonrosefulbright.com/ru-ru/knowledge/publications/d61ee6b6/personal-data-protection-in-the-time-of-coronavirus-covid-19>> accessed 4 October 2020
26. Gan N, Culver D, 'China is fighting the coronavirus with a digital QR code. Here's how it works' CNN Bussiness (2020) <<https://edition.cnn.com/2020/04/15/asia/china-coronavirus-qr-code-intl-hnk/index.html>> accessed 11 October 2020
27. General Office of the National Health Commission of China, "Notice of the General Office of the National Health Commission on Strengthening Informationization to Support the Prevention and Control of Pneumonia Epidemics Caused by the Novel Coronavirus Infection Issuing Authority" 2020 <http://www.gov.cn/zhengce/zhengceku/2020-02/05/content_5474692.htm> accessed 4 October 2020
28. Global Privacy Assembly, < <https://globalprivacyassembly.org/>>, accessed 3 October 2020

29. Gong J, Guo G, Lau N, 'China Cyber Security and Data Protection: China Issues Draft of "Data Security Law' (2020) <<https://www.lexology.com/library/detail.aspx?g=0b312359-b397-445e-b659-5a5bf19a4e62>> accessed 4 October 2020
30. Holmes A, 'China is reportedly making people download an Alibaba-backed app that decides whether they'll be quarantined for coronavirus' Business Insider, 2020 <<https://www.businessinsider.com/alibaba-coronavirus-chinese-app-quarantine-color-code-2020-3?r=DE&IR=T>> accessed 12 October 2020
31. International Data Protection Guidelines on Coronavirus/COVID-19 <<https://www.jonesday.com/-/media/files/publications/2020/04/covid19-cybersecurity/global-dpas-guidelines-on-coronavirus.pdf?la=en&hash=CBD0BBF9DDA4C329A088037F4B6BE109>> accessed 13 October 2020
32. International Transport Forum, 'Covid-19 Transport Brief: Drones in the Era of Coronavirus' <<https://www.itf-oecd.org/sites/default/files/drones-covid-19.pdf>> accessed 20 October 2020
33. Kuo L, 'The new normal': China's excessive coronavirus public monitoring could be here to stay', (2020), The Guardian <<https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay>> accessed 12 October 2020
34. Lawtimes, 'Personal information protection law amendment passed the National Assembly' (2020) <<https://m.lawtimes.co.kr/Content/Article?serial=158894>> accessed 6 October 2020
35. Lee S, 'Coming into Focus: China's Facial Recognition Regulations'(2020), Centre for Strategic and International Studies <<https://www.csis.org/blogs/trustee-china-hand/coming-focus-chinas-facial-recognition-regulations>> accessed 6 October 2020
36. Lei R, 'Beyond the Exit Strategy: ethical uses of data-driven technology in the fight against COVID-19' Huazhong University of Science and Technology, Wuhan, China, Nuffield Council on Bioethics and Ada Lovelace Institute webinar (2020) <<https://www.nuffieldbioethics.org/publications/covid-19/webinar-beyond-the-exit-strategy-ethical-usesof-data-driven-technology-in-the-fight-against-covid-19>> accessed 12 October 2020
37. Lund J from EDRI and member IT-pool, 'Danish DPA approves Automated Facial Recognition' <<https://edri.org/our-work/danish-dpa-approves-automated-facial-recognition/>> accessed 18 October 2020

38. Luniya V, 'COVID-19 and data protection and privacy' (2020) <<https://www.internationallawoffice.com/Newsletters/Tech-Data-Telecoms-Media/India/Clasis-Law/COVID-19-and-data-protection-and-privacy>> accessed 29 October 2020
39. Luo Y, Yu Z, 'China issued the Draft Data Security Law' (2020), <<https://www.insideprivacy.com/data-security/china-issued-the-draft-data-security-law/>> accessed 4 October 2020
40. Mark Scott, Zosia Wanat, 'Poland's coronavirus app offers playbook for other governments' (2020) POLITICO <<https://www.politico.eu/article/poland-coronavirus-app-offers-playbook-for-other-governments/>> accessed 14 October 2020
41. McCurry J, 'Test, trace, contain: how South Korea flattened its coronavirus curve' the Guardian (2020) <<https://www.theguardian.com/world/2020/apr/23/test-trace-contain-how-south-korea-flattened-its-coronavirus-curve>> accessed 6 October 2020
42. Mesmer P, 'Endiguer le coronavirus : Singapour et la Corée du Sud, des exemples à suivre', L'Express (2020) <https://www.lexpress.fr/actualite/monde/asie/endiguer-le-coronavirus-singapour-et-la-coree-du-sud-des-exemples-a-suivre_2121024.html> accessed 6 October 2020
43. Merriam-Webster Dictionary, Anonymize <<https://www.merriam-webster.com/dictionary/anonymize>> accessed 5 October
44. Nación L, 'Quiénes son y de dónde vinieron los 21 infectados por coronavirus en la Argentina' (2020), <https://www.lanacion.com.ar/sociedad/quienes-son-17-infectados-coronavirus-argentina-nid2341456>> accessed 5 October 2020
45. Mogg T, 'French police the latest to use speaker drones to enforce coronavirus lockdown (2020) <<https://www.digitaltrends.com/cool-tech/french-cops-use-speaker-drones-to-enforce-coronavirus-lockdown/>> accessed 20 October 2020
46. Natalie Moreno, 'Coronavirus and contact tracing apps: Global privacy perspective' (2020) 6 <https://www.addleshawgoddard.com/globalassets/insights/data-protection/coronavirus-and-contact-tracing-apps-article_spreads.pdf> accessed 3 October
47. Office of the Australian Information Commissioner, 'Australians wants more control over privacy, survey shows', 2020, <https://www.oaic.gov.au/updates/news-and-media/australians-want-more-control-over-privacy-survey-shows/>> accessed 4 October 2020
48. Office of the High Commissioner United Nations Human Rights, 'Preliminary evaluation of the privacy dimensions of the coronavirus disease (COVID-19) pandemic: report',

- 2020, <<https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/COVID-19.aspx>> accessed 3 October 2020
49. O'Neill P H, Ryan-Mosley T, Johnson B, 'A flood of coronavirus apps are tracking us Now it's time to keep track of them' MIT Technology Review (2020) <<https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker>> accessed 7 October 2020
 50. O'Neil P H, 'India is forcing people to use its covid app, unlike any other democracy' (2020), <https://www.technologyreview.com/2020/05/07/1001360/india-aarogya-setu-covid-app-mandatory/>> accessed 9 October 2020
 51. Personal Data Protection Commission in Singapore, 'PDPA Overview' <<https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act>> accessed 3 October 2020
 52. Pollard M, 'Even mask-wearers can be ID'd, China facial recognition firm says' (2020) <<https://uk.reuters.com/article/us-health-coronavirus-facial-recognition/even-mask-wearers-can-be-idd-china-facial-recognition-firm-says-idUKKBN20W0WL>> accessed 15 October 2020
 53. Pressgrove J, 'Do Drones Have a Realistic Place in the COVID-19 Fight?' (2020) <<https://www.govtech.com/products/Do-Drones-Have-a-Realistic-Place-in-the-COVID-19-Fight.html>> accessed 25 October 2020
 54. Press Release of Ministry of Public Administration and Security e-Government Bureau Privacy Policy Division of the South Korea, 'Personal information protection law amendment passed the National Assembly' (2020) <<https://eiec.kdi.re.kr/main.do4>> accessed 10 October 2020
 55. Qingxiu B, 'Human flesh search' in china: The double-edged sword'. International Data Privacy Law. 2013 3(3)
 56. Ross L, Zhou K, Liu T, 'China Issues New Personal Information Security Specification' (2020) WilmerHale <<https://www.wilmerhale.com/en/insights/client-alerts/20200324-china-issues-new-personal-information-security-specification>> accessed 15 October 2020
 57. Sellars C, 'The use of facial recognition technology to combat COVID-19' (2020), <<https://ropesgrayinsights.passle.net/post/102g6qx/the-use-of-facial-recognition-technology-to-combat-covid-19>> accessed 13 October 2020
 58. Steven Chabinsky, Paul Pittman, 'USA: Data protection Laws and Regulations' (2020) <<https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa>> accessed 2 October 2020

59. Shen X, 'Facial recognition data leaks are rampant in China as Covid-19 pushes wider use of the technology' (2020) <<https://www.scmp.com/abacus/tech/article/3104512/facial-recognition-data-leaks-rampant-across-china-covid-19-pushes>>, accessed 13 October 2020
60. Shen X, 'China ranks as the worst country at collecting, using and storing biometric data' (2020) <<https://www.scmp.com/abacus/tech/article/3040841/china-ranks-worst-country-collecting-using-and-storing-biometric-data>> accessed 14 October 2020
61. Watts D, 'COVIDSafe, Australia's Digital Contact Tracing App: The Legal Issues' (2020) <<https://ssrn.com/abstract=3591622>> accessed 28 October 2020
62. Tiffany L, 'Give All My Data to Google and the CDC' (2020) Slate, <<https://slate.com/technology/2020/04/google-cdc-data-privacy-covid19.html>> accessed 27 October 2020
63. Townend D, 'Conclusion: Harmonization in Genomic and Health Data Sharing for Research: An Impossible Dream?' 137 Hum. Genetics, 657 661 (2018)
64. *The Economist*, 'To curb covid-19, China is using its high-tech surveillance tools' (2020) <<https://www.economist.com/china/2020/02/29/to-curb-covid-19-china-is-using-its-high-tech-surveillance-tools>> accessed 3 October 2020
65. The Office of Cyberspace Affairs in China, 'Notice on Doing a Good Job in Personal Information Protection and Using Big Data to Support Joint Prevention and Control Work' (2020) <<https://perma.cc/6WUS-ZLQV>>, accessed 4 October 2020
66. The GSMA, 'Data Privacy Frameworks in MENA. Emerging approaches and common principles', (2019), Executive Summary 5 <<https://www.gsma.com/mena/wp-content/uploads/2019/07/GSMA-Data-Privacy-in-MENA-Exec-Summary.pdf>> accessed 3 October 2020
67. The Spanish Data Protection Agency <<https://www.aepd.es/es/documento/2020-0036.pdf>> accessed 20 October 2020
68. UNCTAD, 'Data protection regulations and international data flows: Implications for trade and development' (2016) 24 <https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf> accessed 3 October 2020
69. UNCTAD, 'Data Protection and Privacy Legislation Worldwide' <<https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>> accessed 2 October 2020

70. Vodafone Group's Five-Point Plan to Help Counter the Impact of COVID-19' <<https://www.vodafone.com/news-and-media/vodafone-group-releases/news/vodafone-launches-five-point-plan-to-help-counter-the-impacts-of-the-covid-19-outbreak>> accessed 8 October 2020
71. WHO, 'Naming the coronavirus disease (COVID-19) and the virus that causes it' <[https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-\(covid-2019\)-and-the-virus-that-causes-it](https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it)> accessed 30 September 2020
72. WHO, 'Coronavirus disease 2019 (Covid-19)' Situation Report 94 (2020) <https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200423-sitrep-94-covid-19.pdf?sfvrsn=b8304bf0_2#:~:text=Retrospective%20investigations%20by%20Chinese%20authorities,%2C%20some%20did%20not> accessed 1 October 2020
73. WHO, 'WHO Director-General's opening remarks at the media briefing on COVID-19 - 8 May 2020' (2020) <<https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---8-may-2020>> accessed 1 October 2020
74. Yesui Z, 'The formulation of a personal information protection law has been included in this legislative plan' (2019) <http://www.china.com.cn/lianghui/news/2019-03/04/content_74529251.shtml> accessed 4 October 2020
75. Yves-Alexandre de Montjoye and others 'Evaluating COVID-19 contact tracing apps? Here are 8 privacy questions we think you should ask' Computational Privacy Group (2020) <<https://cpg.doc.ic.ac.uk/blog/evaluating-contact-tracing-apps-here-are-8-privacy-questions-we-think-you-should-ask/>> accessed 8 October 2020
76. Zastrow M, 'South Korea is reporting intimate details of COVID-19 cases: has it helped?' (2020) Journal "Nature" <<https://www.nature.com/articles/d41586-020-00740-y>> accessed 5 October 2020
77. University of Oxford, 'Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown' (2020) <<https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown>> accessed 27 October 2020