澳門大學
UNIVERSIDADE DE MACAU
UNIVERSITY OF MACAU

FACULTY OF LAW

PROJECT REPORT

Project title: **Personal Data Protection and Decentralized Contact Tracing in the EU - The European Technologic Response to the COVID-19 Pandemic**

Programme: **MASTER'S DEGREE PROGRAMME**

Major: **EUROPEAN UNION LAW**

Student Name: **TAO DONGLAI**

Student Number: **MB951083**

Supervisor: **Vera Lúcia Carapeto RAPOSO**

Declaration of Originality

I declare that the project report here submitted is original except for the source materials explicitly acknowledged and that this report as a whole, or any part of this report has not been previously submitted for the same degree or for a different degree.

I also acknowledge that I have read and understood the Rules on Handling Student Academic Dishonesty and the Regulations of the Student Discipline of the University of Macau.

Declarant: TAO DONGLAI

Date: *2021 / 03 / 25*
YYYY / MM / DD

Acknowledgements

First, I am very grateful to my supervisor Prof. Vera, for her careful guidance of my project report, which greatly improved my understanding of academic writing and let me know specific study skills. That guidance let me get over the difficulties of language and work out a qualified report.

Second, I'd like to express my gratitude to Prof. Sten, Prof. Tu, Prof. Perumal. They taught me the research methodology and writing and other legal lessons, which help me to develop my academic skills and broaden my eyesight.

Then, I am very grateful to my parents for their support, which let me can have enough food and no need to tolerate starving. I also need to thank my classmates and friends. During this period, we encourage each other to let us keep confident to get over the difficulties we met. So that, we can keep a good spirit toward the writing.

What's more, I need to thank Bill Gates and his teams. The Word of MS office is so useful and helpful that we cannot praise this program too much. I also need to thank the University of Macau, whose library and database are so…… fantastic that I can find nearly all the study materials I need to finish this work.

Abstract

Since the COVID-19 become one of the most serious pandemics in the world, digital contact tracing tools have become a popular choice of pandemic control measures. These decentralized contact tracing apps can help to accelerate the contact tracing work and stop further spreading of the virus. However, these useful apps also need to face legality problems. This report examines the legality issues of the application of decentralized contact tracing apps in the EU from the perspective of personal data protection and fundamental right protection.

About the personal data protection issues, this report first provides an analysis of the categories of the data. The data collected and processed on these apps should be qualified data concerning health, where there are likely reasonable means to combine additional information to identify the data subjects. Hence, only the API providers and public health authorities should be qualified as data controllers.

However, the centralized management system will face the challenge of a decentralized framework. Difficulties in access to the data on users' devices will make it harder for users to exercise their rights to data protection. Difficulties in management will further limit the users' chance to exercise their rights. However, due to strict fundamental protection rules, it could be impossible for the Union and the Member States to adopt mandatory measures to apply decentralized contact tracing apps. Voluntary application is the only choice. Therefore, it is important for the authorities of EU Member States to find creative ways to effectively promote the voluntary use of decentralized contact tracing to fight against the COVID-19 pandemic.

Key words: EU law, decentralized contact tracing, personal data protection, proportionality

Table of Contents

1 Introduction

The COVID-19 could be the most serious pandemic in the world in the 21st century. This infectious and deadly virus appeared silently and spread quickly in crowds in 2019. Up to now, millions of people have been infected. Thousands of people dead. Due to the rapid spreading and the lack of specific medicine, the medical institution became overburden, and preventing transmission is of great importance. Under this circumstance, the only way to stop the spreading is to timely test and isolate the potential infected or carrier of the COVID-19. Manual contact tracing conduct by public health authorities is the traditional method to find out the virus carriers. Comparing with the rapid spreading of the COVID-19 pandemic, this method of contact tracing is too slow. Because lots of the transmissions of the COVID-19 virus occurred before the warning sign of symptoms, even the asymptomatic transmission, which lead to a very short window of time for contact tracing and quarantine to stop the rapid transmission of the COVID-19 pandemic.[1] Facing the challenge of the COVID-19 pandemic, most countries took very strict response measures to slow down the spreading of the COVID-19, such as lockdown measures, social isolation order, or stay-at-home order. The authorities close the shopping mall, schools, sightseeing, or other public places and limited the size of the gathering. The spreading of coronavirus was stopped after the stop of people's movement and communication.

Up to now, there is still no specific medicine that was allowed to be used in the fight against COVID-19. Achieving herd immunity may take 1 to 2 years or more time after large-scale vaccination.[2] Besides, there are more and more signs that the COVID-19 virus will become a long-last global problem.[3] However, control measures, such as lockdown and stay-at-home order, cannot last for a long time. It is an urgent need to recover society's function and economic production while preventing the COVID-19 pandemic. The need of restarting social production, strengthening surveillance ability, and accelerate the response measures become the key point of control measures. Contact tracing will play an important role in the surveillance, controlling, and prevention measures.[4] Reinforce and accelerate the contact tracing becomes an urgent matter. To solve this problem, digital contact tracing tools were widely used in many countries.[5]

---

[1] Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., & Abeler-Dorner, L. et al. (2020). Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Retrieved 30 December 2020, from https://science.sciencemag.org/content/368/6491/eabb6936/tab-pdf.

[2] Li, D. (2020). Expert: Large-scale vaccination will take 1-2 years. Retrieved 30 December 2020, from https://www.chinadaily.com.cn/a/202009/25/WS5f6d9777a31024ad0ba7bdf3.html.

[3] Sorace, S. (2020). Europe braces for more coronavirus lockdowns and restrictions as cases spike, winter looms. Retrieved 31 December 2020, from https://www.foxnews.com/world/europe-coronavirus-lockdowns-restrictions-winter.

[4] WHO, (2021). Critical preparedness, readiness and response actions for COVID-19. Retrieved 1 January 2021, from https://www.who.int/publications/i/item/critical-preparedness-readiness-and-response-actions-for-covid-19.

[5] Ibid.

In most countries, contact tracing and warning apps were the main approaches. These apps are the application of contact tracing based on smartphone and internet technology. The app aims to accelerate the searching of virus carriers and warning dangerous contact. According to research, the traditional manual contact tracing always has a several-day delay, which may not enough to even slow down the rapid transmission of COVID-19.[6] Comparing with the manual way, digitalized contact tracing tools can provide more timely warnings to health authorities and users. This kind of measure is firstly taken in Asian Countries, which have been proved effective in finding the confirmed cases and the people who have contact with the confirmed cases.

This successful use of contact tracing based on the smartphone app attracts the eyesight of many countries, including the European countries. Before the initiative of the European Union (EU), many European Member States have begun their project of the application of digital contact tracing tools.[7] Based on the project of EU member states, the EU began the project at the Union level. Similar to these measures taken in Asian countries, the publishing of the EU project of mobile contact tracing and warning apps leading to even more controversy. About the controversial legality question, the public main concern about data protection.

In Europe, people are very concerned about their personal data, which is a part of privacy, which was thought of as the ability to withhold one's information to keep one's life from public view.[8] A large number of internet technology will indeed cause danger to move in a surveillance society or the internet, which will record the people's online or physical activities.[9] Besides, some internet technology such as predictive data mining always provides "information" about individuals.[10] Hence, most applications of new technology will unavoidably suffer the concern of privacy, which may become a panic with improper media hype. Even the panic will be relieved after most people began to understand and use the technology. This panic will inevitably slow down the application of the new technology, even result in ill-conceived policy responses that fail to adequately promote potentially beneficial technologies, which is the influence of the 'privacy panic circle'.[11] This problem will also occur in the

[6] Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., & Abeler-Dorner, L. et al. (2020). *supra* note 1.

[7] eHealth Network, (2020). Mobile applications to support contact tracing in the EU' s fight against COVID-19 Common EU Toolbox for Member States, pp. 10-12. Retrieved 1 October 2020, from https://ec.europa.eu/health/ehealth/key_documents_en#anchor0.

[8] Savin, A. (2013). *EU Internet law*. Edward Elgar, p. 190.

[9] Castelluccia C. (2012). Behavioural Tracking on the Internet: A Technical Perspective. In: Gutwirth S., Leenes R., De Hert P., Poullet Y. (eds) *European Data Protection: In Good Health?*. Springer, Dordrecht, p. 22.

[10] Jonas, J., & Harper, J. (2006). Effective Counterterrorism and the Limited Role of Predictive Data Mining. Cato Institute. Retrieved 1 October 2020, from http://www.jstor.org/stable/resrep04886.

[11] Castro, D., & McQuinn, A. (2015). The Privacy Panic Cycle: A Guide to Public Fears About New Technologies, pp. 1-2. Information Technology & Innovation Foundation. Retrieved 30 December 2020, from https://itif.org/publications/2015/09/10/privacy-panic-cycle-guide-public-fears-about-new-technologies.

application of digital contact tracing tools. To avoid the influence of the 'privacy panic circle', the following factors need to be taken into consideration: the level of technological obscurity; the level of trust in the producers or users of the technology; the perceived value of the technology. [12] Let the public have a better knowledge of digital contact tracing tools. This popular science propaganda will effectively promote the public to accept this new technology. Therefore, it is important to show the data protection level of the digital contact tracing tool before introducing this measure to the public.

This report will focus on whether the decentralized contact tracing and warning apps can ensure the users' rights to data protection under the framework of the General Data Protection Regulation (GDPR). The GDPR aims to entitle data subjects to have more control over their personal data. So, if the application of digital contact tracing tools can be proved to comply with the framework of GDPR, the potential users will know more about the digitalized contact tracing technologies. Better knowledge about these technologies will relieve the worry about privacy issues, and promote more European people to determine to install and enable mobile contact tracing and warning apps. This is a very important condition for these apps to effectively work in pandemic surveillance and prevention. A required coverage rate of the use of these apps is the basic need to breach the transmitted chain.[13] As the European Data Protection Board (EDPB) noted in their guidelines: the legality of mobile contact tracing and warning apps will win the trust of people, which could create the conditions for the effectiveness of these measures.[14]

Except for removing people's worry, the decentralized contact tracing tools are a wide range of applications of decentralized digital systems. This provides a good sample to study the applicability of the current data protection framework. The legality research of the decentralized contact tracing apps will be the foundation of this further study and the improvement of the data protection framework which can be effectively applied to both centralized or decentralized systems.

To understand the legality of mobile contact tracing and warning apps under the GDPR framework, it will be necessary to study how these smartphone apps work. After we know how it runs and the detailed function of these smartphone apps, we can check these apps with the requirements of GDPR. So, in Part II, this report will introduce the work and function of the mobile contact tracing and warning apps, including the conceptions about contact tracing and contact tracing apps, to establish a general knowledge of decentralized contact tracing apps. Part III will first examine whether there are personal data processed on decentralized contact tracing apps. That's

[12] Ibid, pp. 6-8.

[13] Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., & Abeler-Dorner, L. et al. (2020). *supra* note 1.

[14] EDPB. (2020). Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, p. 3. Retrieved 6 January 2021, from https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-042020-use-location-data-and-contact-tracing-tools_en.

the precondition to applying rights to data protection.[15] Then, this part will further analyze who should undertake the data protection responsibility, what rights do data subjects have how the data subjects exercise their rights to data protection, and are there any difficulties during the data subjects exercising their rights to data protection in decentralized contact tracing? This report will then proceed in Part IV. In part IV, this report will analyze the legality issues from the perspective of fundamental rights protection. Several tests will be applied to the mandatory application of these apps. In the last part, this report will conclude the legality of mobile contact tracing and warning apps and try to give some suggestions about how to make better use of these smartphone apps.

2 Contact Tracing based on the smartphone app

The present part will lay out the background of the analysis in this report by providing a cursory overview of contact tracing and contact tracing mobile phone apps. It must be clear from the outside that digital contact tracing technology is used to enhance surveillance to help public health management. This technology is designed to take the place of some manual process. Therefore, understanding the function of manual contact tracing will help us understand the function of digital contact tracing tools. Furthermore, this will become the foundation of analyzing the legality problems of decentralized contact tracing apps applied in EU member states.

2.1 Introduction of contact tracing apps in the EU

To have comprehensive knowledge of decentralized contact tracing apps, several conceptions need to be clarified first, including contact tracing, contact tracing apps, and classification of contact tracing apps. Then, this report can analyze the features of the decentralized contact tracing and the potential challenges of the application of GDPR.

2.1.1 Contact tracing and digital tools

[15] General Data Protection Regulation, Regulation(EU) 2016/679, article 11.

Contact tracing is a classical response measure against communicable diseases.[16] According to the guidance of WHO, contact tracing is a process of finding potential infections.[17] People in close contact with someone who is infected with a virus are at higher risk of becoming infected themselves, and of potentially further infecting others. The application of this measure will help the contact to get medical care and might prevent further transmission. Usually, contact tracing measure contains three basic steps: Contact identification, Contact listing, Contact follow-up.[18] Contact identification is the process to try to find more people who have contact with the confirmed cases. Contact listing is the next step after contact identification, which will impose control measures on the people on the contact list, those measures including provide medical care to the people who have developed symptoms, quarantine, or isolation. During the entire process, contact identification could be the most important step. Because all other measures could only be taken after the confirmed cases and contacts were found. About how to identify enough contact which will help to prevent further transmission of the COVID-19 virus, the standard of contact needs to be clarified.

According to the guidance published by WHO, there are 4 standards, if the people who were questioned satisfied one standard. The people could be defined as 'contact' with the infection. A contact is defined as anyone with the following exposures to a COVID-19 case，from 2 days before to 14 days after the case's onset of illness:

• Being within 1 meter of a COVID-19 case for >15 minutes;

• Direct physical contact with a COVID-19 case;

• Providing direct care for patients with COVID-19 disease without using proper personal protective equipment (PPE);

• Other definitions, as indicated by local risk assessments. If confirmed cases are asymptomatic, contacts should be managed in the same way as for asymptomatic cases with an exposure period from 2 days before the case was sampled, to 14 days after.[19]

These standards are very clear and helpful to find the people who have contact with the virus. The members of the contact tracing interview team will gather information by question the diagnosed cases and try to find the contact. Usually, a

[16] Levine, M. L, (1988). Contact Tracing for HIV Infection: A Plea for Privacy, *Columbia Human Rights Law Review, Vol.20(1)*, p. 161. See also in Centers for Disease Control, Additional Guidelines for Testing and Counseling of Persons with HIV Infection and AIDs app IV, at 1(1987).

[17] WHO. (2021). Contact tracing in the context of COVID-19. Retrieved 20 February 2021, from https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19.

[18] WHO. (2017). Infection control: Contact tracing. Retrieved 30 December 2020, from https://www.who.int/news-room/q-a-detail/contact-tracing.

[19] WHO. (2021). *supra* note 17.

confirmed case may contact several hundred people in 2 weeks. The problem is the manual conducted contact tracing relying on the memory of the confirmed cases and other investigators. However, most people are not able to memorize so many people who have contact with them in 2 weeks. Some confirmed cases may be in bad condition and cannot be questioned by public health investigators. It will be difficult to find the required amount of contact.[20]

Besides, the question process often takes much time. In the guidance of WHO, the authority needs to identify, report, and data included in the epidemiological analysis of the new cases within 24 hours.[21] Due to the rapid transmission and big work for manual investigating the contact, manual investigation of contact will have difficulty in preventing or slowing the spreading of the COVID-19 virus. That's the reason why a more powerful contact tracing tool is needed in contact identification. Contact tracing based on smartphone apps could be a useful tool for surveillance and investigation. The application of this method needs some conditions. The advantage of this method is that these apps can accelerate the completion of contact identification. Taking timely response measures is of great importance in fighting against the COVID-19 pandemic. The more efficiency in finish contact identification, the less further transmission will occur.

Digital contact tracing tools were applied by EU member states in early March. The response measures at the EU level are about a month later. Most EU member states publish their nation contact tracing apps. In April, the EU Commission published a recommendation about the digital contact tracing tool.[22] After the publishing of this recommendation, the eHealth Network published a guidance document about the requirement and summary of nation contact tracing apps, which summarizes the application of digital tools in EU member states and reveals the detail about the requirements of decentralized contact tracing.

2.1.2 Classification of contact tracing apps

There are different types of contact tracing mobile phone apps in the EU, including the StopCovid, Corona-Warn-App, and other apps. Different kinds of technology were applied to these smartphone apps, for example, the choice of France

[20] At least 80% of contact needs to be found out in 24 hours can prevent further transmission.
[21] WHO. (2020). Surveillance strategies for COVID-19 human infection. Retrieved 30 December 2020, from https://apps.who.int/iris/bitstream/handle/10665/332051/WHO-2019-nCoV-National_Surveillance-2020.1-eng.pdf?sequence=1&isAllowed=y.
[22] The European Commission, (2020). Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data. Retrieved 30 December 2020, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020H0518&qid=1615189292172.

government origins from Pan-European Privacy-Preserving Proximity Tracing(PEPP-PT), the Germany and Italy government choose to develop the contact tracing app based on the platform provided by the Apple & Google as their national solution. Different types of contact tracing apps represent the application of different technology solutions. These solutions could be generally grouped into two different categories---Decentralized processing and Backend server solution.[23]

The backend server solution is a centralized design. This type of digital contact tracing tool will be based on a central server. All collected personal data will be sent to the database of the central server automatically, including tracing and contact information. The center server will process this data to tracing and notifying the people that could potentially be infected.[24] The users will get the notice when they suffered the risk of exposure to the COVID-19 virus. The users may seek medical help from healthy institutions, and avoid contact with other healthy people. The controllers of this solution are generally the public health authorities. The public health authorities will get more timely information about the potential spreading of the COVID-19 virus. Except for the contact information, this method can easily integrate more functions, and collect more types of information, including location data, tracing data, or other users' personal information. The backend server solution was widely used in Korea, China, Russia, etc. In the EU, this type of contact tracing apps can also be applied. Because of cultural reasons, this type of apps is more possible to be questioned by the public about the necessity of this surveillance. In this option, the backend server of this system can only store and process the contact information in an anonymous way, which cannot be directly identified through this identifier.[25]

Another solution is decentralized processing. The decentralized processing solution is the contact information will be stored and processed in users' devices. In the decentralized solution, arbitrary identifiers were still an important design for privacy protection, which also play the role of identifiers of users. The decentralized processing solution functions based on the proximity data stored in the users' devices.[26] Except for arbitrary identifiers, additional information is also needed in realizing the contact tracing and exposure notification. For safeguard reasons, the arbitrary identifiers are used to record contact information, and not able to directly identify a user. The arbitrary identifiers are separate from the additional information[27] which is used to identify a user. The additional information will be used after encrypted processing.

[23] eHealth Network, (2020). *supra* note 7, p. 27.
[24] eHealth Network, (2020). *supra* note 7, p. 28.
[25] eHealth Network, (2020). *supra* note 7, p. 28.
[26] eHealth Network, (2020). *supra* note 7, p. 27.
[27] Additional information is the necessary information to identify a user's devices.

In the EU, most decentralized contact tracing apps use the Exposure Notifications API[28] provided by Google and Apple.[29] Hence, taking the Exposure Notification API as an example, the arbitrary identifiers are called Temporary Exposure Key(TEK) [30] , Rolling Proximity Identifier(RPI). [31] The Associated Encrypted Metadata(AEM)[32] records the additional encrypted information which is necessary to identify the users. These 2 sets of data are usually stored separately. When the users of this API enable the decentralized contact tracing apps, TEK will be generated every day. RPI will be produced based on TEK every 15 minutes. AEM and RPI will be exchanged between users' devices to produce contact information. This information will be processed on users' devices.

When a user was tested positive, his TEK will become Diagnosed Key.[33] The Diagnosed key will be transmitted to the other users whose smartphone has record the contact combining with AEM. Their equipment will warn the users. The users will get the necessary information for deciding whether to seek help from the public health authorities or other medical institutions. As the recommendation of the EU, this should be voluntary for users to decide whether to join in. The users shall be allowed to decide whether to connect with the public health authorities, and whether to get medical care.

No matter which solution was applied in the end, privacy protection needs to be taken into consideration. Appropriate measures and necessary safeguards need to be taken to provide effective implementation of data protection and ensure the data subjects' rights and freedoms by design and by default.[34] In the current stage, the contact tracing digital tools are involved in many safeguard measures to reduce the risks to identify or trace the users. These measures, such as encryption, will reduce the

---

[28] Application Programming Interface(API) is a software-to-software interface that defines the contract for apps to talk to each other on a network without users' interaction. There are different types of API. The Exposure Notification API is an API for operation systems, which is used by system hardware and apps. See Brajesh De. (2017). *API Management: An Architect's Guide to Developing and Managing APIs for Your Organization* , Apress, Berkeley, CA, pp. 1-3.

[29] eHealth Network, (2020). European Proximity Tracing-An Interoperability Architecture for contact tracing and warning apps, p. 8. Retrieved 30 December 2020, from https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interop_architecture_en.pdf.

[30] See Apple & Google, (2020). Exposure Notification Bluetooth® Specification Preliminary-Subject to Modification and Extension, p. 3. Retrieved 30 October 2020, from https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.2.pdf. Temporary Exposure Key is a key that' s generated every 24 hours for privacy consideration.

[31] Ibid. Rolling Proximity Identifier is a privacy-preserving identifier derived from the Temporary Exposure Key and sent in the broadcast of the Bluetooth payload. The identifier changes about every 15 minutes to prevent wireless tracking of the device.

[32] Ibid. Associated Encrypted Metadata (AEM) — A privacy-preserving encrypted metadata that shall be used to carry protocol versioning and transmit (Tx) power for better distance approximation.

[33] Ibid. Diagnosis Key — The subset of Temporary Exposure Keys uploaded when the device owner is diagnosed as positive for the coronavirus..

[34] EDPB, (2019). Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, p.4. Retrieved 1 October 2020, from https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

potential risks that the users may be singled out and traced, which is believed to enhance the protection over the users' privacy.

2.2 Features of decentralized contact tracing

According to the relevant document, there are 4 basic requirements for the application of contact tracing apps: voluntary; approved by the national health authority; privacy-preserving personal data is securely encrypted; and dismantled as soon as no longer needed.[35] Comparing these two kinds of contact tracing technology, there are several different places. The decentralized contact tracing apps have the following features.

First, point-to-point transmission: In a decentralized contact tracing system, the contact information was stored and processed on users' devices. Most personal data are transmitted between the users' smartphones who have contact with each other. Except for the diagnosed cases, whose information will be transmitted to medical institutions' and public health authorities' databases. Hence, there are only a few data will be transmitted to the public health authorities, or other third parties. This mechanism limits the scope of information transmission. The point-to-point transmission will strengthen data security and privacy protection.

Second, decentralized data storage and processing framework: decentralized contact tracing apps feature decentralized data storage and processing. Personal data used in this system is temporarily stored in each users' smartphone. What's more, the data will mainly be processed on users' devices. Only the personal data of diagnosed infected will be processed in the central database of public health authorities. Hence, the processing of personal data more relies on the automatic processing of the decentralized contact tracing app on users' devices. This processing will also sift through the necessary data for public health authorities. The public authorities may only collect the necessary personal data, such as the personal data of infected or asymptomatic infected of COVID-19. This will help the public authorities to conduct targeted personal collection and processing, which will relieve the burden of daily surveillance.

2.3 Challenges to personal data protection

The application of these decentralized apps may bring the following challenges.

[35] eHealth Network, (2020). *supra* note 7, pp. 10-12.

The first challenge arises from the safeguard measures which are used to reduce the chance to identify or single out the users. These measures include typical technology of anonymization. If the data on decentralized contact tracing apps should be regarded as anonymous information[36], these data in decentralized contact tracing apps will not get protection like personal data. The application of GDPR will be influenced. Hence, it is necessary to analyze the conditions for the data on the decentralized contact tracing apps to be qualified as personal data.

Second, these decentralized contact tracing apps raise a few challenges in the coordination of a large number of individuals.[37] Coordination and management need to be done in a more distributed way.[38] Due to the point-to-point transmission and decentralized data storage and processing, most personal data, the contact information, will be stored and transmitted between users' devices. However, the data controllers undertake the main obligations of personal data protection. Hence, it is important to analyze who is the data controller.

Moreover, rights to data protection are an important part of personal data protection. The exercise of the rights to data protection relies on the coordination and management of controllers. The decentralized data storage and processing framework will bring difficulties to coordination and management. These difficulties will finally influence exercising rights to data protection.

Last but not the least, mandatory applying these decentralized contact tracing apps will bring the legality problems of fundamental rights protection since the rights to data protection are fundamental rights.[39] It is a basic requirement for mandatory applying of these apps to comply with the rules of fundamental rights protection, especially the principle of proportionality.[40] Hence, proportionality tests need to be applied to analyze the legality of mandatory applying these apps.

3 Applying GDPR to Contact Tracing based on smartphone apps

After knowing about contact tracing and relevant digital tools, the next question is the legality of decentralized contact tracing in the EU. The impact of these

[36] See General Data Protection Regulation, Regulation(EU) 2016/679, recital 26.Anonymous information means information that doesn't relate to an identified or identifiable natural person, or to personal data rendered anonymous in such a manner that the data subjects are not or no longer identifiable. This regulation does not, therefore, concern the processing of such anonymous information, including for statistical or research purposes.

[37] De Filippi, P. (2016). The interplay between decentralization and privacy: the case of blockchain technologies. *Journal of Peer Production, Vol.7*. Retrieved 30 December 2020, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852689.

[38] Ibid.

[39] Charter of Fundamental Rights of the European Union, 2012/C 326/02, article 8.

[40] Charter of Fundamental Rights of the European Union, 2012/C 326/02, article 52. 1.

apps on the application of the GDPR also needs to be evaluated. In the EU, data protection was regarded as a fundamental right.[41] GDPR could be the most important legislation and pillar of the data protection law in the EU. Comparing with the Data Protection Directive, GDPR adds more new concepts and making several provisions more precise.[42] This helped make the GDPR easier to be applied. Now that the GDPR is the cornerstone of the current EU data protection framework. The main legal basis of the analysis will also be the GDPR, and the applicability needs to be first discussed.

3.1 Personal data

The GDPR is set up to establish a high standard for EU citizens' personal data protection, which mainly controls the processing of personal data. To apply GDPR to decentralized contact tracing apps, the precondition is that the data transmitted and processed on these apps can be qualified as personal data.[43] The GDPR defines personal data as any information related to an identified or identifiable natural person.[44] "Identified" means "single out" or "distinguish" someone from a group of people. [45] "Identifiable" means someone was not identified, but he can be "singled out" or "distinguished" from a group of people with other information.[46] The GDPR set a very low threshold for the determination of "personal data", if some data was possible to directly or indirectly identify some natural people, this data will constitute personal data.[47] When these apps process personal data, the data subjects can exercise their rights under GDPR article 15 to 20.[48]

On a decentralized contact tracing app, there are two sets of data processed in the system: arbitrary identifiers and additional encrypted information. Therefore, the precondition of the applicability of GDPR of decentralized contact tracing app is that arbitrary identifiers and additional encrypted information can constitute personal data. In the EU, most decentralized contact tracing apps were designed based on the Exposure Notification API provided by Apple and Google. Hence, this section will take the technology provided by Apple and Google as an example to analyze whether

[41] Charter of Fundamental Rights of the European Union, 2012/C 326/02, article 8.
[42] Savin, A. (2013). *supra* note 8, p. 206.
[43] Finck, M. (2018). Blockchains and Data Protection in the European Union, *European Data Protection Law Review, Vol.4(1),* p. 22.
[44] General Data Protection Regulation, Regulation(EU) 2016/679, article 4 (1)
[45] Jasserand, C. (2016). Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data. *European Data Protection Law Review, Vol.2(3)*, p. 302. See also Article 29 Data Protection Working Party (A29WP), Opinion 4/2007(n 36) 12-13.
[46] Ibid.
[47] Gstrein, O. J., & Ritsema van Eck, G. J. (2018). Mobile devices as stigmatizing security sensors: the GDPR and a future of crowdsourced 'broken windows'. *International Data Privacy Law, Vol.8(1)*, p. 80.
[48] General Data Protection Regulation, Regulation(EU) 2016/679, article 11.

the data processed on a decentralized contact tracing system could be defined as personal data.

3.1.1 Arbitrary identifiers

The arbitrary identifier is a set of random numbers that represents a user's device, which indirectly represents the user in the contact record.[49] This identifier will be rapidly generated, which could provide better protection to the users' privacy. In the API provided by Apple and Google, the users' devices will be named TEK and RPI.

The TEK contains information relating to the health status of the users. Firstly, after a user being diagnosed as the infected patient of COVID-19, their TEK in the past 14 days(or other lengths of a period) will be classified as Diagnosed Key, which means that the user is the diagnosed case or carrier of COVID-19 virus. Therefore, before the users are diagnosed as infected with the COVID-19, TEK can represent the users are healthy people. Combining with additional encrypted information, the TEK can finally be related to the users.

Hence, the TEK is related to an identifiable or identified natural person and constitutes personal data. Moreover, there are several different categories of personal data in the classification of GDPR. The level of data protection is different between different categories of personal data.[50] Therefore, to determine the personal data on a decentralized contact tracing app will get which standards of personal data protection, the categories of personal data need to be confirmed.

Under the framework of GDPR, special categories of personal data will be given a higher standard of protection. These special categories of personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data to uniquely identify a natural person, data concerning shall be prohibited.[51] Personal data concerning health usually are very sensitive to individuals in Europe due to some cultural reasons. Hence, European tend to give a very general definition of "Personal data concerning health". As the practice of the European Court of Justice(ECJ), the expression "data concerning health" must be given a wide interpretation to include

[49] On most occasions, the devices, such as smartphones, can play the role of the ID card of a natural person. So, identifying a device will identify the owner of this device.

[50] For example, the common personal data will only get the basic protection such as principle relating to the processing of personal data(Article 5, GDPR), lawfulness processing(Article 6, GDPR), consent(Article 7, GDPR). However, GDPR imposes a more strict restriction on the processing of the data of children(Article 8, GDPR) and special categories of personal data.

[51] General Data Protection Regulation, Regulation(EU) 2016/679, article 9.

information concerning all aspects.[52] In related GDPR provisions, personal data related to the physical and mental health of a natural person, including the provision of health care service, which reveals information about the natural persons' health status, constitute "data concerning health". [53] In the preamble of GDPR, the content of personal data concerning health should include all data relating to the health status of the data subject which reveals the information relating to the past, current or future physical or mental health status of data subjects.[54] This definition includes all the collected personal data which may be used to reveal or predict the health status of a natural person.[55] As the personal data which may predict the future health status of a natural person constitute 'data concerning to health', the data which can predict the 'disease risk' should be a part of the 'data concerning to health'. In other words, as soon as the data can be used to identify disease risk, the data could be qualified as data concerning health.[56]

As having been discussed before, in the European Union's technical response measures against the COVID-19 pandemic, TEK, RPI, and Diagnosed Key all related to the health status of the users, an identified or identifiable natural person. Therefore, in the EU's technical response measures against COVID-19, the TEK, RPI, and Diagnosed Key are used to reveal the risk of being infected with the COVID-19 virus. These three kinds of data constitute personal data concerning health.

3.1.2 Additional encrypted information

For safeguard reasons, important data will be separated stored. On the contact tracing system, contact information will be separated from the additional information which will be related to an identified or identifiable natural person. In the API provided by Apple and Google, Associated Metadata plays the role of additional information, recording the time, the Bluetooth identifier, IP address, or other similar identity information.[57] AEM plays the role of additional encrypted information in the Exposure Notification API provided by Apple and Google. AEM is encrypted from Associated Metadata to enhance the safety level of data protection.

The associated metadata contains the IP address of each device, ensuring that two devices can be correctly identified and that no contact recorded data packets are

[52] ECJ (2003). Case C-101/01 Lindqvist case, EU:C:2003:596, para 50.
[53] General Data Protection Regulation, Regulation(EU) 2016/679, article 4 (15).
[54] General Data Protection Regulation, Regulation(EU) 2016/679, Recital (35).
[55] Mulder, T. (2019). The Protection of Data Concerning Health in Europe. *European Data Protection Law Review, Vol.5(2)*, p. 216.
[56] Ibid, p. 217.
[57] For example, Peter' s smartphone gets TEK-1 and produces RPI-1 through method-1 of encryption at 19:00, 9/29. This information will be recorded by Associated Metadata.

misdelivered.[58] In the Scarlet Extended case, the ECJ held that the IP address of internet users constitutes personal data, which may be used to precisely identify the data subject.[59] In Patrick Breyer v. Germany case, the ECJ further confirmed that the dynamic IP may be regard as personal data with additional information stored by controllers or third parties.[60] Hence, there is no doubt that the associate metadata constitutes personal data. The question is what's the impact of encryption processing under the framework of GDPR? Encryption is a typical pseudonymization technique,[61] which may also be used for anonymous techniques. The GDPR leaves no doubt that personal data has 'undergone pseudonymization, which could be attributed to a natural person by the use of additional information' constitutes personal data.[62] Under the framework of GDPR, pseudonymization means the processing of personal data which makes it cannot be related to an identified or identifiable natural person without the reference of other specific data or information.[63] What's more, the material of Apple & Google's contact tracing technology shows that the AEM connects to Bluetooth identifier which may be traced back to the IP addresses.[64] Most AEM is stored in users' devices. The AEM cannot directly trace back to the IP address of users. There are still some necessary preconditions to decrypt the AEM and trace the IP address, such as the decryption mechanism. Currently, the information and technology of decryption of the AEM which can be traced back to the users' IP are held by the API provider and public health authorities.[65]

To determine whether a person can be identified by AEM, it is based on a pseudonymous data account that has to be taken of 'all means reasonably likely to be used by controllers or third parties.[66] Recital 26 of GDPR refers to the means reasonably likely to be used by the controller or another person, directly or indirectly.[67] "indirectly" suggest that it is not necessary the information alone allows the data subject to be identified when this information was treated as personal data.[68] For AEM to be treated as "personal data", it is not required all the information enabling the identification of the data subject must be held by one person.[69]

---

[58] Froomkin, A. M. (2000). The death of privacy? *Stanford Law Review, Vol.52*(5), p. 1491.
[59] ECJ (2011). Case C-70/10 Scarlet Extended case, EU:C:2011:771, para 51.
[60] ECJ (2016). Case C-582/14 Breyer case, EU:C:2016:779, para 49.
[61] A29WP. (2014). Opinion 05/2014 on Anonymisation Techniques, p. 20. Retrieved 30 December 2020, from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.
[62] General Data Protection Regulation, Regulation(EU) 2016/679, recital (26).
[63] General Data Protection Regulation, Regulation(EU) 2016/679, article 4 (5).
[64] Apple & Google, (2020). *supra* note 30, pp. 4-6.
[65] API providers develop such API. It is reasonable to believe they have the technology to decrypt the AEM and use this information to trace the users. The public health authorities need to decrypt the AEM of users so that they can find the people who have contact with the COVID-19 virus.
[66] Finck, M. (2018). *supra* note 43, p. 24.
[67] General Data Protection Regulation, Regulation(EU) 2016/679, recital (26).
[68] ECJ (2016). *supra* note 60, para 41.
[69] Ibid, para 43.

Hence, whether the possibility of AEM combines with the decryption information and technology constitutes a means likely reasonably to be used to identify the users of decentralized apps will determine whether AEM constitutes personal data. In dynamic IP case, the ECJ held if the identification of data subjects was prohibited by law or practically impossible on the account of the fact that it requires disproportionate efforts in terms of time, cost, and man-power, such means of processing personal data cannot be regarded as likely reasonably means.[70] There is no doubt that the API providers have the means or technology to combine the AEM with decryption. The public health authorities can use the AEM to identify the users for communicable disease prevention with the decryption technology provided by API providers. According to the guideline of EDPB, the public health authorities can use personal data, such as proximity data, for COVID-19 pandemic prevention.[71] Therefore, the AEM constitutes personal data when it was used by API providers and public health authorities for communicable diseases prevention.

To conclude, detecting and recording the 'contact' between different users is the basic function of the decentralized contact tracing apps. The record of contact is the basis for tracing the contact. To realize this design, there will be unavoidable processing of the data which will be connected to the devices and the users. Furthermore, due to the results of contact will be the evidence to predict the health status of the users, the data processed on decentralized contact tracing apps constitute data concerning health.

With the right additional information and decryption processing, the arbitrary identifiers and AEM could be related to the users, a natural person. Now that the data processed on decentralized contact tracing apps should be qualified as personal data concerning health, the controllers and processors need to make sure of the safety of personal data, observe the administration of data protection authorities, and protect the rights of data subjects.[72] Hence, the data concerning health can be processed during the period against the COVID-19 pandemic, but the processing needs to comply with the requirements of GDPR.

3.2 Data Controller

The GDPR has a salient innovation---extend jurisdiction.[73] Due to the extended jurisdiction of GDPR, this regulation applies to all establishments, including

[70] Ibid, para 46.
[71] EDPB. (2020). *supra* note 14, p. 10.
[72] Porcedda, M.G. (2012). Law Enforcement in the Clouds: Is the EU Data Protection Legal Framework up to the Task?. In: Gutwirth S., Leenes R., De Hert P., Poullet Y. (eds) *European Data Protection: In Good Health?*. Springer, Dordrecht. p. 209.
[73] Trivellato, U. (2019) Microdata for Social Sciences and Policy Evaluation as a Public Good. In: Crato, N., Paruolo, P. (eds) *Data-Driven Policy Impact Evaluation*. Springer, Cham, p. 31.

enterprises, public bodies, or other individuals or entities, processing the personal data of the EU residents.[74] The territorial scope won't obstacle the GDPR applies to the decentralized contact tracing apps. In GDPR, there are three important players in personal data protection: the data subject, the data controller, and the data processor. Data controllers are the party responsible for ensuring that the processing of personal data is in accordance with the GDPR.[75] On decentralized contact tracing apps, two important players are public health authorities and users. The provider of the development platform is also an important participator.

It is no doubt that the users in the decentralized contact tracing play the data subjects' role, from whom the personal data is collected. However, who is the data controller could be a problem. Public health authorities are the operators of the apps. The users' devices keep and process personal data. The development platform is the foundation for many decentralized contact tracing apps. The providers may have decision-making power about the processing at some level. This section will answer the question that who can be qualified as data controllers on decentralized contact tracing.

3.2.1 Public Health Authorities

On decentralized contact tracing apps, public health authorities still play one of the most important roles. Some apps are even directly developed by these authorities, or developed based on the technology or the platform provided by others. They set up the detailed national standards of 'contact' for the apps.[76] These standards will be applied to the decentralized contact tracing apps. The public health authority will also process the arbitrary identifiers of diagnosed cases and inform the users who have recorded contact with the diagnosed cases. So, public health authorities are possible to be qualified as controllers, which the GDPR is addressed.[77]

The data controller is defined as any natural or legal person, public authority, or other body, alone or jointly with others, who can determine the purposes or means of the processing of personal data.[78] In other words, the data controller is the natural person or legal person who can determine including how to make use of the personal data, which data will be collected, who to collect data from, and so on.[79]

---

[74] General Data Protection Regulation, Regulation(EU) 2016/679, article 3.
[75] Governance, I. T. (Ed.). (2017). *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide*. IT Governance Publishing, p. 17.
[76] WHO' s standard is technical guidance which can be referred by every country to set up their own standards.
[77] Finck, M. (2018). *supra* note 43, p. 26.
[78] General Data Protection Regulation, Regulation(EU) 2016/679, article 4(7).
[79] Governance, I. T. (Ed.). (2017). *supra* note 75, p. 18.

From the definition of the data controller, it can be confirmed that the legal definition consists of five main components: (1) a natural or legal person, public authority or other body; (2) alone or jointly with others; (3) determine; (4) the purposes or means; (5) of processing of personal data.[80] In judicial practice, the ECJ tends to hold effective and complete protection of the persons concerned, through a broad definition of the concept of 'controller'.[81] It's easy to apply GDPR to the owner of a centralized database and centralized intermediary operator.[82] Controllership depends upon decision-making power,[83] which relates to two key components: "determine" and "the purpose or means".

"Determine" is an important component of the controller concept, which refers to the controller's influence over the processing by exercising decision-making power.[84] The competence of controllership may stem from the law or an analysis of the factual elements.[85] The legal basis includes Union or Member State law, no matter explicit or implicit.[86] "Purposes and means" is another important component of the controller concept, which refers to the object of the controllers' influence of processing of personal data.[87] Controllers must determine both "purposes and means" of the processing. That means the controller cannot settle with only determining the purposes. What's more, the controllers need to determine the essential means of the processing.[88] Essential means are closely linked to the purpose and scope of the processing of personal data, such as which data should be processed, etc.[89]

At the Union level, the European Center for Disease Prevention and Control(ECDC) undertakes the operation of the early warning and response system against infectious disease. Within the field of its mission, the ECDC shall collect, process personal data for relevant scientific and technical purposes.[90] This provision directly provides the legal basis to ECDC collect and process relevant data, which shall include necessary personal data for fulfilling the mission of ECDC.[91] The national competent authorities shall provide relevant data to ECDC.[92] Hence, data collection

[80] EDPB. (2020). Guidelines 07/2020 on the concepts of controller and processor in the GDPR, p. 9. Retrieved 30 December 2020, from https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en.
[81] ECJ (2018). Case C-210/16 Wirtschaftsakademie Schleswig-Holstein case, EU:C:2018:388, para 28.
[82] Finck, M. (2018). *supra* note 43, p. 26.
[83] Voigt, P., & von dem Bussche, A.(2017). *The EU General Data Protection Regulation (GDPR)-A Practical Guide*: Springer, Cham, p. 19.
[84] EDPB. (2020). *supra* note 80, p. 10.
[85] Ibid.
[86] Ibid, p. 11.
[87] Ibid, p. 13.
[88] Ibid.
[89] Ibid, p. 14.
[90] Regulation (EC) No 851/2004 of the European Parliament and of the Council of 21 April 2004 establishing a European Centre for disease prevention and control, (2004), article 2.
[91] Regulation (EC) No 851/2004 of the European Parliament and of the Council of 21 April 2004 establishing a European Centre for disease prevention and control, (2004), article 20. 4.
[92] Regulation (EC) No 851/2004 of the European Parliament and of the Council of 21 April 2004 establishing a European Centre for disease prevention and control, (2004), article 4.

and processing are implicitly required in this provision. In the EU, the decentralized contact tracing apps are directly operated by each Member States. The national public health authorities could be qualified as data controllers.[93]

Furthermore, the prevention of infectious disease is within the scope of public health. In this circumstance, the public health authorities can even collect personal data, which is necessary to carry out their task for the public interest, without the consent of data subjects.[94] Besides, public health authorities may define the standard of dangerous contact. These standards determine the categories of data that shall be collected and processed in decentralized contact tracing apps. They can also function as operators to collect and process users' personal data. The diagnosed case will transmit their arbitrary identifiers to public health authorities' databases. The public health authorities will mark these identifiers as diagnosed, then send the exposure notification or contact warning to according the recording of the diagnosed case. These all indicate that the public health authorities indeed determine the essential means of the processing of personal data. Therefore, public health authorities constitute the data controller.

3.2.2 API Provider

As has been discussed above, the controller can alone or jointly with others determine the means or purpose of the processing of personal data.[95] Where two or more controllers jointly determine such processing, they shall be joint controllers.[96] Hence, the API provider may jointly determine the means and purposes of the processing of personal data on decentralized contact tracing. Different from the public health authorities, most API providers didn't have any competence. The qualification of the API provider as controllers needs to be established on the basis of an assessment of factual specific data processing activities.[97]

The providers have a great influence on the means of the processing of personal data. Exposure Notification API is a platform for public health authorities to develop decentralized apps. It integrates access to the data of the Bluetooth and other related functions of the Android and IOS system. This API also has the following designs, including recording the contact between the people, establishing a link between these records. The public health authorities can integrate their national or regional standards for contact and length of the data storage into their national or regional apps based on

[93] The European Commission, (2020). *supra* note 22.
[94] General Data Protection Regulation, Regulation(EU) 2016/679, article 6. 1.(e) and article 9. 2. (i).
[95] General Data Protection Regulation, Regulation(EU) 2016/679, article 4(7).
[96] General Data Protection Regulation, Regulation(EU) 2016/679, article 26, 1.
[97] EDPB. (2020). *supra* note 80, p. 11.

this API. Therefore, before developing apps, the public health authorities need to get the permissions to access these data from the system and users.

The public health authorities can indeed request the provider to provide some specific functions. The provider can refuse some requests. They can negotiate with public health authorities and play an important role in determining the means of processing personal data.[98] The provider also has great influences in the determination of the purpose of the processing. For example, Google and Apple request that the apps developed based on their platform shall not have the function of publishing advertisements before the authorization.

Now that the API provider has a determinative influence on the purposes and means of the processing of persona data on decentralized contact tracing apps. The API providers, including Apple and Google, shall be qualified as data controllers even though they may never have actual access to the data.[99]

3.2.3 The user

There is no doubt that the users are the data subject of decentralized contact tracing apps. Due to the features of decentralized processing, each node is separated from the others. The users join in the operation of these apps. Their personal data were stored in their devices with other users' contact records. That's why these apps were believed to let users get more control over their personal data. However, the users didn't alone or jointly join in determining the means and purposes of the processing of personal data. Hence, the users of decentralized contact tracing apps cannot be qualified as data controllers or joint controllers.

To sum up, the GDPR gives the concept of 'controller' in a sufficient broad way to ensure accountability and the effective and comprehensive protection of personal data.[100] The public health authorities and providers of the development platform could be qualified as the controllers of decentralized contact tracing. The users cannot be qualified as data controllers or joint controllers.

3.3 Rights to personal data protection

[98] For example, Apple & Google refuse the requirement of the German government to insist on a decentralized system. The result is that the Germany Government compromised and agreed with the decentralized contact tracing application.
[99] EDPB. (2020). *supra* note 80, p. 16.
[100] Ibid, p. 9.

After the analysis above, this report has shown that the GDPR can be applied to the decentralized contact tracing, and the platform provider should undertake the personal data protection obligation together with the public health authorities. All their processing needs to comply with the requirements of GDPR.

To ground the personal data protection, the GDPR also entitles the data subjects to have a series of rights, mainly including the right to access, right to rectification, right to be forgotten, right to restriction of processing, right to data portability, right to object, etc.[101] Data subjects can exercise these rights to control their personal data and protect their privacy. Rights to personal data protection are rights to claim. Data subjects may exercise these rights by requesting the controller to provide specific processing on their personal data. The rules of GDPR draw a beautiful blueprint for data protection. But there are more problems in applying these rules, especially when new data, computing, or internet technology were applied.

When the decentralized contact tracing apps are voluntary, the compliance of these apps will be limited to personal data protection issues. Mandatory applying these apps need to meet higher requirements than voluntary join in and out. Rights to data protection are fundamental rights in the EU.[102] Although, rights to data protection or right to privacy are not absolute rights, which must be considered in relation to its function in society.[103] Article 23 GDPR allowed member states to restrict the right to data protection by legislative measures. These restrictions also need to comply with the condition for specific processing situations[104] and the rule of fundamental right protection.[105] Hence, comparing with voluntary applying these apps, mandatory applying will have different impacts on the rights to data protection.

The following part will briefly introduce each right to data protection while unfolding the analysis of the impact of decentralized contact tracing apps on these rights from two mechanisms of applying these apps.

3.3.1 Right to access

The right to access means the right of data subject to access the personal data and the relevant information, including processing purposes, the categories of personal data processed, the recipients or categories of recipients, etc.[106] The setting of right to access is to give the data subject the comprehensive information right and impose the

[101] General Data Protection Regulation, Regulation(EU) 2016/679, article 12-21.
[102] General Data Protection Regulation, Regulation(EU) 2016/679, article 1. 2.
[103] ECJ (2010). Joint case C-92/09 and C-93/09 Volker und Markus Scheche and Eifert case, EU:C:2010:662, para 48.
[104] General Data Protection Regulation, Regulation(EU) 2016/679, 89. 3.
[105] Charter of Fundamental Rights of the European Union, 2012/C 326/02, article 52. 1.
[106] General Data Protection Regulation, Regulation(EU) 2016/679, article 15.

corresponding obligations on the controllers.[107] The users can also request the controllers to provide copies of their personal data. Therefore, this right plays a central role in the exercise of the substantial rights in the GDPR framework---it is the foundation to exercise other rights.

As for how to exercise the right to access? The data subject can request the controller provide the information they need. The controllers have the obligation to answer these requests. Not all requests of the data subjects will be given a positive answer, if the requests are "unfounded or excessive", the controller may refuse the request or charge a "reasonable fee" to cover the resulting administrative cost.[108] Besides, the right to access should not harm the rights or freedoms of others,[109] including the potential effects.[110] The controllers thereby need to be able to provide such information and copies of selected personal data.

From the perspective of technology, the decentralized data processing framework will complicate the access to personal data stored in users' devices. Public health authorities or API providers cannot easily get access to personal data stored in users' devices. The public health authorities may not get the necessary information. They may not know where the personal data stored. The management will be difficult for public health authorities and API providers. When these apps are voluntary join-in and out, the users may have difficulties in identifying the controllers, while the public health authorities and API providers cannot provide help. If healthy users want to get their contact data, they need to find other users who have contact with them.

What's more, in a decentralized data processing framework, most data stored and processed in users' devices are contact information, containing others' personal information, and need to get access to the other users' devices. Exercising the right to access will influence other users' right to privacy. The realizing of access will need the consent of the other users. This need to establish coordination between the need of different users. These will become the controllers' reasons to reject the users' requests. Moreover, on the decentralized contact tracing system, how to find the right user, whose devices store the target data, is also a problem. The users will have difficulties getting such information which is necessary to exercise their rights. This information may also bring too much transparency to the system. Even the right user and devices were finally found, verifying the accuracy of the received data could also be a problem. Therefore, the decentralized contact tracing app might be more acceptable for EU citizens but remains unfeasible in fully exercise the data protection right.

When the public health authorities require the mandatory use of these decentralized contact tracing apps. Union or Member States competent authorities may

[107] Voigt, P., & von dem Bussche, A. (2017). *supra* note 82, p. 150.
[108] General Data Protection Regulation, Regulation(EU) 2016/679, article 12(5).
[109] General Data Protection Regulation, Regulation(EU) 2016/679, article 15. 4.
[110] Voigt, P., & von dem Bussche, A. (2017). *supra* note 82, p. 153.

impose necessary derogations on the right to access.[111] The Union or Member States law can also provide grounds for restrictions on this right.[112] It is a practical choice to restrict the exercise of the right to access the personal data stored in users' devices, no need to provide related information or copies. In this way, public health authorities can avoid technical difficulties in management.

3.3.2 Right to rectification

Under Article 16 of the GDPR, individuals have the right to have inaccurate personal data rectified.[113] This right closely links to the accuracy principle.[114] The accuracy principle is one of the principles relating to the processing of personal data.[115] This principle requests that the data subject shall have the right to rectify and erase the inaccurate data.[116] Inaccurate data include incomplete data.[117] As data processing can negatively affect the rights and freedoms of data subjects, especially where it involves incorrect or incomplete data.[118] In the application of decentralized contact tracing digital tools, inaccurate data may result in the stigmatization of people who have been linked to the COVID-19 virus or disease.[119] Hence, it is necessary to entitle data subjects the right to rectify their personal data and help to correct or prevent negative effects on the rights of data subjects.[120]

The way of exercise the right is also requesting the controller to rectify. The controller shall not refuse this request without reasonable excuses. The controller shall rectify without undue delay. Similar to the right to access, the data subject needs to exercise this right by requesting the controller to provide information and rectification.

The decentralized contact tracing app is characterized by a decentralized data processing and storage framework. No matter these apps are voluntary to use by citizens or mandatory applied by authorities, controllers and data subjects will have difficulties in getting the inaccurate data stored in other users' devices, which leads to the rectification procedure that cannot continue. Therefore, it could be difficult to directly rectifying data on users' devices.

---

[111] General Data Protection Regulation, Regulation(EU) 2016/679, article 89. 3.
[112] General Data Protection Regulation, Regulation(EU) 2016/679, article 23. 1.(e).
[113] General Data Protection Regulation, Regulation(EU) 2016/679, article 16.
[114] Voigt, P., & von dem Bussche, A. (2017). *supra* note 82, p. 154.
[115] General Data Protection Regulation, Regulation(EU) 2016/679, article 5. 1. (d).
[116] General Data Protection Regulation, Regulation(EU) 2016/679, article 5. 1. (d).
[117] Governance, I. T. (Ed.). (2017). *supra* note 75, p. 58.
[118] Voigt, P., & von dem Bussche, A. (2017). *supra* note 82, p. 154.
[119] The European Commission, (2020). *supra* note 22.
[120] Voigt, P., & von dem Bussche, A. (2017). *supra* note 82, p. 154.

3.3.3 Right to be forgotten

Right to be forgotten is the right to request that their personal data be erased without undue delay if the grounds of the data processing are no longer exist.[121] According to the requirements of lawfulness processing of personal data, the grounds include consent, legal obligation, public interests, etc. In decentralized contact tracing apps, the grounds for controllers to process personal data include consent or public interest. This right derives from the Google Spain and Google case (2014)[122] and has now been strengthened in the GDPR framework, which imposes information obligations on the controller towards other parties who have to get the relative personal data.[123] It requires the controller to delete certain personal data, to prevent further disclosure or processing of the data, and to oblige the third party to delete links to such data.[124] In particular, the controller shall erase the personal data as the data subject's request without undue delay in several conditions: including the personal data is no longer necessary for the purposes it was collected or processed; the data subject withdraws consent to the processing, presuming the legal justification for processing doesn't exist; the data subject refuses the processing and there is no other legal basis for processing; data has been unlawfully processed; the data has to be erased under the legal obligation of EU or member states law; the data was collected in relation to "information society services".[125]

In the current scenario, when these apps are voluntary, the users may withdraw their consent at any time. They can only delete the personal data stored in their devices. The public health authorities cannot effectively manage and process the data stored on users' devices. The users are also not able to delete specific personal data. The controllers cannot respond to the users' deletion requests until the automatic deletion of the decentralized contact tracing system. Of course, these apps can provide instant automatic deletion after the users withdraw their consent. However, automatic response to the deletion requests will entitle the users with more autonomy of their personal data on the system. This autonomy will make it more difficult for the coordination and management of the decentralized contact tracing system.

When the decentralized contact tracing apps are mandatorily applied, restrictions on the right to be forgotten could be the inherent requirement of mandatory application.[126] According to article 17, para 3 of the GDPR, the right to be forgotten

[121] Governance, I. T. (Ed.). (2017). *supra* note 75, p. 59.
[122] ECJ (2014). Case C-131/12 Google Spain case, EU:C:2014:317, para 99.
[123] Voigt, P., & von dem Bussche, A. (2017). *supra* note 82, p. 156.
[124] Abril, P. S., & Lipton, J. D. (2014). The Right To Be Forgotten: Who Decides What the World Forgets, *Kentucky Law Journal*, *Vol.103(3)*, p. 365.
[125] General Data Protection Regulation, Regulation(EU) 2016/679, article 17. 1.
[126] General Data Protection Regulation, Regulation(EU) 2016/679, recital 156.

shall not be applied when the personal data were processed for public health.[127] Under current circumstances, the public health authorities use these apps to process users' contact information to prevent the spreading of the COVID-19 pandemic, which is necessary for the reasons of public interests in the area of public health.[128] Hence, the contact information needs to be kept for two weeks or other certain lengths of periods set by the public health authorities. During this period, the users shall not request for deleting the data processed in the system.

3.3.4 Right to restriction of processing

The right to restriction of processing means that the controller can only store or process the personal data within the scope of the consent of data subjects.[129] Unless the data subject gives their further consent to lift the restriction or the processing is necessary for the establishment of a legal claim, the controllers are not allowed to conduct further processing of their data.[130] This right is established to achieve a reconciliation of interests between data subjects and controllers.[131]

GDPR provides for 4 circumstances that the data subject can exercise the right to restriction of processing: data subjects contest the accuracy of the personal data, thereby restricting the controller to verify the accuracy of selected personal data; data subjects object to the deletion of their data when their personal data was unlawfully processed; the data subjects require the controllers for further storage for the establishment, exercising or defense of legal claims; the controllers' processing shall be restricted when the data subjects are exercising the right to object based on Article 21, GDPR.[132] The right to restriction of processing is also exercised through the requests of the data subject. The data subject needs to raise sufficiently clear requests to the controller.[133] However, clear requests may be difficult for data subjects to make since the decentralized framework bring challenges to users' and controllers' access to the data in users' devices.

Besides, this right entitles the data subjects to temporarily stop the processing and keep the target data for future actions, such as rectification, lawsuits. These decentralized contact tracing apps can only temporarily keep the data on users' devices. After a period, such as 14 days, these data will be automatically deleted. Therefore, these apps won't keep the personal data once the storage period is over.

---

[127] General Data Protection Regulation, Regulation(EU) 2016/679, article 17. 3. (c).
[128] General Data Protection Regulation, Regulation(EU) 2016/679, article 9. 2. (i).
[129] General Data Protection Regulation, Regulation(EU) 2016/679, article 18.
[130] Governance, I. T. (Ed.). (2017). *supra* note 75, p. 62.
[131] Voigt, P., & von dem Bussche, A. (2017). *supra* note 82, p. 164.
[132] Ibid, p. 165-166.
[133] Ibid.

Moreover, according to article 18 paragraph 2 of the GDPR, the right to restriction of processing won't be applied when the target data were processed for the reason of important public interests of Union or of a Member state.[134] Personal data in these apps were processed to achieve the objectives of COVID-19 pandemic prevention, which are important public interests of the Union. Hence, when the decentralized contact tracing apps were mandatorily applied, the users cannot exercise the right to restriction of processing to stop the processing of these apps.

3.3.5 Right to data portability

The right to data portability is the right for data subjects to receive the personal data concerning them.[135] This new setting right to data protection aims to allow data subjects to obtain and make use of their personal data for their need of different use,[136] as long as the data is concerning and provided by the data subject.[137] In this way, data subjects will have better control over their personal data where processing is carried out by automated means.[138] The switching costs can be reduced and therefore, prevent a lock-in effect.[139]

There are some conditions to exercise the right to data portability. First, this right can only be applied to cases where the automatic processing is based on consent or contract.[140] Second, the right to data portability shall not be against the tasks carried out for public interest.[141] About decentralized contact tracing apps, most data are contact information stored on users' devices. Switching apps won't need the transmission of data. Hence, there is no need to worry about the cost of changing the choice of decentralized contact tracing apps. Both voluntary or mandatory applying these apps won't affect the users to exercise the right to portability.

3.3.6 Right to object

[134] General Data Protection Regulation, Regulation(EU) 2016/679, article 18. 2.
[135] General Data Protection Regulation, Regulation(EU) 2016/679, article 20. 1.
[136] Wong, J., & Henderson, T. (2019). The right to data portability in practice: exploring the implications of the technologically neutral GDPR. *International Data Privacy Law*, *Vol.9(3)*, p. 174.
[137] A29WP, (2017). Guidelines on the right to data portability, p. 9. Retrieved 30 December 2020, from https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.
[138] Voigt, P., & von dem Bussche, A. (2017). *supra* note 82, p. 168.
[139] Feiler, L., Forgó, N., & Weigl, M. (2018). *The EU General Data Protection Regulation (GDPR): a commentary*. Globe Law and Business, p. 128.
[140] General Data Protection Regulation, Regulation(EU) 2016/679, article 20. 1.
[141] General Data Protection Regulation, Regulation(EU) 2016/679, article 20. 3.

The right to object entitles the data subjects, on the grounds relating to their particular situations, to object to the processing of selected personal data on several occasions, including processing for the purpose of public interest.[142] The balancing under this provision enables account to be taken in a more specific manner of the data subjects' particular situation.[143]

This right can be exercised at any time, no matter whether the processing has begun or not.[144] The data subject can exercise this right by informing the data controller directly with the reason why the controllers need to stop the processing. The request can be raised in oral or writing. As long as the request is reasonable. The controllers need to stop or not begin processing as request. When these apps are mandatorily applied, the data subjects can exercise this right against the mandatory processing of public health authorities. The public health authorities can continue the necessary processing after demonstrating this processing is necessary that overrides the interests, freedoms, and rights of data subjects.[145] When these apps are voluntary, the users can exercise this right. But they still need to face the problems of how to find where the specific data were stored and processed.

4 Legality of mandatory applying the decentralized contact tracing apps

Comparing with voluntary measures, there are more requirements for adopting mandatory measures. Mandatory measures adopted in the EU will be reviewed with strict tests of fundamental rights protection, especially the general principles of fundamental rights protection.

In the current scenario, decentralized contact tracing apps are used to record the contact information to provide exposure notification. On the one hand, this notification will help to find out potential infects as soon as possible, and finally, help to achieve the objectives of COVID-19 pandemic control. On the other hand, these apps play the role of surveillance systems of the COVID-19 pandemic. The risks of abuse are inherent in any system of surveillance,[146] which shall be based on law, and meet the requirements of the proportionality principle.[147] Therefore, the mandatory application of decentralized contact tracing apps needs to be further reviewed with the tests of the proportionality principle. The question is whether mandatory processing

[142] General Data Protection Regulation, Regulation(EU) 2016/679, article 21.
[143] ECJ (2017). Case C-398/15 Manni case, EU:C:2017:197, para 47.
[144] Voigt, P., & von dem Bussche, A. (2017). *supra* note 82, p. 179.
[145] General Data Protection Regulation, Regulation(EU) 2016/679, article 21. 1.
[146] European Court of Human Rights(ECtHR) (2015), Case of Roman Zakharov v. Russia, Application no. 47143/06, para 302.
[147] GDPR, Regulation(EU) 2016/679, Article 6, 4, and Article 9. 2. (g).

contact information for purposes of COVID-19 pandemic control meets the requirements of proportionality?

The proportionality principle is an important general principle in EU law,[148] which can be interpreted in different ways. The most explicit interpretation of the proportionality principle is that an adopted measure must be suitable and necessary for the objectives pursued.[149] This interpretation includes two aspects of this principle, suitability, and necessity. In practice, there is another aspect of the test of proportionality, the proportionality *stricto sensu*. The ECJ generally make reference to the third aspect of the proportionality inquiry when the applicant present arguments directed specifically to it.[150]

Suitability requests the measures used were suitable for the purpose of achieving the objective pursued.[151] This test concerns only the relationship between the end and the means.[152] Necessity requests the measures were not allowed to exceed that which was necessary for the objective pursued.[153] The proportionality *stricto sensu* leaves an open way for the EU courts to apply the balancing inherent in proportionality.[154]

At the Union level, the mandatory application of decentralized contact tracing apps will be a part of the COVID-19 pandemic prevention policy. When the EU policy is reviewed with proportionality, the ECJ often applies 'manifestly inappropriate test' to balance the private and public interests.[155] The ECJ won't strike down a measure unless it considers that it is manifestly inappropriate to achieve its objectives.[156] In the current scenario, the objective of the adopted measure is to use a contact surveillance system to provide timely exposure notification and help the contact tracing work to support the COVID-19 pandemic control. The nature of this measure is to use the privacy of everyone, including healthy people, to enhance the COVID-19 prevention work. Comparing with the objective of fighting against a serious pandemic, these measures are still not manifest inappropriately if only the users' personal data was affected. However, mandatory applying decentralized contact tracing apps not only includes the surveillance system and collection of contact information. To keep these apps being mandatorily used by the public, a mechanism is also needed. This will extend the influence outside of the users' privacy and rights to data protection, which

[148] Craig, P. (2012). *EU administrative law* (2nd ed.). Oxford: Oxford University Press, p. 591.
[149] Harbo, T. (2010). The Function of the Proportionality Principle in EU Law. *European Law Journal: Review of European Law in Context*, *Vol.16(2),* p. 180.
[150] Craig, P. (2012). *supra* note 148, p. 592.
[151] Schwarze, J, *European Administrative Law* (Revised 1st Edition), Sweet and Maxwell, 2006, pp. 855-856.
[152] Ibid, p. 856.
[153] Ibid, p. 857.
[154] Craig, P. (2012). *supra* note 148, p. 592.
[155] Tridimas, T., & Jacobs, F. (2006). *The general principles of EU law* (2nd ed.). Oxford: Oxford University Press, p. 138.
[156] Ibid.

will influence more areas of users' fundamental rights. Therefore, it could be hard for mandatory applying decentralized contact tracing apps to pass the proportionality test.

At the Member States level, the ECJ often applies the less restrictive measures test to review the mandatory measures which impose restrictions on fundamental rights.[157] The less restrictive measures test is much strict than the 'manifestly inappropriate test'. As has been discussed above, the mandatory application of decentralized contact tracing apps has difficulties in passing the 'manifestly inappropriate test'.[158] The chance for the member states' mandatory measures could be much slimmer to pass the less restrictive measures test, which is much more strict than the 'manifestly inappropriate test'.

Moreover, human dignity could be an impassable obstacle for mandatorily applying decentralized contact tracing apps. It is one of the few absolute rights and 'the real basis of fundamental rights'.[159] In the EU law, dignity is an exclusively human quality: it is explicitly qualified as 'human', and protects the most essential attributes of humanity.[160] This absolute right could be used in extreme cases as a last resort, which could be a nuclear option for the judges of the ECJ.[161] In the Omega case, even the commercial exploitation of games simulating homicide as a sport was regarded as an affront to human dignity.[162] When these apps were mandatorily applied, the nature of these measures is mass surveillance by the authorities. The objective of surveillance includes healthy people. The continuing mandatory surveillance on healthy people will be intolerable. Therefore, it could be impossible for mandatory applying decentralized contact tracing apps to pass the proportionality test in ECJ or ECtHR.

5 Conclusions

The decentralized data processing technology will have a great influence on the application of personal data protection law. Not only the impact of technology, but the different implementation modes of the decentralized contact tracing apps will also greatly influence personal data protection.

Both voluntary or mandatory application of decentralized contact tracing apps will suffer the challenge of decentralized technology. In the current framework, the controllers undertake the most obligation of personal data protection. The exercise of the right to personal data protection relies on the controller's response to the requests

[157] Ibid, p. 209.
[158] Ibid.
[159] Peers, S., Hervey, T., Kenner, J., & Ward, A. (2014). *The EU Charter of Fundamental Rights- A Commentary*. Oxford: Hart Publishing, p. 15.
[160] Ibid, p. 16.
[161] Ibid, p. 21.
[162] ECJ (2004). Case C-36/02 Omega Case, EU:C:2004:614, para 41.

of data subjects. To effectively undertaking these obligations, the controllers need to have enough information and access to respond to the requests of data subjects. Hence, the difficulties in managing the system is an important reason account for the difficulties to implement the personal data protection rules.

When these apps are voluntary to join-in or out, the users will have difficulties in finding the right device which stores their personal data, which may result in their failures in exercising their rights. This model of the application of the decentralized contact tracing apps will allow the users to have some level of autonomy, whose behavior might become difficult to predict and regulate.[163] That will result in difficulties in the management of personal data stored and processed in users' devices, especially when the framework of these apps limits the public health authorities or API provides to get the necessary access to these selected data.

Moreover, the fulfillment of the right to data protection relies on the effective management of data controllers and personal data protection frameworks. Without necessary access to selected personal data, the controllers will have difficulties in fulfilling their obligation to manage the selected personal data and respond to the requests of data subjects. This may result in the disfunction of the personal data protection framework. Current decentralized technology still has difficulties in having a balance between autonomy and consistency. These difficulties will leave more system vulnerabilities, leading to more infringement of rights to personal data protection. To solve these difficulties, more information about the selected personal data needs to be provided to controllers and users. The controllers might need to get the ability to process the requests of the data subject. This will unavoidably enhance the surveillance of the decentralized system, which will bring too much transparency to this system. No wonder that De Filippi warns that the decentralized framework might be much more vulnerable to governmental or corporate surveillance than a centralized system.[164] This result conflicts with the initial application of decentralized personal data processing technology. When these apps are voluntary to join in and out, the users need to face a difficult choice between unfulfillable rights to personal data protection or too much transparency. This dilemma will have negative effects on the promotion of decentralized contact tracing apps, which may seriously reduce the coverage rate of these apps. The application of these decentralized contact tracing apps cannot achieve the goal of early warning and communicable disease prevention and control.

It is no doubt that the mandatory application will provide high coverage of the installation and enabling of these apps. However, it is impossible for these apps being mandatorily applied in the EU since this mandatory measure can never pass the strict test of fundamental rights protection. Therefore, the decentralized contact tracing apps cannot be mandatorily applied. The decentralized contact tracing apps need to be

[163] De Filippi, P. (2016). *supra* note 37.
[164] Finck, M. (2018), *supra* note 42, p. 33. See also De Filippi, P. (2016). *supra* note 37.

applied in a creative way, while these apps were voluntarily used by the public. However, pandemic response measures need to be carried out and take effect quickly. Without mandatory application power, it could be a big challenge to quickly establish a system that needs extensive public participation. The possible solutions are to use encourage measures, such as tax exemptions, to promote the public use of these apps and follow other pandemic prevention measures, or request the administrators of public areas or organizers of mass activities to take these apps as a part of security obligations.

Anyway, applying decentralized contact tracing apps against the COVID-19, once again, reflexes the difficulties in taking the balance between the need for fundamental right protection, and technology social management measures in the information age.

The decentralized framework will give the users autonomy at some level, while coordination becomes more difficult, especially in a voluntary system. That needs to be improved by technology means and legislation means. While legislation has always been late than technology development, the conflict between law and technology development becomes increasingly acute with the rapid development of technology in the digital age.[165] On the one hand, the law always plays an important role in promoting the development of technology, while preventing the negative effects of technology itself. On the other hand, data protection allows a positive-sum or win-win game.[166] The development of technology will also provide new solutions to solve the disadvantages of technology, which means technology development will also provide more choices for personal data protection. It is still a long way to have a perfect balance between technology innovation and fundamental right protection.

There are still some shortcomings in this report. For example, the analysis of decentralized systems focuses on decentralized contact tracing apps. The more decentralized technologies, such as decentralized ledger technology, were not discussed. So, this report can only be the start point for further study on data protection on decentralized data technology. Besides, this report didn't go further discussion about the constitutional problems of limitation on rights to data protection during the state of emergency. For data protection in future data technologies, it is necessary to study different types of distributed data technologies and develop the right way for decentralized data technology. To solve the conflicts between fundamental rights protection and technique response measure during the state of emergency, it is also necessary to study the EU fundamental right system to help understand the reason for fairness towards new technology applied by governments. With the development of technology and the change of social concepts, we can find a more reasonable way of

[165] Finck, M. (2018). Supra note 43, p. 33.
[166] Pagallo, U. (2012). On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law. In: Gutwirth S., Leenes R., De Hert P., Poullet Y. (eds) *European Data Protection: In Good Health?*. Springer, Dordrecht, p. 333.

regulating the application of decentralized internet technologies, both in the technical and regulation aspects. We should be confident about the future of the decentralized system. We need rapid study, analysis, and improve the latest technology and rules, and legal framework. So that we can ensure the development of technology will finally promote the development of our society.

References

Books

Brajesh De. (2017). *API Management: An Architect's Guide to Developing and Managing APIs for Your Organization* , Apress, Berkeley, CA.

Feiler, L., Forgó, N., & Weigl, M. (2018). *The EU General Data Protection Regulation (GDPR): a commentary*. Globe Law and Business.

Governance, I. T. (Ed.). (2017). *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide*. IT Governance Publishing.

Peers, S., Hervey, T., Kenner, J., & Ward, A. (2014). *The EU Charter of Fundamental Rights- A Commentary*. Oxford: Hart Publishing.

Savin, A. (2013). *EU Internet law*. Edward Elgar.

Schwarze, J, *European Administrative Law* (Revised 1st Edition), Sweet and Maxwell, 2006.

Tridimas, T., & Jacobs, F. (2006). *The general principles of EU law* (2nd ed.). Oxford: Oxford University Press.

Voigt, P., & von dem Bussche, A.(2017). *The EU General Data Protection Regulation (GDPR)-A Practical Guide*: Springer, Cham.

Articles

Abril, P. S., & Lipton, J. D. (2014). The Right To Be Forgotten: Who Decides What the World Forgets, *Kentucky Law Journal*, *Vol.103(3)*, pp. 363-390.

Castelluccia C. (2012). Behavioural Tracking on the Internet: A Technical Perspective. In: Gutwirth S., Leenes R., De Hert P., Poullet Y. (eds) *European Data Protection: In Good Health?*. Springer, Dordrecht , pp. 21–33.

De Filippi, P. (2016). The interplay between decentralization and privacy: the case of blockchain technologies. *Journal of Peer Production, Vol.*7. Retrieved 30 December 2020, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852689.

Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., & Abeler-Dorner, L. et al. (2020). Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Retrieved 30 December 2020, from https://science.sciencemag.org/content/368/6491/eabb6936/tab-pdf.

Finck, M. (2018). Blockchains and Data Protection in the European Union, *European Data Protection Law Review, Vol.4(1)*, pp. 17-35.

Froomkin, A. M. (2000). The death of privacy?, *Stanford Law Review, Vol.52*(5), pp. 1461-1543.

Harbo, T. (2010). The Function of the Proportionality Principle in EU Law. *European Law Journal: Review of European Law in Context, Vol.16(2)*, pp. 158-185.

Jasserand, C. (2016). Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data. *European Data Protection Law Review, Vol.2(3)*, pp.297-311.

Gstrein, O. J., & Ritsema van Eck, G. J. (2018). Mobile devices as stigmatizing security sensors: the GDPR and a future of crowdsourced 'broken windows'. *International Data Privacy Law, Vol.8*(1), pp. 69-85.

Levine, M. L, (1988). Contact Tracing for HIV Infection: A Plea for Privacy, *Columbia Human Rights Law Review, Vol.20(1)*, pp. 157-210.

Mulder, T. (2019). The Protection of Data Concerning Health in Europe. *European Data Protection Law Review, Vol.5(2)*, pp. 209-220.

Pagallo, U. (2012). On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law. In: Gutwirth S., Leenes R., De Hert P., Poullet Y. (eds) *European Data Protection: In Good Health?*. Springer, Dordrecht, pp. 331-346.

Porcedda, M.G. (2012). Law Enforcement in the Clouds: Is the EU Data Protection Legal Framework up to the Task?. In: Gutwirth S., Leenes R., De Hert P., Poullet Y. (eds) *European Data Protection: In Good Health?*. Springer, Dordrecht., pp. 203-232.

Trivellato, U. (2019) Microdata for Social Sciences and Policy Evaluation as a Public Good. In: Crato, N., Paruolo, P. (eds) *Data-Driven Policy Impact Evaluation*. Springer, Cham, pp. 27-45.

Wong, J., & Henderson, T. (2019). The right to data portability in practice: exploring the implications of the technologically neutral GDPR. *International Data Privacy Law, Vol.9(3)*, pp. 173-191.

Report

Jonas, J., & Harper, J. (2006). Effective Counterterrorism and the Limited Role of Predictive Data Mining. Cato Institute. Retrieved 1 October 2020, from http://www.jstor.org/stable/resrep04886.

Castro, D., & Alan, M. (2015). The Privacy Panic Cycle: A Guide to Public Fears About New Technologies, pp. 1-2. Information Technology & Innovation Foundation. Retrieved 30 December 2020, from https://itif.org/publications/2015/09/10/privacy-panic-cycle-guide-public-fears-about-new-technologies.

Government or other official documents

Apple & Google, (2020). Exposure Notification Bluetooth® Specification Preliminary-Subject to Modification and Extension. Retrieved 30 October 2020, from https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.2.pdf.

A29WP. (2014). Opinion 05/2014 on Anonymisation Techniques. Retrieved 30 December 2020, from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

A29WP, (2017). Guidelines on the right to data portability. Retrieved 30 December 2020, from https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

The European Commission, (2020). Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data. Retrieved 30 December 2020, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020H0518&qid=1615189292172.

eHealth Network, (2020). Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States. Retrieved 1 October 2020, from https://ec.europa.eu/health/ehealth/key_documents_en#anchor0.

eHealth Network, (2020). European Proximity Tracing-An Interoperability Architecture for contact tracing and warning apps. Retrieved 30 December 2020, from https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interop_architecture_en.pdf.

EDPB, (2019). Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, p.4. Retrieved 1 October 2020, from https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en.

EDPB. (2020). Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak. Retrieved 6 January 2021, from https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-042020-use-location-data-and-contact-tracing-tools_en.

EDPB. (2020). Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Retrieved 30 December 2020, from https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en.

WHO. (2021). Contact tracing in the context of COVID-19. Retrieved 20 February 2021, from https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19.

WHO, (2021). Critical preparedness, readiness and response actions for COVID-19. Retrieved 1 January 2021, from https://www.who.int/publications/i/item/critical-preparedness-readiness-and-response-actions-for-covid-19.

WHO. (2020). Surveillance strategies for COVID-19 human infection. Retrieved 30 December 2020, from https://apps.who.int/iris/bitstream/handle/10665/332051/WHO-2019-nCoV-National_Surveillance-2020.1-eng.pdf?sequence=1&isAllowed=y.

Regulation

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

Regulation (EC) No 851/2004 of the European Parliament and of the Council of 21 April 2004 establishing a European Centre for disease prevention and control, (2004)

General Data Protection Regulation, Regulation(EU) 2016/679

Case law

ECJ (2003). Case C-101/01 Lindqvist case, EU:C:2003:596.

ECJ (2004). Case C-36/02 Omega Case, EU:C:2004:614.

ECJ (2011). Case C-70/10 Scarlet Extended case, EU:C:2011:771.

ECJ (2016). Case C-582/14 Breyer case, EU:C:2016:779.

ECJ (2018). Case C-210/16 Wirtschaftsakademie Schleswig-Holstein case, EU:C:2018:388.

ECJ (2010). Joint case C-92/09 and C-93/09 Volker und Markus Scheche and Eifert case, EU:C:2010:662.

ECJ (2014). Case C-131/12 Google Spain case, EU:C:2014:317.

ECJ (2017). Case C-398/15 Manni case, EU:C:2017:197.

European Court of Human Rights(ECtHR) (2015), Case of Roman Zakharov v. Russia, Application no. 47143/06.

Other reference

Li, D. (2020). Expert: Large-scale vaccination will take 1-2 years. Retrieved 30 December 2020, from https://www.chinadaily.com.cn/a/202009/25/WS5f6d9777a31024ad0ba7bdf3.html.

Sorace, S. (2020). Europe braces for more coronavirus lockdowns and restrictions as cases spike, winter looms. Retrieved 31 December 2020, from https://www.foxnews.com/world/europe-coronavirus-lockdowns-restrictions-winter.

WHO (2017). Infection control: Contact tracing. Retrieved 30 December 2020, from https://www.who.int/news-room/q-a-detail/contact-tracing.