https://doi.org/10.48417/technolang.2023.02.10
Research article

Tracing the Tracing Apps: A Technical Response to Covid in Cultural Comparison

Nikita Kesarev and Andrey Korochkin (✉)
Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Polytechnicheskaya, 29, 195251, Russia
kesarev.nr@edu.spbstu.ru; awesome.corochkin@yandex.ru

Abstract

The paper is concerned with studying the tracking apps developed and employed by governments to control the Covid 19 pandemic. Such apps have been implemented by almost all states in the world, however, with different mechanisms. In the present study, three groups of apps are identified, according to their level of control and surveillance (low, medium, high). Apparently, a higher degree of control, as well as the obligation to install them, should correspond to greater efficiency, but it also coincides with greater risk of exposing users' personal data. As much as this assumption tends to be correct, for determining the efficiency or inefficiency of tracking apps, other factors needs to be analyzed. This might be socio-political in nature, such as the public's trust in the actions of governments, or technical, i.e., concerning the actual performativity of such devices. The article also highlights the question of how the use of technology can affect our understanding of freedom and personal responsibility. The international comparison shows, overall, that there are no universals but many cultural determinants. In particular, there is no universal fear of data security that could explain a certain technological design. The study of alternative Covid-tracking applications allows us to see the confluence of ideological, philosophical and technical concepts in the modern world. Their evaluation cannot proceed in isolation from cultural dynamics and value orientations.

Keywords: Corona pandemic; Tracing Apps; Privacy; Trust; Responsibility; Efficiency and performativity; Intercultural comparison of technologies

Acknowledgment We like to thank Daria Bylieva and Andrea Gentili for supporting the writing process.

Citation: Kesarev, N., & Korochkin, A. (2023). Tracing the Tracing Apps: A Technical Response to Covid in Cultural Comparison. *Technology and Language, 4*(2), 97-115. https://doi.org/10.48417/technolang.2023.02.10

УДК 316.72+004
https://doi.org/10.48417/technolang.2023.02.10
Научная статья

Отслеживая приложений для отслеживания: Технический ответ на Covid в культурном сравнении

Никита Романович Кесарев и Андрей Романович Корочкин (✉)
Санкт-Петербургский политехнический университет Петра Великого, ул. Политехническая, д. 29, Санкт-Петербург, 195251, Россия
kesarev.nr@edu.spbstu.ru; awesome.corochkin@yandex.ru

Аннотация
Статья посвящена изучению приложений для отслеживания, разработанных и используемых правительствами для борьбы с пандемией Covid 19. Такие приложения были внедрены почти во всех государствах мира, однако с использованием различных механизмов. В настоящем исследовании определены три группы приложений в соответствии с их уровнем контроля и слежки (низкий, средний, высокий). По-видимому, более высокая степень контроля, а также обязанность по их установке должны соответствовать большей эффективности, но это также совпадает с большим риском раскрытия персональных данных пользователей. Несмотря на то, что это предположение, как правило, верно, для определения эффективности или неэффективности приложений отслеживания необходимо проанализировать другие факторы, социально-политического характера, такие как доверие общественности к действиям правительств, или технические, то есть касающийся реальной производительности таких устройств. В статье также освещается вопрос о том, как использование технологий может повлиять на наше понимание свободы и личной ответственности. Международное сравнение показывает, в целом, что нет универсалий, но много культурных детерминант. Изучение альтернативных приложений Covid-трекинга позволяет увидеть слияние идеологических, философских и технических концепций в современном мире. Их оценка не может происходить в отрыве от культурной динамики и ценностных ориентаций.

Ключевые слова: Пандемия коронавируса; Мобильные приложения; Конфиденциальность; Доверие; Ответственность; Эффективность и производительность; Межкультурное сравнение технологий

Благодарность: Хотим поблагодарить Дарью Сергеевну Быльеву и Андреа Джентили за помощь в процессе написания статья.

Для цитирования: Kesarev, N., & Korochkin, A. Tracing the Tracing Apps: A Technical Response to Covid in Cultural Comparison // Technology and Language. 2023. № 4(2). P. 97-115. https://doi.org/10.48417/technolang.2023.02.10

INTRODUCTION

In 2019, a new strain of coronavirus emerged, producing the disease called Covid 19. It became a serious problem that led to great losses and thousands of human casualties. Digital technologies played a significant role in solving the problem of maintaining social interactions during the period of forced isolation, allowing people to work, learn, and entertain themselves without leaving their homes. However, digital technologies were also called upon to directly combat the spread of infection. Due to the universal increase in digital literacy and the popularization of the market for mobile applications aimed at limiting the spread of the virus, such applications as StopCovid, Social Monitoring, TraceTogether, and many others have emerged.

The specific design of the applications that were created to track contacts in order to combat the spread of the coronavirus reflects certain cultural and philosophical characteristics of the countries that were using them. The national specificity was vividly reflected in the development of technologies to combat the coronavirus, which took place under conditions requiring maximum speed and efficiency. As early as the mid-20th century, Lewis Mumford (1964) noted: “from late neolithic times in the Near East, right down to our own day, two technologies have recurrently existed side by side: one authoritarian, the other democratic, the first system-centered, immensely powerful, but inherently unstable, the other man-centered, relatively weak, but resourceful and durable” (p. 2). Here the philosopher opposes different technologies that have not just different, but opposite goals. In our case, the goal of the technologies under consideration is the same, but employ different ways of implementation, which are manifested in technological solutions and then affect the organization of people, social and technical systems. As Langdon Winner (1998) wrote, “The things we call 'technologies' are ways of building order in our world” (p. 29). Usually, the influence of technologies on social life has long-term and difficult to trace consequences: “Consciously or unconsciously, deliberately or inadvertently, societies choose structures for technologies that influence how people are going to work, communicate, travel, consume, and so forth over a very long time” (p. 29). In the case of applications designed to combat the spread of the coronavirus, their impact on society and effectiveness can be assessed relatively quickly. In addition to asserting that artifacts have politics, Winner was referring to general ideas of governance, whereas modern digital technologies can be a tool of control and management in the most direct and immediate sense.

METHODS

The method of research is the analysis of 73 different applications. The majority of them are so-called tracing apps: applications that track user contacts or the whereabouts of infected persons. Applications from the Czech Republic, Poland, India, Australia, Russia, China, Germany, the United States, Taiwan, and other countries were considered (see Appendix 1). For the study, both the application itself and the data offered by the creators were used, as well as ratings and descriptions of users, media materials and papers dedicated to applications.

All software products listed in the article were created with the participation of the state. The control factor may reflect both the characteristics of the epidemiological situation and certain cultural characteristics of the inhabitants of a particular region. As a result, the most important factor from a philosophical point of view is the level of control over the user.

RESULTS

Levels of Control

The study identified three general levels of control: low, medium, and high. Applications with low control levels were most characteristic of European countries and Australia. The majority of these apps only required Bluetooth protocols to detect nearby devices within a radius of up to 50 meters and establish temporary connections for encrypted data exchange and a phone number to receive notifications of possible infection.

The functionality of such apps was limited to notifying users of their contact with a possible or confirmed carrier of the virus. These apps received many downloads in various app stores (for example, the Czech app eRouška had over 1.7 million downloads, and the Polish app ProteGOSafe had around 1.5 million) because they were easy to use and low-risk with minimal device load. Apps that tracked user contacts were collectively referred to as "tracing apps."

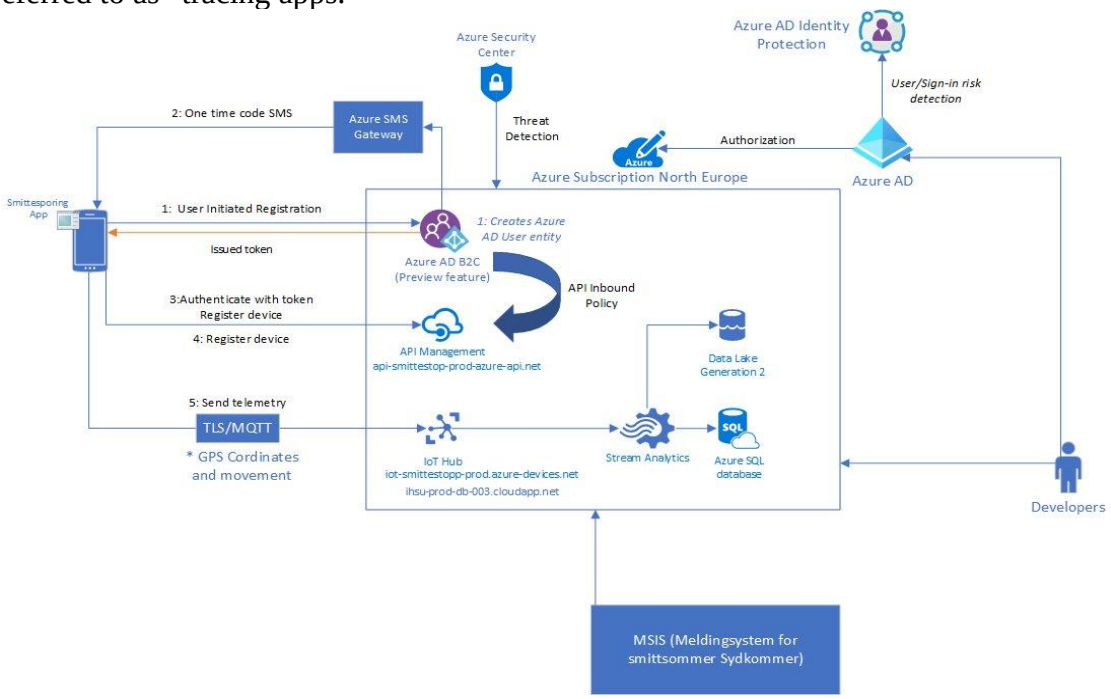

Figure 1. Information Circulation Scheme (Smittestop, 2020).

It is worth noting that about half of the tracing apps operated for no more than a year. Technical issues were a common reason for app closure. For example, the Norwegian app Smittestop was disabled under public pressure after it became known that the app had certain problems with user data protection.

As Marius Sandbu (2020) writes in his article "Technical Analysis of Smittestop backend Azure," the application does not have any backend protection, which allows an attacker to access the user database in real time, the data in this database is also not securely encrypted, therefore an attacker will be able to use the stolen data for selfish purposes. In addition, the application operates on Azure data centers located in Ireland, which makes the data even more vulnerable (Fig. 1).

All these problematic features show not so much the incompetence of the development team itself, as the insufficiently attentive attitude of the government, which was the customer and sponsor of the project. It failed to adequately respect the personal data of citizens who were at risk of theft by third parties as a result of negligence. Getting any personal data (phone number, geolocation, passport data) at the disposal of an attacker can lead to damage to the data holder – from disclosure of his place of residence, to fraud using his phone number, even obtaining a microloan in his name.

Therefore, the Institute of Public Health issued an official apology and soon the application stopped working. However, this case is an exception rather than something ordinary. An example of society's reaction to manipulation of citizens' data is the situation in the United States. In 2019, the American Pew Research Center conducted a survey in which more than 4000 people participated. The purpose of the study was to find out how much Americans were aware of the fact that they are being watched and how they protect their personal information on the Internet. The survey results showed that 8 out of 10 Americans (about 3,200 out of 4,000 respondents) believe that they cannot escape surveillance by the government or private companies. In addition, almost all respondents stated that they had at least once in their lives received advertising that was directed to them based on their Internet search queries or other actions on the network, which confirms the fact of a third-party usage of the user's personal data (search query history) (Auxier, & Rainie, 2019). This is due to the fact that in the modern world more and more information about us is collected and stored on the Internet, as well as with the development of technologies that allow us to track our online activities. However, only 28% of respondents said they were taking any steps to protect their personal information online (Business FM, 2020). This may be because many people do not know how to protect their privacy online, or do not consider this problem important enough. A study by Douglas Leith and Stephen Farrell indicates that apps consist of two separate components: a "client" app managed by the national public health authority and the Google/Apple Exposure Notification (GAEN) service, that on Android devices is managed by Google and is part of Google Play Services. And if in most cases the client does not cause any particular complaints from the point of view of confidentiality (although the privacy of the Irish, Polish, Danish and Latvian apps could be improved), the part related to Google Play Services raises a number of questions. It contacts Google servers roughly every 20 minutes, potentially allowing location tracking via IP address. In addition, the phone IMEI, hardware serial number, SIM serial number and IMSI,

handset phone number etc are shared with Google, together with detailed data on phone activity. This data collection is enabled simply by enabling Google Play Services, even when all other Google services and settings are disabled, and so is unavoidable for users of GAEN-based contact tracing apps on Android (Leith & Farrell, 2021).

Another major problem with tracing apps is the lack of user responsibility. The most affected by this factor was the COVIDsafe application, developed under the leadership of the Australian government. For example, a resident of Australia was quoted as saying, "(the installation of the application) is voluntary, and I decided that I can do without the application for now. It can be put under an anonymous login, but if contact is suddenly recorded for more than 15 minutes with the carrier of the virus, the data is found through the medical system, and doctors contact the person by phone number to inform him that it makes sense to isolate and do a test for coronavirus" (BusinessFM, 2020). From this one can infer that the "doctors" perform the function of push or SMS notification, but no more. The recipient of such notification still reserves the right to completely ignore it and does not bear any responsibility for such an act. "They explained that Amazon will be responsible for storing application data, and everyone is afraid of leaks. I heard that about 5 million people have installed the application – out of 25 million people, that is, every fifth" (BusinessFM, 2020). Despite the absence of any data on the reliability of the private information protection system, as well as due to the lack of obligation to use the application, most of the people who installed it did not use its functionality. Accordingly, this application detected only 2 cases of infection and was closed due to inefficiency.

A logical conclusion from the experience of using applications with a low level of control was the need to increase the latter in combination with the most thorough study of all aspects of the application concerning users' personal data, especially the protection of personal data.

Lucie White and Philippe van Basshuysen argue that the efficiency of applications would be greater if some pseudonymized data were stored on a central server, and not only on users' smartphones, which privacy advocates have cautioned against (White & Basshuysen, 2021). At the same time, data on the central server can be stored using identification numbers, and not user data. The general information on the server allows you to monitor the infection situation as a whole, improving the quality of data. In practice, centralized systems have not been fully implemented. Attempts made in the UK and Australia were unsuccessful, as they could not identify contacts with sufficient accuracy due to the difficulty of designing a functional app on Android and iPhones without the support of Apple and Google (who only support decentralised app architectures).

The next level of control that we have identified is the average level. In it, as we found out, there is supposed to be an exchange data between several devices, including their transfer them to some third party which is a state structure in one form or another. Personal data is transmitted only to a limited extent, or is not distributed. The use of the application is voluntary. Compared to a low level of control, it is worth noting that at a low level the information requested was no more than a phone number, even location data was not required, unlike in the average level.

After analyzing all the characteristics of the applications, we have identified the main difference from low control. This main difference is a slight deviation from strict confidentiality. For example, the Ito (Germany) application worked as follows: If a person had a positive test result, he or she received a code from the Department of Health, which one can enter in the application. Then the pseudonymous ID of the person is uploaded along with the confirmation of a positive test. All users regularly download the latest information for local data comparison on their devices. When the device of a person who has been in contact with an infected person recognizes this pseudonymous identifier, the person will be informed – without revealing the actual identity. Another example is the Covid Shield app of Sri Lanka where a mobile app runs in the background to collect random IDs and exchanges them with nearby phones with Covid Shield installed. It periodically downloads common random identifiers from the server and compares them on each user's device to determine if a possible infection has occurred. If we briefly analyze these two applications, we can conclude that the Ito application (Germany) collects information specifically about the user, as opposed to low-level applications that collect information such as phone number, address, etc. And Covid Shield (Sri Lanka) is based on impact notification technologies provided by Apple and Google, which is currently the most secure approach to maintaining privacy. Thus, we can draw a general conclusion that these applications are fairly vivid examples of clear difference from the low level.

However, in some states, applications directly invaded the privacy of users. Such applications have been identified by us as applications with a high level of control. It should be noted that the more information the application receives about the user, the wider its functionality can be. However, the requirements for the application increase proportionally. Four software products will be considered as examples of applications with a high level of user control: Chinese “AliPayHeathCode,” Singapore “TraceTogether,” Russian “Social Monitoring.” Examples will be considered in ascending order of control.

The TraceTogether app, released on March 20, 2020 and still functioning to this day, requires the user's geolocation, phone number, and passport data to work. It is precisely the latter that sets TraceTogether apart from lower-level apps – it literally gets a copy of the user's identity document, which expands the capabilities of the application. For example, TraceTogether can call an ambulance to the user's location, which will be informed in advance about the user's condition, show the location of the nearest medical centers and blood transfusion points suitable for the user. Despite the daunting requirements and lack of any responsibility for not using the app, Singapore's population continues to use it according to official statistics provided on the Singapore government website (Singapore Government, n.d.). This reflects the philosophy promoted through this application. The headline on the application's homepage reads: “Trace Together, Safe together,” which reflects the main aspect of the application – massiveness. Naturally, the more people conscientiously monitor their contacts, the more effective the application will be.

The effectiveness of the application depends not only on the number of installations but also on the degree of trust users have in it. The number of active TraceTogether users

(90% of the country's population, which is about 5,000,000 people) shows a high level of trust in the government, as well as a high level of personal responsibility and a sense of involvement in such a large-scale project. Therefore, based on the fact that citizens are extremely loyal to government actions, to achieve mass usage the application need not be mandatory but only recommended for use.

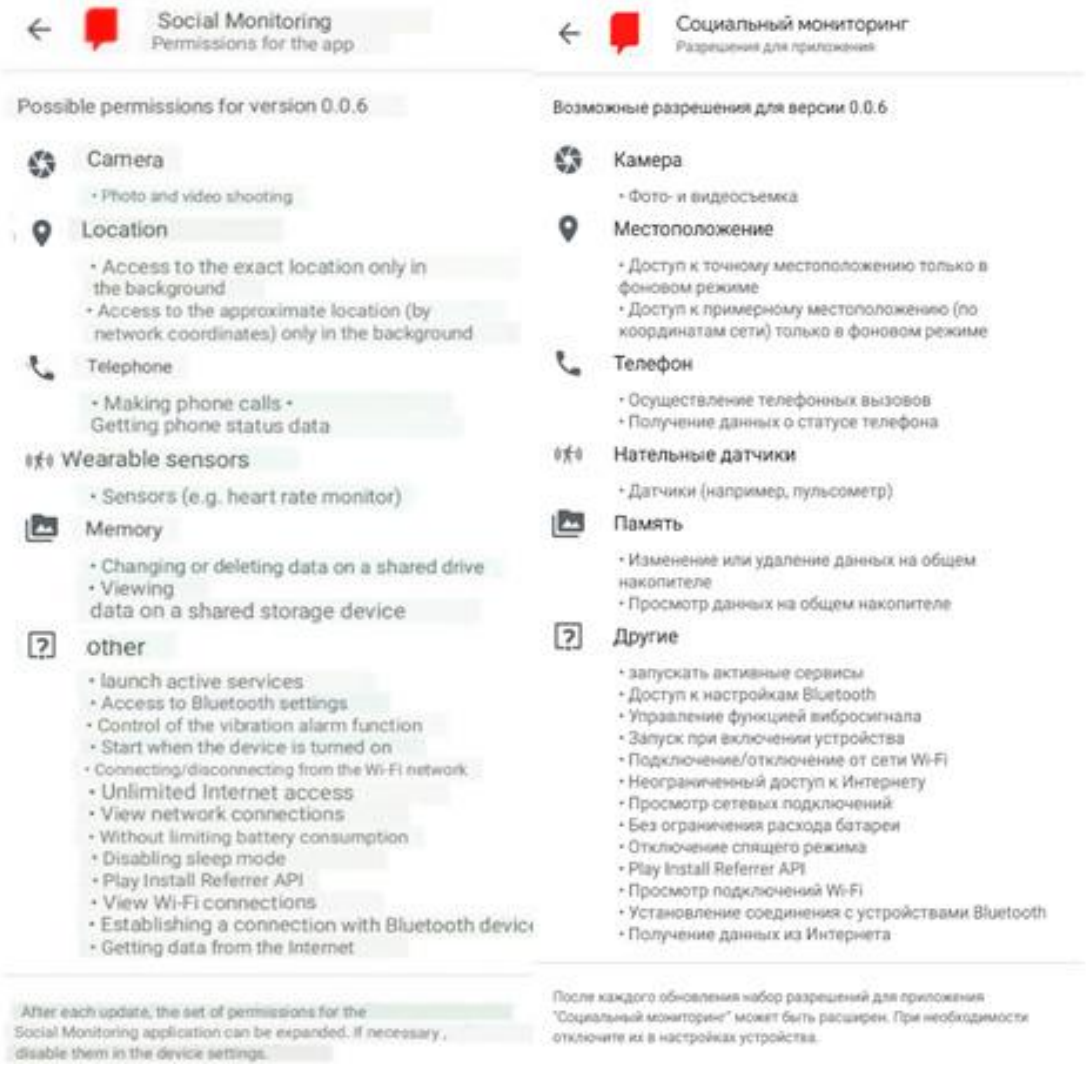

Figure 2 Permissions requested by the Social Monitoring application (presented in two languages)

The Social Monitoring app turned out to be more controversial. The app was distributed in Moscow, so the potential coverage could be more than 12,000,000 people, but its specifics differ from those listed above. The official website of the Mayor of Moscow provides the following description: “Social Monitoring” is a mobile application that helps the city ensure compliance with self-isolation. It is primarily used by those who

have been diagnosed with “coronavirus infection,” i.e., potential users are people who have already been infected with the coronavirus. This factor was probably the main reason why the application was mandatory for installation. It worked as follows: infected users were required to take a photo of themselves at the appointed time, after which the photo, with its geolocation attached, was sent for processing to prove compliance with quarantine regulations. Thus, a resident of Moscow was to establish that they were conscientiously observing the requirement to self-isolate. However, problems arose in almost all aspects of the application's work and quickly reduced citizens' level of trust. The first thing that caught the eye when installing the application was the list of permissions, which differed in several ways from that given on the Mayor of Moscow's website page dedicated to the application.

For the Android operating system, the following requirements were announced: “Take a photo,” “Access to location,” “Background mode of operation,” but after installation, the following confirmation window appeared, which contains many more items (Fig. 2).

The next problem with the Social Monitoring app were the calls and notifications that came at night. According to the decision of the Department of Information Technology, 458 fines totaling about 10 million rubles were canceled due to the fact that the demands to send a photo within an hour came at night. After that, sending notifications at night was prohibited, but another 34.5 thousand fines remained unpaid, and it is not possible to find out how many of them were issued by mistake. In addition, according to user reviews on GooglePlay, AppStore and Irecommendd.ru most users were dissatisfied with the instability of the application, with frequent failures, the quality of technical support, or its complete absence, the complexity of creating the conditions necessary for the snapshot. As a result, the average score accorded to the application in the GooglePlay (2020) shop was 1.3 out of 5 possible points, based on 14.2 thousand reviews, in the AppStore (2020) it was 1.2 out of 5, based on 7.5 thousand reviews. The technical component of the application also had some serious problems. A study of the source code of the application conducted by representatives of the telegram community “IT and COMP” revealed the fact that data is transmitted to the servers of the Moscow City Hall via http protocol, which does not involve data encryption. At the same time, along with the user's data, an IMEI identifier is also sent – a unique identifier of the device in the network. The facial recognition system used in the application belongs to the American company identix.one, therefore, the data of Social Monitoring users is very likely to get to the servers of this company. It was also revealed that the posted e-mail address for user support service did not belong to the subordinate city hall of the State Institution “Information City,” but to the company “Gaskar Integration.” Thus, the situation with Social Monitoring resembles the situation of Smittestopp. However, unlike other applications, Social Monitoring is mandatory and has more serious problems with the quality of its implementation with a larger volume of collected data about the user. At the same time, there were no protests against the use of the application, whereas the subsequent introduction of QR codes confirming vaccination for visiting public places was not without protests, some of which were associated with the unacceptability of using this digital identifier in public.

In Israel, an application was developed that seems very similar in functionality to Social Monitoring – AMAN. The main differences were the free distribution of the application through the AppStore and the verification of compliance with self-isolation based on GPS data, and not on photos constantly sent through the application. The Aman app was created in Israel at the beginning of the COVID-19 pandemic in March 2020. It was designed to help law enforcement agencies monitor people who should be quarantined but do not comply with it. In the first month of using the app, more than 1 million downloads were registered. However, not all users were happy with its functions. Some people have expressed concerns about privacy violations and the possibility of data abuse. Several users have sued the Israeli government, claiming that the app violates their constitutional rights. The advantages of the Aman application are that it allows you to control people who should be quarantined and prevent the spread of COVID-19. It also helps law enforcement agencies respond quickly to quarantine violations. According to the data provided by the Government of Israel, in the first three months of using the application, more than 5,000 cases of quarantine violations were registered which were revealed thanks to the application. Israel was one of the first states outside East-Asia to impose involuntary surveillance measures as a means to combat the virus. To do this, the tool previously used to combat terrorism, developed by the internal security service (Shin Bet) was declassified and implemented to track the location of coronavirus patients, identify infection-chains and notify citizens who have been in close proximity to an identified patient to self-quarantine (Gekker & Ben-David, 2021, p. 149). Although there was a legal battle against its use, it was promoted by only a relatively small group of activists, while the majority of Israelis reacted calmly to universal tracking. The original Shin Bet's surveillance system, called simply "the Tool," was not specially created during the pandemic, but it has been in operation since 2002 and used for continuous trawling collection of all available cell-phone data from every mobile device in Israel and the Palestinian Territories (Gekker & Ben-David, 2021, p. 150). Therefore, in this case, the technical means already existed, they were simply retrained to track the possible spread of Covid. A Bluetooth-based phone app was also developed in Israel (however, not very successfully), but "the Tool" was already in place anyway, which facilitated its mandatory adoption (Das, 2021).

Another application that serves to monitor the user's compliance with the self-isolation mode is the Magen application (Ministry of Health, 2021). One of the main advantages of this software product is that it allows the tracking of user's movements in real time, efficiently permitting to monitor compliance with the self-isolation regime. Users who have been diagnosed with COVID-19 or have been in contact with an infected person get access to the application and must confirm their location and quarantine compliance. In case of an infraction against the rules, the application sends a notification, reporting a violation of self-isolation protocol to the local health services. However, despite these advantages, the Magen application also has a number of disadvantages. For example, the application requires a GPS receiver always turned on, which consumes a lot of energy and quickly drains the device's battery (Moyal, 2020). Digital technologies have been used most consistently to prevent the spread of Covid-19 in China, where telecom operators can collect and use location data that is not constrained by user privacy issues.

Data from hundreds of millions of smartphones with GPS enabled were collected by the government to track the user's route and assess the likelihood that a person is exposed to COVID-19 by comparing his position with that of infected individuals or groups (Iandolo et al., 2021). Users with the highest level of risk were identified using AI, so in some cases they could not understand how and why the “red status” was indicated which did not allow free movement.

China has introduced a number of technological solutions to combat the spread of Covid-19. The state has created a contact tracking system that uses GPS data, mobile networks, and CCTV cameras to monitor people's movements. If someone is infected with Covid-19, the system can quickly identify who they have been in contact with and isolate them (Bogdanov, 2020).

Every person who decides to use a certain COVID tracing app faces the need to sacrifice their privacy to varying degrees in order to fight COVID-19, but a greater sacrifice does not always mean a more effective result. For example, despite the number of permissions obtained by the app (see Fig. 2), the Russian app Social Monitoring was suspended due to incorrect operation (frequent unwarranted fines, lack of encryption, use of elements from other apps that operate with personal user data. Thus, it is necessary to ensure a balance between protecting personal data and the effectiveness of fighting COVID-19. To do this, data anonymization methods such as encryption and pseudonymization can be used which allow maintaining user confidentiality while providing the ability to track contacts and identify the infected. In addition, it is important to regularly check the functionality of applications and eliminate any errors found to avoid the unlawful use of users' personal data.

COVID Tracing-apps in Action

Although the use of COVID tracing-applications has been widespread around the world, debates about their usefulness have remained just as popular. It is practically impossible to assess and compare the effectiveness of these applications, both due to the lack of data and the influence of unaccounted factors. Certainly, there are many ways to model their impact, but they are weakly oriented towards real situations, and often assume a simplified, macro-level mathematical model that assumes homogeneous mixing of the population. Nevertheless, there are several empirical studies demonstrating that messages about contacts with sick individuals can slow the spread of the disease. For example, in Taiwan, the effectiveness of a text warning system used among 627,386 individuals who came in contact with SARS-CoV-2 was shown and compared to the general population who did not use such a warning system. The number of cases decreased from 19.23 to 16.87 per 1000 individuals (Jenniskens et al., 2021). The use of the “Test and Trace” application, adopted on the Isle of Wight (UK) by 34,000 individuals, is also interesting. People who came in contact with an individual marked as positive based on a self-report were provided with social distancing advice, which led to a reduction in R_0 (basic reproductive rate) from 1.3 to 0.5. Moreover, after 3 weeks of use, the incidence of SARS-CoV-2 diagnoses declined by around 90 (Kendall et al., 2020).

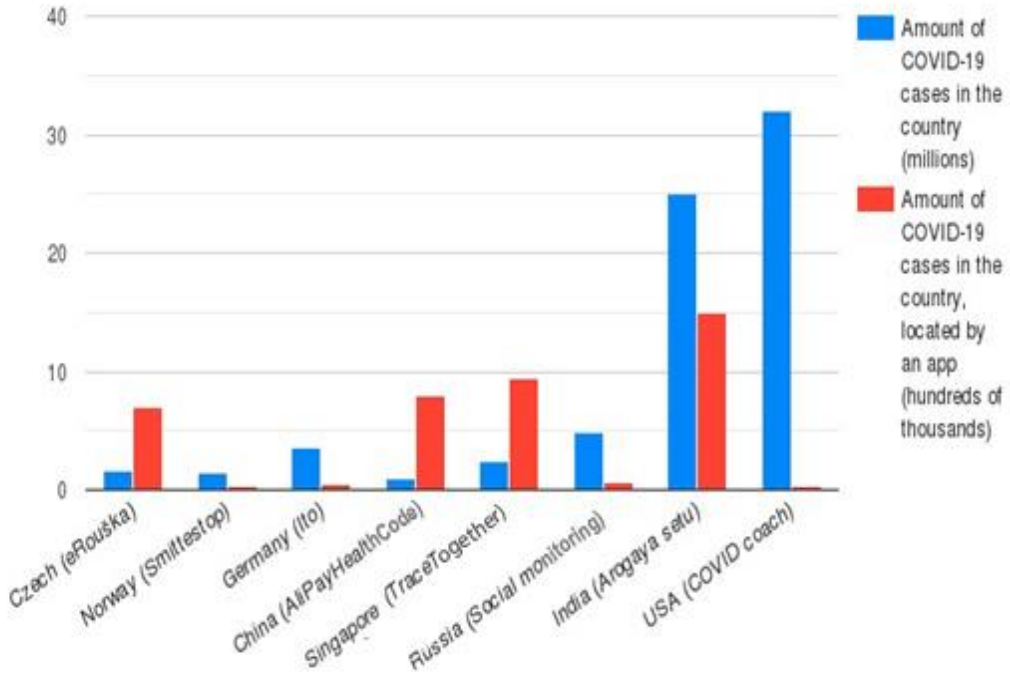

Figure 3. App efficiency

Based on the data illustrated in the diagram above (see Fig. 3), several conclusions can be drawn:

1) The most effective in terms of the number of detected cases of infection is the Indian app Arogaya Setu, but if we consider the effectiveness of the app as a percentage of the total number of cases detected by it, then the Indian software product is in 4th place, having only about 6% (the lowest result are the ones of Smittestop – 2%, Social Monitoring and Ito – 1%, and COVID coach – 0.07% (National site of US health care, 2021)). The leader in percentage terms is the Chinese AliPayHealthCode with a result of approximately 80% case detected. ERouška and TraceTogether have 43% and 38% respectively.
2) Practice shows that the Chinese methodology of universal mandatory implementation of an app that has access to most of users' information allowed to minimize the number of cases of infection and slow down the spread of the virus at the cost of users' privacy and freedom. At the same time, Singapore's TraceTogether was not mandatory to install and also requested important personal user data (passport data, geolocation), but the result was almost half lower than that of AliPayHealthCode.
3) The COVID coach app turned out to be the least effective among those presented. Despite extremely low requirements (the app requested access to geolocation, but

collected data only for past time, i.e. it would be very difficult to track the user due to the use of outdated geo-data, but identifying contact with a potential carrier of the virus would not be difficult.), and the presence of an active data encryption system, the app turned out to be ineffective.

4) From points 2 and 3, it can be concluded that the Chinese app was effective because mandatory installation and use allowed to solve the issues of spread, trust, and responsibility of users (every citizen living in one of the areas where the use of AliPayHealthCode was introduced was obliged to use it in order to have the opportunity to access any places of mass gathering). The Singaporean app was probably less effective because it was not mandatory, so some potential users refused to risk their personal data. The COVID Coach app, developed in the USA, can be called ineffective. Probably, the reason for the low efficiency was the distrust of Americans towards the government (research on this topic was mentioned in the article). Therefore, despite the low level of control of the app over the user, general distrust did not allow users to allow any additional intervention in their own lives by the state. The reason for the low efficiency of the Smittestop app is almost identical – the app had several technical problems that endangered users' data, so citizens practically stopped using the app. Below in the diagram, we presented our assessment of the effectiveness of the analyzed apps (see Fig. 4). As you can see on the scheme, the amount of detected cases is not the criterion which, taken alone, allows to judge the efficiency of apps without any supporting information.

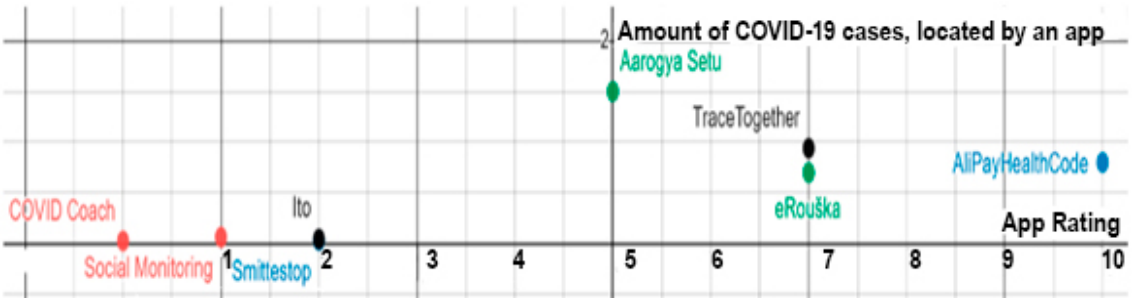

Figure 4. Apps rating by the number of COVID cases detected

DISCUSSION

The pandemic has dramatically exposed the issue of the boundaries of private life and the public good, which in the modern world moved from ethically philosophical to the category of relevant practical. In the interaction of technological and management solutions in China, Iandolo et al. see the manifestation of Collective Knowledge in an Unpredictable Environment (Iandolo et al., 2021). Reacting fast and technologically prepared, the authorities prevented a large-scale spread of the virus. On the other hand, for the effective implementation of Bluetooth-based applications, civic consciousness

was required, that is, people had to understand the responsibility for the spread of the virus and voluntarily install the application and responsibly treat its recommendations.

At the same time, we must not forget about the essence and work of technology, and about the idea of it. Modern digital technologies do not allow citizens to independently assess the principles of their work, which makes it possible to mislead or use information for propaganda, political and other purposes. This makes it difficult to form an objective opinion. Moreover, technical problems and shortcomings become part of the political and ideological discourse. The more voluntary the use of an application is, the greater the responsibility and role of citizens in their effectiveness. On the other hand, the efficiency of centralized technologies, responsible for the control of movements, also implies the acceptance by citizens of high-level digital control. Users' relation to application usage varies between countries of Europe (Witteveen & Pedraza, 2021), more so between countries with greater differences of cultural and ideological values. A study conducted in France shows that, with trust in the government, the development of a tracing app contributes to the healthy mental state of the population (Kurtaliqi et al., 2022). In Germany, among respondents who had trust in government decisions, the level of application use is significantly higher (Munzert et al., 2021). In the US, individual characteristics of residents play a greater role in the adoption of the application than the difference between decentralized design vs. centralized design, location use, and the presentation of security risk (Li et al., 2021). Thus, there is no universal fear of data security that could explain a certain technological design. The choice is determined by certain archetypes or myths that dominate in certain countries.

The study of alternative Covid-tracking applications allows us to see the confluence of ideological, philosophical and technical concepts in the modern world. The evaluation of public health applications and other technologies is deeply related to personal and social life and cannot be conducted in isolation from the dynamics of value orientations.

REFERENCES

AppStore (2020). App Store iOS application "Social Monitoring". https://apps.apple.com/ru/app социальный-мониторинг/id1508591174

Auxier, B., & Rainie, L. (2019, Nov. 15). Key Takeaways on Americans' Views about Privacy, Surveillance and Data-sharing. *Pew Research Center*. https://www.pewresearch.org/short-reads/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/

Bogdanov, A. (2020, Apr. 4). V Kitaye Prilozheniye Reshayet, Mozhno li vam Vyyti iz Doma. Khotite tak zhe? [In China, the App Decides whether you Can Leave your Home. Do you Want the same?] *Hi-News.ru*. https://hi--news-ru.turbopages.org/hi-news.ru/s/technology/zachem-kitaj-nachal-prisvaivat-lyudyam-cvetnye-kody.html

BusinessFM. (2020, May 24). The App Released in Australia is Useless. *BFM.ru*. https://www.bfm.ru/news/444434

Gekker, A., & Ben-David, A. (2021). Data Cudgel or How to Generate Corona-Compliance in Israel. In S. Masiero, E. Milan, & S. Trere (Eds.), *COVID-19 from*

the Margins. Pandemic Invisibilities, Policies and Resistance in the Datafied Society, Institute of Network Cultures (pp. 149-152). Hardinxveld-Giessendam.

GooglePlay. (2020). Google Play Android application "Social Monitoring". https://play.google.com/store/apps/details?id=ru.mos.socmon&hl=ru

Iandolo, F., Loia, F., Fulco, I., Nespoli, C., & Caputo, F. (2021). Combining Big Data and Artificial Intelligence for Managing Collective Knowledge in Unpredictable Environment–Insights from the Chinese Case in Facing COVID-19. *Journal of the Knowledge Economy*, *12*(4), 1982–1996. https://doi.org/10.1007/s13132-020-00703-8

Jenniskens, K., Bootsma, M. C. J., Damen, J. A. A. G., Oerbekke, M. S., Vernooij, R. W. M., Spijker, R., Moons, K. G. M., Kretzschmar, M. E. E., & Hooft, L. (2021). Effectiveness of contact tracing apps for SARS-CoV-2: A rapid systematic review. *BMJ Open*, *11*(7), e050519. https://doi.org/10.1136/bmjopen-2021-050519

Kendall, M., Milsom, L., Abeler-Dörner, L., Wymant, C., Ferretti, L., Briers, M., Holmes, C., Bonsall, D., Abeler, J., & Fraser, C. (2020). Epidemiological changes on the Isle of Wight after the launch of the NHS Test and Trace programme: A preliminary analysis. *The Lancet. Digital Health*, *2*(12), e658–e666. https://doi.org/10.1016/S2589-7500(20)30241-7

Kurtaliqi, F., Zaman, M., & Sohier, R. (2022). The psychological reassurance effect of mobile tracing apps in Covid-19 Era. *Computers in Human Behavior*, *131*, 107210. https://doi.org/10.1016/j.chb.2022.107210

Leith, D. J., & Farrell, S. (2021). Contact Tracing App Privacy: What Data Is Shared By Europe's GAEN Contact Tracing Apps. In *IEEE INFOCOM 2021 – IEEE Conference on Computer Communications*, (pp. 1–10). IEEE https://doi.org/10.1109/INFOCOM42981.2021.9488728

Li, T., Cobb, C., Yang, J., Baviskar, S., Agarwal, Y., Li, B., Bauer, L., & Hong, J. I. (2021). What makes people install a COVID-19 contact-tracing app? Understanding the influence of app design and individual difference on contact-tracing app adoption intention. *Pervasive and Mobile Computing*, *75*, 101439. https://doi.org/10.1016/j.pmcj.2021.101439

Ministry of Health (2021). Hamagen App. https://govextra.gov.il/ministry-of-health/hamagen-app/download-en/

Mumford, L. (1964). Authoritarian and Democratic Technics. *Technology and Culture*, *5*, 1-8.

Munzert, S., Selb, P., Gohdes, A., Stoetzer, L. F., & Lowe, W. (2021). Tracking and promoting the usage of a COVID-19 contact tracing app. *Nature Human Behaviour*, *5*(2), Article 2. https://doi.org/10.1038/s41562-020-01044-x

National site of US health care. (2021, May). Health Apps Can Help Fight COVID-19. https://www.health.gov/news/202105/health-apps-can-help-fight-covid-19

Moyal, O. S. (2020, March 22) "Hamagen" Application – Fighting the Corona Virus, Medium. https://medium.com/proferosec-osm/hamagen-application-fighiting-the-corona-virus-4ecf55eb4f7c

Sandbu M. (2020, 16 Apr.) Technical Analysis of Smittestopp Backend Azure. https://msandbu.org/technical-analysis-of-smittestopp-backend-azure/

Singapore Government Agency Website. (n.d.). Trace Together Safe Together. https://www.tracetogether.gov.sg

White, L., & Basshuysen, P. van. (2021). Without a trace: Why did corona apps fail? *Journal of Medical Ethics*, *47*(12), e83–e83. https://doi.org/10.1136/medethics-2020-107061

Winner, L. (1998). *The Whale and the Reactor: A Search for Limits in an Age of High Technology*. University of Chicago Press.

Witteveen, D., & Pedraza, P. de. (2021). The Roles of General Health and COVID-19 Proximity in Contact Tracing App Usage: Cross-sectional Survey Study. *JMIR Public Health and Surveillance*, *7*(8), e27892. https://doi.org/10.2196/27892

Appendix 1. List of analyzed applications.

1. ERouška – Czech Republic
2. ProteGOSafe – Poland
3. Smittestop – Norway
4. Social Monitoring – Russia
5. AliPayHealthCode – China
6. COVIDsafe – Australia
7. Ito – Germany
8. Covid Shield – Australia
9. TraceTogether – Singapore
10. AMAN – Israel
11. COVID Alert – Canada
12. NHS COVID-19 – United Kingdom
13. Rakning C-19 – Iceland
14. AarogyaSetu – India
15. StopCovid – France
16. StaySafePH – Philippines
17. MySejahtera – Malaysia
18. Shlonik – Oman
19. CoronApp – Colombia
20. Immuni – Italy
21. TraceCovid – Switzerland
22. Care19 – USA
23. COVID Alert NY – USA
24. NZ COVID Tracer – New Zealand
25. BeAware Bahrain – Bahrain
26. Corona-Warn-App – Germany
27. COVID Tracker Ireland – Ireland
28. StaySafe – New Zealand
29. EHTERAZ – Qatar
30. COVIDWISE – USA
31. COCOA – Japan
32. StopCOVID NI – Northern Ireland
33. StaySafePH – Philippines
34. Ehteraz – Qatar
35. Tawakkalna – Saudi Arabia
36. Selangkah – Malaysia
37. CoronaCheck – Switzerland
38. Kwarantannadomowa PL – Poland
39. PeduliLindungi – Indonesia
40. SwissCovid – Switzerland

41. ImmuneHR – Croatia
42. GISAID EpiCoV app DE – Germany
43. COVID-19 AlertaSIS – Peru
44. MyTrace – Malaysia
45. StopKorona! – Serbia
46. EVA Check-in TW – Taiwan
47. Koronavilkku – Finland
48. KoronaStop LT – Lithuania
49. Co-WIN IN – India
50. BeAware UAE – UAE
51. ArogyaSetu Bridge IN – India
52. Ehteraz Oman – Oman
53. COVA HP IN – India
54. Tarassud+ – Morocco
55. COVA Punjab IN – India
56. BeAware Kuwait – Kuwait
57. Tawakkalna KSA – Saudi Arabia
58. StopCovid BE – Belgium
59. Sehha UAE – UAE
60. BeAware Qatar – Qatar
61. Immuni IT – Italy
62. WeTrace SG – Singapore
63. SafeEntry SG – Singapore
64. HealthHub SG – Singapore
65. CA Notify – California, USA
66. Coronamelder NL – Netherlands
67. COVID Coach – USA
68. COVID Symptom Study US – USA
69. HealthBridge HK – Hong Kong
70. LeaveHomeSafe HK – Hong Kong
71. MySejahtera MY – Malaysia
72. CovidPass CH – Switzerland
73. SwissCovid App CH – Switzerland

СВЕДЕНИЯ ОБ АВТОРАХ / THE AUTHORS

Никита Романович Кесарев
kesarev.nr@edu.spbstu.ru
ORCID:0009-0004-3914-8624

Nikita Kesarev
kesarev.nr@edu.spbstu.ru
ORCID:0009-0004-3914-8624

Андрей Романович Корочкин
awesome.corochkin@yandex.ru
ORCID:0009-0006-3398-1353

Andrey Korochkin
awesome.corochkin@yandex.ru
ORCID:0009-0006-3398-1353

Статья поступила 11 февраля 2023
одобрена после рецензирования 14 июня 2023
принята к публикации 18 июня 2023

Received: 11 February 2023
Revised: 14 June 2023
Accepted: 18 June 2023