Journal of Intercultural Management and Ethics

JIME

ISSN 2601 - 5749, ISSN-L 2601 - 5749

published by

Center for Socio-Economic Studies and Multiculturalism
Iasi, Romania
www.csesm.org

TABLE OF CONTENT

Editorial ……..……. 3
Liviu Warter

Ethics & Consciousness in Organizations: A Conceptual Hierarchical Model ……..…..5
Hershey H. Friedman, Kenneth A. Globerman

Ethical Challenges in Online Research.……...…….…….……. 17
Bianca Hanganu, Irina Smaranda Manoilescu, Beatrice Gabriela Ioan

Ethical Challenges of Digital Technologies in Covid-19 Pandemic Management.....25
Simina Petra Simion; Harald Jung

The Image of the Male and Female Doctors in the Covid-19 Pandemic. The First Pandemic with Woman Doctors in the Front Line ……..…….……..…39
Orsolya Horber, Karoly Zilahi

Why Nations Collapse: The Rise and Fall of The United States ……... 45
Hershey H. Friedman, Sarah Hertz

Egocentric Perceptions and Self-Serving Bias in Negotiations: Fairness, Dynamics, and Ethics ….…….…….……..……. 61
Oleg Komlik

ETHICAL CHALLENGES OF DIGITAL TECHNOLOGIES IN COVID-19 PANDEMIC MANAGEMENT

Simina Petra Simion MD[1*]; Harald Jung MD, PhD [1]
[1] Institute of Legal Medicine Târgu Mureș, Romania;
*Corresponding author, E-mail: simionsimina70@yahoo.ro

Abstract

The infectious disease caused by SARS-CoV-2 virus has spread rapidly worldwide, just 48 days after the first case appeared in China (January 30, 2020), becoming a major public health problem. 1/3 of the world's population has been forced into quarantine, the pandemic causing massive restrictions and consecutively substantial social, psychological and economic harms.

Researchers and experts have highlighted the benefits of various digital resources use, with the aim of collection, analysis and correlation of individual data as strategy in the management of the COVID-19 pandemic.

Digital surveillance is accompanied by legal and ethical risks and concerns, thus civil rights organizations and data protection authorities are highlighting the risk of intensified digital surveillance even after the pandemic situation. They emphasize the need to meet basic conditions (legality, proportionality of data processing) but also the need for social justice and equity that must not be overlooked in the urgency of this crisis.

The digital sources used in response to this pandemic include data from telephone towers, various mobile phone applications, Bluetooth connections, video surveillance, and more. We identified four main categories of digital technologies used to manage the pandemic: proximity and contact tracking, symptom monitoring, quarantine control, and individuals flow monitoring.

Although digital technology seems to demonstrate its importance in flattening the incidence curve of SARS-CoV-2 virus infection, notable technical limitations have also been emphasized, such as accuracy, data quality and last but not least the existence of risks related to cybersecurity.

Keywords: COVID-19, digital technology, civil rights

Background

The infectious disease caused by SARS-CoV-2 virus has spread rapidly worldwide, just 48 days after the first case appeared in China (January 30, 2020), becoming a major public health problem. 1/3 of the world's population has been forced into quarantine, the pandemic causing massive restrictions and consecutively substantial social, psychological and economic harms (Boulos & Geraghty, 2020; Klenk & Duijf, 2020; Sarbadhikari & Sarbadhikari, 2020).

Health organizations have responded to the pandemic by rapidly adopting digital solutions; digital technology can attenuate or even solve many challenges by improving control of the spread of the SARS-CoV-2 virus (Blake, Bermingham, Johnson, & Tabner, 2020; Golinelli et al., 2020; Kritikos, 2020). Researchers and experts have highlighted the benefits of various digital resources use, with the aim of collection, analysis and correlation of individual data as strategy in the management of the COVID-19 pandemic (Gasser, Ienca, Scheibner, Sleigh, & Vayena, 2020a; Ting, Carin, Dzau, & Wong, 2020).

Digital surveillance is accompanied by legal and ethical risks and concerns, thus civil rights organizations and data protection authorities are highlighting the risk of intensified digital surveillance even after the pandemic situation. In some countries, applications and other surveillance measures based on mobile phones are imposed on people, thereby violating the right to privacy (Ranisch et al., 2020a; Google. Privacy-Preserving Contact Tracing, 2020).

Although digital technology seems to demonstrate its importance in flattening the incidence curve of SARS-CoV-2 virus infection, notable technical limitations have also been emphasized, such as accuracy, data quality and last but not least the existence of risks related to cybersecurity (Gasser, Ienca, Scheibner, Sleigh, & Vayena, 2020b; Ranisch et al., 2020a; Google. Privacy-Preserving Contact Tracing, 2020; WHO, 2020). Therefore, it is essential to meet basic conditions (legality, proportionality of data processing) but also the need for social justice and equity that must not be overlooked in the urgency of this crisis (Gasser et al., 2020a; Gasser et al., 2020b).

Many countries have shown interest in digital contact tracking applications since March 2020 (Lucivero et al., 2020). The digital sources used in response to this pandemic include data from telephone towers, various mobile phone applications, Bluetooth connections, video surveillance, smart thermometers, websites used for assistance, web portals that provide useful information about COVID-19, electronic gadgets that can detect or scan typical COVID-19 symptoms (Gasser et al., 2020a; Gasser et al., 2020b; Islam, Islam, Munim, & Islam, 2020; WHO, 2020).

To check the spread of the virus, two of the biggest information technology companies (Apple and Google) are providing data concerning the virus spread all over the world (Google. Privacy-Preserving Contact Tracing, 2020). In addition, a number of new mobile phone applications have been launched or are under development. They have a wide variety of features: provide information about COVID-19, monitor quarantined people, track people's movements, or provide users with a quick warning about potential exposure to the SARS-CoV-2 virus (Gasser et al., 2020a; Gasser et al., 2020b; Ranisch et al., 2020a; Woodhams, 2020).

Even though mobile applications are successfully used in chronic diseases management, the COVID-19 pandemic has brought the need to create applications as a first-line solution to reduce the risk of contamination caused by contact with other infected people (Kondylakis et al., 2020).

Being well-known the fact that insecurity of citizens is more and more highlighted, and the uncertainty about the privacy of mobile applications used in the management of COVID-19 is growing, we consider it useful to perform an in-depth analysis of the digital technologies used to fight against SARS-CoV-2 virus.

We aim to illustrate how these applications work but also the risks related to possible misuse of these technologies (e.g. mass surveillance) after the end of the pandemic; we will analyze the need of digital security and need of legal regulations on the use of digital resources in the management of the COVID-19 pandemic.

The opportunity to use digital technologies to control the COVID-19 pandemic

Traditional contact tracking aims to isolate infected individuals and quarantine their contacts to stop the spread of the virus. This reduces the number of transmissions from both symptomatic persons and contacts, the impact on the population being minimized. For example, in 2003, the outbreak of SARS (China) was controlled by traditional contact tracking because transmission occurred mostly after the onset of symptoms (Klenk & Duijf, 2020; Yang et al., 2020).

Traditional methods are difficult to maintain given the epidemiological characteristics of the SARS-CoV-2 virus; various epidemiological studies revealing that nearly 47% of transmissions occur through contact with pre-symptomatic individuals (Klenk & Duijf, 2020; GSMA, 2020).

Digital technology usually involves the use of the Internet and smartphones. Although 4 billion people used the Internet worldwide in 2019, its use was disproportionate, higher in higher-income areas than in low- and middle-income areas (82% in Europe vs. 28% in Africa). Even in high-income countries, susceptible groups do not have access to smartphones (Whitelaw, Mamas, Topol, & Van Spall, 2020).

We identified four main categories of digital technologies used to manage the pandemic: proximity and contact tracking, symptom monitoring, quarantine control, and individual flow monitoring (Gasser et al., 2020a; Gasser et al., 2020b; WHO, 2020).

Available applications differ by: data used (self-reporting, geolocation data, proximity tracking), data source (GPS, Bluetooth), data management (centralized or decentralized architecture), data protection (anonymization / pseudo-anonymization) (Gasser et al., 2020a; Gasser et al., 2020b; Ranisch et al., 2020a; Woodhams, 2020).

Applications used in the COVID-19 pandemic management

1. Proximity and contact tracking

A large number of digital contact tracking applications have been implemented, launched and used worldwide. These are used to measure spatial proximity and interaction between users who have installed and kept the application active on their smartphone (Budd et al., 2020; Gasser et al., 2020b; GSMA, 2020).

Contact tracking is the process of managing people exposed to a disease (by identifying and evaluating them) and preventing the transmission of that disease. Contacts are recorded, stored and digitalized thus saving valuable time (Abuhammad, Khabour, & Alzoubi, 2020; Berman, Carter, García-Herranz, & Sekara, 2020; Budd et al., 2020; Klenk & Duijf, 2020; WHO, 2020). After the registration stage is completed, the contact tracking applications send notifications to the users if they have been near of a person confirmed as infected, and propose the next steps to be followed (Abuhammad et al., 2020; Berman et al., 2020; Ranisch et al., 2020a; GSMA, 2020).

It is an essential public health tool for fighting outbreaks of infectious diseases; the rate of infections is reduced and the impact on the economic level is much lower, compared to more restrictive approaches, such as lockdown (GSMA, 2020).

Proximity tracking, however, has its limitations, this technology cannot record all situations in which a user becomes infected and cannot replace tracking, testing or contact with positive people in the traditional way (Berman et al., 2020; Budd et al., 2020; WHO, 2020).

Digital proximity monitoring depends essentially on the absorption of the population but also on the adherence of users. For an application to make a significant contribution to pandemic management, a large part of the population needs access to digital technologies (smartphones) to install and configure that application, and they must be willing and able to follow the application's instructions correctly (Hinch et al., 2020; Johnson, 2020; Ranisch et al., 2020a; Ranisch et al., 2020b).

A study in the United Kingdom estimated that around 80% of smartphone users should use a contact tracking app to stop the pandemic, a rate comparable to WhatsApp / Facebook-Messenger users in some European countries. The highest rate of use of the contact tracking application has been recorded in Iceland, where approximately 40% of the total population has downloaded a contact tracking application. In Singapore, less than 15% of the population uses such an application. A lower utilization rate has anyway positive effects for

testing and quarantine (Hinch et al., 2020; Johnson, 2020; Ranisch et al., 2020a; Ranisch et al., 2020b).

This population adherence rate could be increased by forcing people to download and use the application; however, the mandatory use of applications would undermine public confidence. For this reason, applications based on voluntary use seem preferred, even if they require a strong public trust in applications and program (which can be built and sustained by a responsible design and appropriate policies). Meanwhile, reports from China have already shown that digital measures using pandemic responses have been used for mass surveillance and that there exist possibilities to massively expand the use of applications even after the pandemic (Ranisch et al., 2020a).

The utility of applications also depends to a large extent on the public health measures behind digital technology (Whitelaw et al., 2020). Although it is a clear advantage, user discipline is crucial (the speed with which they report for example the positive result of a PCR test) (Klenk & Duijf, 2020). To avoid false positive self-reports, health departments / other institutions should confirm the user's infected status (Whitelaw et al., 2020).

In some countries, such as Sweden or Netherlands, application launch have been delayed or even abandoned due to poor security data and doubts about the efficiency and legality of applications. Internationally, applications have already become the subject of conspiracy theories, fake news or scams (Ranisch et al., 2020a; Ranisch et al., 2020b).

Country	Application	Architecture	Data source	Privacy Policy	Data retention period	References
Austria	Stopp Corona	Decentralized	Bluetooth	YES	30 days	(Ciucci & Gouardères, 2020; Austrian Red Cross, 2020; Council of Europe, 2020)
Azerbaijan	Watch COVID	Decentralized	Bluetooth	YES	Does not mention	(Ministry of Economy of Azerbaijan Republic, 2020; Council of Europe, 2020)
Belgium	Coronalert	Decentralized	Bluetooth	YES	14 days	(RPM Brussels, 2020)
Bulgaria	Virusafe	Centralized	GPS	YES	As needed	(Ciucci & Gouardères, 2020; Council of Europe, 2020; Ministry of Health, Bulgaria, 2020)
Croatia	Stop COVID-19	Decentralized	Bluetooth	YES	14 days	(Council of Europe, 2020; Ministry of Health of the Republic of Croatia, 2020)
Cyprus	CovTracer	Decentralized	Bluetooth GPS	YES	1 year	(Ciucci & Gouardères, 2020; Council of Europe, 2020; RISE, 2020)
Czech Republic	eRouška	Centralized	Bluetooth	YES	180 days	(Ciucci & Gouardères, 2020; Council of Europe, 2020; Ministry of Health of the Czech Republic, 2020)
Denmark	Smittestop	Decentralized	Bluetooth	YES	14 days	(Ciucci & Gouardères, 2020; Council of Europe, 2020; Danish Ministry of Health, 2020)
France Monaco	TousAnti Covid	Centralized	Bluetooth	YES	Six months from the end of	(Ciucci & Gouardères, 2020; Council of

					the state of emergency	Europe, 2020; DGS, 2020)
Germany	Corona-Warn-App	Decentralized	Bluetooth	YES	21 days	(Council of Europe, 2020; German Federal Government, 2020)
Gibraltar	Beat Covid Gibraltar	Decentralized	Bluetooth	YES	14 days	(Council of Europe, 2020; HM Government of Gibraltar, 2020)
Hungary	VirusRadar	Centralized	Bluetooth	YES	30 days	(Ciucci & Gouardères, 2020; Council of Europe, 2020; National Center for Public Health, 2020)
Iceland	Rakning C-19	Centralized	GPS	YES	14 days	(Ciucci & Gouardères, 2020; Council of Europe, 2020; Directorate of Health, 2020)
India	Aarogya Setu	Centralized	Bluetooth GPS	YES	60 days	(Government of India, 2021)
Ireland	CovidTracker	Decentralized	Bluetooth	YES	14 days	(Council of Europe, 2020; Health Service Executive, 2020)
Italy	Immuni	Decentralized	Bluetooth	YES	Privacy Policy is not updated.	(Ciucci & Gouardères, 2020; Council of Europe, 2020; GitHub, 2020)
Latvia	Apturi Covid	Decentralized	Bluetooth	YES	14 days	(Council of Europe, 2020; Veselības ministrija un SPKC, 2020)
Morocco	Wiqaytna	Decentralized	Bluetooth	YES	21 days	(Council of Europe, 2020; Royaume du Maroc, 2020)
North Macedonia	Stop Koronal	Centralized	Bluetooth	YES	Does not mention	(Council of Europe, 2020; Ministry of Health, Republic of North Macedonia, 2021)
Poland	ProteGO Safe	Decentralized	Bluetooth	YES	As needed	(Ciucci & Gouardères, 2020; Council of Europe, 2020; Republic of Poland, 2020)
Switzerland	SwissCovid	Centralized	Bluetooth	YES	14 days	(Confederation Suisse, 2020; Council of Europe, 2020)
Tunisia	E7mi	Decentralized	Bluetooth	YES	14 days	(Council of Europe, 2020; Republique Tunisiene. Ministere de la Sante, 2020)
United Kingdom	NHS COVID-19 app	Decentralized	Bluetooth	YES	28 days	(Ciucci & Gouardères, 2020; Council of Europe, 2020; Government Digital Service, 2020)

Table 1. Proximity and contact tracking applications

System architecture type

One of the major problems of any contact tracking application is the preservation of the confidentiality and security of the data collected. Regarding data privacy and security, the type of architecture adopted for data collection is a mandatory topic to address. The applications used are divided into two large groups according to the communication protocols. In this regard, we will discuss centralized and decentralized approaches (Ciucci & Gouardères, 2020).

- Centralized approach

To understand the centralized architecture, we will briefly describe the registration process within these applications and the method of anonymous data processing after it is voluntarily uploaded to a so-called central server.

In order to access such applications, users must initially pre-register on a central server that will generate a "Temporary ID" that serves to preserve the privacy of each user; after completing the registration process, using Bluetooth signals, devices are exchanging these "Temporary IDs" when they are nearby, and if a user receives confirmation of a positive test, he can upload (on a voluntary basis) the collected anonymous data stored in his device on a central server, which is controlled by the government / national public health authority, and it will notify the relevant users of the risk of infection (Berman et al., 2020; GSMA, 2020).

It is highly significant to note that all entries are initially stored on the smartphone (locally), they are not automatically uploaded to the server (Ciucci & Gouardères, 2020). In this case, the risk score analysis is performed by the public health authorities, which are also responsible for the decision to inform / notify users (Berman et al., 2020; Ciucci & Gouardères, 2020). They can notify the users without accessing personal information, through digital solutions or by accessing personal information, by directly contacting people at risk (GSMA, 2020). They will further require certain actions from those who may have been exposed to the virus (Raskar et al., 2020).

Singapore was the pioneer of a Bluetooth technology called Bluetrace that underlies the TraceTogether application and uses the centralized approach (Table 1). TraceTogether uses Bluetooth connections to alert individuals who have been near a positive person (using notifications on mobile phones); if users have been in the vicinity of a positive person they are encouraged to isolate themselves (Gasser et al., 2020b; Goggin, 2020; Nadeem et al., 2020; Whitelaw et al., 2020; GSMA, 2020).

- Decentralized approach

In the case of the decentralized architecture, the main server has minimal implications in the process of tracking contacts. Users do not need to pre-register on the central server. Devices, in this case, will generate certain anonymous codes that will be used in combination with the exact time of the devices approach to generate pseudonyms that have a very short duration (less than 1 minute). These are periodically interchanged with other devices that are nearby (Berman et al., 2020; Ciucci & Gouardères, 2020).

If a user is positive, he can voluntarily upload the anonymous code and exposure moments. In this case, the central server functions as a meeting point, from where other users can download the data uploaded by those infected. The server cannot find identification details only with the help of the anonymous code / pseudonyms. Users could, however, figure out who the positive person was after the time and duration of the exposure, as they are the ones performing the risk analysis here (Ciucci & Gouardères, 2020; GSMA, 2020). Here, exposure notifications are processed directly on the individual's device (Ciucci & Gouardères, 2020). Thus, in a decentralized approach, the data of healthy users will not reach the central server (Raskar et al., 2020).

This analysis of possible architectures was performed to emphasize the importance of the public confidence factor. The difference between the two is not in the existence of the

central server, because both have one. The difference is, in fact, given by the location of the execution of various functionalities, such as the generation of unique identifiers and the risk score calculation (Ciucci & Gouardères, 2020).

Each architecture has integrated privacy protection, but the degree of protection differs considerably between the two types of architecture. In the case of centralized architecture, servers have access to all types of data, so if access to the server is compromised it would be possible to identify all users and their contacts, their privacy being endangered. In the decentralized architecture, existing information is fragmented into pieces and stored in different parts instead of being stored on a central server, so that no entity will have full control or will not be able to have complete information in the event of a problem, resulting in less information leakage than using a centralized architecture (Nadeem et al., 2020; Shubina, Holcer, Gould, & Lohan, 2020; GSMA, 2020).

In the issue, only the centralized versions allows "tracking of contacts" in the true sense of the word, individuals and contacts can be identified retrospectively by a "third party". The decentralized approach warns users in case of contact with an infected individual through a notification, but does not allow centralized tracking of the possible infectious chain. Both have a huge part to play in the digital management strategy during the Covid-19 pandemic (Ranisch et al., 2020a).

In Europe, following a joint attempt to establish a privacy-friendly approach to these applications, multiple countries have launched their own proximity tracking applications. Although the centralized approach was initially considered the most useful for these applications, massive criticism has led to a shift to a decentralized approach. Finally, the countries in Europe are divided, 14 countries choosing to manage data centrally (France) and 25 opting for the decentralized version (Germany, Austria, Belgium, Denmark, Italy, Ireland, Switzerland) (Ranisch et al., 2020a; Council of Europe, 2020).

Apple and Google have worked together to develop a common contact tracking framework that is also based on decentralized data architecture (Ranisch et al., 2020a; Google. Exposure Notifications, 2020).

2. Symptoms monitoring applications

These are syndromic surveillance tools that collect, analyze, interpret and disseminate data related to the health of the individual. Using these applications, the user reports the symptoms and obtain a diagnosis (Table 2), thus performing a so-called "triage" (Gasser et al., 2020b).

Country	Application	Function	References
Finland	Omaolo	Self-diagnosis COVID-19 informations	(Council of Europe, 2020; DigiFinland, 2021)
Mexico	COVID-19MX		(Council of Europe, 2020; Gobierno de la Ciudad de México, 2020)
Spain	CoronaMadrid app		(Comunidad de Madrid, 2020)
Tunisia	StopCorona		(Council of Europe, 2020; ONMNE Tunisie, 2020)
United Kingdom	COVID-19 Symptom Tracker	Self-diagnosis Requiring geographical location	(Council of Europe, 2020)
Uruguay	CoronavirusUY	Self-diagnosis	(Council of Europe, 2020)

Table 2. Symptoms monitoring applications

3. Quarantine control applications

The tools used to verify quarantine compliance are using the monitoring of symptomatic individuals as well as asymptomatic individuals, ensuring that they comply with quarantine restrictions. These applications are tracking the movements of quarantined people using a mobile phone (Gasser et al., 2020b). They have been developed to provide assistance to the police, who receive notifications if, for example, a quarantined person leaves the home (Taiwan's Electronic Fence app – StayHomeSafe, Hong Kong) (The Government of the Hong Kong Special Administrative Region, 2021).

The COVID-19 Smart application launched in United Arab Emirates (COVID-19 DXB Smart Application) provides general information about COVID-19 and tracks patients while being in quarantine or home isolation (Dubai Health Autority, 2020). Through the application, patients can receive support, consultations, or emergency response (Government of Dubai 2020a; Government of Dubai 2020b).

4. Individuals flow monitoring apps

These applications quantify, report and track people's movements in certain geographical regions. These Community Mobility Reports (Google's COVID-19 Community Mobility Reports) are based on aggregated, anonymized data sets from users' geographical location. Flow modulation can provide information on the effectiveness of response policies to combat COVID-19 (Gasser et al., 2020b). The reports describe trends in movement over time, depending on the geographical area, for different categories of locations (such as shops and recreation areas, grocery stores and pharmacies, parks, public transport stations, workplaces and housing) (Gasser et al., 2020b; Google, 2021).

5. Non-specific COVID-19 apps

Some countries are using non-specific COVID-19 applications. In Czech Republic, they are used to highlight outbreaks of COVID-19 in the form of dots on the map, and in Switzerland the Government relies on sending alerts (AlertSwiss) (Council of Europe, 2020).

Ethical and legal challenges retrieved in contact tracking applications

Decision makers (researchers, companies, government / non-governmental organizations) have the obligation to approach ethical and legal challenges and to manage the existing risks. Due to the unique circumstances of this pandemic situation, digital technologies have been launched rapidly, hence best practices for their implementation have not yet materialized (Gasser et al., 2020b).

Such uses of the data may threaten human rights and the right to liberty, both during and after the COVID-19 pandemic. It is necessary to impose strict limits on the use of digital proximity tracking. These technologies can only be effective in countries that have an efficient technological infrastructure and guarantees to ensure ethical use (WHO, 2020).

1. Ensuring public benefit

The ethical use of digital public health technology requires clear evidence that the benefits outweigh the risks. As possible benefits, we mention the anticipating of new outbreaks, the prompt alerting of individuals and the isolation of those exposed. All this in order to reduce or even prevent the spread of the virus and to improve quarantine measures (Gasser et al., 2020b).

In applications that use the centralized architecture, the data generated by the applications are analyzed in public health (public health authorities being the ones that calculate the risk score and send notifications to contacts); in this case, they must always

ensure that the risk analysis is carried out in a meaningful and cost-effective manner. For decentralized applications, however, additional efforts are needed, because the risk analysis is performed on the user's device and the data cannot be verified or tracked by health authorities. Therefore, all contact tracking applications require well-organized institutional efforts. For example, to avoid false positive self-reports, health departments / other institutions should have the ability to confirm the user's infected status (Whitelaw et al., 2020).

2. Ensuring scientific validation and accuracy. Testing and evaluation

The use of the new digital public health technology to combat or reduce the spread of the virus has enjoyed widespread enthusiasm, even though there are little scientific evidence of its effectiveness. The contact tracking applications were launched after several pilot studies, so there is no indicator of their accuracy (Gasser et al., 2020b).

We cannot allow the urgency of the current pandemic situation to be a justification for lowering scientific standards (Gasser et al., 2020b). Decision makers should ensure that a rigorous assessment of this technology is implemented so that its effectiveness can be continuously monitored; even if the use of digital tools improves the pandemic response compared to traditional contact tracking, the quality and integrity of the data is often questioned (Gasser et al., 2020b; WHO, 2020).

3. Protecting privacy. Data security

All digital public health tools can affect an individual's privacy by accessing information about the user's health or location. Privacy risks vary depending on the purpose and data used by digital tools. The increase of the risk of re-identification of an individual after the end of the pandemic is increased by the use of data as specific as possible (Gasser et al., 2020b).

The different ways of data storing in proximity and contact tracking applications have led to varying views on the confidentiality and security of the data collected. Both the centralized and the decentralized approach can maintain data confidentiality, but both have certain vulnerabilities, such as the security of the data collected. Data protection authorities consider that in the decentralized architecture the confidentiality is increased, because the user has control both over his/her own data and over the exercise / consent withdrawal. Within the centralized architecture, efforts should be made to make data collection, storage and processing as transparent as possible. Both approaches should limit data collection to what is strictly necessary to achieve the proposed objectives (WHO, 2020).

And finally, individuals must be provided with clear and easy-to-understand information about the purpose of data collection, how it will be stored and shared and last but not least, how long the data will be stored on the central server / in the application on the user's device (WHO, 2020).

4. Preserving autonomy. Voluntary agreement

A person's decision to download and use such an application must be voluntary and informed. The individual must be free to delete the application and the data that could be collected and stored (WHO, 2020). The government should not require the use of the application and individuals should not be denied rights (right to health care, right to receive financial assistance) if they refuse to use an application or refuse to comply with quarantine measures upon receipt of a notification (Abuhammad et al., 2020; Dubov & Shoptawb, 2020; WHO, 2020).

Data sharing based on consent is the most ethical approach to tracking contacts, thus mitigating privacy risks. However, the implementation of consent procedures should consider

language barriers or possible lack of understanding. In general, for an application to benefit from contact tracking, the user must share their location or activate their Bluetooth settings; even if the current pandemic situation is an emergency, the user should not be forced to share his personal information (Dubov & Shoptawb, 2020).

5. Avoiding discrimination (digital inequality)

These digital tools can be used to collect large amounts of data about an entire population; these data may include ethnic group, gender and socio-economic status. These demographic data are sensitive and are not necessarily related to the person's current state of health, which can lead to the stigmatization of certain social groups (Gasser et al., 2020b). Information such as racial demography could lead to increased discrimination (the increasing of attacks on individuals of South Asian origin during the COVID – 19 crisis) (Gasser et al., 2020b). Thus, it is essential that contact tracking approaches are implemented in a way that reduces people stigmatization. Asian Americans and people returning from cruise ships have already been subjected to pandemic harassment in the United States (Dubov & Shoptawb, 2020).

In other news, solutions based on digital technology that are centered on the use of the smartphones exclude the category of people without access to technology from a geographical, economic or demographic point of view. Even though digital technology is becoming more widespread globally, it is not evenly distributed. In 2019, 2/3 of the world's population did not have a smartphone and 1/3 did not have a mobile phone (Gasser et al., 2020b). In order to support the social category without access to appropriate technology to use these digital tools, additional funding could be considered (Dubov & Shoptawb, 2020). At regional level, lower prices for mobile subscriptions, upgrading of existing devices at lower prices, lending of free Wi-Fi hotspots could provide temporary solutions to these problems (Whitelaw et al., 2020; WHO, 2020). Even with limited access, the digital security of contacts will increase the security of the population (Dubov & Shoptawb, 2020).

We must consider that the category of population susceptible to infection with the Sars-Cov-2 virus (the elderly) could have a much lower degree of "literacy" in digital technology, thus requiring the development of a simplified digital technology or even the implementation of training programs to overcome this impediment (Gasser et al., 2020b; Whitelaw et al., 2020).

6. Data reuse

The use of data for legitimate purposes by public health departments does not eliminate the risk that these digital tools may be used in other forms of surveillance. It is crucial but sometimes impossible to distinguish digital technologies from public health departments that allow third parties to exchange information for non-health purposes from those that do not allow such activities (Gasser et al., 2020b). When data are used for research purposes, they should be aggregated and anonymized. The sale and use of data for commercial purposes / advertising activities should be strictly prohibited (WHO, 2020).

7. Setting an expiration date

Pandemics are a rare situation in which the Democratic Government can take unverified executive actions for the collective good. The measures taken must be temporary and used for a limited purpose, because in the long run they can deprive citizens of their rights, without any guarantee that they will be restored at the end of the crisis. Applications need to clarify from the beginning what kind of data they collect and how long they will have this information (Gasser et al., 2020b; WHO, 2020).

Conclusions

The COVID-19 pandemic situation continues to be a major problem affecting everyone's lifestyle. Although they do not currently play a vital role in pandemic management due to the low rate of population absorption, the new applications are useful for quickly identifying individuals who have been exposed to the virus.

Furthermore, for digital contact tracking to become a valuable component in the management of the COVID-19 pandemic, these tools must be strengthened, scientifically guaranteed and ethically strong to ensure the trust of the population.

The types of applications with a high degree of risk of surveillance or data collection after the end of the pandemic situation are the applications that are monitoring proximity and contacts. Within them, both centralized and decentralized architecture have benefits that make difficult to choose one as “the best approach”. From an ethical and legal point of view, the decentralized architecture would be "the winner", but if we refer to the public benefit in the current pandemic situation (information entered by users in the applications – such as a positive result at a PCR test), then the most useful way would be the centralized architecture, because here public health authorities can retrospectively verify this information, they being the ones who perform the analysis of the risk score.

Given the ethical issues identified, we consider our current review might be useful in drafting legal regulations on digital resources in the management of the COVID-19 pandemic together with strengthen of technologies privacy and cybersecurity.

References

Abuhammad, S., Khabour, OF., & Alzoubi, KH. (2020). Covid-19 Contact-Tracing technology: Acceptability and ethical issues of use. *Patient preference and adherence*, 14, 1639–1647. https://doi.org/10.2147/PPA.S276183

Austrian Red Cross. (2020). *Stopp Corona app*. https://www.stopp-corona.at/

Berman, G., Carter, K., García-Herranz, M. and Sekara, V. (2020). *Digital contact tracing and surveillance during Covid-19.* https://www.unicef.org/mena/sites/unicef.org.mena/files/2020-06/WP2020-01.pdf

Blake, H., Bermingham, F., Johnson, G., & Tabner, A. (2020). Mitigating the psychological impact of Covid-19 on healthcare workers: A digital learning package. *Int. J. Environ Res. Public Health*, 17(9), 2997. doi: 10.3390/ijerph17092997

Boulos, MNK., & Geraghty, EM. (2020). Geographical tracking and mapping of coronavirus disease Covid-19/severe acute respiratory syndrome coronavirus 2 (Sars-CoV-2) epidemic and associated events around the world: how 21st century GIS technologies are supporting the global fight against outbreaks and epidemics. *Int J Health Geogr*, 19 (8). doi: 10.1186/s12942-020-00202-8

Budd, J., Miller, B.S., Manning, E.M., Lampos, V., Zhuang, M., Edelstein, … McKendry, RA. (2020). Digital technologies in the public-health response to COVID-19. *Nat Med* 26, 1183–1192. https://doi.org/10.1038/s41591-020-1011-4

Ciucci, M., & Gouardères, F. (2020). National Covid-19 contact tracing apps. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652711/IPOL_BRI(2020)652711_EN.pdf

Comunidad de Madrid. (2020). *Take your COVID-19 self – assessment.* https://coronavirus.comunidad.madrid/

Confederation Suisse. (2020). *Coronavirus: SwissCovid App and contact tracing*. https://www.bag.admin.ch/bag/de/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/swisscovid-app-und-contact-tracing.html#-728718249

Council of Europe. (2020). *Digital solutions to fight Covid-19*. https://rm.coe.int/report-dp-2020-en/16809fe49c

Danish Ministry of Health, Danish Patient Safety Authority, Danish Health Authority, Danish Agency for Digitisation and Netcompany. (2020). *Processing your personal data*. https://erouska.cz/en/podminky-pouzivani

DigiFinland. (2021). *About Omaolo*. https://www.omaolo.fi/palvelut/oirearviot

DGS du ministère des solidarités et de la santé. (2020). *Données personnelles, application "TousAntiCovid"*. https://bonjour.tousanticovid.gouv.fr/privacy.html

Directorate of Health, Department of Civil Protection and Emergency Management. (2020). *Covid-19 tracing app privacy policy*. https://www.covid.is/app/privacystatement

Dubai Health Autority. (2020). *Covid-19 DXB smart application*. https://www.dha.gov.ae/en/pages/dhahome.aspx

Dubov, A., & Shoptawb, S. (2020). The Value and Ethics of Using Technology to Contain the COVID-19 Epidemic. *The American Journal of Bioethics*, 20 (7), W7-W11. https://doi.org/10.1080/15265161.2020.1764136

Gasser, U., Ienca, M., Scheibner, J., Sleigh, J., & Vayena, E. (2020a). Digital tools against COVID-19: Framing the ethical challenges and how to address them. *ArXiv*. https://arxiv.org/abs/2004.10236

Gasser, U., Ienca, M., Scheibner, J., Sleigh, J., & Vayena, E. (2020b). Digital tools against Covid-19: taxonomy, ethical challenges, and navigation aid. *Lancet Digital Health*, 2, 425–434. https://doi.org/10.1016/S2589-7500(20)30137-0

German Federal Government. (2020). *Privacy notice*. https://www.coronawarn.app/assets/documents/cwa-privacy-notice-en.pdf

GitHub, Inc. (2020). *Immuni's high-level description*. https://github.com/immuni-app/immuni-documentation#privacy

Gobierno de la Ciudad de México. (2020). *Aviso de privacidad simplificado sistema de datos personales del sistema de registro de información de locatel de la agencia digital de innovación pública de la Ciudad de México*. https://app.covid19.cdmx.gob.mx/signup

Goggin, G. (2020). Covid-19 apps in Singapore and Australia: reimagining healthy nations with digital technology. Media International Australia, 177(1), 61–75. https://doi.org/10.1177/1329878X20949770

Golinelli, D., Boetto, E., Carullo, G., Nuzzolese, AG., Landini, MP., & Fantini, MP. (2020). Adoption of Digital Technologies in Health Care During the COVID-19 Pandemic: Systematic Review of Early Scientific Literature. *J Med Internet Res*, 22(11), e22280. doi:10.2196/22280

Google. (2021). *Community mobility reports*. https://www.google.com/covid19/mobility/

Google. (2020). *Exposure Notifications: Using technology to help public health authorities fight COVID-19*. https://www.google.com/covid19/exposurenotifications/

Google. (2020). *Privacy-Preserving Contact Tracing*. https://covid19.apple.com/contacttracing

Government Digital Service. (2020). *Guidance NHS Covid-19 app: privacy notice*. https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-test-and-trace-app-early-adopter-trial-august-2020-privacy-notice

Government of Dubai. (2020a). *Home isolation and quarantine guidelines during coronavirus (Covid-19) pandemic*. https://www.dha.gov.ae/en/HealthRegulation/Documents/Guidelines%20for%20Home%20Isolation%20and%20Quarantine%20for%20COVID-19%20Pandemic.pdf

Government of Dubai. (2020b). *Covid-19 patient pathway*. https://www.dha.gov.ae/en/HealthRegulation/Documents/Attachment%202.pdf

Government of India. (2021). *Aarogya Setu mobile app*. https://www.mygov.in/aarogya-Setu-app/

GSMA. (2020). *Covid-19 digital contact tracing applications*. https://www.gsma.com/newsroom/resources/covid-19-digital-contact-tracing-applications/

HM Government of Gibraltar. (2020). *Beat Covid Gibraltar, privacy notice*. https://www.gibraltar.gov.gi/beatcovidapp/privacy

Health Service Executive. (2020). *Privacy and how we use your data, Covid tracker app*. https://www2.hse.ie/conditions/coronavirus/covid-tracker-app/privacy-and-how-we-use-your-data.html

Hinch, R., Probert, W., Nurtay, A., Kendall, M., Wymant, C., Hall, M., & Fraser C. (2020). Report—Efective configurations of a digital contact tracing app: a report NHSX. https://cdn.theconversation.com/static_files/files/1009/Report_-_Effective_App_Configurations.pdf?1587531217

Islam, MN., Islam, I., Munim, KM., & Islam AKMN. (2020). A review on the mobile applications developed for Covid-19: an exploratory analysis. *IEEE Access*, 8, 145601-145610. doi: 10.1109/ACCESS.2020.3015102

Johnson, B. (2020). Nearly 40% of Icelanders are using a Covid app— and it hasn't helped much. *MIT Tech Review*. https://www.technologyreview.com/2020/05/11/1001541/iceland-rakning-c19-covid-contact-tracing/

Klenk, M., & Duijf, H. (2020). Ethics of digital contact tracing and Covid-19: who is (not) free to go?. *Ethics Inf Technol*, 1-9. doi:10.1007/s10676-020-09544-0

Kondylakis, H., Katehakis, DG., Kouroubali, A., Logothetidis, F., Triantafyllidis, A., Kalamaras, I., Votis, K., & Tzovaras, D. (2020). COVID-19 Mobile apps: a systematic review of the literature. *Journal of medical Internet research*, 22(12), e23170. doi: 10.2196/23170

Kritikos M. (2020). *Ten technologies to fight coronavirus.* https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/641543/EPRS_IDA(2020)641543_EN.pdf

Lucivero, F., Hallowell, N., Johnson, S., Prainsack, B., Samuel, G., & Sharon, T. (2020). Covid-19 and contact tracing apps: ethical challenges for a social experiment on a global scale. *Journal of Bioethical Inquiry*, 17, 835-839. https://doi.org/10.1007/s11673-020-10016-9

Ministry of Health, Republic of North Macedonia. (2021). *StopKorona! privacy precautions*. https://stop.koronavirus.gov.mk/privacy-policy/en

Ministry of Health of the Czech Republic. (2020). *eRouska terms and conditions*. Terms and conditions – eRouška (erouska.cz)

Ministry of Economy of Azerbaijan Republic. (2020). *Covid izle Privacy Policy*. https://sites.google.com/view/covidizle-privacy/home

Ministry of Health, Bulgaria. (2020). *Virusafe Privacy Policy*. https://virusafe.io/information/privacy-policy.html

Ministry of Health of the Republic of Croatia. (2020). *Purpose and operation of Stop COVID-19 ("Application")*. https://stopcovid19.zdravlje.hr/html/pravila-privatnosti.html

Nadeem, A., Regio, M., Wanli, X., Sushmita, R., Robert, M., Salil, … Sanjay, J. (2020). A survey of Covid-19 contact tracing apps. *IEEE Access*, 8, 134577 - 134601. doi: 10.1109/ACCESS.2020.3010226

National Center for Public Health. (2020). *VirusRadar, privacy policy*. https://virusradar.hu/privacy-policy

ONMNE Tunisie. (2020). *About StopCorona*. https://www.stopcorona.gov.tn/

Ranisch, R., Nijsingh, N., Ballantyne, A., Van Bergen, A., Buyx, A., Friedrich, O., … Wild, V. (2020a). Digital contact tracing and exposure notification: ethical guidance for

trustworthy pandemic management. *Ethics Inf Technol*. https://doi.org/10.1007/s10676-020-09566-8

Ranisch, R., Nijsingh, N., Ballantyne, A., Buyx, A., Friedrich, O., Hendl, ... Wild, V. (2020b). Ethics of digital contact tracing apps for the Covid-19 pandemic response. *Kompetenznetz Public Health COVID-19*. doi: 10.13140/RG.2.2.23149.00485

Raskar, R., Nadeau, G., Werner, J., Barbar, R., Mehra, A., Harp, G., Louisy, K. (2020). *Covid-19 contact-tracing mobile apps: evaluation and assessment for decision makers*. https://arxiv.org/abs/2006.05812

Republic of Poland. (2020). *About ProteGO Safe*. https://www.gov.pl/web/koronawirus/protegosafe

Republique Tunisiene. Ministere de la Sante. (2020). *E7mi*. https://e7mi.tn/index_fr.html

RISE Ltd. (2020). *CovTracer privacy policy*. https://covid-19.rise.org.cy/RISE_CovTracer_Privacy_Policy_EN.pdf

Royaume du Maroc. Ministere de la Sante. (2020). *Wiqaytna*. https://www.wiqaytna.ma/Default_Fr.aspx

RPM Brussels. (2020). *Coronalert 2020 privacy and data*. https://coronalert.be/en/privacy-and-data/

Sarbadhikari S, & Sarbadhikari SN. (2020). The global experience of digital health interventions in Covid-19 management. *Indian J Public Health*, 64, S117-24. , doi: 10.4103/ijph.IJPH_457_20

Shubina, V., Holcer, S., Gould, M., & Lohan, E. S. (2020). Survey of decentralized solutions with mobile devices for user location tracking, proximity detection, and contact tracing in the Covid-19 era. *Data*, 5(4), 87. https://doi.org/10.3390/data5040087

The Government of the Hong Kong Special Administrative Region. (2021). *"StayHomeSafe" mobile app user guide*. https://www.coronavirus.gov.hk/eng/stay-home-safe.html

Ting, D., Carin, L., Dzau, V., & Wong, TY. (2020). Digital technology and Covid-19. *Nature Medicine*, 26(4), 459-461. https://doi.org/10.1038/s41591-020-0824-5

Veselības ministrija un SPKC. (2020). *Apturi Covid Lietotnes Privātuma politika*. https://apturicovid.lv/privatuma-politika/

Whitelaw, S., Mamas, MA., Topol, E., & Van Spall, HGC. (2020). Applications of digital technology in Covid-19 pandemic planning and response. *Lancet Digital Health*, 2, e435–440. https://doi.org/10.1016/S2589-7500(20)30142-4

WHO. (2020). *Ethical considerations to guide the use of digital proximity tracking technologies for Covid-19 contact tracing: Interim guidance*. https://apps.who.int/iris/handle/10665/332200

Woodhams, S. (2020). Covid-19 digital rights tracker. https://www.top10vpn.com/news/surveillance/covid-19-digital-rights-tracker/

Yang, Y, Peng, F., Wang, R., Guan, K., Jiang, T., Xu, G., Sun, J., & Chang, C. (2020). The deadly coronaviruses: the 2003 SARS pandemic and the 2020 novel coronavirus epidemic in China. *Journal of Autoimmunity*, 109, 102434. https://doi.org/10.1016/j.jaut.2020.102434