



universität
wien

MASTER THESIS

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

„The Use of Personal and Sensitive Data during COVID-19:
A Balance Between Saving Lives and Data Protection”

verfasst von / submitted by

Helena Nyikos

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, 2020 / Vienna 2020

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

UA 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. hc. Peter Fischer

Abstract

Since the beginning of the Covid-19 pandemic, public authorities and governments have been trying to fight this health crisis by advising social distancing, declaring travel restrictions and imposing quarantine measures. We have also experienced an upsurge in the use of digital surveillance and the development of mobile phone apps that, while exhibiting different functionalities, all aim to assist in combating the pandemic. Using a doctrinal approach, this thesis deals with the adoption of Covid-19 apps that process personal and sensitive data to analyse the spread of the Covid-19 virus, track individuals' movements and conduct contact-tracing. While this thesis focuses merely on the European legal frameworks, it refers to both EU and international app developments to highlight the vast differences that exist between them and to demonstrate the overall benefits and concerns associated with their application. Using the legal lens of European data protection rules, the thesis examines the requirements for the EU Member States when processing personal and sensitive data for Covid-19 apps.

Based on the legal analysis of the GDPR and the ePrivacy Directive, supported by various EU guidelines, the thesis demonstrates how the EU Member States can collect and process citizen's data according to regulations. The thesis finds that EU countries can use these apps to save lives, while also achieve adequate data protection for users by adhering to legal obligations stipulated in the GDPR and ePrivacy Directive and by adopting several ethical recommendations.

Keywords: Covid-19, Mobile Phone Data, Data Protection, GDPR, Personal and Sensitive Data

Deutscher Abstract

Seit Beginn der Covid-19-Pandemie versuchen Behörden und Regierungen diese Gesundheitskrise zu bekämpfen, indem sie soziale Distanzierung empfehlen, Reisebeschränkungen erklären und Quarantänemaßnahmen einführen. Wir erleben auch eine vermehrte Nutzung von digitaler Überwachung und Entwicklung von Handy-Apps, die zwar unterschiedliche Funktionen aufweisen, aber alle zur Bekämpfung der Pandemie beitragen sollen. Unter Verwendung eines doktrinären Ansatzes befasst sich diese Masterarbeit mit der Einführung von Covid-19-Apps, die persönliche und sensible Daten verarbeiten, um die Ausbreitung des Covid-19-Virus zu analysieren, die Bewegungen von Personen nachvollziehen zu können und Übertragungsketten rückzuverfolgen. Diese Masterarbeit konzentriert sich auf die europäischen rechtlichen Rahmenbedingungen und verweist sowohl auf EU-weite als auch auf internationale App-Entwicklungen, um die großen Unterschiede zwischen diesen hervorzuheben und die allgemeinen Vorteile und Bedenken der Anwendung von Apps zu demonstrieren. Unter Berücksichtigung der rechtlichen Aspekte der europäischen Datenschutzbestimmungen untersucht die Arbeit die Anforderungen, die an die EU-Mitgliedstaaten bei der Verarbeitung personenbezogener und sensibler Daten für Covid-19-Apps gestellt werden.

Basierend auf der rechtlichen Analyse der Datenschutz-Grundverordnung (DSGVO) und der Datenschutzrichtlinie für elektronische Kommunikation, unterstützt von verschiedenen EU-Richtlinien, zeigt diese Masterarbeit wie die EU-Mitgliedstaaten Bürgerdaten gemäß den Vorschriften sammeln und verarbeiten können. Die Arbeit stellt fest, dass EU-Länder diese Apps nutzen können, um Leben zu retten und gleichzeitig einen angemessenen Datenschutz für Benutzer zu erreichen, indem sie die in der Datenschutz-Grundverordnung und der Datenschutzrichtlinie für elektronische Kommunikation festgelegten gesetzlichen Verpflichtungen einhalten und verschiedene moralische Empfehlungen übernehmen.

Schlagwörter: Covid-19, Handy-Apps, Datenschutz, DSGVO, Persönliche und Sensible Daten

Table of Contents

List of Figures	IV
Abbreviations	V
1. Introduction.....	1
2. The Use of Mobile Phone Data during Crises.....	2
2.1. The Covid-19 Crisis: An Overview	4
2.2. Mobile Phone Apps During Covid-19	6
2.2.1. Use of Sensitive Data.....	7
2.2.2. Use of Personal Data	9
2.2.3. Noteworthy Contact-Tracing Developments	14
3. Between Data Protection and Saving Lives	20
3.1. Reasons for Using Mobile Phone Apps	21
3.2. Shortcomings Associated with the Use of Mobile Phone Apps.....	22
3.3. Legal Landscape for Processing Data	25
3.3.1. GDPR and ePrivacy: The Principle of <i>Lex Specialis</i>	26
3.3.2. General Principles for the Processing of Data	28
3.3.3. Public or Private Data Controllers	30
3.3.4. Processing Personal Data.....	31
3.3.5. Processing Sensitive Data.....	34
3.3.6. Processing Carried Out for Research Purposes.....	37
3.3.7. ePrivacy Directive	38
3.4. Recommendations for Using Mobile Phone Apps during Covid-19.....	40
3.4.1. Voluntary Use of Apps	41
3.4.2. Limiting Intrusive Data.....	42
3.4.3. Respecting Time Limitation	42
3.4.4. Use of Anonymized Data.....	43
3.4.5. National Health Authorities as Controllers of the App	43
3.4.6. Ensuring Citizens' Trust in Governments and Public Authorities	44
3.4.7. Achieving Interoperability	44
4. Conclusion.....	45
5. Bibliography	47

List of Figures

Figure 1. Map Indicating the Total Number of Cases as of July 25, 2020	4
Figure 2. Number of Confirmed Covid-19 Cases (30 December 2019 – 25 July 2020)	5
Figure 3. TraceTogether App Logo	15
Figure 4. Centralized and Decentralized Approach	18
Figure 5. Stopp Corona App Logo	19

Abbreviations

API	Application Programming Interface
CDR	Call Detail Records
CJEU	Court of Justice of the European Union
ECJ	European Court of Justice
EDPB	European Data Protection Board
EU	European Union
GDPR	General Data Protection Regulation
GPS	Global Positioning System
PEPP-PT	Pan-European Privacy Preserving Proximity Tracing Initiative
PHEIC	Public Health Emergency of International Concern
WHO	World Health Organization

1. Introduction

“You cannot fight a fire blindfolded. And we cannot stop this pandemic if we don’t know who is infected.”¹

Dr. Tedros Adhanom Ghebreyesus (Director General of the World Health Organization)

The Covid-19 virus, also formally known as Severe Acute Respiratory Syndrome Coronavirus 2 (SARS-CoV-2), poses exceptional challenges and has impacted everybody’s life since its outbreak in Wuhan, People’s Republic of China, at the end of 2019.² While the disease continues to disperse rapidly across the world, governments and public health authorities in the European Union (EU) and worldwide are determined to combat the crisis. As a treatment for the virus has yet to be discovered, the current tools implemented in various countries include quarantine and travel restrictions, practices of social distancing and the mandatory wearing of masks. Since the beginning of the pandemic, there has also been an increase in the use of digital surveillance and mobile phone applications (‘apps’) as an additional measure to fight the Covid-19 pandemic. The apps exhibit different functionalities; but within the EU, there has been a shift towards the use of apps that process location data to track individuals’ movements and gather proximity data to conduct contact tracing. While all of these apps aim to combat the Covid-19 crisis, they have also received a great deal of criticism, especially regarding data protection concerns.

The use of mobile phone apps during the Covid-19 pandemic raises multiple questions on the type of data that can be collected and the way it can be processed, that is, while considering the European rules and regulations concerning personal data protection. Throughout recent years, the EU has recognized various limitations to data exploitation and as a response, the General Data and Protection Regulation (EU) 2016/679 (GDPR) came into force in 2018, which constitutes ground-

¹ ‘WHO Director-General’s Opening Remarks at the Media Briefing on COVID-19 - 16 March 2020’ <<https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---16-march-2020>>.

² ‘Timeline of WHO’s Response to COVID-19’ (*World Health Organization*, 29 June 2020) <<https://www.who.int/news-room/detail/29-06-2020-covidtimeline>> accessed 17 July 2020.

breaking standards for protection. The GDPR, together with the Directive 2002/58/EC (“ePrivacy Directive”), provide for specific rules regarding the use of citizen’s data. While various shortcomings, including data protection concerns, continue to exist, there are also several benefits associated with extracting useful data from mobile phone apps, including an increased chance to save lives. Hence, this dissertation attempts to answer the following main research question: **How can EU Member States process citizens’ personal and sensitive data in mobile phone applications to counteract the COVID-19 pandemic while safeguarding the data protection laws stipulated in the GDPR and ePrivacy Directive?**

To answer the essential research question, this thesis commences with an overview of the Covid-19 virus and transcends into a comprehensive discussion about mobile app technology, in particular, the divergent functionality of apps in processing location data and performing contact tracing tools, and their overall relevance during the Covid-19 pandemic. Following the discussion on noteworthy and recent developments of apps, the subsequent section proceeds to highlight various benefits, as well as shortcomings, associated with the use of such apps. Relevant to the main concern about individuals’ data protection, the thesis examines the legal landscape for processing personal and sensitive data in mobile phone apps by exploring several general principles embedded in the GDPR and the ePrivacy Directive and by discussing the various legal bases for processing incorporated in these two legislative acts. Finally, the last section explores various recommendations for using Covid-19 apps and demonstrates how the EU Member States can legally, as well as ethically, use location data and contact tracing tools to combat the crisis.

2. The Use of Mobile Phone Data during Crises

Over the years, human mobility has increased and contributed to a rapid spread of infectious diseases worldwide. Various recent studies highlight the significance of mobile phone data to measure human mobility and the results can help in analysing the dispersion of diseases.³ Mobile phone penetration, referring to the existing number of SIM cards, is steadily increasing, even in

³ Shengjie Lai and others, ‘Measuring Mobility, Disease Connectivity and Individual Risk: A Review of Using Mobile Phone Data and MHealth for Travel Medicine’ [2019] Journal of Travel Medicine 2.

developing countries, and is expected to rise to 6 billion users by 2025.⁴ Without any doubt, mobile phones play a vital role in today's world and can serve as a powerful tool to collect information on people's movements. Mobile phone data, especially call detail records (CDR), which contain entries for calls and texts made or received, have been used to investigate transmission patterns during past health crises, such as malaria, cholera, rubella, Ebola and HIV infections.⁵

Taking the Ebola crisis as an example, the virus spread within the population through human-to-human transmission, arrived in West Africa in 2013, and dispersed rapidly across Guinea, Sierra Leone, Nigeria and Senegal.⁶ A group within the United States Agency for International Development stated that the lack of available data concerning this disease and the spread thereof can have a negative impact on the epidemic response, hence stressing the importance of data access during a global health emergency.⁷ Human mobility is one major driver of the Ebola epidemic and models, using CDRs, can help to reveal travel routes and volume of interactions between different populations; therefore, the "value of these data in the context of a public health emergency like the ongoing Ebola outbreak is undeniable."⁸

Infectious diseases, such as the Ebola virus, as well as the new Covid-19 crisis, pose a growing threat and require improvements in digital surveillance and global coordination.⁹ Exactly for new virus outbreaks, such as the Covid-19, for which official predictions and statistics are insufficient, digital data, specifically mobile phone data, can be a helpful source of information.¹⁰ Before delving into a discussion on mobile phone data collected and the various types of mobile phone apps developed during the past months, I first provide an overview of the Covid-19 crisis.

⁴ *ibid.*

⁵ *ibid* 5.

⁶ The Ebola crisis is an often fatal disease, it first appeared in 1976 and the 2014-2016 Ebola outbreak in West Africa has been the biggest outbreak so far; for more information on the Ebola disease, see: <https://www.who.int/news-room/fact-sheets/detail/ebola-virus-disease>

Amy Wesolowski and others, 'Commentary: Containing the Ebola Outbreak - the Potential and Challenge of Mobile Network Data' [2014] PLOS Currents 3.

⁷ 'Can Digital Health Help Stop the Next Epidemic?' [2019] Center for Strategic & International Studies.

⁸ Wesolowski and others (n 6).

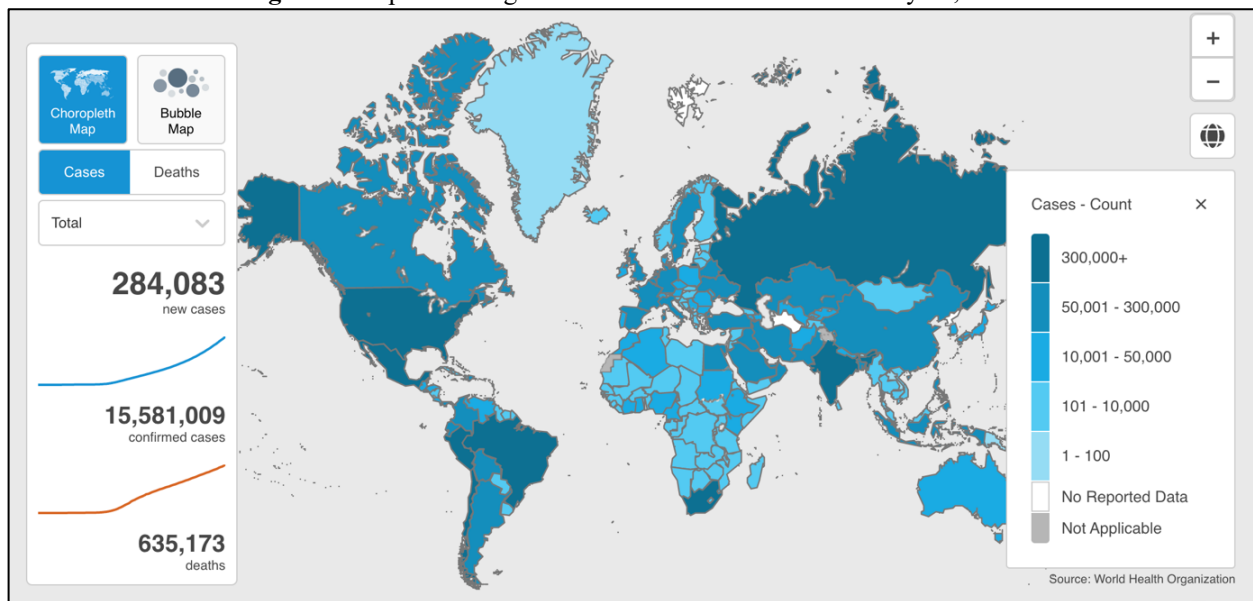
⁹ Caroline Buckee, 'Improving Epidemic Surveillance and Response: Big Data Is Dead, Long Live Big Data' (2020) 2 Lancet Digital Health.

¹⁰ Effy Vayena and Marcello Ienca, 'On the Responsible Use of Digital Data to Tackle the COVID-19 Pandemic' (2020) 26 Nature Medicine 458, 463.

2.1. The Covid-19 Crisis: An Overview

On December 31, 2019, the Wuhan Municipal Health Commission published a media statement on their website referring to various cases of ‘viral pneumonia’ in the city of Wuhan.¹¹ Over the next few days and weeks, more detailed information had been released and as the numbers of infections and deaths grew rapidly worldwide, the World Health Organization (WHO) declared the outbreak of the pandemic a Public Health Emergency of International Concern (PHEIC) on January 30, 2020.¹² As of July 25, 2020, the WHO records 15 581 009 cases of Covid-19 worldwide and counts a total of 635 173 deaths.¹³ Figure 1. highlights the regions that are greatly affected by the Covid-19 virus by indicating the number of cases with a different shade of blue in the respective countries.

Figure 1. Map Indicating the Total Number of Cases as of July 25, 2020



Source: World Health Organization¹⁴

There is no doubt that the Covid-19 pandemic has changed and impacted everyone's life and has challenged public authorities and governments to respond with measures to keep their citizens

¹¹ 'Timeline of WHO's Response to COVID-19' (n 2).

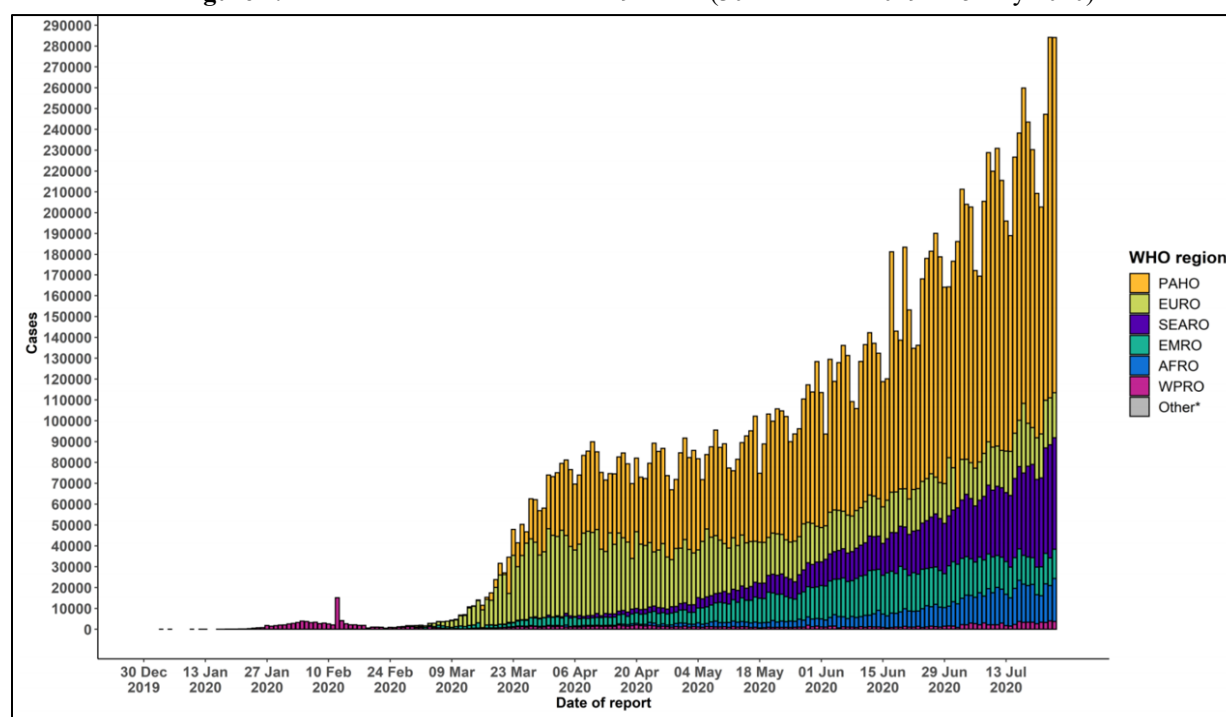
¹² Nadeem Ahmed and others, 'A Survey of COVID-19 Contact Tracing Apps' [2020] IEEE Access 1.

¹³ 'Coronavirus Disease (COVID-19) Situation Report – 187' (World Health Organization 2020) <https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200725-covid-19-sitrep-187.pdf?sfvrsn=1ede1410_2>.

¹⁴ 'WHO Coronavirus Disease (COVID-19) Dashboard' <<https://covid19.who.int>> accessed 26 July 2020.

healthy and safe. To decelerate the spread of the virus, lockdowns have been put into place and self-isolation and social distancing has been recommended to limit people's mobility.¹⁵ While having a lower mortality rate than previously known viruses such as SARS and MERS, Covid-19 is a highly infectious disease and a positive tested person can infect many more before even showing any symptoms.¹⁶ According to the WHO, infected people can transmit the virus via various forms of transmission, such as a droplet, airborne, fomite and bloodborne transmission.¹⁷ Current evidence suggests that most transmissions happen between people who have been in direct or indirect contact through infected secretions, such as saliva or through respiratory droplets, which are ejected when the Covid-19 positive person sneezes, coughs and talks.¹⁸ As indicated in Figure 2., the transmission of the virus is steadily increasing and the number of confirmed cases is rising.

Figure 2. Number of Confirmed Covid-19 Cases (30 December 2019 – 25 July 2020)



Source: WHO Situation Report 187¹⁹

¹⁵ Ahmed and others (n 12) 1.

¹⁶ *ibid.*

¹⁷ 'Transmission of SARS-CoV-2: Implications for Infection Prevention Precautions' (World Health Organization 2020) Scientific Brief 1.

¹⁸ *ibid* 5.

¹⁹ 'Coronavirus Disease (COVID-19) Situation Report – 187' (n 13).

Taking the high infection rate into account, countries try to detect Covid-19 positive individuals as early as possible, to isolate them before disseminating the virus further, and eventually to decelerate the spread of the disease. This led to a rise in the development of apps, which collect and process personal data, to track individuals who are Covid-19 carriers and to alert people who have been in close surroundings of infected people and hence are prone to contract the virus. As mentioned earlier, the use of digital surveillance and mobile phone data has already proven to be effective in previous health crises, such as the Western Africa Ebola crisis, and can be of relevance to combat the crisis in addition to conventional measures, such as quarantine restrictions, regional lockdowns and social distancing that control people's mobility.²⁰ The ensuing subsection shows some examples of different methods and types of apps worldwide and highlights, in particular, the widespread use of location data and contact tracing tools, especially deployed in European countries.

2.2. Mobile Phone Apps During Covid-19

When analysing Covid-19 mobile phone apps, it is essential to keep in mind that these are not all the same. On the contrary, they can differ in collected data (health data, location data, proximity data), data sources (GPS, Bluetooth), data handling (centralized and decentralized approach), as well as countries' data protection laws.²¹ Some apps collect very sensitive data, such as health data, others focus on personal data, including location data or the use of proximity data to allow for so-called 'contact tracing'.

There is currently little to no harmonization or collaboration in the development of these applications, neither worldwide nor within Europe.²² To provide a comprehensive understanding of how these apps work, this thesis will, in addition to European developments, also explore some non-EU mobile phone apps to highlight the diversity in this field. These examples will also help in explaining certain functionalities and methods of apps that primarily exist outside Europe, in

²⁰ Vayena and Ienca (n 10).

²¹ Robert Ranisch and others, 'Ethics of Digital Contact Tracing Apps for the Covid-19 Pandemic Response' (Kompetenznetz Public Health COVID-19 2020) 3.

²² Aida Ponce Del Castillo, 'COVID-19 Contact-Tracing Apps: How to Prevent Privacy from Becoming the next Victim' (2020) 5 ETUI.

particular in East Asia. It is important to understand what data the app collects and how this information is managed because depending on the type of data, the underlying legal provisions for processing such data differ. The GDPR differentiates between ‘personal’ and ‘sensitive’ data; the ensuing subsection provides some examples and hence, offers some insight into these two categories.

2.2.1. Use of Sensitive Data

According to Article 9 of the GDPR, sensitive data, also known as special categories of data, include racial and ethnic origin, political opinions, sexual orientation, genetic and biometric data, as well as data concerning health.²³ Especially concerning is the collection of health data in Covid-19 apps. As such, any health information, which can include knowledge about a person’s blood type, medical conditions and even temperature records, is private by nature and discloses sensitive details about somebody’s life.²⁴

Various countries decided to publish health data as a way to allow its population to evaluate whether somebody had been in contact with a Covid-19 positive individual; even though names were not included, the information that was published was often enough to identify infected people.²⁵ For example, in Argentina, a newspaper printed a list of Covid-19 infected people, containing their age, the name of the hospital where they stayed and their places of recent travel.²⁶ In India, at least two state governments uploaded a list of people who contracted the virus, containing their names, home addresses and latest travel destinations, which was accessible to

²³ 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 (General Data Protection Regulation) (OJ 2016 L 119/1), Art. 9.

²⁴ ‘Recommendations on Privacy and Data Protection in the Fight Against COVID-19’ (Access Now 2020) 5 <<https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf>> accessed 23 April 2020.

²⁵ *ibid.*

²⁶ *ibid* 6.

anybody.²⁷ Various countries, to be specific in East Asia, including China, Singapore and South Korea decided to actively deploy technology that collects such sensitive data.²⁸

2.2.1.1. Apps Using Data Concerning Health

An example for an app collecting very private and sensitive data is the “Health Code” app, a project launched by the Chinese government together with Ant Financial, an affiliate company of the giant Alibaba Group.²⁹ China requires its citizens to install this app, which tracks their movements and generates a colour coded system assigning red, yellow or green codes depending on the person’s health status and travel history; users with green codes are allowed to travel freely within the country, yellow codes signify that the individual should be in-home isolation and red codes imply that the individual has been infected with Covid-19 and should be quarantined.³⁰ The app also offers QR codes, referring to the different colour scheme, that can be scanned by authorities at any time and even restaurants and grocery shops can ask citizens to display codes before entering the respective establishment.³¹

The app arguable relies on users to provide contact and passport details, as well as recent travel history and medical files.³² However, neither the Chinese authorities nor the developing company has to this point clarified how the system works and this lack of transparency has understandably caused fear and confusion among the Chinese population.³³ The design, technology and type of data involved with China’s “Health Code” app raises various concerns about privacy and data protection. While it seems that Chinese authorities accept a grave intrusion into a person’s life,

²⁷ *ibid.*

²⁸ Yasheng Huang, Meicen Sun and Yuze Sui, ‘How Digital Contact Tracing Slowed Covid-19 in East Asia’ [2020] *Harvard Business Review* <<https://hbr.org/2020/04/how-digital-contact-tracing-slowed-covid-19-in-east-asia>> accessed 26 July 2020.

²⁹ Paul Mozur, Raymond Zhong and Aaron Krolik, ‘In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags’ *The New York Times* (1 March 2020) <<https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html>> accessed 14 July 2020.

³⁰ Helen Davidson, ‘China’s Coronavirus Health Code Apps Raise Concerns over Privacy’ *The Guardian* (1 April 2020) <<https://www.theguardian.com/world/2020/apr/01/chinas-coronavirus-health-code-apps-raise-concerns-over-privacy>> accessed 13 June 2020.

³¹ *ibid.*

³² *ibid.*

³³ Mozur, Zhong and Krolik (n 29).

such measures and this level of surveillance and privacy invasion would hardly be possible in Europe because of strict data protection rules.

With the first Covid-19 death in France and the growing number of positive cases in Italy in February 2020, the concern about the pandemic grew and the interest in using technologies and mobile phone apps increased in European countries as well.³⁴ However, in Europe, the majority of the apps developed or, at least, proposed attempts to decrease the amount of sensitive data amassed and focuses primarily on systems that collect location data and support contact tracing tools to conform with relevant regulations and to gain citizen's trust.

2.2.2. Use of Personal Data

Data that is stored on phones refers to information related to an individual, and even though encrypted, can be linked to a natural person, hence amounting to personal data.³⁵ The concept of personal data is very broad and is understood as information concerning an identified or identifiable person. According to Art. 4(1) of the GDPR, “‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, *location data*, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person [emphasis added].”³⁶ In the past there has been some doubt whether location data falls within the category of personal data, but the GDPR has removed any uncertainty by referring explicitly to ‘location data’ in its provision.³⁷

Even proximity data based on Bluetooth technology, which uses radio waves to locate devices nearby and sends out identifier beacons, seems to fall within the meaning of personal data. Recital

³⁴ Klaudia Klonowska, ‘The COVID-19 Pandemic: Two Waves of Technological Responses in the European Union’ [2020] The Hague Centre for Strategic Studies.

³⁵ Laura Bradford, Mateo Aboy and Kathleen Liddell, ‘COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR and Data Protection Regimes’ [2020] Journal of Law and the Biosciences 4.

³⁶ EU General Data Protection Regulation (GDPR), Art. 4(1).

³⁷ ‘ETNO: Study on the Revision of the EPrivacy Directive’ (DLA Piper 2016) 22

<https://etno.eu/datas/publications/studies/DPTS_Study_DLA_04082016_ePrivacy_Final.pdf>.

30 of the GDPR also states that natural persons could be linked to these identifiers and radio frequency identification tags if these are associated with other information received and may, therefore, allow to produce profiles and recognize users.³⁸ As a consequence, location data and data resulting from Bluetooth technology and identifier beacons, such as proximity data, fall within the category of personal data and hence, the processing of such data needs to comply with the GDPR provisions.

According to Klaudia Klonowska, the development of apps in Europe can be explained with a reference to two waves: in the first wave in early March 2020, the EU Member States, including Austria, Belgium, France and Germany aimed at sharing anonymized phone location data; in the second wave, at the end of March, their focus shifted towards promoting contact tracing apps.³⁹ These two approaches will be discussed in more detail below. It is essential to recall that based on the interpretation of the GDPR both, geolocation tracking and proximity signals, that are usually installed on any phone, fall within the category of personal data since the information can relate to an ‘identifiable’ natural person.⁴⁰

2.2.2.1. Apps Using Location Data

Tracking and analysing the location data by using mobile phones has increasingly become an interesting solution to the pandemic. Location data refers to all data indicating the geographical position of a user’s equipment. The use of location data allows for analysing the geographical spread of the virus, tracking the movement of infected people and determining whether people have been complying with quarantine requirements or social distancing measures that have been imposed in countries.⁴¹ Additionally, the analysis of such data can offer further insight into the effectiveness of actions and can identify “hot spots” for transmissions.⁴²

³⁸ EU General Data Protection Regulation (GDPR), Recital 30.

³⁹ Klonowska (n 34).

⁴⁰ Bradford, Aboy and Liddell (n 35) 4.

⁴¹ ‘Mobile Location Data and Covid-19: Q&A’ (*Human Rights Watch*, 13 May 2020)

<<https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa>> accessed 26 June 2020.

⁴² *ibid.*

Location data comes from various sources, such as cell towers (or cell sites), global positioning system (GPS) and Bluetooth beacons; while cell towers and GPS can detect the actual location, hence raw numbers on longitude and latitude, Bluetooth communicates with nearby devices to calculate proximity and therefore can be the preferred and less intrusive tool to track interactions, as is the case for contact tracing.⁴³ In other words, apps that focus solely on extracting the precise location of the individual use a cell phone network data, GPS or Wi-Fi signals to detect geolocations.⁴⁴ In contrast, most Covid-19 apps use Bluetooth to determine the distance between phones and based on the proximity and duration of proximity, the possible exposure to an infected individual can be specified.⁴⁵ To avoid any confusion, and for the purpose of this research, data on exact geolocation extracted from GPS is referred to as location data, and data obtained from Bluetooth technology to calculate the distance to other individual's phones is understood as proximity data.

One European example of an app that uses geolocation data is the StopCovid19 Cat app in Spain. This app records contact details, such as the user's telephone number, health data, including the individual's answers about symptoms, and location data.⁴⁶ The app, therefore, collects the exact latitude and longitude from the user's phone; app developers argue that the geolocations are necessary for the adequate function of the app; in other words, it is essential to know the exact coordinates in case emergency services need to be notified, Covid-19 tests have to be delivered or maps identifying areas with a high number of cases need to be created.⁴⁷

Another app based on location data by using GPS technology is the Self-Quarantine Safety Protection app, developed by the Ministry of the Interior and Safety in South Korea, which collects GPS to monitor the user's exact location and track Covid-19 positive individuals.⁴⁸ With this app, government officials can follow every movement of self-quarantined users to verify whether they

⁴³ *ibid.*

⁴⁴ Robert A Kleinman and Colin Merkel, 'Digital Contact Tracing for COVID-19' (2020) 192 *Canadian Medical Association Journal* 653.

⁴⁵ *ibid.*

⁴⁶ 'STOP COVID19 - Digital Health Platform to Stop SARS Cov-2' (*STOP COVID19*) <<https://stopcovid19.cat/en/stop-covid19-cat/>> accessed 31 July 2020.

⁴⁷ *ibid.*

⁴⁸ Ponce Del Castillo (n 22) 2.

comply with quarantine or social distancing measures; it also collects personal data, such as date of birth, gender, nationality, mobile phone number, address of quarantine and Korea Centre for Disease Control Prevention confesses that they are using “GPS data, surveillance camera footage, and credit card transactions to recreate their route a day before their symptoms showed.”⁴⁹ The Guardian has called South Korea’s approach “more scary than Coronavirus.”⁵⁰

Individuals who have tested positive have to report symptoms to the officials twice a day and if quarantine measures are breached, an alarm is activated and users can face monetary fines or imprisonment for disobeying.⁵¹ Further, this app also allows for the sharing of personal information about the infected individual by text message to other people who may have been in contact with the Covid-19 positive person.⁵² When a person tests positive, the app sends out text messages with a link to a website that offers a list of places the infected person had visited before catching the virus.⁵³ Citizens are increasingly worried that suddenly their life is on display for everybody to see and the text messages do not only release public health information but even uncover extra-marital affairs.⁵⁴ Using GPS and revealing exact geolocations can expose too much personal information that can be considered unnecessary in fighting the Covid-19 crisis, therefore, various EU Member States instead focus on contact tracing tools with the use of Bluetooth technology.

2.2.2.2. *Contact Tracing Apps*

Contact tracing is a process of identifying and alerting individuals who have been in contact or near a possible Covid-19 carrier to check possible risks of infection.⁵⁵ As mentioned before, Covid-19 is a highly infectious disease and a person carrying the Covid-19 virus can also spread the virus

⁴⁹ ‘Coronavirus Privacy: Are South Korea’s Virus Alerts Too Revealing?’ *BBC News* (5 March 2020) <<https://www.bbc.com/news/world-asia-51733145>> accessed 9 July 2020.

⁵⁰ Nemo Kim, “‘More Scary than Coronavirus’: South Korea’s Health Alerts Expose Private Lives’ *The Guardian* (6 March 2020) <<https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives>> accessed 25 July 2020.

⁵¹ Ponce Del Castillo (n 22) 2.

⁵² Kleinman and Merkel (n 44) 655.

⁵³ Kim (n 50).

⁵⁴ *ibid.*

⁵⁵ ‘Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak’ (European Data Protection Board 2020) 3.

without showing symptoms; according to Dutch researchers, pre-symptomatic transmissions of Covid-19 is as high as 48% for Singapore and 62% for Tianjin, China.⁵⁶ These estimates add to the complexity of the Covid-19 spread and increase challenges for tracing efforts.

Traditionally, contact tracing has often been done by conducting interviews with infected people about their whereabouts, and health authorities can then contact identified individuals and recommend self-quarantine measures and treatment to potential virus carriers.⁵⁷ This method had been successful in previous health crises, such as the Ebola virus, however, it is now understood that the old-fashioned approach is time- and labour- intensive and relies on human recollection, which is not always accurate and can cause recall errors that further hamper essential identification of possible infected people.⁵⁸ Therefore, mobile data can aid in painting a more accurate picture and can be a helpful method to detect potentially infected people.⁵⁹ Further, digital contact tracing can reduce some shortcomings experienced in the traditional contact tracing method, such as notification delay and limited identification of unfamiliar people in public spaces.⁶⁰

As emphasized earlier, most mobile phone applications developed by European countries are based on Bluetooth technology that focuses on ‘proximity’ tracking to calculate the distance to others. For this, there is no need to know the exact geolocation. According to the European Data Protection Board (EDPB), the EU body in charge of the application of the GDPR, for contact tracing apps the use of location data is neither required nor recommended, but proximity data should be used.⁶¹ In other words, the information gathered from proximity data, together with the duration of contact with others, which can be transmitted with Bluetooth technology, is enough to efficiently conduct contact tracing and to yield results.

⁵⁶ Frank Diamond, ‘Asymptomatic Carriers of COVID-19 Make It Tough to Target’ (*Infection Control Today*) <<https://www.infectioncontrolday.com/article/asymptomatic-carriers-covid-19-make-it-tough-target>> accessed 13 June 2020.

⁵⁷ Kleinman and Merkel (n 44) 653.

⁵⁸ *ibid.*

⁵⁹ Costica Dumbrava, ‘Tracking Mobile Devices to Fight Coronavirus’ (European Parliamentary Research Service 2020) Briefing 4.

⁶⁰ Kleinman and Merkel (n 44) 653.

⁶¹ ‘Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak’ (n 55) 7.

How does contact tracing via Bluetooth technology work? In brief, when Bluetooth is turned on, our mobile phone detects nearby devices by using radio waves; then it sends out a string of random characters, known as ‘identifier beacons’ with Bluetooth Low Energy and the phones in close distance can make a time-stamped record of that identifier.⁶² Whenever a phone receives an identifier beacon it records that beacon on the phone.⁶³ The identifiers do not carry any information and they change every fifteen to twenty minutes for protection.⁶⁴ The ensuing subsection mentions various apps and software that rely on Bluetooth technology and have developed throughout the Covid-19 pandemic. These examples also demonstrate how Bluetooth technology can be of assistance in Covid-19 contact tracing apps.

2.2.3. Noteworthy Contact-Tracing Developments

With the vast amount of different mobile phone apps manufactured to fight the crisis, it is easy to lose track of significant developments and essential modifications in this area. While it has been emphasized before, it is important to keep in mind, that each app can differ in the collection of personal or sensitive data, technological features, motives for implementing the app and countries can have different systems, strategies and legal provisions in place for manufacturing apps. The examples listed below are some of the most essential and ground-breaking developments in the field of contact tracing since the beginning of the pandemic, starting with the TraceTogether App as one of the first apps focusing on Bluetooth technology, followed by new initiatives and collaborations that have divided the approach taken by European countries into two: on the one hand the centralized and on the other hand the decentralized approach.

2.2.3.1. *TraceTogether App*

One of the first contact tracing implementation and an app that has attracted much attention has been the TraceTogether App launched in by the Singaporean Ministry of Health on March 20,

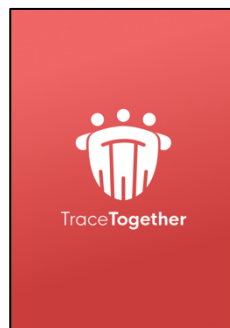
⁶² David Ingram, ‘Your Phone Could Track the Spread of Coronavirus. Here’s What You Should Know.’ (*NBC News*, 20 April 2020) <<https://www.nbcnews.com/tech/tech-news/how-contact-tracing-could-use-bluetooth-track-coronavirus-your-smartphone-n1187796>> accessed 11 July 2020.

⁶³ ‘Exposure Notification: Frequently Asked Questions’ (Apple and Google 2020) <https://blog.google/documents/73/Exposure_Notification_-_FAQ_v1.1.pdf>.

⁶⁴ *ibid.*

2020.⁶⁵ It is a Bluetooth-based app, which uses Bluetooth technology to detect nearby mobile phones and encrypts the data on the device, without collecting any user's location data.⁶⁶ Should a person have tested positive for Covid-19, the Ministry of Health will ask the individual to upload their required information to the app and the Ministry of Health then alerts the people who have been in close surroundings to the infected person.⁶⁷ While it seems that sharing personal information and health data is based on a voluntary basis, it is considered a crime in Singapore not to assist the Ministry of Health.⁶⁸

Figure 3. TraceTogether App Logo



Source: A Singapore Government Agency Website⁶⁹

The TraceTogether App has raised various privacy and data protection concerns. While users of the app are kept confidential from each other, the Singaporean government can, after the individual has released the personal data on the app, build a list and track the individual's contacts.⁷⁰ In general, this app puts a lot of trust and control in the Singaporean government's hand, which has been immensely criticized; while the government can have access to the list of individuals, privacy for users is almost non-existent.⁷¹ While countries such as Singapore, as well as South Korea and China, implement relatively radical approaches and policies, which can amount to infringements of fundamental rights from a European legal lens, there have been some efforts to develop

⁶⁵ Hyunghoon Cho, Daphne Ippolito and Yun William Yu, 'Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-Offs' 25 March 2020.

⁶⁶ Dumbrava (n 59) 5.

⁶⁷ Cho, Ippolito and Yu (n 65) 2.

⁶⁸ *ibid.*

⁶⁹ 'TraceTogether' <<https://www.tracetgether.gov.sg/>> accessed 4 August 2020.

⁷⁰ Cho, Ippolito and Yu (n 65) 2.

⁷¹ *ibid* 3.

initiatives that propose standards and technical features for greater user data protection in mobile phone apps.

2.2.3.2. Google/Apple Collaboration and the PEPP-PT Initiative

While there has been a major boom in new contact tracing apps all over the world, there have also been developments in software that aims to assist countries with the design and manufacture of these apps. Two opposing concepts have recently emerged: the Google/Apple Collaboration and the Pan-European Privacy-Preserving Proximity Tracing Initiative (PEPP-PT).

First, the PEPP-PT was launched on April 1, 2020, by an EU consortium comprising 130 members in eight EU Member States, namely Austria, Belgium, Denmark, France, Germany, Italy, Spain and Switzerland.⁷² The PEPP-PT developed a software code which can support the EU Member States and their national authorities in building Covid-19 contact tracing apps.⁷³ It was an effort of academics and developers to collaborate on a European level to create one single protocol; however, this attempt was disrupted by differing national interests, diverging privacy concerns, as well as, the establishment of the Google/Apple Initiative.⁷⁴

Second, on 10 April 2020, the two tech giants Google and Apple announced their collaboration and later launched their software on May 20, 2020, which aims to assist states, public health authorities and governments in developing applications that alert people when they come in contact with a Covid-19 positive person.⁷⁵ Similar to the PEPP-PT, they did not develop an app but created a so-called application programming interface (API), which they refer to as Exposure Notification, that enables interoperability between both iOS and Android devices using such contact tracing apps.⁷⁶

⁷² Ponce Del Castillo (n 22) 3.

⁷³ *ibid.*

⁷⁴ Javier Espinoza, Joe Miller and Leila Abboud, 'How Europe Splintered over Contact Tracing Apps' *Financial Times* (10 May 2020) <<https://www.ft.com/content/7416269b-0477-4a29-815d-7e4ee8100c10>> accessed 19 July 2020.

⁷⁵ Reed Albergotti, 'Apple and Google Launch Coronavirus Exposure Software' *Washington Post* (20 May 2020) <<https://www.washingtonpost.com/technology/2020/05/20/apple-google-api-launch/>> accessed 11 July 2020.

⁷⁶ Ponce Del Castillo (n 22) 3.

In practice, individuals who use API and decide to carry out contact tracing with an app, their devices produce proximity identifiers, which change about every 15 minutes.⁷⁷ These identifiers are then shared with other devices in close proximity via Bluetooth Low Energy; the identifiers do not disclose any information right away, however, if a user catches the Covid-19 virus, this person can choose to disclose the diagnoses in the app and people who have come into close contact will be alerted.⁷⁸ Several European countries developed and released apps based on the Exposure Notification API, such as the Austrian ‘Stopp Corona App’, Denmark’s ‘Smittestop’, and Germany’s Corona-Warn-App.’⁷⁹

There is one major difference between the Google/Apple Initiative and the PEPP-PT that has led to much debate. According to critics, the main issue with the PEPP-PT is that data is stored centrally.⁸⁰ In other words, this means that the centralized solution allows for data to be reported to a central server which is controlled by a national authority and this could amplify the risk that someone with access to the central server and who has enough willpower and knowledge could deanonymize data.⁸¹ This data protection concern encouraged scientists and researchers to criticize that method in an open letter and shortly after Google/Apple launched their software, some countries decided to switch to the Google/Apple Initiative which supports a decentralized approach to contact tracing; this was the case for Germany.⁸² With the decentralized approach, the data remains on the user’s phone and is not shared with national authorities or any other third parties.⁸³ Figure 3. highlights the differences between the centralized and decentralized approach.

⁷⁷ Aamir Siddiqui, ‘List of Countries Using Google and Apple’s COVID-19 Contact Tracing API’ (*xda-developers*, 26 June 2020) <<https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/>> accessed 11 July 2020.

⁷⁸ *ibid.*

⁷⁹ *ibid.*

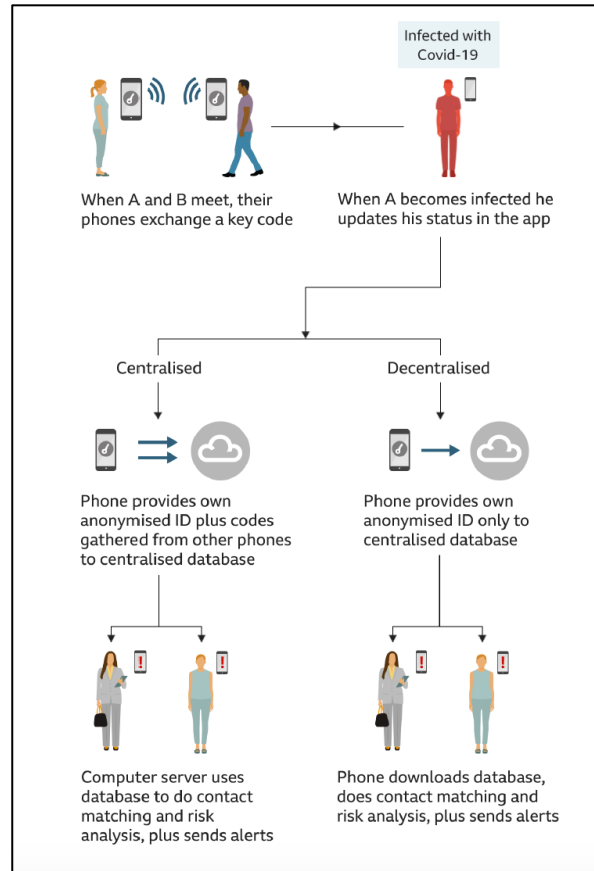
⁸⁰ Michael Baxter, ‘Centralised and Decentralised Contact Tracing Apps Creates Academic Split’ (*PrivSec Report*, 22 April 2020) <<https://gdpr.report/news/2020/04/22/centralised-versus-decentralised-contact-tracing-solutions-pit-privacy-academics-against-each-other/>> accessed 12 July 2020.

⁸¹ Elizabeth Grimwood-Taylor, ‘International: COVID-19 - Contact Tracing Apps - Differing Global Approaches’ (*Baker McKenzie*, 13 May 2020) <https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/international-covid-19-contact-tracing-apps-differing-global-approaches_1> accessed 12 July 2020; Baxter (n 80).

⁸² Douglas Busvine, ‘Germany Flips on Smartphone Contact Tracing, Backs Apple and Google’ *Reuters* (26 April 2020) <<https://www.reuters.com/article/health-coronavirus-europe-tech-idUSL3N2CE03Z>> accessed 12 July 2020; For open letter, see: ‘Joint Statement on Contact Tracing: Date 19th April 2020’ <https://www.mq.edu.au/__data/assets/pdf_file/0012/977493/Joint-Statement-on-Contact-Tracing.pdf>.

⁸³ Grimwood-Taylor (n 81).

Figure 4. Centralized and Decentralized Approach



Source: BBC⁸⁴

These privacy and data protection concerns with the centralized framework, the open letter by scholars criticizing it, and major tech industry players favouring the decentralized approach, could be the reasons that various countries currently support the solution without a central server by Google/Apple and will choose to do so in the future.⁸⁵ While the EDPB acknowledges both, the centralized and decentralized approach, it also admits that the decentralized system better conforms with the principle of data minimization incorporated in the GDPR. Hence, it appears to be the more favourable design from a European legal lens.

⁸⁴ Leo Kelion, 'Apple and Google's Covid-19 "Watershed Moment"' *BBC News* (20 May 2020) <<https://www.bbc.com/news/technology-52740131>> accessed 15 July 2020.

⁸⁵ Grimwood-Taylor (n 81).

2.2.3.3. *European Apps: Diverging Views*

Various European countries are attempting to follow the success of apps in Singapore and China while focusing on less intrusive measures and aiming to provide adequate user data protection and privacy. The approach to do so, however, even differs within Europe. Currently, most European countries including Germany, Austria, Italy and Switzerland favour the Google/Apple Initiative, while some others dismiss the suggestion by the EDPB and prefer homegrown technology to give their authorities more control, which is the currently the case for France and Norway.

For example, Austria was one of the first European countries to offer a functional app called “Stopp Corona”, developed together with the Austrian Red Cross and launched 25 March 2020. The app follows the Google/Apple system, which means that contacts between users are never reported to a central database.⁸⁶ The app uses Bluetooth beacons and does not record any location data.⁸⁷ Further, it saves encounters between people (‘digital handshakes’) that are less than 2 meters apart for longer than 15 minutes and stores these contacts anonymously. As soon as a user tests positive for Covid-19 and shares this information with the app, the app recalls all previous encounters from the past 54 hours and sends out warning messages, which are also anonymous.⁸⁸ Italy’s “Immun”i”, Germany’s “Corona-Warn App” and Switzerland’s “SwissCovid” apps work in a very similar manner.

Figure 5. Stopp Corona App Logo



Source: Google Play⁸⁹

⁸⁶ Philipp Wilhelmer, ‘Bumpy Second Attempt for New “Stopp Corona” App (Holpriger Zweiter Anlauf Für Neue “Stopp Corona”-App)’ *Kurier* (26 June 2020) <<https://kurier.at/wissen/neue-funktionen-zweiter-anlauf-fuer-stop-corona-app/400951679>> accessed 19 July 2020.

⁸⁷ *ibid.*

⁸⁸ *ibid.*

⁸⁹ ‘Stopp Corona - Apps on Google Play’ <https://play.google.com/store/apps/details?id=at.rotekreuz.stopcorona&hl=en_US> accessed 4 August 2020.

In contrast, France's "StopCovid" app follows a centralized approach as proposed by the PEPP-PT, which collects the data on a remote server that executes potential matching.⁹⁰ This approach has caused various controversy, However, French officials and advocates of the centralized approach argue that it allows health authorities to control and analyse data, therefore offering a better insight into the virus, and it gives France sovereignty by circumventing the rules imposed by Apple and Google.⁹¹ Other than the use of a central database, the procedures and aim of "StopCovid" are very similar to the Austrian, Italian and Swiss apps.

This section provided an overview of how the different apps work and illustrated the various developments worldwide. While countries such as China, Singapore and South Korea are opting to collect and process more private and sensitive data, while enforcing a specific degree of compulsion, European apps prefer to use proximity data instead of location data and very little to no sensitive data to safeguard user's data protection rights. While acknowledging these different functionalities of Covid-19 apps, it is also important to keep in mind that all of these apps have one goal in common: supporting the fight against the crisis. The subsequent section focuses on the reason for the existence of apps and how they can benefit in the battle against the Covid-19 pandemic, while also highlighting various concerns and shortcomings that have accompanied the development of apps since the beginning.

3. Between Data Protection and Saving Lives

According to Mila Romanoff, Data and Governance Lead for United Nations Global Pulse, "in emergencies like pandemics, privacy must be weighed against other considerations, like saving lives."⁹² During this Covid-19 pandemic, it has become evident that digital data and mobile phone apps, in particular contact tracing tools, can be a helpful additional measure to decelerate the spread

⁹⁰ Chris O'Brien, 'COVID-19 Tracing Apps Now Live in Germany, France, and Italy; U.K. Rethinks Its Plans' (*VentureBeat*, 19 June 2020) <<https://venturebeat.com/2020/06/19/covid-19-tracing-apps-now-live-in-germany-france-and-italy-u-k-rethinks-its-plans/>> accessed 19 July 2020.

⁹¹ Leo Kelion, 'France's Virus-Tracing App "off to a Good Start"' *BBC News* (3 June 2020) <<https://www.bbc.com/news/technology-52905448>> accessed 19 July 2020; O'Brien (n 90).

⁹² Natasha Singer and Choe Sang-Hun, 'As Coronavirus Surveillance Escalates, Personal Privacy Plummets' *The New York Times* (23 March 2020) <<https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html>> accessed 23 April 2020.

of the virus and eventually contain the Covid-19 pandemic. However, various concerns, mostly raised by citizens, hampers their widespread use. This section highlights some benefits, as well as several shortcomings, associated with the use of Covid-19 apps, especially those that focus on location tracking and contact tracing.

3.1. Reasons for Using Mobile Phone Apps

The use of mobile phone data can offer various benefits. First, it can grant access to population estimates and information on people's movements.⁹³ This can aid in understanding the geographic spread of the virus; it can also highlight some highly affected cities and even locate hotspot areas with greater infection risk. These hotspot areas can then be avoided, or a lockdown can be imposed. Second, various positive and negative effects of implemented measures can be explored.⁹⁴ This will help in answering what the impact of travel restrictions are and how social distancing has shaped the spread of the Covid-19 pandemic. Third, the gathered data helps to make predictions about future risks and opportunities.⁹⁵ All of these result in the key benefit of all: saving lives.

Currently, most mobile phones focus on contact tracing tools, which try to intervene in the chains of infections early before new hotspot areas emerge. The contact tracing tools give people the opportunity to be informed after they had been in contact with a Covid-19 positive person and allow them to take immediate action to isolate themselves before risking to infect friends, family, and especially, people considered as "high risk", for example, elderly and individuals with underlying health conditions. Further, mobile phone contact tracing is also a cost-effective and time-efficient alternative to the traditional form of contact tracing, which requires extensive interviews with patients. Hence, the main benefit of contact tracing is the possibility to offer a more reliable and quicker contact trace history and may limit the spread of the virus faster and efficiently.⁹⁶

⁹³ Nuria Oliver and others, 'Mobile Phone Data and COVID-19: Missing an Opportunity?' 3 <<https://arxiv.org/pdf/2003.12347.pdf>>.

⁹⁴ *ibid.*

⁹⁵ *ibid.*

⁹⁶ Klonowska (n 34) 9.

The use of surveillance and contact tracing has already proven to be effective in various countries. One example is Singapore, which implemented various measures aiming to contain the spread of the virus, such as, contact tracing tools and patient monitoring. According to a report by Centers for Disease Control and Prevention, the strong surveillance methods, in addition to social distancing and quarantine measures, helped to slow the increase of the outbreak, and hence saved lives.⁹⁷ Further, the report stated that such measures might help fight the Covid-19 pandemic in other countries as well.⁹⁸

3.2. Shortcomings Associated with the Use of Mobile Phone Apps

Technology can and should play a role in saving lives, but while acknowledging that these benefits are all relevant, there are still various concerns and shortcomings that overshadow the consistent application of location and contact tracing apps. Not only processing sensitive data has been denounced, but also collecting and analysing of location and proximity data for the fight against Covid-19 has often raised multiple concerns. Some of these shortcomings are listed in the following paragraphs.

First, while it is true that this health crisis requires countries' efforts worldwide, it has been highlighted that a surge in state surveillance could violate individual's rights and may lower trust in the government and public authorities.⁹⁹ Some public authorities seem to be overwhelmed with the sensitive situation of this crisis and often appear to be incompetent to process this highly complex information of health and location data without pre-defined procedures in place.¹⁰⁰ This lack of guidance has often led to delays in developing mobile phone apps and contact tracing tools and the incompetence has not been left unnoticed by the public. Further, Ms Romanoff argued that states should only collect and use data that is absolutely needed to fight the pandemic in order to

⁹⁷ Yixiang Ng and others, 'Evaluation of the Effectiveness of Surveillance and Containment Measures for the First 100 Patients with COVID-19 in Singapore — January 2–February 29, 2020' (Centers for Disease Control and Prevention 2020) Morbidity and Mortality Weekly Report 5.

⁹⁸ *ibid* 311.

⁹⁹ 'Joint Civil Society Statement: States Use of Digital Surveillance Technologies to Fight Pandemic Must Respect Human Rights' (Human Rights Watch 2020) Statement.

¹⁰⁰ Oliver and others (n 93) 8.

reduce the risk of state surveillance violating people's privacy.¹⁰¹ However, it is not easy for authorities to calculate and determine how much data is needed and enough.

Second, the effectiveness of apps depends massively on their adoption by citizens.¹⁰² In other words, they can only work properly and lead to meaningful results if a significant amount of people installs and uses the app. Research indicates that at least 60% to 75% of the population needs to activate the app to meet the threshold needed for effectiveness.¹⁰³ For example in Austria, as of early July 2020, only 600,000 users in a population of 8.75 million, which results in a mere 6.8%, have downloaded the app.¹⁰⁴ Additionally, while the downloading of the app is the first step, people actually have to use the app, including uploading the information if the user is contracted the virus and has tested positive. Further, apps can only identify infected and vulnerable people if both are using the app.¹⁰⁵ This also implies that the effectiveness is hindered if people who are unable or reluctant to use phones, including the elderly population who are considered 'high risk' in the Covid-19 crisis.¹⁰⁶

Third, even if the adoption of apps is extensive, it remains unclear how effective the use of location data and contact tracing actually is. Digital technologies and mobile phone apps cannot be expected to work without faults, and measurement errors can limit success even further.¹⁰⁷ For example, Bluetooth technology can experience significant fluctuations and signals can be weakened with the interference of people between the receiving and the transmitting phone.¹⁰⁸ Further, whereas 1-meter distance seems to be enough for the spread of Covid-19 between two individuals, mobile phones can usually only calculate an individual's position to an accuracy of seven to thirteen meters.¹⁰⁹ This sensitivity and the inability to fully rely on digital technology can, on the one hand,

¹⁰¹ Singer and Sang-Hun (n 92).

¹⁰² Kleinman and Merkel (n 44) 654.

¹⁰³ Klonowska (n 34).

¹⁰⁴ 'Austria Invites Suggestions to Improve Coronavirus Track and Trace App' *Reuters* (8 July 2020) <<https://www.reuters.com/article/healthcoronavirus-austria-apps-idUSL8N2EF1BB>> accessed 25 July 2020.

¹⁰⁵ Kleinman and Merkel (n 44) 654.

¹⁰⁶ *ibid.*

¹⁰⁷ *ibid.*

¹⁰⁸ *ibid.*

¹⁰⁹ Dumbrava (n 59) 4.

generate excessive worry and confusion in case of a false positive, or on the other hand, can lead to missing exposures and the lack of alarming possible carriers with a false negative.

Fourth, and for this research paper most importantly, the use of mobile phone apps and collecting and processing personal data raises various data protection concerns. For example, in South Korea, the Self-Quarantine Safety Protection app allows for the collection of personal data, such as gender, nationality, and mobile phone number and the Korean Centre for Disease Control Prevention even admits to collecting GPS data, surveillance footage and credit card transactions. If this were not enough, personal data of the Covid-19 positive person can then be shared by text message. The existence of such apps, which process this amount of sensitive data is unthinkable in Europe and could hardly be permitted in accordance with the European regulations on data protection, in particular the GDPR and the ePrivacy Directive.

Even the mere processing of geolocation and proximity data raises worries among citizens. According to Diego Naranjo, head of policy of European Digital Rights group, the use of GPS and other location data gives authorities “a very accurate description of your reality and who you are ... it should be avoided at all costs”¹¹⁰ Location data can be very informative and can reveal the user’s home address, places that were visited, including doctor appointments, and interactions with others; hence, suitable safeguards need to be in place to avoid pervasive surveillance. On April 17, 2020, the European Parliament adopted a resolution that “stresses that national and EU authorities must fully comply with data protection and privacy legislation, and national DPA oversight and guidance.”¹¹¹

The EDPB emphasized in a statement on March 19, 2020, that “[d]ata protection rules (such as the GDPR) do not hinder measures taken in the fight against the coronavirus pandemic”¹¹², however,

¹¹⁰ Umberto Bacci, ‘Digital Handshake: Can Contact Tracing Deliver on Its Promise in Coronavirus Battle?’ *Reuters* (5 May 2020) <<https://www.reuters.com/article/us-health-coronavirus-tech-trfn-idUSKBN22H254>> accessed 19 July 2020.

¹¹¹ European Parliament resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences (2020/2616(RSP)) 2020 (P9_TA(2020)0054), para.53; DPA stands for Data Protection Authorities.

¹¹² ‘Statement on the Processing of Personal Data in the Context of the COVID-19 Outbreak.’ (European Data Protection Board 2020) Statement

even during these exceptional times the protection of personal data must be guaranteed. The subsequent subsection inspects the legal frameworks that must be adhered, hence the legal obligations for the EU Member States, when processing personal and sensitive data within mobile phone apps.

3.3. Legal Landscape for Processing Data

While during the time of COVID-19, the collection and analysis of data is essential to monitor the spread of the virus and protection laws should not hinder the fight against the Covid-19 pandemic, the EDPB also clearly stressed that data protection laws continue to exist and have to be upheld.¹¹³ In the EU, the right to data protection, which concerns the protection of any information relating to an identified or identifiable natural (living) person, is a fundamental right guaranteed by Article 8 of the Charter of Fundamental Rights of the EU. Accordingly, “[e]veryone has the right to the protection of personal data concerning him or her.”¹¹⁴

The EDPB further emphasized that the GDPR, as well as the ePrivacy Directive, include specific rules for the use of personal data, such as location data, to support public authorities in observing and repressing the spread of the virus.¹¹⁵ The GDPR itself guarantees in Article 1(2) that it “protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.”¹¹⁶ This research focuses on the applicability of these two frameworks to the issue at hand.

The implementation of the GDPR allowed for new developments and breakthroughs in the field of data protection. The GDPR, which came into effect on May 25, 2018, repealed the Directive 95/46/EC and with it aimed to increase harmonization within the EU and to provide a higher level

<https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf>.

¹¹³ *ibid.*

¹¹⁴ Charter of Fundamental Rights of the European Union 2012 (2012/C 326/02), Art. 8(1).

¹¹⁵ ‘Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak’ (n 55) 3.

¹¹⁶ EU General Data Protection Regulation (GDPR), Art. 1(2).

of protection.¹¹⁷ However, despite the fact that a regulation is directly applicable in all EU Member States, the GDPR permits each country to enact some restrictions or specifications which led to divergent national regimes in privacy and data protection rules.¹¹⁸ In general, the GDPR establishes rules and principles relating to the protection of natural persons concerning the processing of personal data in regard to the free movement of such data within the EU.¹¹⁹

The ePrivacy Directive entered into force in 2002, it has been updated in 2009, and as a directive, in comparison to a regulation, the Member States are free to devise the rules on how to achieve the goal. The ePrivacy Directive stipulates certain rules for tracking and monitoring Internet users and securing personal data in electronic communications. Therefore, it can be assumed that the ePrivacy Directive has more specific rules with regard to the electronic communication sector than the GDPR.¹²⁰ The interaction between these two frameworks has often been discussed and the ensuing subsection sheds light on their co-existence and relevance in regard to the matter at hand.

3.3.1. GDPR and ePrivacy: The Principle of *Lex Specialis*

Case law of the Court of Justice of the European Union (CJEU) suggests that processing activities can fall within the scope of both, the GDPR and the ePrivacy Directive.¹²¹ In Article 1(2), the ePrivacy Directive states that “the provisions of this Directive *particularize* and *complement* Directive 95/46/EC [emphasis added].”¹²² Whilst the Data Protection Directive, Directive 95/46/EC, was the predecessor to the GDPR, the analysis undertaken by the CJEU and the Article 29 Working Party remain relevant to both, the preceding Directive, as well as the GDPR.¹²³

¹¹⁷ Kristina Yuliyanova Chakarova, ‘General Data Protection Regulation: Challenges Posed by the Opening Clauses and Conflict of Laws Issues’ (University of Vienna 2019) 10.

¹¹⁸ Detlev Gabel and Tim Hickman, ‘GDPR Guide to National Implementation’ (*White & Case LLP*) <<https://www.whitecase.com/publications/article/gdpr-guide-national-implementation>> accessed 6 August 2020.

¹¹⁹ *ibid*, Art. 1(1).

¹²⁰ ‘What Are PECR?’ (20 July 2020) <<https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/>> accessed 7 August 2020.

¹²¹ ‘Opinion 5/2019 on the Interplay between the EPrivacy Directive and the GDPR, in Particular Regarding the Competence, Tasks and Powers of Data Protection Authorities’ (European Data Protection Board 2019) Opinion 11 <https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf>.

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) (L 201/37), Art. 1(2).

¹²³ ‘Opinion 5/2019 on the Interplay between the EPrivacy Directive and the GDPR, in Particular Regarding the Competence, Tasks and Powers of Data Protection Authorities’ (n 121) 11.

In cases when the ePrivacy Directive “particularizes” the rules of the GDPR, the specific article of the ePrivacy Directive shall be regarded as *lex specialis*.¹²⁴ The notion of *lex specialis* suggests that if varying sets of rules apply in a certain situation, the legal framework with the specific rules, the *lex specialis*, takes precedence over the legal framework with general rules, the *lex generalis*.¹²⁵ An example when the ePrivacy Directive “particularizes” the rules of the GDPR, hence the more specific rules of the ePrivacy Directive prevail over the general rules of the GDPR, is the Article 6 on “traffic data.”¹²⁶ Further, it applies to the storing of information and the access to information stored on user’s phones according to Article 5(3).¹²⁷

The ePrivacy Directive also includes rules that “complement” the GDPR. Recital 173 of the GDPR specifies that the GDPR “should apply to *all matters* concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data *which are not subject to specific obligations* with the same objective set out in Directive 2002/58/EC [emphasis added].”¹²⁸ In other words, any processing of data that is not explicitly regulated by the ePrivacy Directive, remains subject to the GDPR.

One main difference exists between the GDPR and ePrivacy Directive which is relevant for this research topic. While the GDPR applies to any processing activity of personal data, the ePrivacy Directive only applies to the processing of location data executed by public electronic communication services and networks (telecom operators).¹²⁹ Usually, companies that offer location services and applications, such as WhatsApp and Skype, which could mean also Covid-19 apps with location tracking and contact tracing tools, are information society services, and therefore are excluded from the scope of the ePrivacy Directive.¹³⁰

¹²⁴ *ibid* 13.

¹²⁵ Waseem Ahmad Qureshi, ‘Untangling the Complicated Relationship between International Humanitarian Law and Human Rights Law in Armed Conflict’ (2018) 6 Penn State Journal of Law & International Affairs 219.

¹²⁶ ‘Opinion 5/2019 on the Interplay between the EPrivacy Directive and the GDPR, in Particular Regarding the Competence, Tasks and Powers of Data Protection Authorities’ (n 121) 13.

¹²⁷ ‘Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak’ (n 55) 5.

¹²⁸ EU General Data Protection Regulation (GDPR), Recital 173.

¹²⁹ ‘Opinion 13/2011 on Geolocation Services on Smart Mobile Devices’ (ARTICLE 29 Data Protection Working Party 2011) WP 185 7 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf>.

¹³⁰ *ibid* 8.

For the same reasons and the fact that the GDPR is more general in nature by providing rules for a variety of different areas in data processing, including anonymization, pseudonymization and data minimization, which are important for this topic, this research focuses on the GDPR, while also acknowledging ePrivacy provisions that are relevant in a complementary manner. For a detailed and thorough discussion on the legal landscape, the ensuing subsections first examine the general principles for processing data and second, assess some of the possible legal bases that permit the processing of personal and sensitive data.

3.3.2. General Principles for the Processing of Data

The GDPR defines “processing” as “any operation or set of operations which is performed on personal data or on sets of personal data.”¹³¹ The processing of personal data requires that various general principles are adhered to according to Article 5 GDPR. These general principles include values of **(1)** lawfulness, fairness and transparency, **(2)** purpose limitation, **(3)** data minimisation, **(4)** storage limitation, **(5)** integrity and confidentiality and **(6)** accountability, which all should be taken into account when processing personal and sensitive data in Covid-19 apps.

First, Article 5(1)(a) highlights that data has to be processed lawfully, fairly and in a transparent manner.¹³² As regards the lawfulness, the processing of data should have a clear legal basis according to Art. 6, 9 or 10 and should provide the data subjects with explicit information. As will be discussed in detail later, the processing for personal and sensitive data differs; therefore, apps have to base the legality of processing on the type of data collected. Pursuant to the principle of transparency, data shall be processed in a fair and transparent manner for the data subject; accordingly, the data subject must be informed of any processing operations and must receive all the information stated in Articles 13 and 14 of the GDPR.¹³³ The data collection, as well as the processing activities for apps, should be transparent and in a reader-friendly format with clear language; there should also be a clear indication about how the apps work and operate.¹³⁴

¹³¹ EU General Data Protection Regulation (GDPR), Art. 4(2).

¹³² *ibid*, Art. 5(1)(a).

¹³³ ‘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).

¹³⁴ ‘Ethical Considerations to Guide the Use of Digital Proximity Tracking Technologies for COVID-19 Contact Tracing’ (World Health Organization 2020) Interim Guidance 3.

Second, data should only be collected for specified, explicit and legitimate purposes.¹³⁵ A clear but short description of what the app's purpose is can help to fulfil explicitness. To be legitimate, the purpose cannot violate any other law. For the processing of data in Covid-19 apps, it is important that developers clearly disclose and specify the objective and only process data that falls within the scope of this purpose.

Third, data minimization means that only data shall be processed that is “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.”¹³⁶ Data minimization can be attained with the help of specific and detailed research questions that indicate what data is needed and necessary to answer the particular question at hand.¹³⁷ As such, Covid-19 apps should ensure that no irrelevant or unnecessary data is collected and processed, that is not essential to combat the crisis, to fulfil the data minimization principle.

Data minimization can also be linked to the principle of storage limitation. Hence, fourth, the storage period for data shall be proportionate and only as long as necessary to realise the underlying purpose.¹³⁸ In other words, data collected and retained has to be limited in scope and time. As concerns Covid-19 mobile phone apps, the processing and storing of data should be limited to the time of the pandemic and in regard to medical relevance and shall be deleted following the end of the pandemic.¹³⁹

Fifth, personal data and in particular sensitive data requires insurance that the data is handled with integrity and confidentiality and that it is “processed in a manner that ensures appropriate security of the personal data.”¹⁴⁰ To guarantee safety, it is necessary to have suitable and up-to-date structural and technical processes in place and the EDPB supports the use of data protection

¹³⁵ EU General Data Protection Regulation (GDPR), Art. 5(1)(b).

¹³⁶ *ibid*, Art. 5(1)(c).

¹³⁷ ‘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 133) 9.

¹³⁸ EU General Data Protection Regulation (GDPR) Art. 5(1)(e) .

¹³⁹ ‘Ethical Considerations to Guide the Use of Digital Proximity Tracking Technologies for COVID-19 Contact Tracing’ (n 134) 3.

¹⁴⁰ EU General Data Protection Regulation (GDPR), Art. 5(1)(f).

officers, who can help to consult on processing activities, especially concerning sensitive data.¹⁴¹ Further, apps should also be subject to audits conducted by third-parties and app developers are encouraged to publish details about their security procedures to (potential) users.¹⁴²

Lastly, the principle of accountability emphasizes that the controller is responsible for compliance and shall be able to prove such conformity.¹⁴³ Users of apps should understand who is collecting, aggregating and using the data and who is in charge of managing the app because if individuals are unsatisfied or are subject to unjustifiable surveillance, they need to be able to hold somebody accountable to receive applicable remedies.¹⁴⁴

3.3.3. Public or Private Data Controllers

All of these general principles discussed above shall be respected by both the controller and the processor.¹⁴⁵ The GDPR defines the controller as “the natural or 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”¹⁴⁶ and the processor as “a natural or legal person, public authority, agency or other body which processes personal data *on behalf of the controller* [emphasis added].”¹⁴⁷ The EDPB acknowledges that different controllers are possible for the processing of data, however national health authorities are usually preferred, especially if apps deal with sensitive data; in any case, the data controllers involved should be clearly defined to ensure the principle of accountability.¹⁴⁸

¹⁴¹ ‘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 133) 10.

¹⁴² ‘Ethical Considerations to Guide the Use of Digital Proximity Tracking Technologies for COVID-19 Contact Tracing’ (n 134) 4.

¹⁴³ EU General Data Protection Regulation (GDPR), Art. 5(2).

¹⁴⁴ ‘Ethical Considerations to Guide the Use of Digital Proximity Tracking Technologies for COVID-19 Contact Tracing’ (n 134) 5.

¹⁴⁵ ‘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 133) 7.

¹⁴⁶ EU General Data Protection Regulation (GDPR), Art. 4(7).

¹⁴⁷ *ibid.*, Art. 4(8).

¹⁴⁸ ‘Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak’ (n 51), para. 25.

A data controller can be a public or private entity, and the lawful basis for processing data depends on that distinction since public entities have a public function and private ones do not.¹⁴⁹ In case a country decides to use a private company as a data controller, it will be distinct to a public authority and hence needs a separate legal basis for processing.¹⁵⁰ For example, a private company cannot act in the ‘public interest’, but would, therefore, need to work together or under the direction of public health services.¹⁵¹ Most European Covid-19 apps use public authorities as their data controllers; some countries, including the UK and Australia, have national health services as data controllers and decided to use Amazon and Microsoft for storage and management tasks, therefore these companies are serving as processors, not controllers, that do not need a distinct legal justification.¹⁵² At the moment, private companies are not expected to act as data controllers.

It is important to emphasize that the GDPR does not forbid the processing of data but actually grants the opportunity to do so if these general principles are adhered to. The principle of legality will be further discussed in the ensuing subsections. The legal basis for processing data differs for personal data and sensitive data; Article 6 GDPR refers to some legal bases for the lawful processing of personal data and Article 9 GDPR allows for the processing of sensitive data according to several possible justifications. Since sensitive data is more risk-prone it is regulated in a stricter manner. Hence, when choosing a suitable legal basis, it is important to understand what type of data is collected and processed in the Covid-19 apps. Apps focusing on processing location data and proximity data for contact tracing, which amount to personal data, trigger the use of legal bases included in Article 6 of the GDPR, whereas apps collecting health data and other sensitive information provoke the application of Article 9 of the GDPR.

3.3.4. Processing Personal Data

Article 6 of the GDPR allows for a total of 6 different legal bases. These are (1) consent of the data subject, processing necessary for (2) performance of a contract, (3) compliance with a legal obligation, (4) vital interest of data subject, (5) public interest and (6) legitimate interest pursued

¹⁴⁹ Bradford, Aboy and Liddell (n 35) 12.

¹⁵⁰ *ibid* 15.

¹⁵¹ *ibid* 16.

¹⁵² *ibid* 15.

by controller or third party.¹⁵³ Arguably, the two most relevant legal bases for the processing of personal data, in particular location and proximity data, during the Covid-19 pandemic are the provisions on consent and public interest.¹⁵⁴

3.3.4.1. Consent

According to Article 6(1), 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.”¹⁵⁵ It is of utmost importance that any consent has to be “freely given, specific, informed and unambiguous.”¹⁵⁶ While consent seems to be an easy solution to allow processing of data, there are some issues that need to be examined when justifying processing with the user’s consent.

First, the consent basis requires the capacity to contact the data subject.¹⁵⁷ This also means that in case data has been previously collected for healthcare reasons, data subjects would normally have to be contacted again to get their consent for the repeated use of data in apps, which is in line with the principle on purpose specification, according to Article 5 of the GDPR.¹⁵⁸ Further, contacting sick people and obtaining consent from people who are critically ill and have potentially been hospitalized, which unfortunately happens regularly for Covid-19 patients, can be practically challenging or even impossible.¹⁵⁹ In some cases, patients can be regarded as vulnerable people and consent might not be considered as valid, because “consent will not be free in cases where there is an element of compulsion, pressure or *inability to exercise free will* [emphasis added].”¹⁶⁰

Additionally, the data subject has the right to withdraw his or her consent at any time which adds to the weakness of the consent basis.¹⁶¹ Article 7(3) states that the withdrawal of the consent by

¹⁵³ EU General Data Protection Regulation (GDPR), Art. 6.

¹⁵⁴ Regina Becker and others, ‘COVID-19 Research: Navigating the European General Data Protection Regulation’ [2020] Social Science Research Network <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3593579>.

¹⁵⁵ EU General Data Protection Regulation (GDPR), Art. 6(1).

¹⁵⁶ *ibid.*, Art. 4(11).

¹⁵⁷ Becker and others (n 154) 3.

¹⁵⁸ *ibid.*

¹⁵⁹ *ibid.*

¹⁶⁰ ‘Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, Adopted on 28 November 2017, as Last Revised and Adopted on 10 April 2018 [Guidelines on Consent]’ (2018) WP259 rev.01 29.

¹⁶¹ EU General Data Protection Regulation (GDPR), Art. 7(2).

the data subject should be as easy as giving consent at any point in time.¹⁶² This means that, if there is no other legal basis than consent, and consent is withdrawn, controllers have the duty to delete the data that has been processed.¹⁶³ Also important to keep in mind, if there is another possible legal basis, the controller cannot just switch from consent to the other lawful basis, but needs to notify the data subject of any change.¹⁶⁴ All of this information shows that, while consent is a potential legal basis to justify the processing of personal data, it might not be the most desirable solution for Covid-19 apps. Instead, it might be more advantageous to base the legality of the processing on the public interest defence.

3.3.4.2. Public Interest

It can be assumed that the fight against the pandemic and any assistance in decelerating the spread of the Covid-19 virus is to the benefit of our society and in the interest of us all, therefore the legal basis of public interest seems to be an ideal fit. Article 6(1)(e) allows for the processing of personal data “for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.”¹⁶⁵ Further, the GDPR specifies that the public interest basis must be established by Union law or the law of the Member State.¹⁶⁶ As mentioned before, the GDPR often permits the EU Member States to enact specific provisions. In the case of processing personal data based on the public interest justification, some Member States, including Belgium, Denmark and Luxembourg do not impose any special rules, while others, such as Austria, Finland, France, Germany and Sweden enforce additional rules that require fulfilment to allow the processing of personal data.¹⁶⁷ Hence, understanding the particular national legislation in the respective country is key to fulfil the required principle of lawfulness.

The legal basis on public interest can also overlap with the legal basis for processing “to protect the vital interests of the data subject or of another natural person.”¹⁶⁸ According to Recital 46 of

¹⁶² *ibid*, Art. 7(3).

¹⁶³ ‘Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, Adopted on 28 November 2017, as Last Revised and Adopted on 10 April 2018 [Guidelines on Consent]’ (n 160) 22.

¹⁶⁴ *ibid* 23.

¹⁶⁵ EU General Data Protection Regulation (GDPR), Art. 6(1)(e).

¹⁶⁶ *ibid*, Art. 6(3).

¹⁶⁷ Gabel and Hickman (n 118).

¹⁶⁸ EU General Data Protection Regulation (GDPR), Art. 6(1)(d).

the GDPR, processing of data may serve both, the public interest and the vital interest of the data subject; this is the case “when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies.”¹⁶⁹ Accordingly, and because of the explicit reference to epidemics and humanitarian emergencies, the situation of the Covid-19 virus seems to allow for the processing of data based on public interest and protecting the interests of the data subject.

Since these two justifications have considerably less weaknesses than the consent basis, it is advisable for the EU Member States to base the processing of personal data in Covid-19 apps on the national legislation which permits processing for the performance of a task carried out in the public interest and vital interest of data subject. Member States can hence either rely on pre-existing laws or might enact provisions specifically to fight the Covid-19 pandemic.¹⁷⁰ While these national laws, in particular any specific rules, can vary, they also need to meet the requirements specified in Article 6(3) of the GDPR.¹⁷¹

3.3.5. Processing Sensitive Data

As shown earlier, some apps might require the sharing of sensitive data and uploading of health data, such as the current medical status.¹⁷² Health data, among others, falls within the special categories of data. As specified in Article 4(15) of the GDPR, “‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.”¹⁷³

Taking into consideration the European Court of Justice’s (ECJ) interpretations and the EDPB’s understanding, ‘data concerning health’ can result from various sources. These include (1) information about medical histories gathered by a health care providers, such as outcomes of

¹⁶⁹ *ibid*, Recital 46.

¹⁷⁰ ‘COMMUNICATION FROM THE COMMISSION Guidance on Apps Supporting the Fight against COVID 19 Pandemic in Relation to Data Protection’ (European Commission 2020) C(2020) 2523 final 6.

¹⁷¹ EU General Data Protection Regulation (GDPR), Art. 6(3).

¹⁷² ‘Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak’ (n 55).

¹⁷³ EU General Data Protection Regulation (GDPR), Art. 4(15).

medical assessments and treatments; (2) information revealed from a survey completed by the data subject when answering questions about their health and symptoms; and (3) information that may result in health data when used with a specific frame of reference, such as details about a person's whereabouts during the Covid-19 pandemic.¹⁷⁴

Based on these categories, apps that require users to submit symptoms or even just information about recent trips or stays in certain areas in combination with health-related input can amount to 'data concerning health' and therefore the processing requires a higher threshold of legal protection. Pursuant to the Recital 51 of the GDPR, these special categories of data, that are sensitive to the fundamental rights and freedoms, deserve particular protection because processing of such data could jeopardize the fundamental rights and freedoms and is likely to have an increased harmful impact for the data subject.¹⁷⁵

According to Art. 9 of the GDPR "processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data to uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation *shall be prohibited* [emphasis added]."¹⁷⁶ While the first paragraph of this article outlaws the processing of sensitive data, the second paragraph states some exceptions that allow for the processing. Very similar to the processing of personal data, there are various possible legal justifications. This part of the research focuses on the most relevant grounds for processing sensitive data to the topic at hand.

3.3.5.1. Possible Legal Bases for Processing Sensitive Data

First, there is the possibility to acquire the consent of the data subject. According to the first sentence in Article 9(2)(a) the individual can give explicit consent.¹⁷⁷ The difference to the legal basis of consent when processing personal data can be found in the second sentence. There, Article

¹⁷⁴ '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 133).

¹⁷⁵ EU General Data Protection Regulation (GDPR), Recital 51.

¹⁷⁶ *ibid*, Art. 9(1).

¹⁷⁷ *ibid*, Art. 9(2)(a).

9(2)(a) states that relying on the data subject's consent is possible “*except* where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject [emphasis added].”¹⁷⁸ In other words, the Member State can prohibit the use of consent as a legal basis. There are various EU Member States that have implemented further restrictions and laws that prohibit the processing based on consent in particular cases. For example, Greece and Luxembourg have additional restrictions when processing genetic data and Spain enacts further limitations when processing sensitive data in general to prevent discrimination.¹⁷⁹

As stated in the discussion on processing personal data, the consent basis is generally considered weak because the data subject has the right to revoke consent at any time, and the fact that Member States can prohibit the legal basis of consent further diminishes its value as a plausible justification. Therefore, for EU Member States aiming to process sensitive data in Covid-19 apps, it is advisable to examine other legal bases.

Second, the lawfulness of processing can also be based on national legislation. Article 9(2)(h) allows for processing that is “necessary for the purposes of preventive or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.”¹⁸⁰ Further, Article 9(2)(i) allows for processing that is necessary for the public interest in the field of public health, including the defence against grave cross-border threats to health and guarantee of high-quality medical products and devices.¹⁸¹ As the Covid-19 pandemic seriously and indisputably threatens the life and health of people worldwide and the assurance of medical equipment is of utmost importance, these two legal bases seem to be of great relevance. Both provisions require the basis of Union or Member State law. Therefore, if EU Member States decide to process any of the special categories of data for Covid-19 apps, it would be useful to base it on national legislation and one of the two relevant provisions.

¹⁷⁸ *ibid*, Art. 9(2)(a).

¹⁷⁹ Gabel and Hickman (n 118).

¹⁸⁰ *ibid*, Art. 9(2)(h).

¹⁸¹ *ibid*, Art. 9(2)(i).

3.3.6. Processing Carried Out for Research Purposes

GDPR offers one more legal basis for processing activities for research purposes. This justification is laid down in Article 89 of the GDPR, which states that “processing for archiving purposes in the *public interest*, scientific or historical *research purposes* or statistical purposes, shall be subject to appropriate safeguards [emphasis added]” and this provision “may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21.”¹⁸² These articles all refer to rights of data subjects, including right of access to the personal data (Article 15), right to rectification of inaccurate data (Article 16), right to restriction of processing (Article 18) and right to object to processing (Article 21).

Recital 159 argues that “the processing of personal data for scientific research purposes should be interpreted *in a broad manner* [emphasis added]” and “scientific research purposes should also include studies conducted in the public interest in the area of public health.”¹⁸³ Based on the this wording, public health research can be understood as a subset of scientific research.¹⁸⁴ Recital 54 defines public health as “all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality.”¹⁸⁵ Pursuant to this broad interpretation, the activities of social media, and especially the use of apps may count as public health research and can therefore rely on Article 89.¹⁸⁶ As an example, Finland allows the processing of personal data necessary for research based on the public interest basis in its national legislation.¹⁸⁷

¹⁸² *ibid*, Art. 89.

¹⁸³ *ibid*, Recital 159.

¹⁸⁴ Giulia Schneider, ‘Disentangling Health Data Networks: A Critical Analysis of Articles 9(2) and 89 GDPR’ (2019) 9 International Data Privacy Law 268.

¹⁸⁵ EU General Data Protection Regulation (GDPR), Recital 54.

¹⁸⁶ Schneider (n 184) 268.

¹⁸⁷ Lov om behandling av personopplysninger (personopplysningsloven) (The Act on the Processing of Personal Data) 2018, according to §8: " Personal data may be processed on the basis of the Privacy Ordinance Article 6 No. 1 letter e if it is necessary for archival purposes in the public interest, purposes related to scientific or historical research or statistical purposes. The processing shall be covered by the necessary guarantees in accordance with Article 89 (1) of the Privacy Regulation".

If processing of data is based on Article 89, controllers must ensure that “technical and organizational measures are in place in particular in order to ensure respect for the principle of data minimization.”¹⁸⁸ One of these measures explicitly referred to is pseudonymization. According to the GDPR pseudonymization means that “the personal data can no longer be attributed to a specific data subject *without the use of additional information* [emphasis added],”¹⁸⁹ in other words, full anonymization implies that data cannot be identified by any means. It is important to distinguish between pseudonymization and anonymization for the application of GDPR. While processing pseudonymous data falls within the scope of the GDPR, anonymous data falls outside of its reach.¹⁹⁰

This section has so far provided EU Member States with a variety of different legal justifications for processing personal and sensitive data according to the GDPR. To ensure that this thesis elaborates on a variety of relevant legal justifications for processing data, the subsequent subsection discusses some of the provisions incorporated within the ePrivacy Directive.

3.3.7. ePrivacy Directive

As mentioned earlier, the ePrivacy Directive can serve in a complementary manner to the GDPR, especially with regard to processing data by telecom providers. The ePrivacy Directive is mainly concerned with personal data in the electronic communication field, including location data and traffic data.¹⁹¹ To provide a bigger picture of legal provisions applicable to this research topic, this subsection discusses some relevant articles, in particular Articles 9, 15 and 5(3), respectively, of the ePrivacy Directive.

Article 9 of the ePrivacy Directive contains relevant rules for processing location data. Accordingly, “data may only be processed when they are made *anonymous*, or with the *consent* of the users or subscribers to the *extent* and for the *duration necessary* for the provision of a value-

¹⁸⁸ EU General Data Protection Regulation (GDPR), Art. 89.

¹⁸⁹ *ibid.*, Art. 4(5).

¹⁹⁰ Schneider (n 184) 269.

¹⁹¹ ePrivacy Directive, Art. 2(b) Definition for traffic data: “‘traffic data’ means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.

added service [emphasis added].”¹⁹² Taking a look at the various terms, first, Article 29 Working Party affirms that consent is the main relevant basis for processing location data in the ePrivacy Directive and telecom operators have the obligation to always acquire the user’s consent before processing.¹⁹³ Further, if consent is not obtained, telecom providers may only process the data if it is made anonymous. Lastly, the reference to the extent and duration relates to the concern that data, when stored over a longer period, may allow to draw references to people’s lives.¹⁹⁴ In comparison to the GDPR, Article 5 of the GDPR only allows for the processing of personal data that is adequate, relevant and limited (data minimization principle) and personal data may not be kept for longer than is necessary (storage limitation principle).

Article 15 of the ePrivacy Directive allows Member States to limit obligations outlined in Article 9 if, “such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or unauthorised use of the electronic communication system.”¹⁹⁵ In other words, Member States can limit the scope of Article 9, if they deem it necessary for national security reasons. It further emphasizes that any procedures taken within this article must be in accordance with Community law, including the Charter of Fundamental Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms.¹⁹⁶

With regard to storage or access to information already stored on the user’s phone, Article 5(3) of the ePrivacy Directive is applicable. One main example for an information stored in the terminal equipment of a mobile phones are cookies. Hence, if location tracking or contact tracing apps are using cookies, they also have to comply with this provision of the ePrivacy Directive which requires “free, specific, informed and unambiguous consent for installing cookies.”¹⁹⁷ The storing

¹⁹² ePrivacy Directive, Art. 9(1).

¹⁹³ ‘ETNO: Study on the Revision of the EPrivacy Directive’ (n 37) 24.

¹⁹⁴ *ibid.*

¹⁹⁵ ePrivacy Directive, Art. 15(1).

¹⁹⁶ ‘Statement on the Processing of Personal Data in the Context of the COVID-19 Outbreak.’ (n 112) 2; ePrivacy Directive, Art. 15(1).

¹⁹⁷ ‘ETNO: Study on the Revision of the EPrivacy Directive’ (n 37) 29.

of information or the gaining access to the information stored is only allowed if the user has consented or if it absolutely necessary for the information society service requested by the user.¹⁹⁸

This section on the legal landscape highlights the possibility to process data according to the GDPR and ePrivacy Directive, if, and only if, the general principles to processing are obeyed and one of the possible legal bases is adhered to. While these two legal frameworks offer EU Member States various legal bases to lawfully process data, arguably the most adequate justifications are based on national legislation. In particular, the most relevant legal bases for processing personal data are Articles 6(1)(e) and (d), Article 9(2)(i) for processing sensitive data or Article 89 if processing activities are conducted for research purposes. If telecom providers process such data or if the processing refers to data already stored on the phone, then the ePrivacy Directive and its Articles 9 and 5(3), respectively, have to be taking into account. It has been emphasized that EU Member States can differ substantially in applicable rules since they may adopt additional restrictions. Therefore, when defining the legal basis for processing data in Covid-19 apps, developers need to analyse and be aware of their country's specific national legislation.

While this section emphasized the legal obligations of EU Member States laid down in the GDPR and the ePrivacy Directive and demonstrated how countries can legally process citizen's data, the ensuing subsection discusses various recommendations that countries are encouraged to follow; these guidelines are either linked or go beyond the requirements originating from data protection laws.

3.4. Recommendations for Using Mobile Phone Apps during Covid-19

The most important recommendation for EU Member States when developing and using mobile phone apps is to understand and respect the underlying legal requirements; these include the general principles of processing such as, data minimization and purpose limitation, as well as the legal basis for processing citizen's data. While the legality of processing plays an undisputed essential role in the application of apps, there are various other important ethical considerations

¹⁹⁸ 'Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak' (n 55) 5.

that EU Member States need to take into consideration when deciding to process citizen's data in mobile phone apps.

The ensuing paragraphs highlight some recommendations that can guide EU Member States in using Covid-19 mobile phones, in particular, apps that process location or proximity data for contact tracing, and finding a balance between data protection laws and saving lives. Some of these recommendations put the legal provisions discussed above into practice, while others are mere advices not stemming from legal frameworks; however, all aim to provide guidance on reducing intrusiveness while also offering assistance in fighting the Covid-19 pandemic with apps. This subsection discusses the voluntary use of apps, limiting intrusive data, respecting time limitations, using anonymized data, ensuring citizen's trust in public authorities, appointing national authorities as the data controller and improving interoperability.

3.4.1. Voluntary Use of Apps

First and foremost, while not specifically set out in the GDPR or the ePrivacy Directive, the voluntary basis for using the apps is important; mandatory apps would conflict with European legal frameworks and any guidelines issued by the EDPB. EU Member States should not offer any incentives or other inducements to people using the app.¹⁹⁹ The reason for this, the constant monitoring and contact tracing of individuals can be considered an intrusion into their private lives and can only be justified with a voluntary adoption of the app by the user.²⁰⁰ Therefore, the use of such apps must be strictly voluntary, individuals must have and retain total control over data and should be free to choose if they trust the app with any personal or sensitive information.²⁰¹ The voluntary use necessity does not automatically entail the legal basis of consent but requires that data subjects keep some of the GDPR default rules, including the right to object to processing.²⁰²

¹⁹⁹ 'Ethical Considerations to Guide the Use of Digital Proximity Tracking Technologies for COVID-19 Contact Tracing' (n 134) 3.

²⁰⁰ 'Contact Tracing Apps – A Privacy Primer' (A&L Goodbody 2020) 4
<https://www.algoodbody.com/files/uploads/news_insights_pub/COVID-19_-_Contact_Tracing_Apps_A_Privacy_Primer.pdf>.

²⁰¹ 'Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak' (n 55) 11.

²⁰² Bradford, Aboy and Liddell (n 35) 15.

3.4.2. Limiting Intrusive Data

EU Member States should ensure that the app limits the use of personal and sensitive data, which is linked to the principle of data minimization incorporated in the GDPR. Especially sensitive data, such as names, date of birth, home address or data concerning health, should under no circumstances be shared with the public. Limiting personal data can also apply to location and proximity data; as such, apps with contact tracing tools do not need the exact locations of the individual but can perform the task of identifying contacts with proximity data alone. The use of Bluetooth technology to perform contact tracing seems to be the least intrusive measure. According to Wojciech Wiewiórowski, European Data Board Supervisor, the “use of temporary broadcast identifiers and Bluetooth technology for contact tracing seems to be a useful path to achieve privacy and personal data protection effectively.”²⁰³ In other words, the less data collected that can identify the user, the better for the user’s data protection. Hence, it is recommended for EU Member States to use Bluetooth technology for contact tracing tools.

3.4.3. Respecting Time Limitation

One of the GDPR general principles refers to storage limitation and states that data can only be used and stored as long as necessary. The same is true for the general use of mobile phone apps to track individuals or undertake contact tracing; in other words, EU Member States shall ensure that the use of such apps should only be temporary.²⁰⁴ It is evident that the Covid-19 situation requires unprecedented efforts. However, any monitoring or digital surveillance in apps that collect health data, location data or merely proximity data raise sincere concerns about privacy and data protection.²⁰⁵ Hence, these measures should be timely restricted, and the further use of such apps should be prevented when the pandemic has ended.

²⁰³ Wojciech Wiewiórowski, ‘EU Digital Solidarity: A Call for a Pan-European Approach against the Pandemic’ (European Data Protection Supervisor 2020) Statement <https://edps.europa.eu/sites/edp/files/publication/2020-04-06_eu_digital_solidarity_covid19_en.pdf>.

²⁰⁴ ‘Ethical Considerations to Guide the Use of Digital Proximity Tracking Technologies for COVID-19 Contact Tracing’ (n 134) 3.

²⁰⁵ *ibid.*

3.4.4. Use of Anonymized Data

When Member States decide to use location data, or any other type of personal data, they should guarantee that the data is anonymized. When applications to combat Covid-19 received increased attention, various app developers argued that the use of anonymized data allows for circumventing the application of the GDPR, since anonymized data falls outside the scope for the GDPR, while pseudonymised data does not. While this is true, the idea of anonymization is often misunderstood for pseudonymization and studies have shown that pseudonymization is not enough to prevent the re-identification of users in mobile phone data, and hence does not assure the needed protection for users.²⁰⁶

Anonymization can only take place for data as a whole and the single data traces of people are often too unique, therefore making users vulnerable to re-identification.²⁰⁷ In other words, true anonymization for location data is very tricky and often data believed to be anonymized was in fact not. The EDPB acknowledges that true data anonymization is a very high burden to meet and app developers often fail to actually anonymize data, however, the EDPB still motivates the use of anonymized data to avoid linking data to a natural person.²⁰⁸ While it is advisable for EU Member States to fully anonymize data, each country has to make sure that anonymization is possible, and it is further recommended to conduct regular analyses to assure true anonymization.

3.4.5. National Health Authorities as Controllers of the App

For users of the app, it is important to know who the controller is, and hence who is accountable for the processing of data. As discussed before, a data controller can be either a public or private entity, either way it is important to explicitly define the controller. For example, the Austria's 'StoppCorona App' clearly outlines that the Austrian Red Cross serves as the data controller. Users of the app should know who is deciding on the method and purpose of processing and therefore

²⁰⁶ Yves-Alexandre de Montjoye and others, 'On the Privacy Conscientious Use of Mobile Phone Data' (2018) 5 Scientific Data 1.

²⁰⁷ 'Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak' (n 55) 6.

²⁰⁸ *ibid* 5.

who is responsible for conforming with underlying legal provisions.²⁰⁹ While there is no rule on who the controller should be, the EU Commission prefers national health authorities, entities executing tasks in the public interest in the area of health, taking on the role of controllers in mobile phone apps because of the sensitivity of data.²¹⁰

3.4.6. Ensuring Citizens' Trust in Governments and Public Authorities

As mentioned before the public has to trust their governments or public health officials that personal and sensitive data is not mishandled but dealt with according to regulations. As the app can only work efficiently if a certain percentage of citizens adopts and uses the app, it is necessary that enough people entrust their data to the public authorities in charge and feel confident in sharing their private information with the app. Withdrawing or limiting privacy and data protection rights for surveillance may lead to distrusts; for example, reports state that the digital control exercised in China as a way to control the outbreak might have led to aggravated stigmatization and public distrust.²¹¹ This could also occur in countries with a general scepticism for the government, such as the United States, and to avoid this, the public should be regularly and correctly informed about any processing of data by public authorities.²¹² Therefore, EU Member States have to understand that communicating information to their citizens is key to transparency and important to guarantee trust.

3.4.7. Achieving Interoperability

Not only the government's communication to its population is required to adequately fight the virus, but also the interaction to other countries, because the infection and the spread of the Covid-19 virus does not stop at borders. While the EDPB supports efforts to find a common approach and interoperable frameworks to deal with the crisis, currently there are still differences in standards of digital surveillance, data protection rules and a vast number of apps that vary in technology, design and collection of personal and sensitive data. As interoperability of contact

²⁰⁹ 'COMMUNICATION FROM THE COMMISSION Guidance on Apps Supporting the Fight against COVID 19 Pandemic in Relation to Data Protection' (n 170) 4.

²¹⁰ *ibid* 5.

²¹¹ Vayena and Ienca (n 10).

²¹² *ibid*.

tracing apps, the EDPB understands the “ability to exchange between themselves the minimum information necessary for individual app users, wherever they are located in the EU, to be alerted, in accordance with the procedures defined by public health authorities, if they have been in proximity with another user who has notified the app that he/she has tested positively for COVID-19.”²¹³

The interoperability of apps, at least within the EU, may increase effectiveness because more contacts can be traced, and it may also simplify the use of such apps, especially for people who travel across borders and can still use the same app wherever they are.²¹⁴ While the EDPB acknowledges that interoperability is not easy to achieve since Member States have different approaches, it encourages app developers to at least agree on a collective protocol and use the same technology for apps, which will be a first step to enable interoperability.²¹⁵ For example, the divide in centralized and decentralized approaches for processing data in Europe is one major concern in achieving efficient interoperability. Further, it seems that the centralized system, which stores the information in one database, usually controlled by the country’s government, hinders interoperability as long as countries, such as France, support this approach. Therefore, it would be recommended for EU Member States to uniformly support the decentralized approach within the EU.

4. Conclusion

The Covid-19 pandemic truly creates an exceptional situation and as a global health crisis, it requires extraordinary measures. EU Member States and countries worldwide, turned towards the use of technology and mobile phone data, in addition to social distancing, quarantine enforcements and regional and country-wide lockdowns, to fight the crisis. While the apps on the market differ greatly, this research indicates that EU Member States generally focus on processing proximity

²¹³ ‘Interoperability Guidelines for Approved Contact Tracing Mobile Applications in the EU’ (eHealth Network 2020) <https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf>.

²¹⁴ ‘Statement on the Data Protection Impact of the Interoperability of Contact Tracing Apps’ (European Data Protection Board 2020) Statement 2 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statementinteroperabilitycontacttracingapps_en_0.pdf>.

²¹⁵ *ibid.*

data based on Bluetooth technology for contact tracing efforts to limit the use of sensitive and intrusive data as a way to conform with the legal provisions on data protection and to ensure citizen's trust in using the app.

This dissertation has provided the necessary contextual framework to the functionality of Covid-19 mobile phone apps, by explaining the use of location data and proximity data to conduct contact tracing and by highlighting some noteworthy European and international developments in this field. Further, it has outlined various benefits, as well as shortcomings, relating to the processing of personal and sensitive data in apps to highlight the struggle between saving lives and dealing with various shortcomings. As a response to the concern about data protection, the thesis has elaborated on the legal landscape, in particular the GDPR and the ePrivacy Directive, and their applicable provisions that allow EU Member States to process citizen's data according to explicit rules. It is important to keep in mind that the GDPR does not hinder the processing of data in Covid-19 mobile phone apps, but rather provides a functional and flexible blueprint for the various types of apps.

This dissertation asserts that mobile phone apps can aid in combating the crisis, if EU Member States take into account various legal, as well as, ethical recommendations mentioned in this research. As such the principles of legality, transparency and proportionality of processing the data in these apps have to be prioritized. Further, EU Member States should ensure that the use of the app is completely voluntary, the processing of intrusive data is limited in scope and restricted to the duration of the pandemic. Additionally, countries are encouraged to transfer the role of data controller to the national health authorities. EU Member States need to convey information to its citizens in an unambiguous and user-friendly manner because only if a significant percentage of the population uses the app, benefits can be reaped. While there is a fine line between contributing to saving lives and risking data protection violations, finding a balance is possible and necessary for EU Member States to ensure that Covid-19 apps can successfully aid in combating the Covid-19 pandemic.

5. Bibliography

Legislation

Charter of Fundamental Rights of the European Union 2012 (2012/C 326/02)

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) (L 201/37)

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 (General Data Protection Regulation) (OJ 2016 L 119/1)

European Parliament resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences (2020/2616(RSP)) 2020 (P9_TA(2020)0054)

Lov om behandling av personopplysninger (personopplysningsloven) (The Act on the Processing of Personal Data) 2018

European Data Protection Board Documents

‘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)

‘Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak’ (European Data Protection Board 2020)

‘Opinion 5/2019 on the Interplay between the EPrivacy Directive and the GDPR, in Particular Regarding the Competence, Tasks and Powers of Data Protection Authorities’ (European Data Protection Board 2019) Opinion

‘Statement on the Data Protection Impact of the Interoperability of Contact Tracing Apps’ (European Data Protection Board 2020) Statement
<https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statementinteroperabilitycontacttracingapps_en_0.pdf>

‘Statement on the Processing of Personal Data in the Context of the COVID-19 Outbreak.’ (European Data Protection Board 2020) Statement
<https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf>

Wiewiórowski W, 'EU Digital Solidarity: A Call for a Pan-European Approach against the Pandemic' (European Data Protection Supervisor 2020) Statement
<https://edps.europa.eu/sites/edp/files/publication/2020-04-06_eu_digital_solidarity_covid19_en.pdf>

Academic Sources

Ahmed N and others, 'A Survey of COVID-19 Contact Tracing Apps' [2020] IEEE Access

'Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, Adopted on 28 November 2017, as Last Revised and Adopted on 10 April 2018 [Guidelines on Consent]' (2018) WP259 rev.01

Becker R and others, 'COVID-19 Research: Navigating the European General Data Protection Regulation' [2020] Social Science Research Network
<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3593579>

Bradford L, Aboy M and Liddell K, 'COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR and Data Protection Regimes' [2020] Journal of Law and the Biosciences

Buckee C, 'Improving Epidemic Surveillance and Response: Big Data Is Dead, Long Live Big Data' (2020) 2 Lancet Digital Health

'Can Digital Health Help Stop the Next Epidemic?' [2019] Center for Strategic & International Studies

Chakarova KY, 'General Data Protection Regulation: Challenges Posed by the Opening Clauses and Conflict of Laws Issues' (University of Vienna 2019)

Cho H, Ippolito D and Yu YW, 'Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-Offs' 25 March 2020

'COMMUNICATION FROM THE COMMISSION Guidance on Apps Supporting the Fight against COVID 19 Pandemic in Relation to Data Protection' (European Commission 2020) C(2020) 2523 final

'Coronavirus Disease (COVID-19) Situation Report – 187' (World Health Organization 2020)
<https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200725-covid-19-sitrep-187.pdf?sfvrsn=1ede1410_2>

de Montjoye Y-A and others, 'On the Privacy Conscientious Use of Mobile Phone Data' (2018) 5 Scientific Data

Dumbrava C, 'Tracking Mobile Devices to Fight Coronavirus' (European Parliamentary Research Service 2020) Briefing

‘Ethical Considerations to Guide the Use of Digital Proximity Tracking Technologies for COVID-19 Contact Tracing’ (World Health Organization 2020) Interim Guidance

‘ETNO: Study on the Revision of the EPrivacy Directive’ (DLA Piper 2016)
<https://etno.eu/datas/publications/studies/DPTS_Study_DLA_04082016_ePrivacy_Final.pdf>

Huang Y, Sun M and Sui Y, ‘How Digital Contact Tracing Slowed Covid-19 in East Asia’ [2020] *Harvard Business Review* <<https://hbr.org/2020/04/how-digital-contact-tracing-slowed-covid-19-in-east-asia>> accessed 26 July 2020

‘Interoperability Guidelines for Approved Contact Tracing Mobile Applications in the EU’ (eHealth Network 2020)
<https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf>

Kleinman RA and Merkel C, ‘Digital Contact Tracing for COVID-19’ (2020) 192 *Canadian Medical Association Journal*

Klonowska K, ‘The COVID-19 Pandemic: Two Waves of Technological Responses in the European Union’ [2020] The Hague Centre for Strategic Studies

Lai S and others, ‘Measuring Mobility, Disease Connectivity and Individual Risk: A Review of Using Mobile Phone Data and MHealth for Travel Medicine’ [2019] *Journal of Travel Medicine*

Ng Y and others, ‘Evaluation of the Effectiveness of Surveillance and Containment Measures for the First 100 Patients with COVID-19 in Singapore — January 2–February 29, 2020’ (Centers for Disease Control and Prevention 2020) *Morbidity and Mortality Weekly Report*

Oliver N and others, ‘Mobile Phone Data and COVID-19: Missing an Opportunity?’
<<https://arxiv.org/pdf/2003.12347.pdf>>

‘Opinion 13/2011 on Geolocation Services on Smart Mobile Devices’ (ARTICLE 29 Data Protection Working Party 2011) WP 185 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf>

Ponce Del Castillo A, ‘COVID-19 Contact-Tracing Apps: How to Prevent Privacy from Becoming the next Victim’ (2020) 5 *ETUI*

Qureshi WA, ‘Untangling the Complicated Relationship between International Humanitarian Law and Human Rights Law in Armed Conflict’ (2018) 6 *Penn State Journal of Law & International Affairs*

Ranisch R and others, ‘Ethics of Digital Contact Tracing Apps for the Covid-19 Pandemic Response’ (Kompetenznetz Public Health COVID-19 2020)

Schneider G, ‘Disentangling Health Data Networks: A Critical Analysis of Articles 9(2) and 89 GDPR’ (2019) 9 *International Data Privacy Law*

‘Transmission of SARS-CoV-2: Implications for Infection Prevention Precautions’ (World Health Organization 2020) Scientific Brief

Vayena E and Ienca M, ‘On the Responsible Use of Digital Data to Tackle the COVID-19 Pandemic’ (2020) 26 *Nature Medicine* 458

Wesolowski A and others, ‘Commentary: Containing the Ebola Outbreak - the Potential and Challenge of Mobile Network Data’ [2014] *PLOS Currents*

Other Documents and Web Sources

Albergotti R, ‘Apple and Google Launch Coronavirus Exposure Software’ *Washington Post* (20 May 2020) <<https://www.washingtonpost.com/technology/2020/05/20/apple-google-api-launch/>> accessed 11 July 2020

‘Austria Invites Suggestions to Improve Coronavirus Track and Trace App’ *Reuters* (8 July 2020) <<https://www.reuters.com/article/healthcoronavirus-austria-apps-idUSL8N2EF1BB>> accessed 25 July 2020

Bacci U, ‘Digital Handshake: Can Contact Tracing Deliver on Its Promise in Coronavirus Battle?’ *Reuters* (5 May 2020) <<https://www.reuters.com/article/us-health-coronavirus-tech-trfn-idUSKBN22H254>> accessed 19 July 2020

Baxter M, ‘Centralised and Decentralised Contact Tracing Apps Creates Academic Split’ (*PrivSec Report*, 22 April 2020) <<https://gdpr.report/news/2020/04/22/centralised-versus-decentralised-contact-tracing-solutions-pit-privacy-academics-against-each-other/>> accessed 12 July 2020

Busvine D, ‘Germany Flips on Smartphone Contact Tracing, Backs Apple and Google’ *Reuters* (26 April 2020) <<https://www.reuters.com/article/health-coronavirus-europe-tech-idUSL3N2CE03Z>> accessed 12 July 2020

‘Contact Tracing Apps – A Privacy Primer’ (A&L Goodbody 2020) <https://www.algoodbody.com/files/uploads/news_insights_pub/COVID-19_-_Contact_Tracing_Apps_A_Privacy_Primer.pdf>

‘Coronavirus Privacy: Are South Korea’s Virus Alerts Too Revealing?’ *BBC News* (5 March 2020) <<https://www.bbc.com/news/world-asia-51733145>> accessed 9 July 2020

Davidson H, ‘China’s Coronavirus Health Code Apps Raise Concerns over Privacy’ *The Guardian* (1 April 2020) <<https://www.theguardian.com/world/2020/apr/01/chinas-coronavirus-health-code-apps-raise-concerns-over-privacy>> accessed 13 June 2020

Diamond F, ‘Asymptomatic Carriers of COVID-19 Make It Tough to Target’ (*Infection Control Today*) <<https://www.infectioncontroltoday.com/article/asymptomatic-carriers-covid-19-make-it-tough-target>> accessed 13 June 2020

Espinoza J, Miller J and Abboud L, ‘How Europe Splintered over Contact Tracing Apps’ *Financial Times* (10 May 2020) <<https://www.ft.com/content/7416269b-0477-4a29-815d-7e4ee8100c10>> accessed 19 July 2020

‘Exposure Notification: Frequently Asked Questions’ (Apple and Google 2020)
<https://blog.google/documents/73/Exposure_Notification_-_FAQ_v1.1.pdf>

Gabel D and Hickman T, ‘GDPR Guide to National Implementation’ (*White & Case LLP*)
<<https://www.whitecase.com/publications/article/gdpr-guide-national-implementation>> accessed 6 August 2020

Grimwood-Taylor E, ‘International: COVID-19 - Contact Tracing Apps - Differing Global Approaches’ (*Baker McKenzie*, 13 May 2020)
<https://insightplus.bakermckenzie.com/bm/technology-media-telecommunications_1/international-covid-19-contact-tracing-apps-differing-global-approaches_1> accessed 12 July 2020

Ingram D, ‘Your Phone Could Track the Spread of Coronavirus. Here’s What You Should Know.’ (*NBC News*, 20 April 2020) <<https://www.nbcnews.com/tech/tech-news/how-contact-tracing-could-use-bluetooth-track-coronavirus-your-smartphone-n1187796>> accessed 11 July 2020

‘Joint Civil Society Statement: States Use of Digital Surveillance Technologies to Fight Pandemic Must Respect Human Rights’ (Human Rights Watch 2020) Statement
<<https://www.hrw.org/news/2020/04/02/joint-civil-society-statement-states-use-digital-surveillance-technologies-fight>> accessed 26 June 2020

‘Joint Statement on Contact Tracing: Date 19th April 2020’
<https://www.mq.edu.au/__data/assets/pdf_file/0012/977493/Joint-Statement-on-Contact-Tracing.pdf>

Kelion L, ‘Apple and Google’s Covid-19 “Watershed Moment”’ *BBC News* (20 May 2020)
<<https://www.bbc.com/news/technology-52740131>> accessed 15 July 2020

— —, ‘France’s Virus-Tracing App “off to a Good Start”’ *BBC News* (3 June 2020)
<<https://www.bbc.com/news/technology-52905448>> accessed 19 July 2020

Kim N, “‘More Scary than Coronavirus’: South Korea’s Health Alerts Expose Private Lives’ *The Guardian* (6 March 2020) <<https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives>> accessed 25 July 2020

‘Mobile Location Data and Covid-19: Q&A’ (*Human Rights Watch*, 13 May 2020)
<<https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa>> accessed 26 June 2020

Mozur P, Zhong R and Krolik A, ‘In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags’ *The New York Times* (1 March 2020)

<<https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html>> accessed 14 July 2020

O'Brien C, 'COVID-19 Tracing Apps Now Live in Germany, France, and Italy; U.K. Rethinks Its Plans' (*VentureBeat*, 19 June 2020) <<https://venturebeat.com/2020/06/19/covid-19-tracing-apps-now-live-in-germany-france-and-italy-u-k-rethinks-its-plans/>> accessed 19 July 2020

'Recommendations on Privacy and Data Protection in the Fight Against COVID-19' (Access Now 2020) <<https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf>> accessed 23 April 2020

Siddiqui A, 'List of Countries Using Google and Apple's COVID-19 Contact Tracing API' (*xda-developers*, 26 June 2020) <<https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/>> accessed 11 July 2020

Singer N and Sang-Hun C, 'As Coronavirus Surveillance Escalates, Personal Privacy Plummets' *The New York Times* (23 March 2020) <<https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html>> accessed 23 April 2020

'STOP COVID19 - Digital Health Platform to Stop SARS Cov-2' (*STOP COVID19*) <<https://stopcovid19.cat/en/stop-covid19-cat/>> accessed 31 July 2020

'Stopp Corona - Apps on Google Play' <https://play.google.com/store/apps/details?id=at.rotekreuz.stopcorona&hl=en_US> accessed 4 August 2020

'Timeline of WHO's Response to COVID-19' (*World Health Organization*, 29 June 2020) <<https://www.who.int/news-room/detail/29-06-2020-covidtimeline>> accessed 17 July 2020

'TraceTogether' <<https://www.tracetogether.gov.sg/>> accessed 4 August 2020

'What Are PECR?' (20 July 2020) <<https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/>> accessed 7 August 2020

'WHO Coronavirus Disease (COVID-19) Dashboard' <<https://covid19.who.int>> accessed 26 July 2020

'WHO Director-General's Opening Remarks at the Media Briefing on COVID-19 - 16 March 2020' <<https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---16-march-2020>>

Wilhelmer P, 'Bumpy Second Attempt for New "Stopp Corona" App (Holpriger Zweiter Anlauf Für Neue "Stopp Corona"-App)' *Kurier* (26 June 2020) <<https://kurier.at/wissen/neue-funktionen-zweiter-anlauf-fuer-stopp-corona-app/400951679>> accessed 19 July 2020