International Journal of Public Health Science (IJPHS)
Vol. 12, No. 3, September 2023, pp. 1232~1242
ISSN: 2252-8806, DOI: 10.11591/ijphs.v12i3.21480

Balancing privacy at the time of pandemic: global observation

Zoran Jordanoski, Luis Felipe M. Ramos, Moinul Zaber
United Nations University - Operating Unit on Policy-Driven Electronic Governance (UNU-EGOV), Guimaraes, Portugal

Article Info

Article history:

Received Oct 26, 2021
Revised May 24, 2023
Accepted Jun 10, 2023

Keywords:

COVID-19
Data protection
Mobile applications
Privacy
Public health

ABSTRACT

The rapid outbreak of COVID-19 has initiated the development of mobile applications aiming at helping public health authorities to slow down viral diffusion. The proliferation of these applications engenders challenges to forge a balance between 'public health utility' and 'personal privacy'. This paper scrutinizes various applications that collect personal data according to their functions and data protection compliance. These applications are mostly of three broader categories- contact tracing, self-assessment, and quarantine enforcement. We conduct systematic categorization based on five parameters- type of owner or provider, host platform, functionalities, the existence of privacy policy, and state of the source code. A total of 122 apps encompassing 83 countries were assessed during a research period of 20 days (June 1 to 20, 2020). Findings suggest that although the majority of the applications publish a privacy policy, many applications do not give information in detail, making the issue of privacy obscure. The majority of the applications collect various sensitive personal data irrespective of their functionalities, provider, and platform. Most applications are not open source raising concerns over trust and transparency. The findings are valuable to policymakers who are formulating short, mid, and long-term technology policies to strike a balance between functionality and personal privacy.

Corresponding Author:

Zoran Jordanoski
United Nations University - Operating Unit on Policy-Driven Electronic Governance (UNU-EGOV
Campus de Couros, Rua de Vila Flor 166, 4810-445 Guimaraes, Portugal
Email: jordanoski@unu.edu

1. INTRODUCTION

The rapid outbreak of COVID-19 has initiated the development of mobile applications aiming at helping public health authorities to slow down viral diffusion. Digital innovations to educate, connect and alert the residents via web and application platforms have proliferated around the world. However, one of the criteria of successful digital interventions is 'trust' they ensure. Many of these applications have concerns regarding their ability to strike a balance between 'public health utility' and 'personal privacy'. Striking this balance has been a challenge that needs to be overcome, not only for short-term COVID-19 response but also for the mid and long-term responses to the ensuing post-COVID-19 era.

This paper scrutinizes a number of mobile applications developed to help public health authorities to slow down the virus outbreak. Most of these applications are collecting personal data that if misused may cause personal privacy intrusion. This paper focuses on mobile applications that collect personal data. We categorize various applications according to their functions and data protection compliance. These applications are mostly of three broader categories-contact tracing applications, self-assessment applications and quarantine enforcement applications. Apart from these, we have also analysed a few other applications that have provisions to collect personal data. These were analysed based on five different parameters: type of owner or provider, host platform, functionalities, existence of privacy policy, and state of the source code.

Findings suggest that although the majority of the applications publish privacy policy or give information related to data use mechanisms, many applications do not explain the reasons behind the collection of specific data. In most cases, the propensity is towards adopting a general privacy policy as opposed to being more specific to various features of the applications. We observe that only a few applications publish source code, rendering third-party scrutiny of the codes impossible. The most worrying fact is that a majority of the applications we have assessed, irrespective of their functionalities, collect location data. As location data directly invades privacy, unjustified collection of these data may create serious damage to trust. The assessments should help the policymakers and developers who are envisioning new interventions in the fight against COVID-19. This should also help assess and compare public health applications with issues of personal privacy. With the proliferation of interventions that accumulate data, managing individual privacy is becoming a regulatory challenge. In a broader aspect, this paper should also contribute to formulating a general framework for balancing functionalities and personal privacy.

The remainder of this article is organized as follows: in section 2 we review the literature on technology use during a public health crisis. In section 3 we present our research methodology. Section 4 is dedicated to our assessment of the applications based on collected data, following which is the concluding section delineating the importance of the findings for policymakers and indicating the future scope of current research.

2. LITERATURE REVIEW

Traditionally, in order to control the spread of contagious diseases, many different measures are adopted. These range from approaches like prophylactic vaccination and drug treatments to pre-emptive culling. One possible approach is to interrupt the transmission from person to person, which can be achieved through reduction of epidemiological contacts (i.e. social distancing) or through tracing the contacts of known cases (i.e. contact tracing) [1]. Nowadays, the use of personal digital devices is ubiquitous, with an estimated 8.3 billion mobile-cellular telephone subscriptions worldwide in 2019, representing approximately 108 subscriptions per 100 inhabitants and 97% of the world population living within reach of a mobile cellular signal [2]. This made many different digital systems developed by governments, private actors, and research institutions, among others to be deployed worldwide. A number of applications have been developed using different specifications and characteristics, deployed in different mobile platforms, using different communication protocols, and data storage mechanisms. Humans move across locations. This contributes to the transmission of communicable diseases, requiring the adoption of actions that can interrupt this contagious process [3]. Among various measures, epidemiological contact tracing (CT) is considered crucial to prevent further transmission of many infectious diseases [1], [4]–[6]. According to the World Health Organization (WHO), three basic elements compose CT [7] identifying persons who may have been exposed to the disease as a result of being in contact with an infected person, tracing the identified contacts, and monitoring the contacts regularly.

Traditional contact tracing of following up cases and contacts using public health staff is resource-intensive [8]. In this context, the adoption of solutions based on information and communication technologies (ICT), such as contact management software and mobile contact tracing applications, may improve the efficiency of CT methods [3], [9]–[13]. Other applications were proven beneficial in disseminating health knowledge and experience [14]–[16]. Many governments and non-governmental organizations launched numerous applications in an attempt to "flatten the curve" and provide citizens with information about the outbreak, and track statistics. These were also deployed to aid the citizens to self-assess symptoms, monitor symptoms, track statistics, schedule doctor's appointments, and issue moving permits [17]. The role of privacy in information systems and technology design is well-established in almost all domains of ICT [18]. This includes health-related applications. Even before the outbreak of COVID-19, several contact tracking applications involving mobile applications, wireless technologies, and global positioning system (GPS) were introduced in the literature [19]–[21]. Considering the increasing concern about the protection of personal data, some of the most recently released applications propose privacy-oriented solutions [8], [22]. All these tools vary in purpose, features, and complexity.

However, just like the traditional CT methods raise privacy concerns [23], [24], digital CT presents privacy risks, which must be carefully addressed in order for individuals to trust the apps. As these apps deal with personal data, location data, and sometimes even sensitive data such as health data, they require intense scrutiny of their data protection policies and practices [25]–[27]. The protection of privacy for infected persons, besides being a legal requirement in most jurisdictions, also represents an important requirement to facilitate the cooperation of individuals. Risks to privacy from traditional and digital interventions vary from data breaches to government surveillance. Examples of governmental mass surveillance can be seen in Israel, which approved emergency legislation, authorization of the general security service to assist the national effort to reduce the spread of the novel coronavirus, allowing the government to use sensitive data to track coronavirus carriers, and in South Korea, that deployed a government-controlled central database that stores tracking data from mobile phones along with credit card records, surveillance video and personal interviews with patients in order to track the infectious spreading.

In this context, the concept of "privacy by design" can be applied to mitigate the risks. "Taking a comprehensive, properly implemented risk-based approach-where globally defined risks are anticipated, and countermeasures are built into systems and operations, by design-can be far more effective, and more likely to respond to the broad range of requirements in multiple jurisdictions" [28] [28]. Originating as a concept in 1995 [29], coined by Cavoukian in 2011 [30], and formulated in the European Union (EU) General Data Protection Regulation (GDPR) in 2016 [31], "privacy by design" became a gold standard in application development and systems engineering [32]. It encompasses seven fundamental principles directly injected into the solution, including transparency and the user's control of his or her data [18], [30], [32].

In order to mitigate these risks, the European Commission went ahead and edited guidelines for apps supporting the fight against the COVID-19 pandemic concerning data protection [33], [34]. European Data Protection Board (EDPB) published some guidelines on the use of location data and contact tracing tools [35]. The US Centers for Disease Control and Prevention (CDC) has also published some criteria for the evaluation of digital CT tools [36].

3. METHOD

3.1. Database design

The research was conducted between 1 and 20 June 2020, and it aimed to provide a detailed overview of the developed mobile applications as a response to the COVID-19 pandemic. It focused on mobile applications due to the fact that mobile phones frequently carried by the user make applications more accessible and easily adopted. On the other side, several web platforms were developed as a response to the COVD-19 pandemic, most of them related to information dissemination or symptom checker. However, due to the massive production of mobile applications, the research focused exclusively on applications that collect and process personal data. The applications whose purpose is the dissemination of information only and the web platforms were excluded from the research. Also, since the number of mobile applications is changing over time, this research was focused on the currently available applications, i.e. the applications that are currently in use (122), while the application in the pilot phase (6), announced (9) and discontinued (2) were excluded due to the lack of information and privacy policy unavailability.

Due to the lack of a global approach, each country developed its unique strategy to slow down the spread of the infection. The research was focused on the United Nations (UN) member states only. Out of 193 UN member states assessed, only 83 countries (43%) have developed at least one mobile application that collects personal data, while one application is categorised as global and used worldwide. The database design was structured in a way to answer the most important questions, such as who the provider (owner of the application) is, the availability of different mobile platforms, functionalities of the applications, the availability of privacy policy or statement, availability of open-source code and collection of location data, including information about users' GPS location. During the assessment period, all 122 available applications were assessed in terms of their purpose and functionalities. For those with the privacy policy available, the research analysed the categories of personal data collected, collection of sensitive data, and the use of GPS protocol for information about user's location to assess the impact on citizens privacy. Table 1 summarizes the database design used for the assessment of mobile applications.

Table 1. Database design

Category	Possible answers
Provider	Government
	Private company
	Non-government organisation
	Joint initiatives
Mobile platforms	Android
	iOS
	Huawei
	Other
Functionalities	Contact tracing applications
	Self-assessment/medical reporting applications
	Quarantine enforcement/isolation registration applications
	Other applications
Privacy policy available	Yes
	No
	Yes, but it does not contain enough information
Opensource	Yes
	No
Use GPS location data	Yes
	No

3.2. Data description

The first assessment is aimed at identifying the provider of the applications that act as the data controller. The provider of the application is defined as a natural or legal entity that "determines the purposes and means of the processing of personal data". The question of the data controller is essential and shows who establishes the purposes and means for processing personal data. The data controller should always be held accountable for the lawfulness of personal data processing. Keeping in mind that privacy is a fundamental human right and needs to be respected during the pandemic, it is important to determine who collects citizens data, i.e. if it is the government, a private company, an Non-governmental organization (NGO or it is some joint initiative.

The mobile applications were categorized using the following criteria: i) Government: the data controller is an institution/body/organization of public law; ii) private company: the data controller is registered and operates under commercial law regulations; iii) non-governmental organization (NGO): the data controller is registered under the regulations of civil society and non-profit organisations; iv) joint initiative: the data controller is formally registered or informally operates as an initiative of two or more different entities (government, a private company, NGO, academia, and volunteers); v) other: other non-categorised providers of mobile applications.

The second assessment was related to their availability for different "Mobile platforms". It has two dimensions. First, the availability of more platforms means more extensive outreach, which probably will increase the application success rate. Second, the availability in some mobile platforms, such as iOS, means that the application passed additional filters in terms of security, valuable content, and application performance. The categorization was based on the following criteria: i) Android: the application is available in the official Play Store. The availability of an Android Package Kit (APK) file only does not result in a positive value; ii) iOS: the mobile application is available in the official App Store; iii) Huawei: the mobile application is available in the official Huawei App Gallery; iv) Other: All other mobile applications available for different mobile platforms.

The third assessment was made based on the functionalities and features of the applications. Since the functions of the applications evolve, 82 of the applications had only one function, while 40 were multifunctional and combined at least two functions. The essential question is about the functions provided by these applications. Hence, the first assessment was to categorize mobile applications based on their functionalities. Second, all these functionalities need to be measured against what this means in terms of privacy, and what benefit can bring to the fight against COVID-19. The balance between citizens' privacy and the tools for fighting COVID-19 needs to be appropriate.

Since all 40 multipurpose applications encompass important functions and collect personal data, the applications were assessed based on their functions and the following criteria: i) contact tracing applications: the application aimed to register the user contacts and determine his/her risk of exposure to the infection. Also, the aim is to notify all users that were in close contact with an infected person. The applications can use different protocols, such as Bluetooth, GPS, or any other method for contact tracing; ii) self-assessment/medical reporting applications: the applications should offer possibilities for users to check their symptoms, report their medical conditions to health authorities or report their COVID-19 status (test results); iii) quarantine enforcement/Isolation registration applications: the applications should offer possibilities for registering people in isolation or self-isolation and/or monitoring their movements and complying with the authority's orders during the quarantine period; iv) other applications: all other non-categorized mobile applications that collect personal data.

The fourth assessment was focused on "privacy policy availability." Although the privacy policy or statement does not intend to overrule, replace or fill the gaps in the national data protection regulations, its availability is the first step toward building trust between data controllers and data subjects. The aim is to provide effective grounds for establishing a solid data protection system for mobile applications. The sensitivity of the situation, as well as the level of data collected, requires significant attention to protect citizens' privacy. For that purpose, the availability of a privacy policy or statement that explains all legal and technical elements regarding the collection and use of the citizens' data by these mobile applications is necessary. From that perspective, the research aimed to determine the percentage of the applications that have well-defined and elaborated privacy policies available.

The applications were categorised based on the following criteria: i) Yes: A comprehensive privacy policy or statement with the most important information (data controller, data processor, categories of personal data collected, the purpose of the collection, retention period and the rights of the data subjects) is available; ii) No: a privacy policy is not available; iii) Yes, but it does not contain enough information: a privacy policy is made available, but it is usually a general website privacy policy and does not contain adequate information regarding the data controller, categories of personal data collected, the purpose of the collection, retention period and the rights of the data subjects.

The fifth assessment was dedicated to the transparency of the mobile applications and whether the application is "Open-source". This element, also related to trust and transparency, addresses the availability of the application source code. From a privacy perspective, it is important to answer the question of how many providers published the application source code, which allows independent experts to review the code. This category was chosen because it will show the readiness of the providers to be more transparent when it comes to balancing privacy at the time of the pandemic. The applications were categorized based on the following criteria: i) Yes: the source code of the application is available; ii) No: the source code of the application is not available.

Lastly, the sixth criteria for assessing the applications were the collection or use of GPS location data. The question about collecting and using the users' GPS location data is important to be assessed since numerous applications with different functions seek permission to use users' GPS location data in order to be able to use the application. For that purpose, it is important to determine how many applications are using GPS location data and what this means to citizens' privacy. The classification was made based on the following criteria: i) Yes: the application makes mandatory or voluntary use of the user's GPS location data; ii) No: the application does not use or collect the user's GPS location data. Finally, a discussion over dependencies of the above-mentioned classifications and criteria is presented in order to understand their relations and impact on the application functionalities and impact on privacy.

4. STATE OF THE ART OF THE APPLICATIONS

Among all COVID-19 applications we have assessed, the majority is provided by governments (78.69%), followed by joint initiatives (8.2%), private companies (7.38%), NGOs (4.10%), academic institutions (0.82%), and a group of volunteers (0.82%) as Figure 1 shows. Regarding platform availability, 96 applications (79%) are available for the two most advanced and used platforms (Android and iOS), while 23 are available for Android only (19%) and two are available for iOS only (2%). Only one application is available for use neither on the Android nor the iOS platform. In other classifications, 119 applications are available for Android, 98 for iOS, 7 for Huawei, and 1 for other platforms. This indicates that application providers have plans for widespread use irrespective of the platforms. This is an important criterion as applications that would trace contact would best work if used at least by a critical mass [37].

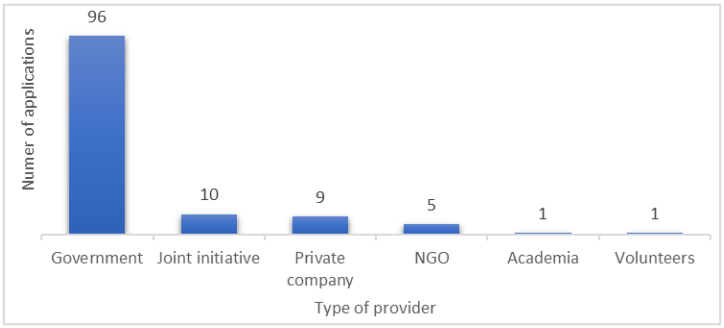

Figure 1. Data protection controller of the mobile applications

Concerning functionalities criteria, 67% of the applications had only one function, while 33% contained two or more functions. Based on the functions each application presents, Figure 2 shows that most of them are aimed to provide self-assessment or medical reporting, followed by contact tracing applications, quarantine enforcement or isolation registration, and other applications. The question of privacy and transparency remains key in terms of balancing the functionalities of the applications and citizens' privacy. Among all assessed applications, Figure 3(a) Comparing privacy and transparency in terms of the availability of privacy policy or statement shows that 90 of them (74%) have published privacy policy or statement that contains enough information about the data controller, categories of personal data collected, the purpose of collection, retention period, rights of users and all other necessary information that gives users sufficient information about their rights. What is worrying is that 25 applications (20%) do not present a privacy policy or statement, while 7 applications (6%) are linked to some sort of privacy policy or statement, but do not contain enough information for users to understand why, how and for what purpose their data is collected, and what are their rights. However, a general recommendation is that all mobile applications need to have their

own, especially adopted and available privacy policy or statement, and not to be linked to some general organizational policy statements. Related to the privacy aspects, the question of transparency also becomes important. The assessment showed that only 18 providers (15%) made the application's source code available, while 104 providers (85%) did not provide the source code, as shown in Figure 3(b) comparing privacy and transparency in terms of the availability of the application source code. This means that most of the providers of the applications are not ready for expert scrutiny.

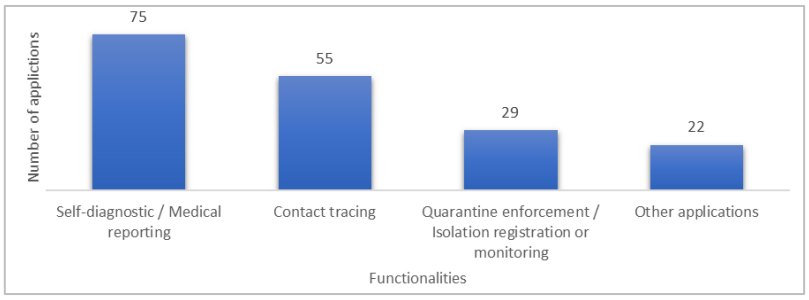

Figure 2. Classification of applications based on functionalities

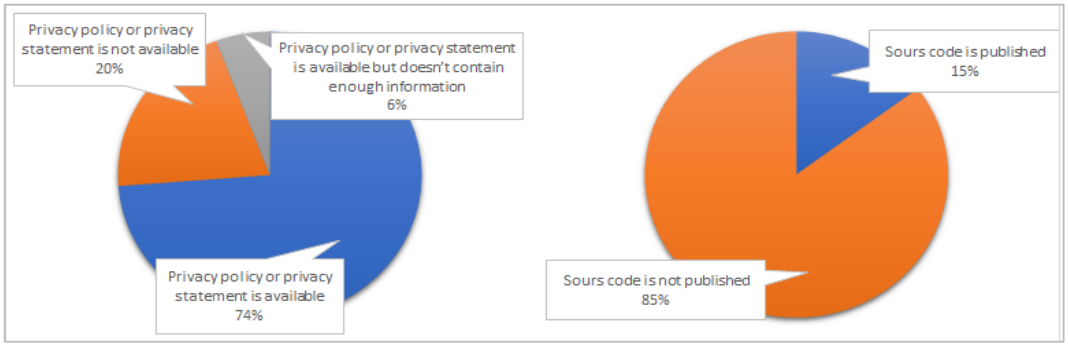

Figure 3. Comparing privacy and transparency in terms of the (a) availability of privacy policy or statement and (b) availability of the application source code

Lastly, a worrisome fact is that 82 applications (67%) collect users' GPS locations, while 40 applications (33%) either exclusively indicate that they do not collect users' GPS location data, or the assessment could not find information if such data is collected or not. A general recommendation is that the use of users' GPS location data needs to be carefully examined, and it is only justifiable as the last possible option for authorities. If the goal is achievable through other, less-invasive tools, the use of the GPS location data should be avoided. In the following subsections, we describe the applications based on their types (contact tracing applications, self-assessment/medical reporting applications, quarantine enforcement/isolation registration applications, and all other applications) and based on their features (provider, platform, functionality, privacy policy, open source, location data acquisition), their positive effects in terms of slowing down the infection, their impact and negative effects to citizens' privacy.

4.1. Self-assessment/medical reporting applications

The assessment showed that 75 out of 122 applications contain self-assessment or medical reporting function. The majority of the applications are provided by governments (55), followed by joint initiatives (9), private companies (6), NGOs (3), academic institution (1), and a group of volunteers (1). In terms of the platform availability, 72 applications are available for the Android platform, 56 for iOS, 4 for Huawei and 1 is available on another platform. The main objective of these applications is to allow users to perform a quick regular assessment of their symptoms in order to understand their medical conditions and possibilities of infection. The self-checker asks the user a series of questions about symptoms they are experiencing and compares those symptoms to a list of documented COVID-19 virus symptoms. Additionally, some of these applications enable users to schedule an appointment or to submit their symptoms to health authorities for

obtaining an opinion on whether they should schedule a test or be isolated at their homes. However, the majority of these applications provide a basic survey where users answer several questions to get quick feedback on their potential infection. Importantly, most of them contain a disclaimer that the result or advice given at the end of the survey is not a doctors' opinion and should be taken only as a recommendation.

However, the real benefit of using these applications is the quick and easily accessible symptom checker tools and possible scheduling of an appointment. This, in general, will reduce the pressure on the other communication channels with the health authorities (telephone, e-mail or in-person consultation). All these applications fall into the group of less innovative solutions from a technology perspective.

On the other side, the real threat to privacy is the volume of data collection and its purpose. Common for all these applications is the collection of data about the users' health conditions, which are considered sensitive data. In general observation, 52 applications (69%) contain appropriate privacy policy or statement, while four applications (6%) made some privacy policy available, but not adequate in terms of providing enough information. However, having in mind the sensitive data collected by these applications, it is worrying that 19 applications (25%) do not contain any privacy policy or statement. Additionally, 54 applications (72%) collect users' GPS location. Another worrying fact is that only three providers (4%) have made the source code available.

Regarding the balance between the benefits of these applications and their invasive nature, the findings are that they collect more data than is necessary. These applications need to be reviewed and re-designed in a way that will not collect personal data, i.e. will not keep a record of the symptoms provided by users. The data provided during the short survey should be used only to give a recommendation to users in terms of the possibility of infection. In that regard, health authorities do not need any records of the user's medical conditions until a regular test is conducted. Additionally, the collection of users' GPS location data is not justifiable and is against the principles of data minimization and proportionality.

4.2. Contact tracing applications

The research found out that 55 mobile applications contain a contact tracing function. Almost all applications are provided by governments (45), followed by a private company (4), NGO (3), joint initiative (2), and a group of volunteers (1). In terms of platform availability, 54 of 55 of the applications are available for the Android platform, 46 for iOS, two for the Huawei platform, and one for other platforms.

Contact tracing is the process of recognising, estimating, and managing people who have been exposed to a disease to prevent onward transmission. Contact tracing for COVID-19 requires identifying people who may have been exposed to the COVID-19 virus and following them daily for 14 to 21 days from the last point of exposure. The main objective of these applications is to automate the contact tracing process and to help health departments in the detection and discovery of all people that have been in contact with an infected person during the incubation period. There is a provision for the health department to let the person know that they have probably been exposed to the COVID-19. This mechanism should facilitate guidance as to how the affected individuals should act to keep the pathogen contained [38]

The basic working principle of these applications is as follows: when two users that have installed the application are in close contact, their devices exchange anonymous "digital information." If one user tests positive, the result can be sent to health authorities. From there the persons who may have been in contact with the index case will be informed through the application. This application should help the health department to guide people's mobility and reduce the spread of the virus [38], [39]. The applications work through mostly Bluetooth or GPS protocols. People must always keep the phone and Bluetooth and/or GPS tracking connection turned on. This strains the mobile battery and is a reason for customer dissatisfaction.

However, besides it is a more advanced technological solution, its success depends mostly on non-technological factors. Namely, to achieve greater success and efficiency, a large proportion of the population needs to install and use the application. Another factor is access to the COVID-19 tests database to ensure accurate information and notification for users that have been in close contact with an infected person. Lastly, it relies on the infected user consent to allow health authorities to access the "digital contacts" in order to notify them. In smaller communities, this can be problematic since a lot of stigmatization cases could emerge.

On the other side, these CT applications raise many privacy concerns. First, the question of who collects and owns the collected data is essential. Namely, there are decentralized data management applications where the data are stored in the user location only, in an anonymous and encrypted form. These data can be uploaded to the server only if the user is infected and he/she gives explicit consent. On the other side, centralized data management is a more privacy-invasive solution since it uploads the data to the central server once they are collected. In this scenario, the user already gave consent for uploading his/her data once he/she agreed to use the application. Additionally, the use of data protection by design and by default principles when designing CT applications will increase their compliance with the general data protection regulations.

Another concern is the encryption and anonymization techniques. The practice showed that there are always possibilities for data breaches and decryption and re-identification of the users which can lead to massive violation of citizens' privacy. The potential effects are huge since the collected data can be used for tracing the citizens' most common relationships with other people, most frequently used locations, habits, and other important aspects of citizens' private life. Falling this data into the wrong hands (non-democratic government regimes, private companies aimed to commercialize such data, or any other criminal cyberattacks) can cause massive privacy violations.

In that regard, 42 applications contain appropriate privacy policy or statements explaining who collects the data, what data are being collected, the purpose for collection and users' rights. On the other side, 10 mobile applications are not presenting any privacy policy or statement, while 3 have some privacy policy or statement available, but the information provided is not adequate. In terms of transparency, only 18 providers have made the source code available, while the other 37 are closed for an independent audit.

In conclusion, the practice showed that these applications could not be successful and provide positive effects in the short term. The massive production of CT applications around the world showed that citizens are still not ready to trust the governments (or other providers) with their data in the fight against COVID-19. For example, the Norwegian government terminated the "Smittestopp" CT application after a warning from the Norwegian Data Protection Authority [37]. However, an additional reason for termination was the low number of downloads (1.6 million, which is just over 10% of Norway's population, or around 14% of the population aged over 16) and active users (600.000) [37], although Norway is categorised as a country with high trust in government (68.7% in 2018) [40].

4.3. Quarantine enforcement/Isolation registration

The assessment found out that 29 of 122 applications contain quarantine enforcement or isolation registration function. Almost all the applications are provided by governments (28), while one application is developed by a non-profit organisation. In terms of the platform availability, all 29 applications are available for the Android platform, 22 for iOS and only one for the Huawei platform.

The main objective of these applications is to register all citizens that are confirmed COVID-19 patients but are receiving their treatment at their homes. Also, these applications register citizens that were in close contact with COVID-19 positive patients in the last 14 days and are asked to stay isolated at their homes for some period (usually 14 days). Enforcement is the process of ensuring acquiescence with laws, regulations and social norms. If anyone receives self-quarantine subjects from their health department, they are legally prohibited from leaving their quarantine areas. At their home, they are instructed to maintain strict separation from other people, including family members. The aim is to ensure that these citizens obey the government decisions to stay isolated at their homes, i.e. to monitor their movements in case they leave their homes. Some of these applications are mandatory and only citizens that will sign a written declaration that does not own a smartphone can be exempted from the order. In all other cases, citizens must install the application, keep the mobile phone and the GPS tracking location turned ON, and in some cases send a selfie from their home upon request. Notably, 27 of 29 applications are using users' GPS location to track movements, while two applications are not using this function.

In terms of privacy issues, these applications are aimed to monitor and record the user's movement and locations. Only 19 applications (66%) contain a privacy policy, 3 applications (10%) have a privacy policy that does not contain enough and appropriate information, while 7 applications (24%) do not contain any privacy policy or statement. Significantly, no one of the applications providers made the source code available.

Concerning the balance between the positive effects of these applications with the privacy aspects, the use of these applications can be justified only during the government order. Namely, the citizens' movement can be restricted by government (or court) order to prevent the future spreading of the virus. In that sense, the government can use a different type of method to ensure that citizens will stay quarantined and isolated at their homes. Examples of this exist in practice in the past, like random controls by police officers or special ankle GPS bracelets used for home detention, etc. Following this, the use of mobile applications to monitor citizens' movement and ensuring their presence at their homes is another tool that can help governments in the fight against COVID-19. However, what is worrisome is the retention period of such data and the need to keep them. According to the data protection principles, such data need to be deleted once the purpose of collection is achieved after the end of the mandatory isolation period.

4.4. Other applications

Apart from the three main categories, a number of applications (20) with other functions were identified. However, most of these functions are integrated into multifunction applications (19), and only one application is specially developed for curfew management. In general, these other functions can be divided into three main categories: curfew management, proving COVID-19 status and mapping infected areas. The curfew management function in the applications (10) is used to enforce movement permits in cases of necessity during

the curfew inside the city or between cities. The main objective is to facilitate the issuance of electronic movement permits. These can help authorities allow people with medical appointments and delivery applications agents to obtain movement permits during the curfew period [41]. These applications collect personal information and give authorities access to the day to day lives of the people which can be a serious threat to individual privacy. However, if well designed and developed following the data protection principles, these applications can be very useful tools for public authorities in order to manage the restrictions during the curfew. The data protection principles for data minimisation, purpose and storage limitation must be implemented.

Similarly, several applications (6) contain a function where users can verify their COVID-19 status (verified by public authorities). These applications are designed for citizens to be able to provide valid proof of their status, for example, a negative or positive test, or even a presence of antibodies. The principle of these applications is similar to the mobile ID cards and boarding passes, where the user can provide reliable proof of his/her status through a QR code that can be easily verified. In terms of positive effects to the COVID-19 management, these applications can be used in the future after a significant number of the population develop antibodies or a vaccine is developed. On the other side, these applications raise many privacy concerns since they are based on the collection of health data. Similar to the CT applications, the sensitiveness of the data and the vulnerabilities of the systems can endanger citizens' privacy.

Lastly, few applications contain functions to map the infected areas (6) in order to warn other citizens to avoid these places. These applications are based on the voluntarily shared data by the users, and their effectiveness is questioned. Namely, the main threat is that these applications are based on the users' data which is not confirmed or validated by the authorities. This can lead to distributing false information and possibilities of stigmatization of areas.

5. CONCLUSION

For mitigation and containment of the viral spread of SARS-CoV-2 (COVID-19), countries around the world have been taking several notable measures, some of which are highly technology inclusive. Several mobile applications were developed around the globe, to help public health authorities to slow down the virus rapid outbreak. However, like any digital application that initiates a close connection between the 'thing' and the 'user', COVID-19 digital interventions also have concerns related to the balance between 'public health utility' versus 'personal privacy'. The objective of this paper is to scrutinize identified mobile applications that collect personal data.

We categorize various applications according to their functions and data protection compliance. The applications analysed are mostly of three broader categories- contact tracing applications, self-assessment applications and quarantine enforcement applications. These applications were analysed based on several parameters such as the owner or provider, platform of existence, functionalities, existence of privacy policy, and state of the source code. A total of 122 apps encompassing 83 countries of the world were assessed during a research period of 20 days (June 1 to 20, 2020).

Findings suggest that although the majority of the applications published privacy policy, many applications do not give information in detail making the issue of privacy obscure. We also note that the majority of the applications collect various sensitive personal data irrespective of their purpose. This paper gives recommendations to the policymakers who are formulating short, mid, and long-term policies to strike a balance between personal privacy and functionality applicable to the current and post-COVID-19 era. For further research, it will be beneficial to explore the efficacy of these applications aiding in slowing down the infection.

ACKNOWLEDGEMENTS

This article is a result of the project "INOV.EGOV-Digital Governance Innovation for Inclusive, Resilient and Sustainable Societies / NORTE-01-0145-FEDER-000087", supported by the Norte Portugal Regional Operational Programme (NORTE 2020), under the PORTUGAL 2020 Partnership Agreement, through the European Regional Development Fund (EFDR).

REFERENCES

[1] T. House and M. J. Keeling, "The impact of contact tracing in clustered populations," *PLoS Computational Biology*, vol. 6, no. 3, p. e1000721, Mar. 2010, doi: 10.1371/journal.pcbi.1000721.

[2] D. Bogdan-Martin, "Measuring digital development: Facts & figures 2019," *The UN specialized agency for ICTs (ITU)*, 2020. https://www.itu.int/hub/2020/05/measuring-digital-development-facts-figures-2019/

[3] B. C. de Jong *et al.*, "Ethical considerations for movement mapping to identify disease transmission hotspots," *Emerging Infectious Diseases*, vol. 25, no. 7, Jul. 2019, doi: 10.3201/eid2507.181421.

[4] B. Armbruster and M. L. Brandeau, "Contact tracing to control infectious disease: when enough is enough," *Health Care Management Science*, vol. 10, no. 4, pp. 341–355, Dec. 2007, doi: 10.1007/s10729-007-9027-6.
[5] S. Glasauer, S. Kröger, W. Haas, and N. Perumal, "International tuberculosis contact-tracing notifications in Germany: analysis of national data from 2010 to 2018 and implications for efficiency," *BMC Infectious Diseases*, vol. 20, no. 1, p. 267, Dec. 2020, doi: 10.1186/s12879-020-04982-z.
[6] S. Kojaku, L. Hébert-Dufresne, E. Mones, S. Lehmann, and Y.-Y. Ahn, "The effectiveness of backward contact tracing in networks," *Nature Physics*, vol. 17, no. 5, pp. 652–658, May 2021, doi: 10.1038/s41567-021-01187-2.
[7] O. Fawole, M. Dalhat, M. Park, C. Hall, P. Nguku, and A. Peter, "Contact tracing following outbreak of ebola virus disease in Urban Settings in Nigeria," *Pan African Medical Journal*, vol. 27, Jun. 2017, doi: 10.11604/pamj.supp.2017.27.1.12565.
[8] A. Berke, M. Bakker, P. Vepakomma, K. Larson, and A. "Sandy" Pentland, "Assessing disease exposure risk with location data: a proposal for cryptographic preservation of privacy," *arXiv:2003.14412v2*, pp. 1–15, 2020, [Online]. Available: https://arxiv.org/pdf/2003.14412.pdf
[9] L. Ferretti *et al.*, "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing," *Science (1979)*, vol. 368, no. 6491, pp. 1–7, May 2020, doi: 10.1126/science.abb6936.
[10] ECDC Technical Report, "Contact tracing for COVID-19: Current evidence, options for scale-up and an assessment of resources needed," 2020. Accessed: Jun. 19, 2020. [Online]. Available: https://www.ecdc.europa.eu/sites/default/files/documents/COVID-19-Contract-tracing-scale-up.pdf
[11] WHO Team, "2019 Novel Coronavirus (2019-nCoV): Strategic preparedness and response plan," 2020. Accessed: Jun. 19, 2020. [Online]. Available: https://www.who.int/publications/i/item/strategic-preparedness-and-response-plan-for-the-new-coronavirus
[12] World Health Organization, "Contact tracing in the context of COVID-19: interim guidance," 2020. Accessed: Jun. 19, 2020. [Online]. Available: https://apps.who.int/iris/bitstream/handle/10665/332049/WHO-2019-nCoV-Contact_Tracing-2020.1-eng.pdf?sequence=1&isAllowed=y
[13] World Health Organization, "Critical preparedness, readiness and response actions COVID-19: interim guidance," 2020. Accessed: Jun. 19, 2020. [Online]. Available: https://apps.who.int/iris/bitstream/handle/10665/331511/Critical%20preparedness%20readiness%20and%20response%20actions%20COVID-10%202020-03-22_FINAL-eng.pdf?sequence=1&isAllowed=y
[14] M. H. Mobasheri, M. Johnston, D. King, D. Leff, P. Thiruchelvam, and A. Darzi, "Smartphone breast applications – What's the evidence?," *The Breast*, vol. 23, no. 5, pp. 683–689, Oct. 2014, doi: 10.1016/j.breast.2014.07.006.
[15] K. M. J. Azar *et al.*, "Mobile Applications for Weight Management," *American Journal of Preventive Medicine*, vol. 45, no. 5, pp. 583–589, Nov. 2013, doi: 10.1016/j.amepre.2013.07.005.
[16] E. Grasaas *et al.*, "iCanCope with pain: cultural adaptation and usability testing of a self-management app for adolescents with persistent pain in Norway," *JMIR Research Protocols*, vol. 8, no. 6, p. e12940, Jun. 2019, doi: 10.2196/12940.
[17] N. Noronha *et al.*, "Mobile Applications for COVID-19: A Scoping Review of the Initial Response in Canada," *Research Square*, 2020.
[18] K. Wahlstrom, A. Ul-haq, and O. Burmeister, "Privacy by design," *Australasian Journal of Information Systems*, vol. 24, Jun. 2020, doi: 10.3127/ajis.v24i0.2801.
[19] T. Altuwaiyan, M. Hadian, and X. Liang, "EPIC: efficient privacy-preserving contact tracing for infection detection," in *2018 IEEE International Conference on Communications (ICC)*, Kansas City, MO, USA: IEEE, May 2018, pp. 1–6. doi: 10.1109/ICC.2018.8422886.
[20] L. O. Danquah *et al.*, "Use of a mobile application for Ebola contact tracing and monitoring in northern Sierra Leone: a proof-of-concept study," *BMC Infectious Diseases*, vol. 19, no. 1, p. 810, Dec. 2019, doi: 10.1186/s12879-019-4354-z.
[21] E. Reddy, S. Kumar, N. Rollings, and R. Chandra, "Mobile application for dengue fever monitoring and tracking via GPS: case study for Fiji," *arXiv preprint: 1503.00814*, 2015.
[22] A. Hekmati, G. Ramachandran, and B. Krishnamachari, "CONTAIN: privacy-oriented contact tracing protocols for epidemics," in *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, Bordeaux, France: IEEE, 2021, pp. 872–877.
[23] R. F. Wykoff, "Contact tracing to identify human immunodeficiency virus infection in a rural community," *JAMA: The Journal of the American Medical Association*, vol. 259, no. 24, pp. 3563–3566, Jun. 1988, doi: 10.1001/jama.259.24.3563.
[24] M. L. Levine, "Contact tracing for HIV infection: a plea for privacy," *Columbia Human Rights Law Review*, vol. 20, no. 1, pp. 157–201, 1988.
[25] S. Bu-Pasha, A. Alén-Savikko, J. Mäkinen, R. Guinness, and P. Korpisaari, "EU law perspectives on location data privacy in smartphones and informed consent for transparency," *European Data Protection Law Review*, vol. 2, no. 3, pp. 312–323, 2016, doi: 10.21552/EDPL/2016/3/7.
[26] E. Vayena, J. Dzenowagis, J. S. Brownstein, and A. Sheikh, "Policy implications of big data in the health sector," *Bull World Health Organ*, vol. 96, no. 1, pp. 66–68, Dec. 2018, doi: 10.2471/BLT.17.197426.
[27] L. O. Gostin, S. F. Halabi, and K. Wilson, "Health data and privacy in the digital era," *JAMA*, vol. 320, no. 3, pp. 233–234, Jul. 2018, doi: 10.1001/jama.2018.8374.
[28] Ryerson University, "Privacy by design setting a new standard for privacy certification," *Deloitte*, pp. 1–12, 2016. Accessed: Jun. 19, 2020. [Online]. Available: https://www2.deloitte.com/ca/en/pages/risk/articles/Privacybydesign.html
[29] H. van Rossum, "Privacy enhancing Technologies: The Path to Anonymity," Den Haag, 1995.
[30] A. Cavoukian, "Privacy Protection Measures and Technologies in Business Organizations," in *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards*, G. O. M. Yee, Ed., Hershey, PA: IGI Global, 2012, pp. 170–208. doi: 10.4018/978-1-61350-501-4.
[31] C. Kurtz, M. Semmann, and T. Böhmann, "Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors," *Conference: Americas Conference on Information SystemsAt: New Orleans, Louisiana*, Jun. 2018.
[32] NearForm, "Bringing privacy by design to contact tracing apps," *NearForm*, 2020. https://www.nearform.com/blog/bringing-privacy-by-design-to-contact-tracing-apps/ (accessed Jun. 19, 2020).
[33] eHealth Network, "Mobile applications to support contact tracing in the Eu's fight against COVID-19: common EU toolbox for member states," EU, 2020. Accessed: Jun. 19, 2020. [Online]. Available: https://health.ec.europa.eu/system/files/2020-04/covid-19_apps_en_0.pdf
[34] European Commission, "Communication from the Commission: Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01," EUR-Lex, 2020. Accessed: Jun. 19, 2020 [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC0417%2808%29
[35] European Data Protection Board, "Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak," 2020. Accessed: Jun. 19, 2020. [Online]. Available: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en

[36] Centers for Disease Control and Prevention (U.S.), "Preliminary criteria for the evaluation of digital contact tracing tools for COVID-19 : preliminary criteria for the evaluation of digital contact tracing tools for COVID-19," *Centers for Disease Control and Prevention (CDC)*, 2020. https://stacks.cdc.gov/view/cdc/87515 (accessed Jun. 19, 2020).
[37] N. Lomas, "Norway pulls its coronavirus contacts-tracing app after privacy watchdog's warning," *TechCrunch*, 2020. https://techcrunch.com/2020/06/15/norway-pulls-its-coronavirus-contacts-tracing-app-after-privacy-watchdogs-warning/ (accessed Jun. 19, 2020).
[38] M. Liu, S. Zhou, Q. Jin, S. Nishimura, and A. Ogihara, "Effectiveness, policy, and user acceptance of COVID-19 contact tracing applications (CTAs) during the post-COVID-19 pandemic: An experience and comparative study (Preprint)," *JMIR Public Health Surveill*, vol. 8, Jun. 2022, doi: 10.2196/40233
[39] J. Spears and A. Padyab, "Privacy risk in contact tracing systems," *Behaviour & Information Technology*, vol. 42, pp. 1–22, Jun. 2021, doi: 10.1080/0144929X.2021.1901990
[40] Organisation for Economic Cooperation and Development (OECD), "Trust in government," *OECD*, 2019. https://data.oecd.org/gga/trust-in-government.htm?fbclid=IwAR1eGZbajb4L9MbRTAmpJR_TPHuM3aWHpTK7KGcIbLupzI_G1jUxJgL2IE8 (accessed Jun. 19, 2020).
[41] Saudi Press Agency, "SDAIA launches Tawakkalna App to facilitate the issuance of movement permits electronically during the curfew period," *SPA*, 2020. https://www.spa.gov.sa/viewfullstory.php?lang=en&newsid=2082059 (accessed Jun. 19, 2020).

BIOGRAPHIES OF AUTHORS

Zoran Jordanoski is a Senior Research Analyst at UNU-EGOV where he focuses on the digital transformation and emerging technologies within the public sector, eGovernment, and sustainable development, eGovernance planning and design, eGovernance monitoring and assessing incl. the UN EGDI, EU DESI, World Bank Ease of Doing Business and Transparency Internationals Corruption Perception benchmarks. He holds a PhD in International Law and an LL.M in International Law and International Relations, both from the University of Ss Cyril and Methodius in Skopje (North Macedonia). His work also includes regulatory and legal frameworks – or digitization-ready-legislation – to facilitate the digital transformation of the public sector service production and delivery ecosystems for improved productivity and service quality through the integrated administrative process and optimized personalized user-journeys and experiences. He can be contacted at email: jordanoski@unu.edu.

Luis Felipe M. Ramos is currently a Ph.D. student in Law at the University of Minho (Portugal). He holds a Master's degree in Law and Informatics from the University of Minho (Portugal) and an MBA from the Franciscana University (Brazil). He has also acted a Research Assistant at the United Nations University Operating Unity on Policy-Driven Electronic Governance (UNU-EGOV). His main research interests are in the areas of law and informatics, privacy and data protection, cybersecurity, emerging technologies, and intellectual property. He is currently focused on the legal framework regarding emerging technologies and their impact on personal data and privacy. He can be contacted at email: lfelipe.sm@gmail.com.

Moinul Zaber is the senior academic fellow at United Nations' University-EGOV, Portugal. Moinul is a computational social scientist and technology policy. He conducts research on artificial intelligence and machine learning for public policy, algorithmic and data ethics, usable privacy, data for public policy, ICT inclusion and data for urban design, network science, spectrum management policies, institutional challenges of telecommunications regulation and future of human-technology frontiers. He is currently on leave from University of Dhaka, Bangladesh and has worked at Tokyo University, Japan, Chalmers University, Sweden, LIRNEasia, Sri Lanka, Instituto Superior Tecnico, Portugal, Carnegie Mellon University, USA. He is a PhD, in engineering and public policy from Carnegie Mellon University, Pittsburgh, PA, USA. Dr. Moinul is well published and regularly gives invited talks at international and national governmental and nongovernmental conferences, forums and committees as an expert. He can be contacted at email: zaber@unu.edu.