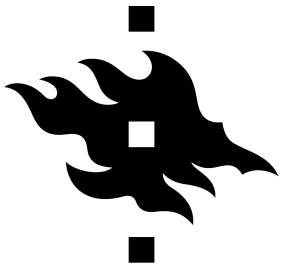

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Contact-Tracing Mobile Applications as Health Governance: Issues and Implications for the Future

Venla Ailasmäki, Juho Majanen, Milla Pirttilahti, Jessica Pyöriä & Megan Rollerson

Faculty of Social Sciences, University of Helsinki
Master's Programme in Global Politics and Communication

Abstract

With the increased digitalisation of our data and the rise of e-governance, much of our interactions with and information held by public services has moved online, including our private health records. During the COVID-19 pandemic, governments around the world launched and employed digital applications and systems to aid in contact tracing and predicting infections. The pandemic served as a useful mechanism to bring to public attention the interests of governments to control or steer citizens' health, particularly as it pertained to infectious diseases, via digital means. In this paper, we look at the application and implications of digital health governance at the national level. We address this by providing a theoretical background with Foucault's conception of biopower and addressing several themes related to these applications: privacy, ethics, and information security; perceptions and efficacy of health governance via digital apps; contemporary examples of applications; and the question of legitimacy. By examining current literature, this research paper aims to take a critical look at the benefits of government digitalisation of citizens' health, but also at the challenges it poses for democracy.

Key words: biopower, contact-tracing, mobile apps, COVID-19, public health

1.Introduction

The COVID-19 pandemic introduced a variety of challenges for health governance. One particular trend that surfaced in multiple countries was the introduction of specially designed mobile phone applications used for tracing contacts and notifying people of possible exposure to the virus. These contact-tracing applications (CTAs, applications, apps) could be voluntarily downloaded to a personal mobile device and, by doing so, the user would agree to data collection and sharing. Ideally, the applications would effectively steer people's behaviour by providing accurate information about the spread of the virus. In practice, the applications were met with serious questions and concerns about the technologies' effectiveness, the ownership and application of citizens' data, and the ethics of data privacy. To address these concerns, we need more research on CTAs' current and future developments, public opinion, and the issue of legitimacy.

In this paper, our goal is to offer an introduction to these topics and create the space for further discussion. The paper will investigate CTAs from the perspective of health governance, as well as several issues emerging from the applications. We first build on the theoretical background provided by Foucault's conception of biopower as power over life for the betterment and control of public health. This provides a background for the development of applications as they can be seen as a form of power. This paper will seek to critically assess this form of power, by first, introducing biopower as a concept and its relation to health governance through applications. The second chapter will touch on the privacy, security, and ethical aspects of the applications, considering the moral argument of trading privacy for public safety. The third chapter will discuss the efficacy of CTAs by focusing on citizen perceptions of CTAs and examining different reasons for choosing to adopt or reject their use.

The fourth chapter will introduce case examples of health governance via CTAs in China and Finland. It will examine how two different COVID-19 applications, the Chinese *Health Code* and the Finnish *Koronavilkku*, function, how and why the apps are used, and what has been the government's approach to legitimise the use of CTAs during the pandemic. The final chapter will examine the issue of legitimacy in the case of CTAs. Legitimacy is recognized to be a critical concept that defines the success of the entire policy process of introducing CTAs to the public.

2. The concept of biopower and health governance - the basis for health applications?

Jessica Pyöriä

This chapter will formulate a basis for modern health governance through the examination of Michel Foucault's concept of biopower, which was first introduced in *The History of Sexuality*, volume 1 (published in 1976) as a concept to help describe changes in mechanisms of power since the 17th century (Oksala, 2013, pp. 320-321). Following this, this chapter seeks to answer the following questions: What are the motivations for, and measures applied, to control the health of a population, and what does this mean for contemporary health governance, for example, during the COVID-19 pandemic? How does the concept of biopower help us understand the motivation behind and promotion of mobile health applications?

2.1 Foucault's concept of biopower

Foucault's conception of biopower is reliant on his discussion of sovereign power: a power that gave the sovereign the right to kill. This power was based on deduction and the right to collect taxes and goods from the people, even to take their bodies to fight the sovereign's wars. Life was held in the hands of the ruler, who could use his power to end it (Oksala, 2013, pp. 320-321). Power in modern Western societies, Foucault argues, has been transformed, and this sovereign power based on the fear of violence has been, at least in part, replaced by biopower. Biopower "exerts a positive influence on life", with the aim to increase life instead of taking it away (Oksala, 2013, p. 321).

Biopower is characterised by "investing in life" through different biopolitical techniques, which, for example, have to do with coordinating medical care and creating norms to better the conditions of human life by controlling and regulating it. These techniques are often based on expert knowledge, and not the result of parliamentary decisions but part of administrative procedures (Oksala, 2013, p. 321). Rabinow and Rose (2006, p. 197) characterise biopolitics as strategies and disputes around "human vitality, morbidity and mortality" and the knowledge and practices around these. The historical phenomena that Foucault sees as power over life, biopower, are, for example, the beginning of interventions regarding birth rates and the promotion of public hygiene measures to contain routinely existing illnesses. The concept of biopower and its characteristics are grounded strictly in historical developments and their analysis (Rabinow & Rose, 2006, p. 199)

Rabinow and Rose (2006, p. 197) formulate three core elements of biopower, as follows. First, biopower is characterised by the truth discourses about human life and vitality, defined by competent authorities. Second, biopower contains "strategies for intervention upon collective existence in the name of life and health", such as the historical examples introduced above, which seek to further population health through different controlling and regulating measures. Thirdly, modes of subjectification are a part of biopower, and through them individuals "work on themselves" for both their own health as well as that of a collective, even of the whole population. Moral responsibility is put on the individual to do one's part. As Nadesan (2008, p. 4) argues, biopower offers "tools for societal self-government" and a possibility of a "society of self-regulating individuals". Knowledge and the control of it, interventions upon public health and the subjectification of individuals to play their part are central to Foucault's conception of biopower.

Constantinou (2021) examines COVID-19 responses through the lens of biopower. These observations will be used in this chapter to shed some more light on the manifestations of biopower during the recent years under the pandemic. The second element of biopower, strategies of intervention in the name of health, were naturally present as COVID-19 mitigation measures were used to slow down the virus. The first element of biopower regarding truth discourses was prominent during the pandemic, and governments depended on science and expert knowledge to instruct people about the actions needed to control the virus. The way experts and administrators talked about the virus created knowledge about it and this knowledge enabled the use of power by the government and its different institutions to assert guidelines and regulations. This knowledge also normalised power and made people "want to do what must be done", as if they thought of doing it on their own (Constantinou 2021, p. 30). This exhibits the third element of biopower, when people act for the benefit of public health due to their own motivation.

One more specific example given by Constantinou was the use of masks in COVID-19 prevention and control. Confirmation of the benefit of wearing masks came from scientists, and this legitimised the practice of recommending or requiring the use of masks in public spaces. This knowledge was repeated by both politicians and scientists with the help of the media, and this enabled laypeople to understand and adopt the measure to control the spread of the virus (Constantinou 2021, p. 32.). As Constantinou (2021) argues, the use of biopower can help people understand a phenomenon through the discourse around producing knowledge, and thus take up measures that protect both the individual and the collective: it is not a bad thing, but it does imply the use of control over people in the name of health and life (p. 37).

2.2 Implications of biopower for mobile applications in health governance

The argument of this research paper is that mobile applications in health governance, such as contact-tracing applications, are a form of biopower and biopolitics: they are a way to invest in life by trying to prevent illness and even death, and their use is based on knowledge of, for example, how an illness spreads and how it should be treated. As an example, COVID-19 is known to spread in close contact, through droplet infection, and even airborne transmission (THL, 2022), and thus the Finnish application, Koronavilkku, needed to be able to connect with the phones around the infected person to send an alert. In addition, knowledge about the way the virus spread needed to be presented to the public to argue for the need of as many people as possible to download and use the application. The motivation for this was to control the spread of the virus and thus, have less people get infected. Similarly, a contact-tracing application for a sexually transmitted disease would also be based on expert knowledge about the spread and symptoms of the disease, and this information about the disease could be used to argue for the need of the wide-spread use of the application.

Davis (2022) argues that the medical system is a system of control, and when it functions well it is powered by "self-will rather than heavy-handed regulation". The third element of biopower makes people self-regulate, and different mobile health applications can help this to be achieved. The applications can be versatile and cover multiple different areas of life: they can be, like the examples provided above, about transmittable disease prevention, or about preventing other health conditions, such as heart disease, by tracking habits. These applications can benefit public health and the health of the individual, but they can also function to create a society of self-regulators, acting as a form of control over life to better it. Essentially, they can be argued to act as a form of biopower and thus need to be assessed critically.

3. Privacy, ethics, and information security in digital health apps

Megan Rollerson

As citizens, we assume certain rights to privacy and personal data security. However, we lawfully and legitimately concede the use of data daily to mobile apps, through terms and conditions. In the context of a global pandemic, the right to privacy may be waived by the state,

with access deemed necessary to curb transmission. There is a trade-off that occurs between privacy and public and commercial interest. Is this justified and what are the ethical considerations and implications? The moral argument is that privacy rights should not come at the expense of preservation of life. Moral responsibility aside, the scope of private data collected and shared should draw concerns as to whether it is wholly necessary, ethical, and justifiable.

3.1 Privacy & information security

An increasing amount of personal data is stored and tracked through mobile devices. As we use mobile apps, we agree to terms and conditions and privacy policies, most unread due to their ever-increasing length (Suver & Kuwana, 2021, p. 76). We thus consent to share numerous personal data points, often beyond what is necessary for the basic functionality of the application, and which may be sold and shared with "marketers, researchers and other groups" (Kucharski, 2020, p. 257), as well as companies and insurance providers who use data to "influence people's health-related behaviors" (Suver & Kuwana, 2021, p. 71). Access to private data and behaviour patterns is often rooted in business rather than health interests.

To mitigate this, there are eight global privacy principles for the use and collection of personal data. It must be lawful, purposeful, limited, quality, secure, used as intended, transparent, and controllable (Suver & Kuwana, 2021, p. 73-74). These principles were reemphasized by the WHO in the context of the pandemic, as collection of personal data surged (2021, p. 74). Within these principles is the ethical matter of informed consent, or lack thereof. Prainsack (2020) proposes that the drive for digitising data has created a "datafication of the bodies, lives, and practices of people who have no realistic chance to opt out" (p. 444). She illustrates this point with the case of a UK hospital which gave millions of patient records to Google's "DeepMind" AI for kidney disease research (p. 439). While Prainsack notes that the AI was never successfully developed, the important takeaway is that patients were never informed nor was consent given. It was not lawful or transparent according to the principles.

With mHealth and contact tracing apps, a wealth of data is shared. This is done under the guise of improved app functionality, health safety, and wellbeing. mHealth apps collect data on location, physical activity, sleep, stress, heart rate, nutrition, glucose levels, blood pressure, even mood (Suver & Kuwana, 2021). From the COVID-19 pandemic, Suver and Kuwana (2021) studied nearly five hundred COVID-related apps and, aside from location tracking permission, found the following data access requests: 44% phone camera, 22% microphone,

32% photos, and 11% contacts (p. 75). Citizens were urged to share their personal information for contact tracing purposes and did so with the hope of protecting themselves, (Akinsanmi & Salami, 2021) and subsequently others. However, the necessity of information collected should draw scrutiny.

In the context of a public health emergency and contact tracing, there is considered a necessary trade-off between privacy and public safety/ public health interests (Akinsanmi & Salami, 2021; Suver & Kuwana, 2021). This is because tracing requires that individuals share private information with health officials, and global disease prevention considers "contact tracing … the cornerstone of effective public health responses in the face of infectious disease outbreaks" (Parker et al, 2020, p. 427). However, Akinsanmi and Salami (2021) consider this trade-off a "false choice" and problematic to justify sacrificing privacy to ensure security. They favour the use of decentralised contact tracing apps over a "contact tracing model that processes more user data" (2021, p. 4). The idea of a decentralised app is based on algorithmic governance and autonomous management of data, with architecture and user protocols in place to protect privacy and security of personal data.

3.2 Ethics of Shared Private Data

In the face of privacy concerns, one way to look at the ethics of data sharing is to apply Seumas Miller's (2010) view of collective moral responsibility to contact tracing apps. Accepting that our private data will be shared with an app, to reduce the spread of a disease, involves individual action by agents acting jointly to achieve collective moral responsibility. While the actions of each individual are not significant in and of themselves, the outcome is conditioned on collective contributions. At the same time, individuals are not individually responsible for the failed contribution of others. The moral concern with infectious disease is prevention of harm. There is a "moral significance of international spread and massive scale of impact", wrote Parker et al. (2020) early in the pandemic, before knowing its scale, scope, and duration (p. 427-428). They considered the implementation of contract tracing apps "ethically acceptable" and "obligatory", as well as preferable and a lesser interruption of people's rights than lockdowns and quarantines (2021, p. 428). However, they foresaw neither that both measures would be used in tandem, nor the scope of data collected. Prevention of harm is relative and must factor in ethical handling of data by the state to prevent misuse and individual harm.

3.3 Justifiable?

So, is the sharing of personal data justifiable? Parker et al. (2020) argue "some privacy infringements are potentially justifiable" (p. 428). They suggest preservation of life is the greater good and that there is a moral imperative to forego privacy in the name of public safety.

The case of South Korea's COVID-19 contact tracing strategy, however, reveals the flaw in treating privacy as a trade-off. In early 2020, South Korea was collecting extensive data for contact tracing, beyond location mapping, including prescription and medical history, immigration records, and credit card data (Park et al., 2020, p. 2129). Park et al.'s (2020) work also shows that the Minister of Health and Welfare and municipalities were publishing data online; detailed enough information to reveal patterns of movement and behaviour and identify individuals, regardless of de-identification. Reidentification supposedly occurred and infected people experienced invasions of privacy (p. 2129). Even when anonymised, with a larger breadth of data shared, there is a greater likelihood of reidentification (Suver & Kuwana, 2021, p. 75). This was a theory proven in the mid-1990s using anonymised medical databases in the US (Kucharski, 2020, p. 253). While this led to changes in the handling of medical records, the case of South Korea again demonstrated how sharing seemingly anonymised data of infected persons can lead to identification.

Again, is a trade-off justified? A look at COVID-19 contact tracing highlights the need for secure, decentralised apps that use aggregated data and notify people of exposure events based solely on location proximity data. The literature advocates algorithmic solutions if we are to justify sharing private data. Park et al. (2020) recommend algorithmic data collection to aggregate data, so that aggregated data rather than individual data is used to control contagion (p. 2130). Parker et al. (2020) stress the need for "transparency about proposed and actual data uses", oversight, and data protection (p. 428), and Akinsanmi and Salami (2021) argue it is necessary to ensure digital security, privacy policies, data confidentiality and authentication" (p. 2). Algorithmic measures would arguably create a more ethical approach to contact tracing that upholds the collective moral responsibility to share data but preserves privacy.

4. Citizen perspectives and the efficacy of contact-tracing applications

Milla Pirttilahti

The efficacy of COVID-19 contact-tracing applications relies heavily on how citizens react to the introduction of these applications. The mere existence of such applications does not help much if citizens are not willing to partake in the use of these applications and download them to their mobile phones. In order for a contact-tracing application to be effective, a sufficient proportion of an area's population has to download the application, agree to its terms of service, and use the app in its intended way. However, if citizens react negatively to the introduction of such applications and refuse to use them, the existence of contact-tracing applications becomes meaningless. Therefore, public reaction to CTAs is crucial for the usefulness of these applications. For this reason, it is important to research citizen reactions to COVID-19 CTAs.

In this chapter, we will examine COVID-19 contact-tracing applications by looking into how ordinary citizens view these applications and their legitimacy. We will look at the efficacy of using CTAs for pandemic management. The main question that we pose in this chapter is: what are the reasons for which citizens choose to adopt or refuse contact-tracing applications?

4.1 The efficacy of CTAs in managing the COVID-19 pandemic

Examining the efficacy of contact-tracing applications raises a key question of how many people have to use a CTA on a national level in order for the application to become an effective tool for pandemic management. According to Buhr et al. (2022), contact-tracing apps for COVID-19 would need at least 60%-70% uptake in order for them to be validated as effective tools for pandemic management. Another study by Ferretti et al. (2020) suggests that the adoption rate of COVID-19 CTAs would have to be 50–60% at the very least for them to be able to limit the spread of the virus. Sharma et al. (2020) claim that the successful implementation of contact-tracing apps would require that CTAs have a higher "transmission rate" than COVID-19.

These results imply that at least 60% of the population of a nation should adopt CTAs for the applications to be an effective tool for COVID-19 pandemic management. However, a study conducted in the UK in the beginning of the pandemic suggested that even though 97% of the survey participants were aware of contact-tracing apps, only 56% were intending to use CTAs themselves, once an app was to become available (Jones & Thompson, 2021). An adoption rate of 56% would barely be sufficient for efficient management of the pandemic.

However, 21% of the respondents in the same survey were still unsure of whether they would use a COVID-19 contact-tracing app or not (Jones & Thompson, 2021). Next, we will delve into reasons for which citizens might choose to adopt or refuse the use of CTAs.

4.2 Reasons for CTAs

In a survey conducted in the UK, when citizens were asked for reasons for their willingness to use CTAs, the three most common reasons were controlling the spread of the virus, mitigating others' risk of catching the virus, and mitigating your own risk of catching the virus (Jones & Thompson, 2021). Other reasons included e.g., increasing freedoms and benefiting society. When given a chance to elaborate their answers, some interviewees mentioned their own peace of mind, providing scientists with 'good data', and managing the pandemic. However, less than 5% of the respondents mentioned social responsibility or feeling safe as reasons for willingness to use a contact-tracing app (Jones & Thompson, 2021.) In another UK survey, some of the reasons for supporting the use of CTAs mentioned by interviewees were supporting research, controlling the spread of the virus, and easing lockdowns (Samuel et al., 2022, p. 35).

Even though many citizens responded positively to the idea of using contact-tracing apps, as Samuel et al. (2022, p. 35) put it, many viewed the use of CTAs as a "balancing act – weighing up, on the one side, infringements of privacy, with, on the other side, the potential benefits of using an app". According to Sharma et al. (2020), citizens are more willing to share their personal information for the use of CTAs when they are informed of how their information will be used and are able to trust that their information will be well protected.

4.3 Reasons against CTAs

When discussing common user concerns, researchers Ahmed et. al (2020) name transparency, battery usage, compatibility between operating systems and different apps, and the ability to withdraw consent as possible user concerns regarding the use of CTAs. However, when looking at surveys conducted on the matter, technical factors such as mobile phone battery life or operating system compatibility rarely come up. Instead, different survey results show a heavy focus on questions of privacy and surveillance as citizens' concerns (Buhr et al., 2022; Jones & Thompson, 2021; Samuel et al., 2022; Sharma et al., 2020). In a survey conducted in Wales, citizens' three most common reasons for their unwillingness to use a contact-tracing app were mistrust towards the Welsh government, concerns about data security, and concerns about data

privacy (Jones & Thompson, 2021). When asked to elaborate on reasons for their unwillingness, the respondents mentioned worries about the government storing data on a centralised system, the government using the data for purposes beyond tracing the virus, and a belief that personal information will be hacked or misused. One respondent expressed their mistrust towards the government by describing the use of CTAs as "creepy, 1984 stuff". (Jones & Thompson, 2021.) In another public perception survey conducted in the UK, one interviewee described CTAs as "flipping Orwellian" (Samuel et al., 2022, p. 36). These are both references to George Orwell's novel, *Nineteen Eighty-Four*, which portrays a dystopian society characterised by surveillance and totalitarianism.

Survey results from Samuel et al. (2022) support Jones and Thompson's findings by suggesting that many people were wary of using CTAs because of worries about CTAs being used to track individuals, and that leading to increased surveillance in society (p. 35–36). However, according to Samuel et al. (2022, p. 36) many of these concerns were due to citizens' misunderstanding CTAs as GPS location trackers instead of applications relying on Bluetooth connections. Still, the most prominent worries expressed by interviewees in Samuel et al. 's (2022) survey were regarding surveillance and violations of privacy (p. 35). In addition, these worries about surveillance, privacy and data protection were often linked to broader mistrust of the government (Samuel et al., 2022, p. 37). In contrast to this, a study conducted in Germany found that German smartphone users had a much higher trust in governmental or state-funded organisations as providers for pandemic apps, rather than private organisations (Buhr et al., 2022).

So as not to paint a false picture, it must be mentioned that some user concerns regarding technical matters do appear in survey results as well. In Jones and Thompson's (2021) survey, not owning a smartphone was the fifth most common reason for unwillingness to use CTAs and 'phone usage problem' was the seventh most common reason. However, it seems that technical issues are not the main concern that users have regarding CTAs, with mistrust towards government and data privacy taking the top spots.

5. Contemporary examples of health governance via health applications: Brief glimpses into the cases of Finland and China

Venla Ailasmäki

COVID-19 pandemic shows an interesting example of health governing and monitoring via various COVID tracing apps that countries have developed with short notice to respond and control the threat to public health. In this section, I will look at how countries have used the COVID-19 applications. I will focus on two examples, the Finnish *Koronavilkku (trans. COVID blinker)* and the Chinese *Health Code.* I review what governments have said and how they have legitimised the use of these applications, and why and how these applications have been or are currently being used.

5.1 The Chinese *Health Code* by Alipay and We Chat – Protecting health by monitoring people

The Chinese companies Alipay and WeChat launched the Chinese COVID-19-application, known as *The Health Code* (Kim et al., 2021), in the beginning of February 2020 in Hangzhou and nationwide by the end of February (National Health Commission of PRC, 2020, p. 2). *The Health Code* is built upon the existing data and infrastructure from the Chinese Social Credit System (Kim et al., 2021). *The Health Code* collects data from a person's reports of daily symptoms, travel history, location data of the mobile phone and financial transactions (Kim et al., 2021). Based on the data the app creates a QR-code for the app-user that will present either green (safe), yellow (caution) or red (high risk and need for quarantine) colour that is supposed to be presented to local authorities while entering buildings and public transport (Kim et al., 2021). Despite being available nationwide, the tracking features of the application are used differently depending on the region and province (Mozur et al., 2020; Xinhuanet, 2020; Yang et al., 2021). The management of the code categories and their descriptions also vary by province (Yang et al., 2021).

The functioning mechanisms are not clearly presented on the Health Commission's English website, but the authorities' message is that by using the app people can help local authorities to efficiently monitor, prevent, and control the spreading virus and pandemic (National Health Commission of PRC, 2020, p. 4). In state-owned Shenzhen Securities Times, *The Health Code* is said to work efficiently only if citizens self-monitor each other and are self-

disciplined so they can "create a trusting society" (Xie, 2020; Kim et al., 2021). In Hangzhou, some of the names and the last four digits of personal ID numbers from the Social Credits system were published in The Paper if people falsely reported their health conditions (He, 2020; Kim et al, 2021).

5.2 The Finnish *Koronavilkku* - Protecting health, protecting privacy

The Finnish Institute for Health and Welfare (THL) launched the COVID-19 app, *Koronavilkku*, in August 2020 and disabled it during the summer of 2022, being no longer in use. *Koronavilkku* worked in mobile phones via Bluetooth connection by which the app connected to the other app users in near distance (Viljanen & Parviainen, 2022). The app created a random and anonymous, unidentifiable code for each device that changed every 15 minutes and stored the codes from other devices (Köykkä & Kaikkonen, 2020). When an app user got infected with COVID-19 and got tested by health care services, they received a code to voluntarily insert in the application. The algorithm then proceeded to notify all the app-using devices that fulfilled the conditions of having been close enough in distance (Köykkä & Kaikkonen, 2020; Viljanen & Parviainen, 2022). *Koronavilkku*'s operating principles were based on anonymity of users and voluntary information sharing and this is highlighted by the app creators as well. In the Finnish government's press release, the Director of Information Services at THL, Yrttiaho, stated that the use of *Koronavilkku* is voluntary (Valtioneuvosto, 2020; THL, 2020).

The Finnish government's press release stresses the participation of people in order to stop the virus and the willingness to "protect their own and their loved one's health" (Valtioneuvosto, 2020 & THL, 2020). The information from the official website for *Koronavilkku* has now been removed as the application is out of use. At the time of writing, it reads on the website that the application can now be removed from mobile phones, and it no longer collects data (Koronavilkku, 2022). The app was used by 2.5 million people, and it was one of the most used COVID-19 applications per capita (Koronavilkku, 2022). The website does not inform whether the data collected during the pandemic is being stored but based on the app's mechanisms, the data should remain anonymous to its viewers. In the government's proposal about the Finnish COVID-application and it's compatibility with other European COVID apps, from November 2021, the data security and protection are emphasised. The use of personal information would be restricted to the necessary information for the purpose of use;

the period of storage would only be 21 days; and the processed information would be pseudonymous to reduce privacy risks (Parliament of Finland, 2021).

5.3 Discussion

The governments of Finland and China have had different approaches to their dialogues about the COVID-19 apps and the health monitoring of citizens. In Finland, the central themes are voluntary participation and privacy policies. In China, the rhetoric of voluntary self-monitoring is applied but without *The Health Code* it has been impossible to access some buildings or other parts of the city. Therefore, it can be regarded as more mandatory to the local people so that they can continue their normal daily activities.

The Finnish government has paid attention to reassure users that their data is being collected anonymously and in respect of their privacy. The Chinese government has highlighted the usefulness of data collection and monitoring in order to keep its citizens safe. Not participating in the monitoring has been seen as disrespectful behaviour towards the state and towards other people, while in Finland there have been no consequences for not using the application. The usefulness of the applications for preventing the spread of the virus is questionable in both cases. With *Koronavilkku*, sharing one's COVID-19 test result is completely voluntary, so some people may not be informed of a possible exposure. In the Chinese application, the different management procedures by region can lead to confusing results of collected data. False reports or other failures in the application can also cause misleading judgements or difficulties for the users. Neither of the apps actually offer protection to the app-users themselves as the apps notify only after the case of a possible exposure to the virus.

Koronavilkku does not collect personal data, contrary to *The Health Code* where officials can see a person's financial transactions alongside their location and therefore can identify the users. With data that *The Health Code* collects, it would be possible to monitor things other than health, such as consumption behaviour or movement. With *Koronavilkku* even the person's health monitoring is very limited since users will upload only the positive covid test result if they choose to, and there is no symptom-tracking afterwards. Finnish *Koronavilkku* is close to Foucault's definition of biopower as explained in chapter 1. However, China's *Health Code* provides an example of a more explicit exploitation of control. The two examples show that there are different possibilities for governments to monitor health that can be done in various levels of privacy depending on how the applications are developed and what rules there

are to regulate them. Governments can modify the rules according to their interests but as the examples show, governments also seek to legitimise the use of health monitoring in the eyes of the public.

6. Legitimising CTAs: Building blocks for legitimate health governance

Juho Majanen

Several case studies have shown how supposed efficacy and privacy concerns are linked to the use of coronavirus contact-tracing applications (CTAs) (Hogan et al., 2021; Lucivero et al., 2021; Samuel et al., 2021). A central argument here is that citizens' evaluation of the legitimacy of the application will affect its use and eventual effectiveness (see Li, 2021). The concept of legitimacy has not been largely applied to the study of CTAs. In this chapter, the goal is to assess how legitimacy is connected to other considerations concerning CTAs and to discuss whether a potential legitimacy-deficit can affect future trials of similar applications.

Legitimacy is about citizens' evaluations of the government's right to exercise power. Here, I employ Schmidt's (2013, 2020) subtler definition of legitimacy by dividing it into input, output, and throughput legitimacy. Input legitimacy is realised when people hold the view that the government takes into account the public debate and opinion in decision making, whereas output legitimacy describes how citizens accept the exercise of power and evaluate its adherence to norms and values (Schmidt, 2020, p. 31). Throughput focuses on the "black box" of events that create the process of governance between the input and the output, and evaluations of its righteousness (2020, p. 25).

As presented in this paper, digital surveillance presents a dilemma with no easy way out. Balancing between individual freedom and common good is as fundamental to ethics as it gets. Complicating the matter, disease tracing applications concern issues not only of digitalisation and data collection, but also right to self-governance in health. From a normative perspective, these considerations should be addressed thoroughly in each step of the policy process. Yet, drawing from a recent example, digital governance of health became unquestioned in the time of the COVID-19 crisis (Susi, 2022, p. 284). *Does it work (save lives)?* was a more frequent question than *is it right (legitimate/legal)?* In this context, it is not important to be able to clearly calculate the power balance between public health and individual interests that has taken place in the latest epidemic. Actually, a more nuanced understanding of the factors affecting perceptions is needed instead of settling for a simple binary (Lucivero et al., 2022). This is

because understanding citizens' evaluations of the foundational principles in question is at the core of assessing input legitimacy. In order for governments to find legitimation for the application, the public has to deem the concept of digital public health surveillance appropriate and justifiable. If the public opinion strongly disavows the collection of personal data, it is evident that the public will delegitimize the application altogether.

Epidemics are treated with several prevention mechanisms all requiring legitimation. Applications represent only one in many. Digital surveillance methods in mobile phone applications present an alternative to other measures in combating disease spread. Evaluation of the necessity and efficacy of applications should be based on countersuggestions, meaning consideration whether the application can replace stricter legislative restrictions or surveillance methods (Mello & Wang, 2020, p. 953). Also, according to public health principles, the chosen method should place the least burden on people (2020, p. 953). With simple reasoning, one could argue that having a quasi-mandatory application for disease surveillance/tracing juxtaposed with using other public health measures, such as government-imposed quarantines, seems the most obvious choice for an effective and least-burdensome method of governance. Theoretically this could imply that digital applications would dominate the market of disease governance strategies. Governments could resort to legislating the use of applications and not much else. Realities welcomed, however, this future falls short on plausibility. It is obvious that during the worst crisis, the government will use other measures as well.

The evidence from the coronavirus pandemic reveals a mixed-to-poor efficacy of the applications, on top of what lies heightened hesitancy and agnosticism towards using them (see sections 3 and 4). Not to take the ineffectiveness of CTAs for granted; if they were completely useless, this paper would probably not exist. But the *supposed* ineffectiveness of the applications affects output legitimacy. If using the application holds no supposed value for people, it loses legitimacy: there is no reason for the government imposing it. The cumulative effect of prevention measures makes determining the effectiveness only harder. During the COVID-19-pandemic, contact-tracing applications were used in tandem with other control methods and restrictions, making the digital dimension only an additional nuisance for people to bear. You could ask why the public would use an application if they were also expected to practise social distancing, for instance. Although, from a public health perspective, measures together create the ends, citizens tend to evaluate them individually (Mækelæ et al., 2020). That is why legitimation for CTAs does not automatically follow the legitimation of other prevention measures.

The achieved output legitimacy can bear fruit on future occasions. The flip side of the coin is suspectedly negative: not granting output legitimacy for a failed undertaking means finding input legitimacy in similar future occasions becomes difficult. Lund-Tønnesen and Christensen (2021) come to this conclusion as well when discussing the Norwegian Smittestop applications. Low output legitimacy associated with the two versions of the app created potential distrust to similar technologies (Lund-Tønnesen & Christensen, 2021, p. 15). To avoid this circularity, clear parameters are expected from which each issue at hand can be evaluated.

Throughput legitimacy in the case of CTAs is built up by making the application development process transparent and open to evaluation. Governments may have a public mandate to issue applications but fail on their way to the finished product. According to Lund-Tønnesen and Christensen's (2021) research, the first version of Smittestop lacked throughput legitimacy because its development process was relatively closed (p. 11). This legitimacy-deficit contributed to cancellation of the first version. Smittestop 2 regained legitimacy by being open about the parties involved in the development process and explicating the technology in national media. The Norwegian case is an excellent example of how a government tries to consciously enhance throughput legitimacy in an attempt to increase favourability among people.

Governments face an uphill battle in trying to introduce any application collecting personal data. In the time of a crisis exceptional measures are more easily legitimised. Are CTAs only an exceptional measure, however? The technology could be employed to combat seasonal flu, or, in smaller scale, several STDs. If this is not the place to discuss technical aspects, assessments of legitimacy can be reviewed. Seasonal flu is potentially more widespread than COVID-19, but less lethal; no government is issuing a lockdown due to influenza. Governments introducing an application that is not deemed absolutely necessary may find it hard to legitimise. This concerns both input and output legitimacy. Data collection and surveillance, already voiced concerns, are harder to dismiss politically if there is no absolute need for it. As for output legitimacy, the threshold of acceptance rises when values of individual freedom and autonomy outweigh the public good. This applies intra-case-wise, too. Most of the COVID-19 CTAs were scrapped when the air of crisis dissipated.

Schmidt's tripartite definition of legitimacy leads us to think that building legitimacy is a continuous project. This helps us imagine that when governments issue CTAs, it has similar phases as any public policy process. Assessing faults and successes in each phase is a precondition for legitimacy. When considering future cases, linearity of the process transforms

into circularity: prior experiences and attitudes influence how input legitimacy is achieved. And why consider legitimacy as something worthwhile besides ethics and privacy? I define legitimacy to be a sum of all these considerations that is eventually interpreted from the face of the government. Assessing legitimacy is a tool through which democracy is evaluated.

7. Conclusion

This paper used the recent COVID-19 pandemic as context from which to consider the use of contact-tracing applications (CTAs) for eHealth governance, as well as their implications and issues for future use. An initial theoretical background, considering Foucault's concept of biopower, was integral to argue that these applications are based on this conception of power and thus they are based on truth discourses, and rely on self-regulation and active, conscious individuals who feel and acknowledge a moral responsibility to contribute to public health. However, biopower is a form of citizen control and thus issues of privacy, data security and ethics of use arise.

Contact-tracing remains an integral and effective tool for infectious disease prevention and mitigation. CTAs are an extension of current tracing methods and seen as necessary for rapid and widespread tracing. However, the contrast of the employed examples, between China and the Nordic countries, shows that CTAs vary in their effectiveness and supposed legitimacy. Future technological innovations could make the tracing process more transparent or easier, but this does not take away the fact that people need to orient themselves to use the applications. When considering the future possibilities of CTAs, one needs to take into account both the technological aspect and people's attitudes and willingness to use them.

From the research, there seem to be two issues operating in parallel, the first concerns free will and moral responsibility, with Foucault's idea of biopower and voluntary buy-in to the system at one end of the spectrum and state control at the other. The second is the issue of privacy and the scope of personal information collected, used, and shared. Citizens are wary of CTAs, equating the application of such technology to an Orwellian surveillance society. Privacy concerns present a real obstacle in the function of launching CTAs, and the normative assumption is that there must be a trade-off between privacy and public security. A proper and thorough consideration of all aspects of data collection, use, and processing is required.

Both issues contribute to the eventual use of the applications; to ignore these considerations means that legitimacy will be lost. Solutions proposed by literature centre around digital architecture, algorithmic governance, and autonomous management of collected

and anonymised data to better ensure privacy protection. As the final chapter suggests, CTAs should be considered as public policy and, therefore, all concerns arising in each phase of the policy process should be thoroughly addressed to ensure legitimacy – and democratic governance.

References

Ahmed, N., Michelin, R.A., Xue, W., Ruj, S., Malaney, R., Kanhere, S.S., Seneviratne, A., Hu, W., Janicke, H. & Jha, S.K. (2020). A survey of COVID-19 contact tracing apps. *IEEE Access, 8*, 134577–134601. https://doi.org/10.1109/ACCESS.2020.3010226

Akinsanmi, T., & Salami, A. (2021). Evaluating the trade-off between privacy, public health safety, and digital security in a pandemic. *Data & Policy*, 3, E27. doi:10.1017/dap.2021.24

Buhr, L., Schicktanz, S. & Nordmeyer, E. (2022). Attitudes toward mobile apps for pandemic research among smartphone users in Germany: National Survey. *JMIR Mhealth Uhealth*, *10*(1), e31857. https://doi.org/10.2196/31857

Constantinou, C. S. (2021). Responses to COVID-19 as a form of 'biopower'. *International Review of Sociology,* 32(1), pp. 29-39. https://doi.org/10.1080/03906701.2021.2000069

Davis, L. (2021). 'In the Time of Pandemic, the Deep Structure of Biopower Is Laid Bare.' *Critical Inquiry,* 47(2), 138-142. https://doi.org/10.1086/711458open_in_new

Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L., Parker, M., Bonsall, D., & Fraser, C. (2020). Quantifying sars-cov-2 transmission suggests epidemic control with digital contact tracing. *Science, 368*(6491). https://doi.org/10.1126/science.abb6936

Finnish Institute for Health and Welfare, THL (2022). *Transmission and protection.* Retrieved November 1, 2022, from https://thl.fi/en/web/infectious-diseases-and-vaccinations/what-s-new/coronavirus-covid-19-latest-updates/transmission-and-protection-coronavirus

Finnish Institute for Health and Welfare THL. (2020). *Koronavilkku on nyt julkaistu* Retrieved October 28, 2022, from https://thl.fi/fi/-/koronavilkku-on-nyt-julkaistu-lataa-sovellus-puhelimeesi-

Hogan, K., Macedo, B., Macha, V., Barman, A., & Jiang, X. (2021). Contact tracing Apps: lessons learned on privacy, autonomy, and the need for detailed and thoughtful implementation. *JMIR Medical Informatics,* 9(7). https://doi-org.ludwig.lub.lu.se/10.2196/27449

Jones, K. & Thompson, R. (2021). To use or not to use a COVID-19 contact tracing app: mixed methods survey in Wales. *JMIR Mhealth Uhealth, 9*(11). https://doi.org/10.2196/29181

Kim, Y., Chen, Y., & Liang, F. (2021). Engineering care in pandemic techno governance: The politics of care in China and South Korea's COVID-19 tracking apps. *New Media & Society*, 0(0). https://doi.org/10.1177/14614448211020752

Kucharski, A. (2020). *The Rules of Contagion: Why Things Spread--And Why They Stop*. Basic Books.

Köykkä, S., & Kaikkonen, R. (2020). *Näin toimii koronavirusaltistuksia jäljittävä mobiilisovellus*. Retrieved October 26, 2022, from https://www.solita.fi/blogit/nain-toimii-suomen-koronavirusaltistuksia-jaljittava-mobiilisovellus/

Li, Y.-T. (2021). Accounting for "the social" in contact tracing applications: The paradox between public health governance and mistrust of government's data use. *Big Data & Society,* 8(2). https://doi-org.ludwig.lub.lu.se/10.1177/20539517211054277

Liu, C. (2021). Health information systems amid COVID-19 outbreak: Lessons from China. *Health Information Management : Journal of the Health Information Management Association of Australia*, 50(1–2), 99–100. https://doi.org/10.1177/1833358320947557

Lucivero, Federica, et al. (2021). Normative positions towards COVID-19 contact-tracing apps: findings from a large-scale qualitative study in nine European countries. *Critical Public Health* 32(1), 5-18. https://doi-org.ludwig.lub.lu.se/10.1080/09581596.2021.1925634

Lund-Tønnesen, J., & Christensen, T. (2022). The dynamics of governance capacity and legitimacy: the case of a digital tracing technology during the COVID-19 pandemic. *International Public Management Journal*, 1-19. https://doi-org.ludwig.lub.lu.se/10.1080/10967494.2022.2112328

Mello, M. M., & Wang, C. J. (2020). Ethics and governance for digital disease surveillance. *Science* 368(6494), 951-954. https://doi-org.ludwig.lub.lu.se/10.1126/science.abb9045

Mækelæ, M. J., Reggev, N., Dutra, N., Tamayo, R. M., Silva-Sobrinho, R. A., Klevjer, K., & Pfuhl, G. (2020). Perceived efficacy of COVID-19 restrictions, reactions and their impact on mental health during the early phase of the outbreak in six countries. *Royal Society Open Science*, 7(8). https://doi-org.ludwig.lub.lu.se/10.1098/rsos.200644

Miller, S. (2010). T*he moral foundations of social institutions: a philosophical study.* Cambridge University Press.

Nadisan, M. H. (2008). *Governmentality, Biopower, and Everyday Life*. New York: Routledge.

National Health Commission of the People's Republic of China. (2020). *Health QR code helps curb the spread of COVID-19*. Retrieved October 26, 2022, from http://en.nhc.gov.cn/2020-03/28/c_78415.htm

Oksala, J. (2013). 'From Biopower to Governmentality'. In C. Falzon, T. O'Leary & J. Sawicki (Eds.), *A Companion to Foucault*, First Edition, 320-336. Hoboken: Blackwell Publishing Ltd.

Park, S., Choi, G. J., & Ko, H. (2020). Information Technology-Based Tracing Strategy in Response to COVID-19 in South Korea - Privacy Controversies. *JAMA - Journal of the American Medical Association,* 323(21), 2129-2130. https://doi-org.ludwig.lub.lu.se/10.1001/jama.2020.6602

Parker, M.J., Fraser, C., Abeler-Dörner, L., & Bonsall, D. (2020). Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic. *Journal of Medical Ethics*, 46(7), 427–431. https://doi.org/10.1136/medethics-2020-106314

Parliament of Finland. (2020). H*allituksen esitys eduskunnalle laiksi tartuntatautilain väliaikaisesta muuttamisesta annetun lain muuttamisesta.* Retrieved October 26, 2022, from https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_225+2020.aspx

Prainsack, B. (2020). The political economy of digital data: introduction to the special issue. Policy Studies, 41(5), 439–446. https://doi.org/10.1080/01442872.2020.1723519

Rabinow, P., & Rose, N. (2006). 'Biopower Today'. *Biosocieties, 1*(2), 195-217. https://doi.org/10.1017/S1745855206040014

Samuel, G., Roberts, S.L., Fiske, A., Lucivero, F., McLennan, S., Phillips, A., Hayes, S. & Johnson, S.B. (2022). COVID-19 contact tracing apps: UK public perceptions. *Critical Public Health, 32*(1), 31–43. https://doi.org/10.1080/09581596.2021.1909707

Sharma, S., Singh, G., Sharma, R., Jones, P., Kraus, S., & Dwivedi, Y. K. (2020). Digital health innovation: exploring adoption of COVID-19 digital contact tracing apps. *IEEE Transactions on Engineering Management*. https://doi.org/10.1109/TEM.2020.3019033.

Schmidt, V. A. (2013). Democracy and Legitimacy in the European Union Revisited: Input, Output and "Throughput." *Political Studies*, 61(1), 2–22. https://doi-org.ludwig.lub.lu.se/10.1111/j.1467-9248.2012.00962.x

Schmidt, V. A. (2020). *Europe's Crisis of Legitimacy : Governing by Rules and Ruling by Numbers in the Eurozone.* First edition. Oxford University Press.

Susi, M. (2022). Digital Human Rights Proportionality During Global Crisis. In M. C Ketteman, & K. Lachmeyer (eds.), P*andemocracy in Europe: Power, Parliaments and People in Times of COVID-19*. Oxford: Hart Publishing. 283-298.

Suver, C., & Kuwana, E. (2021). mHealth wearables and smartphone health tracking apps: A changing privacy landscape. *Information Services & Use,* 41(1/2), 71–79. https://doi-org.ludwig.lub.lu.se/10.3233/ISU-210114

THL. (2022). *Koronavilkku.* Retrieved November 3, 2022, from https://koronavilkku.fi/en/

Valtioneuvosto. (2020). *Koronavilkku has now been published – download the app to your phone!* Retrieved October 28, 2022, from https://valtioneuvosto.fi/en/-//1271139/koronavilkku-has-now-been-published-download-the-app-to-your-phone-

Viljanen M., & Parviainen H., (2022). AI Applications and Regulation: Mapping the Regulatory Strata. *Frontiers in Computer Science*, 3. https://doi.org/10.3389/fcomp.2021.779957

Yang, F., Heemsbergen, L., & Fordyce, R. (2021). Comparative analysis of China's Health Code, Australia's COVIDSafe and New Zealand's COVID Tracer Surveillance Apps: a new corona of public health governmentality? *Media International Australia*, 178(1), 182–197. https://doi.org/10.1177/1329878X20968277