DO EU GOVERNMENTS CONTINUE TO OPERATE CONTACT TRACING APPS ILLEGITIMATELY?

#trackthetrackers

October 2021

CIVIL LIBERTIES UNION FOR EUROPE

Publisher
Civil Liberties Union for Europe e.V
Ringbahnstraße 16-18-20
12099 Berlin, Germany
www.liberties.eu

Editor
Orsolya Reich

Assistant Editor
Jascha Galaski

Copy Editor
Jonathan Day

Authors
Olga Cronin, Irish Council for Civil Liberties (Ireland); Krzysztof Izdebski, ePanstwo Foundation (Poland); Adela Katchaounova, Bulgarian Helsinki Committee (Bulgaria); Liina Laanpere, Estonian Human Rights Centre (Estonia); Ricardo Laufente, D3 – Defesa dos Diretios Digitais (Portugal); Sergio Carrasco Mayans, Rights International Spain (Spain); Orsolya Reich, Civil Liberties Union for Europe (Introduction); Ádám Remport, Hungarian Civil Liberties Union (Hungary); Egert Rünne, Estonian Human Rights Centre (Estonia); Tommaso Scannicchio, CILD – Italian Coalition for Civil Liberties and Rights (Italy); Iza Thaler, Peace Institute (Slovenia); Christian Thönnes, Civil Liberties Union for Europe (Germany);

This project has been supported by the European AI Fund, a collaborative initiative of the Network of European Foundations (NEF). The sole responsibility for the project lies with the organiser(s) and the content may not necessarily reflect the positions of the European AI Fund, NEF or the European AI Fund's Partner Foundations.

Executive summary

After the first few weeks of the first wave of the coronavirus pandemic in Europe, several European Union Member State governments started to consider the idea of launching contact tracing mobile applications.

Promoters of the technology expected that mobile applications can be taught to do something human contact tracers cannot do – they would be able to identify potential infections between people who do not know each other. They would also do that faster than humans could ever do. The technological optimists believed that with a high enough uptake of the apps, the pandemic would be won over in a matter of weeks.

Even though human rights organizations and academic institutions alike warned governments early on that the techno-optimist dream may not hold up as the technology is not yet tested, most Member States bought into the dream and introduced their national contact tracing apps by the end of 2020.[1]

The questionable efficacy of the proposed contact tracing apps was not the only concern academics and human rights defenders raised. The digital rights community feared that the widespread use of such technology could open the door to mass surveillance. In an earlier study, *COVID-19 Technology in the EU: A Bittersweet Victory for Human Rights?*, the Civil Liberties Union for Europe (henceforth Liberties) has shown how European Union Member States avoided introducing the most privacy-breaching potential technological solutions in fighting the pandemic.[2]

In the present study, Liberties and partners describe how contact tracing apps in ten Member States were introduced, and what the authorities know and/or want to know about their impact on the spread of the pandemic, on the economy and on the most vulnerable social groups of the society (Bulgaria: ViruSafe; Estonia: HOIA; Germany: Corona-Warn-App and Luca App; Hungary: VírusRadar; Ireland: CovidTracker; Italy: Immuni and regional apps; Poland: STOP COVID / ProteGo Safe; Portugal: Stayaway COVID; Slovenia: #OstaniZdrav; Spain: Radar COVID).

The study finds not only that the ten examined European Union Member States typically have not yet conducted efficiency and social impact assessments on the contact tracing apps, even though these have been in operation for more than a year, but also that they plan to keep operating the unassessed apps until (at least) the "end of the pandemic" without ever conducting such research.

1 Information on the release dates is available here.

2 Liberties' first study on contact tracing apps is available here.

When Member States provided Liberties' partner researchers with explanations for why impact evaluation for apps maintained using public resources has not been made and is not even planned, they typically pointed to the privacy-protecting nature of their apps that make such an evaluation difficult. True, apps based on a decentralized architecture do not automatically provide authorities with data on how many people were notified of a potential infection and how many of them were later proven to have been infected by the coronavirus. We accept that having the relevant data readily at hand would certainly be convenient to the relevant authorities. However, it is difficult to see how the privacy-protecting nature of the apps exonerates governments from the obligation to investigate whether the technology actually works. Such research is by no means impossible. Germany, for example, did investigate the efficacy of the Corona-Warn-App by making use of two sources of data: event-independent data donations and event-driven user surveys.

Based on the information obtained by Liberties' partners, it is plausible to think that contact tracing apps in most investigated countries had negligible impact (if any) on the spread of the pandemic, and, due to the low uptake, in most places similarly negligible social impact. Member States seem to have come at the same conclusion. Even though by the summer of 2021 traveling between Member States for tourism became possible again (typically with relatively recent negative test results, or a recovery certification, or a vaccination pass), and most contact tracing apps in Europe had by then long been interoperable, there was no detectable governmental push to revive the use of such apps and thereby decrease the risks created by restarting tourism.

Instead, Member States chose to keep operating contact tracing apps silently, hoping that people will simply forget how digital contact tracing technology failed to fulfil the dreams their governments actively cultivated. Such conduct is against the principles of good governance.[3] It is against the principle of efficiency and effectiveness, for without impact assessments Member States cannot know whether they make the most of the resources available. It is against the principle of accountability, for public officials are trying to avoid taking responsibility for the failure of the contact tracing apps. It is against the principle of openness and transparency, for Member States do not communicate about the reasons for letting the idea of digital contact tracing fade away. Member States should conduct research on why the technology and/or its implementations failed, communicate the findings, correct the mistakes if they are worth correcting and if not, retire the apps.

3 One widely accepted formulation of these principles can be found here.

Lessons to learn for future emergencies

Contact tracing apps were launched without much prior research on their potential efficacy and without much opportunity for public scrutiny into the risks they may carry. This resulted in spending public resources on a potentially useless technology, and a low uptake of said technology (that can render an even potentially useful technology useless).

> *Member State governments should never deploy untested technologies. New technologies with a potential to resolve emergencies (or any social problems) must be carefully tested, and subjected to public scrutiny before launch.*

Contact tracing apps were typically promoted as direct solutions to the public health emergency Member States have been facing. Insufficient attention was paid to the non-technological environment of said apps, for example, to the health-care systems through which positively tested users would obtain the codes the apps need to notify their contacts. Even the best technology can be rendered useless when the input it needs is not sufficiently provided. This insufficient attention to the social environment the apps operate in resulted in the low usage (and potentially forgone public health benefits) of said apps even in Member States where the download rates were relatively high.

> Member State governments must keep in mind that it is not possible to give a purely technological fix to social emergencies. Technologies always operate in social contexts. Careful consideration must always be given to the legal and social environment a given piece of technology is supposed to operate in.

Contact tracing apps typically operate without the authorities having much data on how the app performs. This prevents the relevant authorities from either adjusting certain features of the apps so that they become more efficient, or, if need be, discontinuing spending public resources on inefficient apps.

> Member State governments should order the relevant authorities to research the efficacy of the technologies they operate, and conduct impact assessments on a regular basis.

Table of contents

Introduction

In mid-March 2020, European Union Member States announced one after the other in a matter of days that, in an attempt to control the spread of the coronavirus, they were closing their borders. Many Europeans, formerly enjoying one of the most basic European freedoms and living in different Member States, rushed to the nearest airport trying to get the last flight to the place they felt most comfortable calling home. It was very clear that life as we know it was going to change fundamentally.

By the end of March, not only were the borders closed, but also schools, shopping malls, restaurants, pubs, museums, clubs and gyms. People were asked or ordered not to leave their houses. Businesses crumbled. Governments were hard-pressed to ensure that we could return to normal life as soon as possible while at the same time prevent the healthcare system from collapsing.

Technological over-optimism on the rise

After the first few weeks of the first wave of the coronavirus pandemic in Europe, several Member State governments started to consider the idea of launching contact tracing mobile applications.

Promoters of the technology expected that mobile applications can be taught to do something human contact tracers cannot do - they would be able to identify chains of infections between strangers. The technology was also expected to be able to notify potentially infected people faster than human contact tracers could ever do. Mobile apps do not need to talk to people who tested positive and try to make them remember whom they have met. Mobile apps are not lied to by people who don't want to reveal where they have been. The techno-optimists dreamed of us simply installing a new app and then being able to return to normal life, use public transport, go to work, to a concert, to have a drink with friends. If one user gets infected by the coronavirus, everyone who could have also gotten it would be notified and would stay at home. If enough of us install the app and follow the instructions given there, the pandemic would be beaten in a matter of weeks.

Human rights organizations and academic institutions alike warned governments early on that the techno-optimist dream may not hold up, that the digital contact tracing technology does indeed seem to suffer from serious limitations, and that the efficacy of such apps is simply unknown and more research is needed.[4] However, the pull was too strong. Most

4 Even the European Centre for Disease Prevention and Control, the agency of the European Union whose mission is to strengthen Europe's defences against infectious diseases, tried to call Member States' attention to the limitations of the technology in a guidiance dated June 2020. See the Guidiance here.

Member State governments decided to give digital contact tracing technology a try.

Concerns about mass surveillance

The questionable efficacy of the proposed contact tracing apps was not the only concern academics and human rights defenders raised. The digital rights community feared not only that the apps would not live up the efficacy expectations policymakers have, but the widespread use of such technology could open the door to mass surveillance. Such an opening is especially concerning against the background of steeply declining democracy and rule of law in a number of EU Member States.[5]

These fears were not groundless. Panicked governments were inclined to resort to extreme measures, including untested technology. There was talk of apps collecting location data on central servers.[6] There was talk of making apps obligatory. [7]

As we wrote elsewhere, thanks to the efforts and engagement of privacy experts developing the so-called DP-3T protocol, and also to a degree to the privacy commitments made by tech giants Google and Apple, the worst possible scenarios have been avoided.[8]

Most of the contact tracing apps that were deployed in Europe are based on the so-called Google Apple Exposure Notification Application Interface (GAEN API). These apps work with Bluetooth Low Energy (henceforth Bluetooth) data instead of location data, and the API does not allow information on whom we spend our time with to be collected on a central server.

Apps built on the GAEN API typically would not provide information to the public health authorities that would help them to trace contacts and track the spread of the infection. [9]Individual users can and must decide what to do with the information they receive through the app when getting a notification of having been in close proximity to someone who had

5 Liberties' relevant report can be found here.

6 Bulgaria ended up doing so. The app was not mandatory there, however, and, presumably partly due to the prying nature of the app, the uptake was extremly low. No misuse of data collected by the app was reported

7 For 5 days, the use of contact tracing app was mandatory in Portugal. In late 2020, for a few weeks it was a precondition for movement across municipality borders in Slovenia. In most Member States, however, governments kept to the EU-wide stipulation that such apps need to be voluntary to use. See for example in the 8th point of the European Data Protection Board's Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, Adopted on 21 April 2020. The Guidelines are available here.

8 https://dq4n3btxmr8c9.cloudfront.net/files/c-5f-T/Liberties_Research_EU_Covid19_Tracing_Apps.pdf

9 Although in some apps, for example in the Irish COVID Tracker Ireland, users can enable some contact-tracing features, see more in Susan Landau: People Count, The MIT Press, Cambridge MA 2021, Chapter 4.

tested positive for COVID-19. Since, however, "contact tracing app" is the term widely used to describe such apps (as opposed to the technically more apt "exposure notification" or "proximity tracking" app), throughout this document we will also call GAEN-based apps contact tracing apps.

A handful of Member States refused to accept that Google and Apple practically control what kind of mobile applications governments can and cannot offer to their electorate and decided to introduce apps that do indeed collect data on a central server. However, the few contact tracing apps in Europe that were not built on the GAEN interface suffered serious difficulties: these apps needed to be run in the foreground (that is, users could not listen to music or check their emails when, for example, riding a train) and they quickly depleted the batteries of the devices they were running on. To tackle these difficulties, the French government invested serious resources into trying (and mostly failing) to resolve these issues and, acting as a sovereign government, offer the application it believed to be appropriate to be offered. Some other Member States, for example Hungary, silently abandoned the project.[10]

The price of privacy-friendliness?

When authorities launched GAEN-based contact tracing apps, they typically emphasized two points. First, that the apps will be extremely helpful in eradicating the pandemic should enough of us download them. Second, that everyone may feel comfortable downloading them as they duly protect users' privacy.

When, after a few months of operating, contract tracing apps had not fulfilled the techno-optimists' dream, op-eds started to flock into European media outlets blaming the decentralized and thereby privacy-protecting nature of the GAEN-based apps for their failure to halt (or at least control) the pandemic. These op-eds suggested that authorities should be able to see who the at-risk people are, and make sure that they do not disregard their obligation to quarantine. Put otherwise, it was increasingly popular to blame privacy protections for the ineffectiveness of contact tracing apps.

However, privacy protections should definitely not be blamed for the technology's apparent inability to live up to the techno-optimists' dreams. The op-eds scapegoating privacy protections were generally based on two highly questionable premises. First, that people would still be willing to install and use apps

10 Information on the French (and also on the Hungarian) developments can be found in Liberties' first contact tracing study here.

that collected and stored their movements and meetings centrally. Second, that it would be justified for Member States to attach legal consequences to what the algorithms of these apps calculate.

As to the first point, there is no good reason to think that people would be just as willing to use apps based on a centralized architecture. Assuming now that contact tracing apps track infection chains sufficiently well, uptake is of primary importance. While the claim in the media that apps needed to be downloaded by 60% of the population to be effective was never made by experts, the number of encounters the apps can detect and the infection chains they can thereby stop does indeed significantly grow with the uptake.[11] Put otherwise, the lower the uptake, the less useful the apps are.

A German study shows that quite a few people feared that even the decentralized and widely celebrated as privacy-friendly Corona-Warn-App allowed third parties to spy on them.[12] But as the level of trust in authorities is relatively high in Germany, people generally believed authorities when they said that the app was constructed in a way that they would have no access to users' data. Therefore, the uptake was relatively high (in a country of 83 million people there were 27 million downloads in ten months after the launch) – even people highly aware of privacy risks downloaded the app because of its privacy-protecting architecture. In countries where the apps were not similarly privacy protecting (and people do not trust that the authorities will not misuse their data) the uptake was significantly lower.[13]

There is also little reason to think that it would be justified to attach legal consequences to the risk calculations the apps produce. As long as there is no rigorous assessment made on the effectiveness of the apps in identifying infection cases, authorities are, at best, justified in asking people to take precautions. Mandating individual citizens to stay at home, not to visit their aging parents, give up their daily routines and stay away from their businesses based on calculations that may or may not have anything to do with the actual risks of being infected would however be clearly unjustified.

This is not to say that authorities are never justified to issue stay-at-home mandates. Individual citizens, identified by an accepted and sufficiently reliable method to be at risk of being infected and further infecting others, can be mandated to assume their fair share of burdens in trying to stop the pandemic. This is exactly what human contract tracers do when they confine the close-enough contacts of identified positive cases to their houses. However, there still is relatively little data suggesting that the

11 The misunderstanding on the 60% is explained here.

12 See the study here.

13 In 6 and 5 months of operation respectively, the Bulgarian app and the Hungarian app were downloaded by less than 1% of the population. See the data here. Admittedly, the difference in download rates is not determined by the different privacy protections these apps offer.

"cases" contact tracing apps identify are real infection cases in a proportion comparable to the proportion of cases tracked by human contact tracers.

Techno-optimists believed that with the help of Bluetooth signals the spread of the virus could be tracked sufficiently well. This is because first, one of the crucial factors influencing the risk of infection is the proximity to infected persons, and second, because proximity was believed to be able to be reliably indicated by Bluetooth signal strength. A couple of early studies, however, called the second assumption into question. While the strength of the Bluetooth signal in theory indicates the distance between different devices, in real world circumstances signal strengths may not measure distance well enough. When Douglas Leigh and Stephen J. Farrell, researchers from Trinity College Dublin, measured the signals mobile phones received in a real train car, they found that signals, after remaining constant for 1.5-2 meters in distance, started to increase after that. In another experiment they found that signal strength varied greatly by the model of the device used, where the user keeps the device, the shape of the room they were in and the construction materials around them.[14]

Naturally, not all contacts tracked down by human contact tracers are in fact infected. Indeed, most of them are not. But people mandated to home-quarantine by them have a significantly higher chance than random to have indeed been infected. Ordering random people to stay at home for two weeks may also reduce the number of infections, since with their withdrawal from public spaces simply fewer physical interactions take place. However, such an order would likely to be illegal and surely cannot be justified by the risk these specific people pose to others. Depending on the (un)reliability of the Bluetooth-based technology, people identified by the apps as at-risk users may qualify as almost random.

It is important to emphasize that our point is not that digital contact tracing technology does not and cannot work well enough to justify quarantine orders. Our point instead is that governments did not have the necessary data showing that the technology works reliably enough to justify confinement orders based on digital contact tracing technology.[15]

Under these circumstances there is simply nothing privacy protections could have reasonably been traded for.

14 https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0239943#references; https://dl.acm.org/doi/abs/10.1145/3431832.3431840 and Landau ch5

15 REF AlgoWatch Lit review Literature reviews find no conclusive evidence of the effectiveness of contact tracing apps https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8132499/; https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8114870/ Other studies even concluded that there may be no evidence that digital contact tracing ever worked, including for previous outbreaks. In 'Automated and partly automated contact tracing: a systematic review to inform the control of COVID-19', published by The Lancet in November 2020, https://www.thelancet.com/journals/landig/article/PIIS2589-7500(20)30184-9/fulltext)

Technology unresearched

So far we have only argued that the governmental use of digital contact tracing technology to issue quarantine orders and threaten non-compliers with legal consequences would clearly be unjustified because the technology is not proven to be reliable enough. But we also believe that it is not only when legal consequences are at stake that governments ought to investigate the reliability and efficacy of technologies they deploy. Government-deployed apps must do what they are said to do. By appropriately investigating the impacts of the technology, national authorities could have avoided the misuse of resources, could have increased the uptake and could have even made the applications more efficient. However, Member States have typically chosen not to do so.

In the present study, Liberties and partners investigated the deployment of contact tracing apps in ten Member States (Bulgaria: ViruSafe; Estonia: HOIA; Germany: Corona-Warn-App and Luca App; Hungary: VírusRadar; Ireland: CovidTracker; Italy: Immuni and regional apps; Poland: STOP COVID / ProteGo Safe; Portugal: Stayaway COVID; Slovenia: #OstaniZdrav; Spain: Radar COVID). Researchers participating in this project investigated (a) how the different centralized and decentralized contact tracing apps work, (b) what kind of data they collect and how those data are processed, (c) how transparently they operate, (d) how efficient these apps are, (e) how the apps could worsen existing social problems (exclusion, discrimination) and (f) how the launch and the operation of these apps fit to our concept of good governance.

In addition to conducting desktop research, partners were encouraged to submit freedom of information requests to the relevant authorities asking the following questions:

- How many people downloaded the app (starting from the launch)?
- How many active users does the app have?
- What kind of efficiency-related problems were detected and how were they resolved?
- How many positive test result were uploaded by users of the app?
- After X months of operating the app, is there data on how many of those receiving a notification self-quarantined or got tested?
- After X months of operating the app, is there any data on how many of these people were really infected?
- After X months of operating the app, is there any data or model calculation on the social costs of the app (the costs of working-time lost vs chances of really being infected, etc.)?
- Is there any clear governmental plan for revoking the app? What are the conditions under which it will happen? (X number of cases out of 100.00, etc.)

As our country reports show, the majority of the investigated national apps were built on the GAEN API (with the exception of ViruSafe, STOP COVID and VírusRadar) and users' data were presumably not misused by authorities.

Relative privacy-friendliness notwithstanding, our country reports also show that contact tracing apps were deployed haphazardly, without much opportunity for public scrutiny. Operational transparency has been lacking in a number of cases. In Hungary, according to the app's privacy policy the controller does not admit to being the controller and therefore has not answered the questions of our research partners. In Bulgaria, the research partner needed to litigate to get hold of the app's data protection impact assessment. In Spain, the data protection impact assessment eventually published did not correspond to the app originally launched.

The apps seem to have been launched in most cases without any research into their potential efficacy. The lack of transparency and the unproven nature of the technology resulted in spending public resources on a potentially useless technology, and a low uptake of said technology (that can render an even potentially useful technology useless).

The reports also show that while a number of factors significantly influenced how widely used and therefore (potentially) how beneficial the technology could be (e.g., how easy it is for the user to obtain the code the app needs to notify contacts after a positive test, whether the authorities tasked by issuing such codes were already overworked, or whether they were also tasked with resolving problems that look more urgent, whether receiving a notification helped people to obtain test easily, etc.), insufficient attention was paid to optimizing these factors, that is to optimizing the non-technological environment of said apps. In Italy, users who tested positive were supposed to get a code to trigger the notifications of their contacts from public authorities – but these codes were often issued after enormous delays that rendered the whole issuance useless. In Spain only about 7% of the codes requested were entered into the application.

Only a few Member States conducted research on the efficacy of their apps. Our study finds that Member States typically have not yet conducted efficiency and social impact research on contact tracing apps, which have been in operation for more than a year. Furthermore, governments plan to keep operating the untested apps until (at least) the "end of the pandemic" without ever conducting such research.

When Member States provided Liberties' partner researchers with explanations for why they have not been carried out, and do not plan in future an impact evaluation for their apps, they typically pointed to the privacy-protecting nature of their apps that make such an evaluation difficult. Having the relevant data readily at hand would certainly be convenient to the relevant authorities. But it is difficult to see how the privacy-protecting nature of the apps exonerates governments from the obligation to investigate whether the technology they have been investing in and were promoting truly works. Such research is by no

means impossible. Germany, for example, did investigated the efficacy of the Corona-Warn-App by making use of two sources of data: event-independent data donations and event-driven user surveys.

This research is important for a number of reasons. First, if app operators don't have enough data on how their app fares, it prevents them from adjusting certain features of the apps so that the app becomes more efficient. As a consequence, the operators aren't able to maximise the potential public health benefits of the app.[16] Second, without this data, app operators can't decide if it's better to simply discontinue the app and direct public resources on other more effective public health measures.[17]

Based on the information obtained by Liberties' partners, it is reasonable to conclude that contact tracing apps in most investigated countries had negligible impact (if any) on the spread of the pandemic, and, due to the low uptake, in most places similarly negligible social impact. Member States seem to have arrived at the same conclusion. Even though by the summer of 2021 traveling between Member States for tourism became possible again (typically with a relatively recent negative test result, or a recovery certification, or a vaccination pass), and most contact tracing apps in Europe had by then been interoperable for a while, there was no detectable governmental push to revive the use of such apps and thereby decrease the risks that have been created by reintroducing tourism. This suggests that governments assume that the apps are not effective. However, instead of retiring the apps and risking criticism for their failure, Member States chose to keep operating them silently, hoping that people will simply forget how digital contact tracing technology failed to fulfil the dreams their governments have actively cultivated.

Such conduct is against the principles of good governance. It is against the principle of efficiency and effectiveness, for without impact assessments Member States cannot know whether they make the most of the resources available. It is against the principle of accountability, for public officials are trying to avoid taking the responsibility for the failure of the contact tracing apps. It is against the principle of openness and transparency, for Member States do not communicate openly the reasons for letting the idea of digital contact tracing to fade away.

Instead of pretending that the digital contact tracing technology was never taken seriously, Member States should now do their research.

16 On how data can be used in maximising the public health potential, see ECDC's guidiance here.

17 A number of apps were purchased for a symbolic price or for free from socially engaged developers (e.g. Bulgaria, Estonia, Hungary). This does not mean, however, that public resources were not invested. Maintaining apps, fixing bugs, etc. do involve costs.

Country reports

Bulgaria: ViruSafe

Adela Katchaounova (Bulgarian Helsinki Committee)[18]

Introduction

National Information System for Combating COVID-19

In April 2020, the Ministry of Health introduced a National Information System for Combating COVID-19. It consists of five modules: an information portal that provides up-to-date information on the epidemic situation; a mobile application for citizens to report their health status; a register of persons quarantined and persons diagnosed with COVID-19; a software that provides an epidemic prognosis; and geographical maps that visualize the number of quarantined, sick, deceased and recovered persons.

Citizens have access to the information portal and the mobile application. The other modules are only available for a selected list of public authorities, including the Ministry of Health, the national social security and health insurance authorities, regional healthcare inspectorates, general practitioners, medical establishments, municipal authorities, the police and border police. In the register (module 3), the data collected by the authorities include the full name, gender, citizenship, age, telephone number, place of isolation, start and end date of the quarantine, and the identity document number.

Amendment to the Law on Electronic Communication

The National Assembly announced on 13 March 2020 the Act on the Measures and Actions During the State of Emergency, introducing new measures to limit the spread of COVID-19. The Act included an amendment to the Electronic Communication Act (ECA), giving the national police the power to access phone location data from telecommunication companies in order to control citizens put under mandatory quarantine – without court order or a clear time limit. The matter was brought before the Constitutional Court by a group of parliamentarians. On 17 November, the Court decided by 10 votes to 2 that the use of location data to control quarantine compliance is unconstitutional.

Contact tracing app

On 4 April, the government, in the presence of Prime Minister Boyko Borissov, presented the digital tracing and symptom reporting app ViruSafe at a televised briefing. ViruSafe stands out from most other contact tracing apps in the EU as it is based on GPS location data and not on Bluetooth technology. From 7 April on, Bulgarians have been able to download it for free from the Apple Store and Google Play. In the first almost 6 months of

18 Radoslav Stoyanov assisted in the making of this report.

its operation (as of 18 September), only 63,577 people had downloaded the app.

The app was developed by the IT company ScaleFocus for one symbolic Bulgarian lev. Local media have noted that neither the authorities nor the developers released information about whether there had been a legal audit of its data protection compliance. Bulgarian media have also raised concerns about item 31 of ViruSafe's terms of use, which gives the Ministry of Health the authorization to share personal data with "competent authorities" to control the spread of the pandemic, criticizing the vague wording that makes it possible for a wide range of authorities to get access to users' personal information.

ViruSafe – technical details

ViruSafe is a contact tracing app based on GPS location data. It has several features, including a daily symptoms and health status tracker, a location tracker – enabled voluntarily by the user – which allows the creation of heatmaps with potentially infected people, and it provides users with the latest news and practical advice.

After downloading the app, users must go through an SMS validation and enter personal data, such as personal ID, age, any chronic diseases they may have. They also have to allow the app to track their location. The data is collected and stored in a central registry and, according to the official website, only accessible to the Ministry of Health and authorized governmental institutions. Bulgaria has not passed any legislation that provides the legal basis for the introduction of the app and the use of the data collected. The data, including health and location data, is only processed if consent is given by data subjects.

The symptom reporting functionality enables users to enter their health status several times a day (e.g. if they have a temperature or a dry cough). The information is then automatically sent to the general practitioner, who can then decide if and when to intervene.

The use of the app is voluntary, and the source code can be found on GitHub.

Involvement of DPA

The national data protection authority (DPA), the Commissioner for Personal Data Protection (CPDP), has not been involved in the development or assessment of the data protection compliance of the contact tracing app ViruSafe. There is no information available on its website; no reactions, comments, statements or press releases.

Data Protection Impact Assessment

On 8 June 2020, the Bulgarian Helsinki Committee (BHC) sent three separate freedom of information requests (FOI), one to the CPDP, one to the Bulgarian Ministry of Health, and one to the Bulgarian Council of Ministers.

BHC asked the CPDP whether they had taken part in drafting the DPIA (GDPR Art. 35), whether it had taken part in any prior consultations (GDPR Art. 36), whether it raised any concerns in relation to the data processing and storage and whether it found the above-mentioned processing and storage of personal data to breach the GDPR.

The CPDP replied that they did not take part in drafting the DPIA. They also stated that no prior consultations under Art. 36 GDPR was carried out. They noted that they have not raised any concerns regarding the app and the data processing and storage due to the fact that "the DPA does not have such powers". Since the CPDP replied to all the questions, the BHC saw no need to appeal.

The FOI requests sent to the Bulgarian Ministry of Health and the Bulgarian Council of Ministers were identical. The BHC asked whether a DPIA was carried out and if yes, whether they could present it to them. The BHC also asked whether any prior consultations were carried out and whether the Bulgarian CPDP was consulted in the process.

The Council of Ministers forwarded the BHC's request to the Ministry of Health, explaining that they did not hold the information requested. In July, the Ministry of Health replied that a DPIA under Art. 35 (GDPR) was carried out. It also stated that there was no prior consultation carried out as per Art. 36 GDPR, because the impact assessment did not show the data processing would result in a high risk. Hence, it was not necessary to carry out such consultations. As to the request to present the DPIA, it was denied. The Ministry stated that it is not public information and the Bulgarian Freedom of Information Act does not apply in such cases.

The BHC appealed the decision by the Ministry of Health to deny the request to present the DPIA before the Sofia City Administrative court (SCAC), arguing that:

1. The decision to deny access to the information requested is unlawful;

2. The information requested is in fact public information as per the definition of the Bulgarian Freedom of Information Act;

3. The Ministry of Health holds the information requested;

4. The Minister of Health is obligated as per Art. 14 of the Bulgarian Freedom of Information Act to publish any information collected during the execution of their obligations, when it's obligatory by law to collect such information and also when a high public interest exists;

5. The BHC quoted the Guidelines on DPIA and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 of Art. 29 Data Protection Working Party, adopted in 2017. They also quoted ECtHR case law and Art. 10 ECHR.

On 31 May 2021, SCAC decided on the merits of the case and obliged the Ministry of Health to review its decision not to provide

the BHC with the DPIA. While the court proceedings were pending, the Ministry of Health provided the court with the DPIA, but it was not made available to the BHC. The court accepted that the DPIA either cited generally known provisions or copied provisions from the GDPR with few exceptions (namely art. 7.2 – the risk assessment evaluation, art. 8 – technical and organizational measures for meeting personal data risks, art. 9 – the adequate measures undertaken by the administrators for risk minimization, and art. 10 – risk assessment for the measures undertaken after the previous provisions).

The Ministry of Health reviewed its decisions and provided the BHC with the DPIA. According to art. 7.2 ViruSafe receives risk assessment evaluation "high" due to the location tracking functionality and large-scale specific data collection.

The DPIA ends with the statement that no additional measures are needed to minimise any threats for the personal data safety and evaluates the priority of the app at 3, the meaning of which is unclear.

Data security issues

As early as April 2020, personal data security issues were identified and a member of the parliament asked the MH regarding the safety of the app. Mr. Vigenin, former MEP, asked how the safety of the data is guaranteed; which institution would administer the app; how the collected data would be kept; and what guarantees are set in place that no third parties may access the data. Only a day later, the MH provided Mr. Vigenin with a rather short answer, which contained no specific explanations. According to the MH, in the development of the app all conditions of the Information Systems Cyber Security Act had been observed as well as the relevant by-laws. The MH stated that the data transfer between the users and the database was encrypted, that the server is owned by and is located at the state-owned company Information Services (Информационно обслужване) and that it is secured by a perimeter security system. Only a few users had access to the server and their activity was monitored and registered; the server was subjected to a simulated stress test by 6,000,000 users against DDoS attacks; all servers were reinforced with additional security settings.[19]

The BHC team also approached a Bulgarian IT expert, asking him to evaluate the security of the app based on the official reply of the MH. The expert stated the following:

"The reply of the Minister of Health, Mr. Ananiev, sets the goal of the application ViruSafe as 'providing statistical information to the institutions to allow them to create exact prognosis.' Based on this set goal, it seems completely unnecessary to store actual personal information in the database of ViruSafe. A well-known approach in the IT industry to avoid data leaks is to store anonymized

19 The correspondence between Mr. Vigenin and the MH may be found here.

information that doesn't reveal an individual's information (e.g. passwords, credit card numbers, etc). Such information is 'hashed' via some algorithm into a unique form that is sufficient for the purpose of the application but doesn't allow one to extract any personal information that serves as input. Security bugs and data leaks are inevitable, no matter the claims to adherence to some minimal security standards set in state's laws. That is why the only secure way to safeguard personal information is not to store it.

At a more technical level, the reply of the Minister doesn't provide any technical information that could allow one to assess the degree of security of the ViruSafe database. There is no mention of actual technologies used, and concrete measures taken, nor of any kind of security audit, or international security standard.

Some mentioned measures are irrelevant or useless for the purpose of security. For instance, preventing DDoS attacks doesn't increase the security of a system. It only increases the availability of a system. The mention of a team that can 'take measures if needed' is anecdotal – as seen in the history of many high-profile security breaches in recent years, a security breach can easily go unnoticed for months. This can also be seen in the recent data leak of taxpayer information from the Bulgarian tax office. The only thing that a team would do in such cases is to only try to minimize the consequences.

This being said, the most important information about ViruSafe is missing. The reply by the minister doesn't specify in any way exactly who, both persons and organizations, has lawful access to the collected data. While the document mentions that 'access to the server is logged and documented' it is not clear at all what access that is. Is this about the personnel that have physical access? Is it about the users that have direct access to the database server? Is this about external users with web access to the system? How do external organizations get access to the database, both from a technical and organizational perspective? With all these questions unanswered, the provided reply is useless to evaluate the dangers of collecting personal information via ViruSafe."

A new set of questions about ViruSafe

In July 2021 the BHC team asked the MH to answer some specific questions using freedom of information request, which were answered in due time. Below is a translation of the questions and answers, with some comments added where discrepancies between the published information on the app and its actual state were identified:

Question 1: On which platforms is the ViruSafe mobile app available for download?

Answer: The app is available on the Google App and Apple Store platforms.

Question 2: For each platform, from which date is the ViruSafe mobile app available for download?

Answer: The ViruSafe mobile app is available for each platform from April 2020.

Question 3: How many users have downloaded the ViruSafe mobile app as of the date of receipt or processing of this request, regardless of the platforms where it is available for download?

Answer: The mobile application has been downloaded approximately 90,000 times.

Question 4: How many active users are there of the ViruSafe mobile application as of the date of receipt or processing of this request, regardless of the platforms where it is available for download?

Answer: Over 50,000 unique users have submitted their current status about 400,000 times.

Question 5: Does the Ministry or any other institution or organization monitor the effectiveness of the application, namely, in how many cases has it successfully and actually identified SARS-CoV-2 seropositive individuals or contacts of SARS-CoV-2 seropositive individuals?

Answer: The information is tracked by the respective general practitioners (GPs) through their GP software.

Question 6: How many cases have users submitted symptom data through the app?

Answer: The number of symptom data submitted by users through the app is about 400,000.

Question 7: What is the number of symptom data submissions by users of the ViruSafe mobile app where the user has marked "Yes" for any of the symptoms?

Answer: The number of symptom data submissions from ViruSafe mobile app users where the user has indicated "Yes" for any of the symptoms is around 10,000 persons for 2+ symptoms.

Question 8: To the extent that the ViruSafe mobile app is only used to "produce the most accurate statistical analysis possible and to more quickly undo current measures and get the population back on track" and that it only "performs and provides statistical information to institutions to produce accurate forecasts," what are the purposes and functions of collecting current phone number and SSN data from app users?

Answer: The personal data is needed to connect to the person's GP software for tracking.

Question 9: Does the database storing the symptom data submitted by users of the ViruSafe mobile app allow searching for submissions by a user's phone number or unique ID number?

Answer: There is such functionality in the main registry.

Question 10: Are there institutions with access to individual (not statistically aggregated) data of individual users of the ViruSafe mobile app and if so, which ones?

Answer: The Ministry of Health and the Regional Health Inspectorates – the institutions playing a key role in the fight against COVID-19 – have access to individual (not statistically aggregated) data of individual users of the ViruSafe mobile app.

Comment: Some media reported that doctors and general practitioners have access to individualised data, which is not stated in the terms and conditions of the app[20] and is not evident by other source.[21] However, it remains unclear which institutions may have access to the personal data. This is also reported by FairTrials Report:

"In Bulgaria, the GPS location data (only collected voluntarily) and Bluetooth contact-tracing data collected by the 'ViruSafe' app is also stored centrally, by the Bulgarian Ministry of Health and 'authorized governmental institutions'. Users are required to input their personal ID, age and health information, and the developers state that all data is treated as 'strictly confidential'. However, it is unclear who the 'authorized government institutions' are. The Ministry of Health may disclose data to unknown third party service providers…". [22]

Point 28 of the Terms and Conditions of the app states that the Ministry of Health and the competent authorities for the fight against COVID-19 have the right of access to the personal data collected via the app. This is a broader wording than the answer provided by the MH. The wording of the Terms and Conditions is binding and it should be taken into account rather than the answer under the FOI procedure.

Question 11: In case there are institutions with access to the individual data of individual users of the ViruSafe mobile application, is there an established procedure for this access and if so, what is it?

Answer: Access is only granted by means of a qualified electronic signature to authorised persons involved in the fight against COVID-19.

Comment: The provided answer does not answer the question that was asked. The use of a qualified electronic signature is the means to access and does not guarantee by itself how institutions and their representative may receive access to the individualised data that is stored in the app. Therefore, we may conclude that there is no established procedure for access to individual data, as there is no

20 See the app's Terms and Conditions, Art. 30 – 33.

21 See: https://www.euractiv.com/section/digital/news/covid-19-mobile-app-available-to-governments-for-a-symbolic-euro/; https://www.imunitet.bg/контактен-на-болен-от-ковид/.

22 Fair Trials. COVID-19 Surveillance: Guide for lawyers, available here.

protocol, which establishes who permits the access, for what purpose, what duration and who may request the access.

Question 12: Does the Ministry or any other institution collect data on how many of the users of the ViruSafe mobile app who have reported symptoms have actually been quarantined?

Answer: The Ministry of Health collects such data.

Question 13: Does the Ministry or any other institution collect data on how many of the users of the ViruSafe mobile app who have reported symptoms have been proven to be seropositive for SARS-CoV-2 through medical testing?

Answer: The Ministry of Health collects such data.

Question 14: Which institution or organisation currently maintains the ViruSafe mobile app, in particular the servers where the collected data is stored, the analysis of the data collected by the app, and the technical issues and code updates of the app?

Answer: The mobile app was developed and is maintained by Scale Focus plc, who owns the copyright. The data is collected on a server of Information Services.

Question 15: Is there a plan for the possible future termination of the distribution, operation and maintenance of the ViruSafe mobile application and, if so, under what conditions will such termination take place, and will the data collected through it be stored and how?

Answer: Currently, there are no plans to discontinue the ViruSafe mobile application. Such action may be taken after the lifting of the epidemic emergency. Personal data is only processed for the purpose of fighting COVID-19. It will be used until the purpose of combating COVID-19 is achieved, and for purposes thereafter, subject to the principle of limitation of processing in time and out of cases for statistical, research and scientific purposes.

Comment: Regarding the answer to question 15, we need to point out that the Bulgarian app is listed as one that includes an explicit legal sunset clause in a case study performed by the Council of Europe based on a questionnaire sent to CoE[23] governments. As evident from the answer received by the BHC team, the MH does not plan to discontinue the use of ViruSafe app.

Regarding the security of the personal data, the main issue is that there is no known procedure for providing access to the data to third parties but still such access is possible, and the

23 Digital Solutions to fight COVID-19. 2020 Data protection report, available here.

MH confirmed that third parties have access to the data. The scope of the third parties that may receive access to the data is unknown and therefore deemed to be too broad. In order to have the security of the data guaranteed to maximum, the access to the data has to be limited and subjected to a clear procedure. Second to this come any guarantees from outside threats, e.g., viruses, hacks. Any issues that may arise from the ViruSafe app operation remains limited as a relatively small number of users have downloaded it, mainly in 2020 in the wake of the pandemic.

The Bulgarian ViruSafe is said to have failed to achieve some success in its fight with the virus. According to a representative of the IT industry in the country, this failure is due also to data protection legislative requirements that are non-existent in China, for example.[24] However, the article does not mention how similar apps operate in the rest of the European states where the same data protection requirements are at stake, but the respective apps have been shown to be more successful.

ScaleFocus (www.scalefocus.com), the developer of ViruSafe app, received an award for its development in an official ceremony held in June 2021.[25]

24 See: https://www.bloombergtv.bg/a/28-update/85865-mogat-li-tehnologiite-da-pomognat-v-reshavane-to-na-meditsinski-kazusi.

25 See: https://www.economy.bg/charts/view/46041/Vrychiha-pyrvite-profesionalni-nagradi-za-upravlenie-na-proekti-v-Bylgariya.

Estonia: HOIA

Liina Laanpere and Egert Rünne (Estonian Human Rights Centre)

Introduction

Estonia's COVID-19 contact notification app HOIA was launched in August 2020. It was created through voluntary cooperation between 12 Estonian companies, all of whom were working pro-bono, without an official procurement process. The state was represented by the Estonian Ministry of Social Affairs, as well as the Estonian Health Board and the Health and Welfare Information Systems' Centre (TEHIK), which are in the area of responsibility of the Ministry. The consortium of companies included experts in design, software development, and security: Cybernetica, Fujitsu Estonia, Guardtime, Icefire, Iglu, Mobi Lab, Mooncascade, Velvet, FOB Solutions, Heisi IT, Bytelogics and ASA Quality Services.[26] TEHIK is responsible for administering the app after its launch and providing customer support.[27]

How it works

HOIA is based on the contact notification solution DP-3T (Decentralized Privacy-Preserving Proximity Tracing), using Bluetooth Low Energy (BLE) technology. The app also uses Exposure Notification API provided by Google and Apple (GAEN).[28]

When a user activates HOIA application on their phone, the phone transmits random codes to other phones via Bluetooth radio signals. These codes are anonymous and do not include any information that could be associated with a person or location. Other phones store codes that they have received. If a phone user confirms infection of COVID-19 in the app, the application asks the user for the date of onset of symptoms, or the date of the COVID-19 test. After that, the user has to login to the national Patient Portal, through which it can be confirmed that the user is indeed diagnosed with COVID-19. It is not possible to confirm infection without a positive COVID-19 test which is registered in the Patient Portal. If the confirmation is successful, the application uploads the keys of the days when the user was infectious (48 hours before developing symptoms) to the central server, from where other phones download them to check if they have been near the user's phone. When a close contact is detected – if the signal has been sufficiently close (2 metres or closer) and long enough (15 minutes or longer) – an anonymous code referring to a close contact will be stored in the user's phone, and the app will notify the person of the close contact. The comparison of keys happens only in the users' phones. It is not revealed who the infected person was,

26 H. Kirik, Creating HOIA — *The story of Estonian coronavirus contact notification application*

27 J. Petrone, *Estonia's coronavirus app HOIA – the product of a unique, private-public partnership*, September 2020

28 H. Kirik, Creating HOIA — *The story of Estonian coronavirus contact notification application*.

with whom they were in contact, or any other information that would allow indirect identification of the infected person. The notification includes instructions to stay at home for a certain period of time and monitor health for symptoms.[29]

HOIA app notifies only the close contacts that the infected person had before they confirmed infection in the app – it is assumed that when a person has received a positive COVID-19 test result, they will stay in isolation, which is why the app stops monitoring close contacts after infection is confirmed. When the person recovers, they have the option to either download the application again or delete the data from the app settings, and the app will start working again as before confirming infection.[30]

The use of Estonia's online health system, Patient Portal, helps to make sure that the contact notifications are only coming from people with actual positive COVID-19 test results. Logging into Patient Portal requires authentication with Smart-ID or Mobile-ID. This limitation to the ways of confirming identity has been criticised in the media. The Ministry of Social Affairs has argued in response that this form of authentication is widely used – there are 500,000 Smart-ID users and 250,000 Mobile-ID users in Estonia.[31]

Data collection and processing

HOIA app is designed to minimise the amount of data collected. The data collected by the app is not personally identifiable and no new database was created for the app. The app server, which receives the anonymous codes of the infected persons, is located in the Estonian Government Cloud. If someone could access the server, they could not identify anyone's identity based on the codes.[32]

The app processes data such as the infection status, start date of the symptoms or, in the absence of symptoms, the date of COVID-19 test. All this data can be deleted anytime by clicking "Delete data" button in the application. In addition to the application, the user's phone's operating system also processes data, such as the non-personalised codes exchanged with other phones and non-personalised codes of infected persons from the app server. This data can be deleted at the operating system level of the phone.[33]

In addition, the application server processes the non-personalised codes, which are received by the server once a user has successfully confirmed a COVID-19 infection. Unlike information stored in the app or on the phone, these codes cannot be deleted from the server on demand because they are not associated with

29 HOIA documentation (Koroonaviiruse SARS-CoV-2 lähikontaktsete tuvastamise rakendus HOIA)

30 A. Pau (Delfi), *Eesti koroonahaiged on segaduses: HOIA rakendus lakkab töötamast*, 18 February 2021

31 H.-L. Allik (Postimees), *Series of flops or how HOIA failed*, 22 February 2021

32 HOIA application's home page

33 HOIA application's privacy policy

any person (the server administrator would not be able to tell which codes belong to which person). These codes are automatically deleted from the server after 14 days.[34]

Transparency and data protection

The code and documentation of HOIA application were made available under the European Union Public Licence (EUPL), including the security analysis. The code and the documentation are available at https://koodivaramu.eesti.ee/tehik/hoia. According to one of the app creators, Dan Bogdanov, the security analysis of HOIA app is arguably one of the most thorough security analyses that has been published in Estonia.[35]

The Estonian Data Protection Inspectorate has confirmed that since HOIA app does not allow users, or the state, to know with whom and when and where there has been close contact, excessive data processing has been successfully avoided. The Office of the Chancellor of Justice has also approved the app, stating that as it is not a mandatory application, there is no location tracking, and no personal data is shared, the confidentiality of both the infected person and their close contacts is guaranteed and the privacy of the application users is protected.[36]

Usability

As of 18 June 2021, HOIA app had been downloaded 278,026 times.[37] According to the Health Board, the number of downloads has been decreasing, the app was mostly downloaded in 2020.[38] There are approximately 1.325 million people in Estonia and 400,000 mobile phones in use in the country on which the HOIA app can be used.[39] In order to use the app, the phone must be based on Android or iOS operating system and usability is limited to phones manufactured in the last 5 years.[40]

A public opinion survey conducted by Turu-uuringute AS in November 2020 revealed that 27% of women and 28% of men had downloaded the app, which was most popular among residents of Tallinn (34%) and young people (43% of those aged 15-24). The survey also showed that the app was being used by 31% of Estonians, but by only one in five speakers of other languages. Of those not

34 HOIA application's privacy policy

35 TalTech IT Kolledž, HOIA rakenduse seminar, 11 September 2020

36 R. Liive (Digigeenius), *AKI peab eestlaste koroonaäppi sobilikuks, õiguskantsleri büroo jagab tunnustust*, 19 August 2020

37 Health Board, Coronavirus dataset, 18 June 2021

38 A. Veedla (ERR), *HOIA äpi allalaadimine on vähenenud*, 10 June 2021

39 S. Vedler (Eesti Ekspress), *HOIA-äppi kasutab vaid iga kümnes nakatunu*, 9 December 2021

40 ERR, *Estonia launches coronavirus exposure notification app 'HOIA'*, 20 August 2020

using the app, 40% said that this was because they doubted the app would help to restrict the spread of the virus, while 23% said that they were avoiding places in which large numbers of people congregate anyway, and 18% said they were concerned about the security of their data.[41]

The app was developed with as much respect for privacy as possible, due to which information is not being gathered about how many people who downloaded the app continue to make active use of it and how many have since deleted it.[42]

Effectiveness

As of 18 June 2021, Estonia had recorded 130,695 confirmed cases of COVID-19, 6,853 people had marked themselves as infected via the HOIA app, and there were 9 active cases in the app.[43]

The app does not collect data on how many notifications have been sent to close contacts, nor are there any data regarding how many close contacts have subsequently tested positive for COVID-19.[44] According to the statistics collected by the Health Board, they have been contacted by people who have been notified through the HOIA app 239 times.[45] However, it is not possible to know how many people have received a close contact notification through the app and not contacted the Health Board.

Neither the effectiveness nor the social impact of HOIA app has been studied.[46] The Health Board plans to analyse the impact of the app, but this has not yet been done.[47] According to the Health Board, HOIA app is so privacy-friendly that its real impact is difficult to assess, but the app has been useful in identifying close contacts that the Health Board cannot identify and sending notifications faster. The Health Board still works on contact tracing, but notifying close contacts by the Health Board could be delayed for a number of reasons – for example, infected persons might not cooperate with the Health Board, or know or remember all their close contacts.[48]

The Health Board has acknowledged that, at first, HOIA application found only 35% of the actual close contacts, but after an update

41 S. Vedler, *HOIA-äppi kasutab vaid iga kümnes nakatunu*, 9 December 2021

42 Health and Welfare Information Systems Centre (TEHIK), Response to request for information, 21 May 2021.

43 Health Board, Coronavirus dataset, 18 June 2021

44 Health and Welfare Information Systems Centre (TEHIK), Response to request for information, 21 May 2021.

45 Health Board, Response to request for information, 17 June 2021.

46 Health and Welfare Information Systems Centre (TEHIK), Response to request for information, 21 May 2021.

47 Health Board, Response to request for information, 17 June 2021.

48 G. Põlluste, G. Palgi (Delfi), *Terviseameti spetsialist: HOIA äpp on sedavõrd privaatne, et selle tegelikku mõju on lausa raske hinnata*, 21 November 2020

in March 2021 this percentage increased to 66%.[49]

Problem areas

The first problem, which arose as soon as the app became available, affected the partially sighted users. The design of the app did not make use of the Veera style guide applied to the state's e-services, making it harder for visually impaired users to use the app. The problem was that the app uses too bright a shade of blue, which can be painful for the partially sighted to look at. An accessibility audit was conducted on the app, but this problem did not manifest itself immediately and people with visual impairments were not involved in the development of the app.[50] The app's creators conceded that the criticism was justified but added that given the limited time they had to develop the app, speed and flexibility were the primary criteria.[51]

An article was published in the media in January 2021 about the partner of an infected person not being notified by the app about being a close contact. The user stated that they had marked themselves as positive as soon as they were diagnosed with COVID-19 and that the app had indicated that their status was active. The app was also being actively used by their partner, who nevertheless failed to be notified of the close contact. A representative of the Estonian Health and Welfare Information Systems Centre (TEHIK) noted that because of the way the HOIA app is structured, it was difficult to say in hindsight what had gone wrong. Since HOIA respects people's privacy, nobody can check what was done in the app after the fact.[52]

Indrek Saar, the leader of the opposition party Social Democrats, has also criticised the app, asking the Ministry of Social Affairs why the app, which got off to such a flying start, has essentially become useless. Saar noted that a public procurement to find a contractual partner to further develop had failed in January 2021. Saar's main criticism was that in order to mark themselves as positive, people needed a Mobile-ID or a Smart-ID. He found that the process should be simpler so that more notifications could be issued. He also pointed to the fact that the app can only be used within Estonia and cannot be linked to other apps.[53]

The Health and Welfare Information Systems Centre, which administers the app, has not noted any significant technical issues with the

49 C.-R. Puhm, *Terviseamet tunnistab: HOIA rakendus leidis üles vaid kolmandiku lähikontaktseid*, 26 March 2021

50 R. Liive (Digigeenius), *Koroonaäpi HOIA arendamisel ei järgitud riiklike e-teenuste stiiliraamatut, vaegnägijatel on äppi keeruline kasutada*, 28 August 2020

51 Geenius, *Koroonaäpi üks loojatest: tegime disaini osas kaalutletud otsuse ja kõige parema valiku*, 28 August 2020

52 T. Raestik, *HOIA äpp ei teavitanud nakatunu elukaaslast lähikontaktist: keegi ei tea miks*, 19 January 2021

53 I. Saar, *Indrek Saar küsib Tanel Kiigelt, miks hoogsalt startinud koroonaäpp HOIA on muutunud kasutuks*, 4 February 2021

app.[54] The Health Board finds that a notification counting system could have been built into the initial version of the app, which would have been of help in assessing the effectiveness of the app.[55]

Future

The Health Board feels that the usefulness of the HOIA app will continue to be seen at least until the end of 2021, and there are plans to further develop it in the meantime, to make the app more user-friendly and to find ways to collect statistics.[56]

In order to find a partner for further development of the app, a public procurement was carried out by the Health and Welfare Information Systems' Centre (TEHIK). An agreement was signed with some of the companies involved in the creation of the app, which will also start working on creating a cross-border solution. TEHIK will continue to administer HOIA and provide technical user support.[57]

54 Health and Welfare Information Systems Centre (TEHIK), Response to request for information, 21 May 2021.

55 Health Board, Response to request for information, 17 June 2021.

56 Health Board, Response to request for information, 17 June 2021.

57 TEHIK, *HOIA mobiilirakenduse arendustööd jätkuvad*, 9 April 202

Germany: Corona-Warn-App and Luca App

Christian Thönnes (Civil Liberties Union For Europe)

Introduction

The deployment of the contact tracing app Corona-Warn-App (CWA) has been one of the main pillars of the German government's early tech response to COVID-19.

At first glance, the merits and demerits of Decentralized Privacy-Preserving Proximity Tracing appear to be a highly specific topic of debate. The German policy process and public debate around tracing apps, however, do yield larger insights into the patterns and the state of German digital policy. Based on an analysis of the German tech response, this report shall attempt to extract some tentative lessons. These lessons could provide some guidance to civil society stakeholders and policymakers in the development and critical assessment of future state-sponsored data-driven solutions for public crises.

Tracing apps in practice – The German tech response during the first, second and third pandemic wave

During the summer of 2020, Germany was widely praised for its pandemic response. [58] During the first wave, lasting roughly from March to June of 2020, Germany had managed to flatten the proverbial curve quite efficiently. On 12 June 2020, the date of the Corona-Warn-App's release, there were about 3 known COVID-19 cases per 100,000 inhabitants in Germany.[59] However, new waves of infections arrived, trust in the government's handling of the pandemic declined and policymakers came under pressure. This way, the German debate around tracing apps was thus transformed as pandemic waves came and went. To highlight this change, it appears useful to retell and analyse the German tech response through the pandemic's main phases.

Tracing apps during and after the first wave – Off to a good start?

From the pandemic's start, German policymakers perceived contact tracing apps as a milder alternative to strict lockdown measures. How contact tracing apps were to work, however, remained a contentious topic. The Federal Ministry for Health originally proposed to oblige providers of telecommunications

58 New York Times, A German Exception? Why the Country's Coronavirus Death Rate Is Low

59 https://de.statista.com/statistik/daten/studie/1192085/umfrage/coronainfektionen-covid-19-in-den-letzten-sieben-tagen-in-deutschland/

services to share location and movement (so most likely GPS) data with health authorities.[60] After much public criticism, the German government withdrew this idea and decided to opt for app models based on Bluetooth Low Energy.

The main subject of public debate then became the choice between centralized and decentralized solutions. Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT), a centralized standard, was at first favored by German Federal Minister of Health, Jens Spahn.[61] This led a group consisting of 300 academics and numerous organizations, including the Chaos Computer Club (CCC), D64e.V., the Foundation for Data Protection (Stiftung Datenschutz) and many more to publish open letters advocating against the PEPP-PT standard and for a decentralized approach.[62]

After German officials failed to convince Apple and Google to grant a PEPP-PT-based app access to GAEN since Apple and Google limited access to decentralized apps, the German government decided to change course and opt for a decentralized, DP-3T approach.[63] The Federal Ministry of Health and the RKI commissioned SAP and Deutsche Telekom with developing a contact tracing app – and born was the plan for the Corona-Warn-App. The CWA was released on 12 June 2020.

Independent IT experts ¬– among others, the Chaos Computer Club, which is usually highly skeptical of governmental IT projects – reviewed the source code and found no significant data security or privacy risks. A detailed data protection impact assessment for the CWA was released.[64] The CWA was developed in close cooperation with the German Federal Commissioner for Data Protection and Freedom of Information (BfDI), Prof. Ulrich Kelber, who supported the CWA from the start. Until this day, at least according to public knowledge, the CWA has suffered from no significant data breaches or other security problems. The BfDI responded to an FOI that they received 122 data protection complaints. So far, these complaints have not led to any widely-reported-on or widely scandalized investigations though.

In the course of the CWA's release, a debate sparked around the adequate legal basis for its processing of personal data. The CWA processes, among other data points, IP addresses

60 The draft can be accessed here.

61 Handelsblatt, Spahn entscheidet sich für umstrittenes Corona-App-Modell.

62 Offener Brief zu Kontaktverfolgungs-Apps beim Coronavirus, accessible via: https://www.sciencemediacenter.de/alle-angebote/rapid-reaction/details/news/offener-brief-zu-kontaktverfolgungs-apps-beim-coronavirus/; https://www.ccc.de/system/uploads/300/original/Offener_Brief_Corona_App_BMG.pdf

63 Reuters, Germany flips to Apple-Google approach on smartphone contact tracing.

64 Corona-Warn-App, Bericht zur Datenschutz-Folgenabschätzung für die Corona-Warn-App der Bundesrepublik Deutschland, öffentliche Version, current version: 1.12 from 11 May 2021 (in following notes: CWA DPIA)

which are constitute personal data.[65] For this processing a legal basis is required (Art. 6 § 1, Art. 9 § 2 GDPR). The RKI considers consent (Art. 6 § 1 letter a; Art. 9 § 2 letter a GDPR) to be an appropriate legal basis.[66] There is, however, reason to doubt this claim. Several civil society actors, such as a group of legal experts led by Dr. Malte Engeler as well as the Gesellschaft für Freiheitsrechte, advocated for a formal legal basis for the app's usage, in accordance with Art. 6 § 1 (e), Art. 9 § 2 (g) GDPR.[67] This legal basis should have, in their opinion, explicitly prohibited state and powerful private actors from tying punitive measures (such as tax or insurance penalties, denials of access to public places and transportation or penalties in labor law) to non-usage of the app.

"The GDPR stipulates that there is such a power imbalance in the relationship between the state and the individual that citizens usually cannot consent to processing in a truly voluntary fashion. This becomes clear from recital 43 of the GDPR," said Mr. Engeler. "The CWA is run by the RKI, a government entity - so consent just doesn't come voluntarily."

Mr. Engeler's arguments did not fall on fertile ground. To this day, Germany has not created a legal basis for the CWA. This stands in contrast to other countries like Switzerland, which have created legal bases for their contact tracing apps.[68]

As the RKI states on page 136 of their DPIA's current version, there is no publicly available indication which would suggest that state or powerful private actors have exerted direct or indirect pressure which would have rendered the CWA's use de facto mandatory. A response by the Berlin Commissioner for Data Protection to an FOI request points in the same direction: In replying to our respective questions, they confirm that they have received no complaint which would suggest otherwise. This does not, however, make the initial legal assessment that a legal basis would be required, redundant or false. It just means that choosing a potentially inadequate legal basis did not yield severe consequences.

[This report's full-length version contains a detailed description of how the CWA works. It can be accessed here.]

65 European Court of Justice, Judgment of the Court, 19 October 2016, C-582/14, „Breyer".

66 CWA DPIA, pages 129 and following.

67 Mr. Engeler published a draft law which can be accessed here.

68 See Art. 60a of the Swiss "Bundesgesetz über die Bekämpfung übertragbarer Krankheiten" (Federal Law on the Control of Infectious Diseases), entitled "Proximity-Tracing-System für das Coronavirus" (Proximity Tracing System for the coronavirus).; accessible here.

Tracing apps during the second wave – Peculiar inaction

Throughout the summer of 2020, user numbers for the CWA were steadily rising. By September, roughly 18 million people had downloaded app.[69] This is equivalent to about 22% of the German population. While the summer and early fall of 2020 were times of relative pandemic calm, infection rates exploded in October: By 9 November, there were already 139 infections per 100,000 inhabitants.[70]

During this time, many experts proposed updates to the CWA's functionalities so that digital contact tracing could become an even more effective tool in combatting an impending second wave. Due to new scientific insights into the corona virus's dissemination dynamics, cluster recognition was chief among the functionalities demanded. For example, in an op-ed published in German weekly newspaper DIE ZEIT on 1 September 2020,[71] Henning Tillmann, along with German member of parliament and epidemiological expert Karl Lauterbach, called for numerous updates to the CWA, including an automatic cluster recognition feature.[72]

The CWA did receive some updates during the second wave: Among other things, testing laboratories became better connected (by fall 90 percent were integrated[73]), the CWA became interoperable with other European tracing apps,[74] a contact journal was added,[75] and the risk calculation method was improved.[76] A cluster recognition or event registration feature, however, was lacking among these updates.

Tracing apps during the third wave – Panic

While Germany managed to suppress their infection rates down from 167 per 100,000 on 11 January 2021 down to 57 on 14 February, by 30 March they were up to 135 again, reaching their peak on 26 April, with 169.[77] A third pandemic wave was coming. In the eyes of

69 https://de.statista.com/statistik/daten/studie/1125951/umfrage/downloads-der-corona-warn-app/

70 https://de.statista.com/statistik/daten/studie/1192085/umfrage/coronainfektionen-covid-19-in-den-letzten-sieben-tagen-in-deutschland/#:~:text=Bis%20zum%2018.,10%20F%C3%A4lle%20je%20100.000%20Einwohner

71 Die ZEIT, Vier Upgrades, die die Corona-Warn-App jetzt braucht

72 This report's full-length version contains a detailed description of how an automatic cluster recognition feature could work.

73 Ärztezeitung, 90 Prozent der Labore melden an Corona-Warn-App

74 https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1904

75 https://github.com/corona-warn-app/cwa-app-android/releases/tag/v1.10.1

76 https://github.com/corona-warn-app/cwa-app-ios/releases/tag/v1.9.1

77 https://de.statista.com/statistik/daten/studie/1192085/umfrage/coronainfektionen-covid-19-in-den-letzten-sieben-tagen-in-deutschland/

many, this renewed explosion of infection rates revealed gross incompetence and flawed management on the government's part. During the early months of 2021, trust in the government's handling of the pandemic sharply declined.[78] Consequently, during this period, responsible policymakers were under a lot of pressure to "do something" to alleviate the situation of a populace under significant pandemic fatigue.

Data protection as a political scapegoat

This growing sentiment of political anxiety and frustration created incentives for policymakers and governmental authorities to simulate action and point fingers. Many found a suitable scapegoat in data protection. In late 2020 and early 2021, there was a flurry of op-eds and statements.

Politicians like Bavarian Minister-President and then-contender for the CDU/CSU chancellor candidacy Markus Söder, or the mayor of Tübingen, Boris Palmer, claimed that all-too-strict data protection standards were standing in the way of more efficient containment strategies. They claimed that the CWA was a "toothless tiger"[79] which would be more effective if it only collected more personal data.[80]

In these articles, some Asian countries like Japan, South Korea, Taiwan or Singapore were often mentioned as having braved the pandemic better by collecting more personal data. This is highly misleading. Japan uses a decentralized tracing app; the South Korean and Taiwanese apps only monitor compliance with quarantine obligations by handing out special SIM cards.[81] In Singapore, warnings against centralized systems became reality: the police have gained access to contact tracing data.[82]

It thus becomes clear that the main gap left by the CWA was not one of too strict data protection but one of lacking updates.

78 https://de.statista.com/statistik/daten/studie/1221212/umfrage/entwicklung-des-vertrauens-in-die-bundesregierung-waehrend-der-corona-krise/#professional

79 Bayerischer Rundfunk, Söder: Corona-Warn-App "bisher ein zahnloser Tiger"

80 Other articles making similar arguments: https://www.focus.de/politik/deutschland/schwarzer-kanal/die-focus-kolumne-von-jan-fleischhauer-ahnungslos-durch-die-krise-der-verhaengnisvollste-fehler-in-merkels-corona-politik_id_12631609.html; https://www.zeit.de/2021/01/corona-kontaktverfolgung-taiwan-suedkorea-app-datentechnologie; https://www.zeit.de/2021/21/thomas-de-maziere-corona-politik-macht-grundgesetz.

81 For a summary of this debate and refutal of its central arguments: https://www.berliner-zeitung.de/wirtschaft-verantwortung/hemmt-der-datenschutz-die-pandemiebekaempfung-li.147271

82 https://netzpolitik.org/2021/polizei-in-singapur-darf-daten-der-kontakt-tracing-anwendung-nutzen/

The Luca App: Why it exists and how it works

Luca promised to fill the gap that the CWA had left by failing to integrate a cluster recognition or event registration feature.

By the spring of 2021, most of the federated states' ("Bundesländer") SARS-CoV-2 Infection Protection Measures Ordinances ("Infektionsschutzverordnungen") required hosts of social gatherings (restaurant owners and so forth), to record their guests' personal data. This was done in order to enable health authorities to conduct manual contact tracing. Up until this point, the recording of personal data had been done manually, on physical slips of paper. This in turn opened room for all sorts of privacy abuses such as stalking by restaurant owners or data transfers to law enforcement.[83]

Luca convinced many policymakers by offering to digitize this seemingly anachronistic manual contact recording process. Its PR success was bolstered by the fact that Luca was promoted by Smudo, a member of the famous German hiphop group Die Fantastischen Vier. "The main privacy problem Luca solved was preventing restaurant owners from gaining access to their guests' sensitive personal data," Henning Tillmann said.

In Luca, users can sign up with their name and contact details. All data are stored on Luca's central server. According to the Luca team, personal data are encrypted twice, thus preventing both the Luca team and restaurant owners from gaining access.

In case of an infection, it is incumbent on health authorities to initiate a decryption procedure and gain access to relevant data. Health authorities can trigger a central warning to all affected users – note that this differs from the CWA's decentralized approach where affected users are warned directly upon submission of verified positive test results without any central government entity having to intervene. Thus, while the Luca app relies on the competence (and resources) of government authorities to compel users through binding legal force, the CWA relies on individual users' responsibility to comply with their duty to self-quarantine.

[This report's full-length version contains a more detailed description of how Luca works. It can be accessed here.]

Government authorities' concerning reaction to Luca

From the start, Luca was beset with technical problems and security breaches. Among these problems were the following:

Dissatisfying key management: All Luca encryption keys are centrally managed by the Luca app team. At least initially, all health authorities in Germany were provided with the same public encryption key. This would mean that

83 taz, Lust auf Liste

a successful infiltration or deception of the Luca team – for example by faking a decryption request – could put the whole system at risk.

Movement profiles through physical keyring pendants: The Luca team offers physical keyring pendants, which are equipped with printed QR codes. Since these codes remain static, a photo of them suffices to be capable to track all check-ins that were conducted throughout the past 30 days.[84]

Code Injection through CSV files: The Luca team neglected to disable the use of special characters (such as "=") in their name registration forms which would have allowed hackers to infiltrate health authorities' IT systems with malware by programming Excel macro codes into CSV files.[85]

These and numerous other security problems led many experts to speak out: 70 leading German IT security researchers published an open letter in which they sharply criticized Luca and strongly warned against its purchase and use.[86] The CCC demanded a "federal emergency break" ("Bundesnotbremse") for Luca.[87]

All these concerns did not prevent 13 of the 16 German federated states from purchasing licenses for a combined sum of more than 20 million euros.[88] During spring, most of these federated states changed their Infection Protection Measures Ordinances specifically to allow for the manual contact data registration to be replaced with Luca. Potentially even more concerning is the role played by data protection authorities.[89] Their approval of Luca has been criticized by many experts in data protection law as being politically motivated.[90] Malte Engeler states, "The accusation that could be levelled at the Data Protection Commissioner of Baden-Württemberg is that he acted in a politically motivated manner. Data protection authorities saw the pandemic as an opportunity to get rid of their bad reputation by not standing in the way of a supposedly innovative technical solution. They also appeared to be a bit impressed by the media fuss around data protection."

84 netzpolitik.org, Schlüsselanhänger mit Folgen.

85 Die ZEIT, Hacker können Gesundheitsämter über Luca angreifen

86 Gemeinsame Stellungnahme zur digitalen Kontaktverfolgung

87 Chaos Computer Club, CCC fordert Bundesnotbremse für die Luca-App

88 Netzpolitik.org, Mehr als 20 Millionen Euro für Luca

89 His press statements are accessible here: https://www.baden-wuerttemberg.datenschutz.de/lfdi-brink-unterstuetzt-nutzung-der-luca-app/; https://www.baden-wuerttemberg.datenschutz.de/stellungnahme-des-landesbeauftragten-zur-luca-app-online/

90 Die Zeit, Luca ist leider auch keine Lösun

Tracing apps after the third wave – Belated consolidation

Right around the spring 2021 peak in infection numbers, on 21 April 2021, the CWA's version 2.0.3 was released.[91] It included an alteration of a long-called-for feature: manual event registration.

This feature enables users to scan a QR code at restaurants or other event locations. When a user receives a positive test result for COVID-19 and decides to share it via the CWA, all users who were registered in the same location around the same time are warned immediately.[92] This feature differs from Luca in two important ways: The CWA never requires users to register with their contact details. Secondly, warnings to exposed risk contacts are triggered directly after a positive test result is submitted, while for Luca, health authorities first have to trigger warnings.

It is not clear, however, that the CWA's added event registration feature contributed anything to containment of the pandemic. That is due to three reasons. Firstly, it stands to reason that the update simply came too late. As described above, by the time the update was finally released, infection rates were roughly at their peak. Only about a month later, by 1 June 2020, infection rates had sunk from 160 to 35 per 100,000 inhabitants.[93] It was therefore absent when it would have been needed most. "You would have needed the cluster recognition feature before the second pandemic wave. If it had been integrated into the CWA last fall before, then the federated states' legal bases would have been adapted to the CWA - and Luca probably would not have been needed," Henning Tillmann said.

Secondly, the update potentially could have been more user-friendly. Contrary to Tillmann's originally proposed automatic cluster recognition feature, the CWA's event registration feature requires users to actively register by scanning QR codes. According to Tillmann, "The CWA's big perk is that it just works in the background. What we proposed just doesn't require any proactive manual user activity, so it would have taken advantage of the CWA's biggest strength. The German government and SAP/Telekom could have proposed this feature to Apple and Google."

Thirdly, state authorities were very slow in making use of the CWA's added potential. Soon after the update's release, the Federal Commissioner for Data Protection and Freedom of Information as well as the DSK recommended to quickly adapt the federated states' legal bases so that manual contact registration for events could not only be replaced

91 https://github.com/corona-warn-app/cwa-app-ios/releases/tag/v2.0.3

92 Tagesschau, Im Restaurant einchecken per QR-Code.

93 https://de.statista.com/statistik/daten/studie/1192085/umfrage/coronainfektionen-covid-19-in-den-letzten-sieben-tagen-in-deutschland/

with Luca but also with the CWA.[94] Most of the German states, however, did not do so but kept the requirement to provide non-pseudonymized contact data. At the time of writing, only Saxony has changed its Infection Protection Measures Ordinance in order to allow event check-ins through the CWA.[95] As long as other federated states do not follow suit, event hosts will still be legally required to either register their guests' personal data manually or have them use Luca. In explaining the states' unwillingness to change their legal bases, Malte Engeler references the recent media onslaught on data protection law: "The framing 'data protection prevents pandemic control' had so much power that people did not dare to give up on Luca. Many responsible parties did not dare to refute this false argument. The CWA also took a lot of sustained fire and therefore some lost confidence in it. Policymakers did not realize what a treasure they had in the CWA." He believes that sunk cost fallacies also played a role: "The states had already invested several millions into Luca and it was difficult to give up on it in a way that was face-saving politically. The embarrassment of having acted too hastily and made a political mistake was simply not something to which they were willing to admit."

Most recent added features: Digital vaccination certifications and rapid test integration

With the pandemic's third wave declining and vaccination rates rapidly rising, some new features were added to the CWA including integration of rapid test results[96] and vaccination certificates.[97]

The CWA's effectiveness

The question remains whether the CWA actually helped reduce COVID infections. Answering this question is not only a hallmark of good digital policy, but also a requirement of data protection law: Interferences with the right to data protection are only justified as long as they are suitable to fulfil a public purpose.

Measuring "effectiveness" of contact tracing apps, however, is a very complex undertaking. For one, there is no central source for data. Instead, data have to be collected from different sources – some data points simply remain unknown and have to be statistically inferred.[98]

Moreover, the term "effectiveness" can mean a lot of things. "Effectiveness occurs when

94 The DSK's statement can be accessed here; The BfDI's statement can be accessed here

95 MDR, Corona-Warn-App zur Kontakterfassung – Sachsen prescht vor

96 https://github.com/corona-warn-app/cwa-app-android/releases/tag/v2.2.1; https://github.com/corona-warn-app/cwa-app-ios/releases/tag/v2.1.3

97 https://github.com/corona-warn-app/cwa-app-android/releases/tag/v2.3.2

98 This difficulty is noted here

more contacts are alerted more quickly than by manual contact tracing, and those contacts then end up 'doing the right thing'. In this sense, effectiveness depends on several factors, including technical ones – how well does the app measure risk exposure? – on the users themselves – who needs the app and do users follow instructions? – as well as on the actions of warned contacts – do they get tested or not?" said Professor Viktor von Wyl, an epidemiologist at the University of Zurich, who was responsible for evaluating Switzerland's Swiss-Covid app. "The latter also depends on societal incentives, for example whether Covid-19 tests are available for free. Effectiveness is therefore not only created by the app alone, but also by its proper embedding in the overall system." Professor von Wyl notes that most research is limited to two sub-aspects of effectiveness: "Can more people can be warned by the app than by manual contact tracing, and does the app tend to warn risk contacts more quickly than manual contact tracing?"

Numbers for the CWA

Since the CWA's release, the RKI has routinely released some CWA use parameters. At the time of writing, the most recent numbers were from 25 June 2021.[99] On this date, the CWA had been downloaded 29.2 million times. 29.2 million is equivalent to approximately 35.6% of the German population. 773,462 verified positive test results had been registered in the CWA, of which 475,151 (61%) had been shared. Due to the CWA's decentralized nature, certain data points, including how many users were warned through the CWA, were not included in these numbers.

That is why, in March 2021, the RKI launched an effort to properly evaluate the CWA's effectiveness.[100] In so doing, the RKI mainly made use of two data sources: event-independent data donations and event-driven user surveys amongst users who were notified of an increased risk.

The evaluation's results are mostly in line with other international studies[101] which demonstrated contact tracing apps' effectiveness: On

99 https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Archiv_Kennzahlen/Kennzahlen_25062021.pdf?__blob=publicationFile

100 The evaluation report can be accessed here.

101 von Wyl et al., Early evidence of effectiveness of digital contact tracing for SARS-CoV-2 in Switzerland, Swiss Med Wkly. 2020;150:w20457, accessible here; von Wyl et al., Digital proximity tracing app notifications lead to faster quarantine in non-household contacts: results from the Zurich SARS-CoV-2 Cohort Study, accessible here; von Wyl et al., The role of the SwissCovid digital proximity tracing app during the pandemic response: results for the Canton of Zurich, accessible:; Fraser et al., The epidemiological impact of the NHS COVID-19 app, Nature volume 594, pages408–412 (2021), accessible here; Rodríguez, P. et al. Nature Commun. 12, 587 (2021), accessible here.

average, each user who shared their positive test results, warned 6 other people through the app. Approximately 73% of users receiving a status warning of "increased risk" through the app, say that they were "surprised" by that warning – indicating that without using the app, they may not have registered their risk of exposure at all. Approximately 87% of users receiving a status warning of "increased risk" through the app, subsequently get tested. Out of these users who are getting tested after receiving a risk notification through the CWA, approximately 6% are tested positive for COVID-19 –which is very similar to the equivalent rate for manual contact tracing.

According to Professor von Wyl, these results point towards the CWA's effectiveness in the above-described sense. "The methodology is convincing," He said. "The fact that many users are surprised by the warning indicates that the app registers risks outside their own household, i.e. situations where people sometimes do not know each other by name. The fact that more than 80% then got themselves tested is also a sign of effectiveness. They took the warning seriously and became active." For the near-future, the RKI plans to conduct more in-depth evaluations, notably by putting their results into context with the above-mentioned international studies.

Usefulness of cluster recognition and event registration apps

Cluster recognition features have not yet been scientifically reviewed to the same extent as tracing apps' more "traditional" tracing feature. One of the most interesting questions to investigate in this regard will be whether the CWA's strictly pseudonymized and decentralized approach or Luca's centralized top-down approach help avert infections more effectively.

These two alternatives reflect an important policy choice. "The choice between centralized and decentralized event registration or cluster recognition systems depends on how much personal responsibility you trust individual citizens to bear. The central question is: Do we want health authorities in the picture or not?" Tillmann said.

Some initial evidence suggests that Luca's centralized event registration feature may not be very effective at all. This evidence largely stems from German health authorities reporting that Luca is not very helpful for them. In a survey conducted by netzpolitik.org, only 3 out of 137 health authorities reported regularly using Luca.[102] Health authorities cite poor data quality, irrelevance of the received data, poor customer support and general work overload as reasons for not regularly making use of Luca. Many health authorities report that they

102 Netzpolitik.org, Gesundheitsämter nutzen Luca kaum

usually do not work with restaurant-provided contact data lists at all.[103]

Some tentative lessons

The end of the third pandemic does not necessarily mean the end of the story of German contact tracing apps. The Delta variant might bring about yet another surge of cases, once again challenging Germany's tech response. However, some tentative policy lessons can be drawn the case study of Germany's tech response to the pandemic:

First of all, the CWA has proven that data protection law poses no hindrance to innovation or public safety. Despite all ill-considered diatribes which suggested the contrary, privacy-preserving tech responses can be just as effective as – or even more so than – surveillance machines. Developments in relation with Luca have also shown that, in order for data protection law to serve its purpose, data protection authorities must maintain their independence under political pressure. It is to be expected that politicians sometimes ponder sacrificing data protection and data security in the name of political expediency. Data protection authorities, however – while their activities are always political – may never submit themselves to these incentives. They must instead perform their vital function of oversight and counterbalance, even in the face of political adversity. During the third pandemic wave, some data protection authorities failed to fulfil that role so as not to stand in the way of "innovation". This should not happen again.

Especially when public authorities falter, an engaged and critical civil society is vital. The discourse around tracing apps was a prime example of the inestimable value of open social debate. Many positive developments – be it the rejection of invasive GPS data, suggestions for meaningful updates to the CWA, or the exposure of the extent of Luca's security problems – would not have been possible without this degree of openness and commitment. We should maintain this high level of social vigilance for future digital policy debates.

The CWA's development also highlights that democratic societies must retain sovereignty in the face of corporate power. The CWA's development during the first pandemic wave can be described as an open and successful dialogue of civil society – but it can also viewed through the prism of corporate power. While this time Google and Apple exerted their power to impose a privacy-friendly app architecture, the next time might be different.

The pandemic also revealed many things about the larger state of digitization in Germany. While app releases may garner the most publicity, they are only the tip of the digital iceberg. Responsible digital policy means more

103 Die Zeit, Luca ist leider auch keine Lösung, accessible here; for a thorough report from the health authority of Weimar: https://stadt.weimar.de/fileadmin/redaktion/Dokumente/corona/Evaluation_des_Weimarer_Modells_final_Stand20210412_1523.pdf

than making an app. Once released, public tech solutions must be continuously monitored and updated. Moreover, sound digital policy in the end comes down to the nuts and bolts of governance: spending money intelligently on critical infrastructure. Intelligent technological solutions only work in an environment where they can flourish and fundamental rights are protected. The general congestion in so many parts of Germany's infrastructure – be it schools, public administration or health authorities – has demonstrated how underequipped Germany is when it comes to digital infrastructure. The pandemic has therefore once again emphasized that public money should be spent prudently and sustainably – instead of making quick, ill-considered purchases of undercooked pieces of software from some start-up in order to performatively feign the promotion of "innovation".

Tech responses to public crises can only be targeted and effective when accompanied by thorough evaluation efforts. Therefore, empirical research must be prepared from the start. Research can be particularly challenging when it is conducted in a privacy-friendly environment. Governments should actively incentivize and promote this research by providing the necessary funding.

Hungary: VírusRadar

Ádám Remport (Hungarian Civil Liberties Union)

Introduction of the apps and (the missing) public debate

The first two month of the first wave of the coronavirus pandemic saw no governmental plans announced about a contact tracing app and, consequently, no public deliberation over introducing mobile applications to help fight against the spread of the disease.

The country's contact tracing app, VírusRadar, was launched on 13 May. The technology was given free of charge by the North Macedonian software company NextSense. The app is implemented by the Ministry of Innovation and Technology (ITM) with the support of the Hungarian IT company biztributor, and is managed by the Hungarian Government Agency for Development of Informatics (KIFÜ). According to the app's privacy policy, the data controller is the National Center for Public Health (NNK).

The app's release was not widely publicized. Consequently, the initial uptake of the app was relatively low. Only 15,000 Hungarian smartphone users downloaded the app one week after its release. In early September, the Hungarian branch of Radio Free Europe/Radio Liberty (RFE/RL), Szabad Európa, asked KIFÜ how many active users the app had and how efficient the app was at contact tracing. The outlet was not given an answer (not even to the freedom of information request Szabad Európa submitted). However, shortly after their inquiry, ITM held another press conference on the app, announcing that since May the app had been downloaded by 35,000 users. As RFE/RL reported, a few days later Google Play showed more than 50,000 downloads. Another Hungarian outlet, 24.hu found out that in September, ITM had started to encourage university students through the unified education system(s), Neptun, to download the app. By the end of September, more than 75,000 downloads had already been registered, according to the ministry's announcement.

As of mid-June 2021, Google Play showed that more than 100,000 users downloaded VírusRadar. There has still not been a governmental campaign or some noticeable governmental push encouraging Hungarian smartphone users to download the app. In the Apple Store, the app is currently unavailable.

Technical details

The VírusRadar app uses Bluetooth Low Energy to communicate with other nearby users running the application. It does not use the Google/Apple (GAEN) API most European contact tracing applications use. The app generates unique IDs upon registration, and these IDs are stored in a central database running on the servers of KIFÜ, along with the telephone numbers corresponding to the IDs. Distance and duration data relevant to infection are stored for 14 days in encrypted and anonymized format on the user's device.

If a user becomes infected with the virus, they may decide to share the data stored on their device with contact tracing professionals. During the contact investigation procedure, the data storage center decrypts the encrypted device IDs and provides exclusive access to the telephone numbers of the potentially infected people to the National Center for Public Health. Professionals will then notify users that they have been exposed to a proven COVID-19 infection and inform them of the steps they need to take (e.g., home quarantine, monitoring for symptoms, and possibly medical examinations). During the procedure, the name and details of the infected user will not be revealed to the contacts.

Reaction of data protection authorities (DPA) and privacy watchdogs

The Hungarian data protection authority (National Authority for Data Protection and Freedom of Information, NAIH) was not involved in the development of the app in any way and did not issue public statements or opinions connected to the app. Since the app was not widely advertised by the government and the uptake was consequently very low, developments around the app were not deemed to be of primary significance by the media or human rights organizations.

Uncertainties concerning the identity of the data controller

On 8 June 2020, the Hungarian Civil Liberties Union (HCLU) filed freedom of information requests (FOIs) with the NNK and the ITM requesting the data protection impact assessment (DPIA) of VirusRadar and information on other possible ongoing projects to develop further applications in relation to the coronavirus. Another aim of filing the FOIs was to find out who exactly the data controller was, as this was unclear.

The HCLU also sent a query to the NAIH, asking whether it was involved in the development of the app in any way, and if so, when the cooperation took place; whether the DPA was consulted during the drafting of the DPIA and whether the DPA had any recommendations or concerns during the process and whether these were properly addressed by the controller. The NAIH responded that it was not involved in the development of the app.

The NNK and the ITM both denied being the data controller of the contact tracing app, even though: a) according to an information note presented to the NAIH, the NNK was the data controller and the ITM had also been involved in the consultation; b) no other body can really be considered apart from these two; and c) the application's own privacy policy states that the NNK is the data controller.

In consequence, on 14 July 2020 the HCLU filed a complaint with the NAIH. The HCLU asked the NAIH to investigate who the actual data controller was; whether the DPA had

been falsely informed about the NNK being the data controller of the app; whether the app had a DPIA, and whether information had been illegally retained from them. After a lengthy, 9-month procedure – which, incidentally, revealed that the identity of the data controller had been contested by different government organs since the introduction of the app – the NAIH concluded that the ITM was the data controller. It also called on the ITM to clarify whether it was a joint controller along with other government bodies, as well as to update the DPIA and send it to the HCLU. The ITM contested the NAIH's decision – which is therefore not final – and refused to take the actions prescribed in the NAIH's note.

Questions of efficiency

In order to find out detailed information about the app, the HCLU filed a FOI with the ITM after the NAIH decided that it was the data controller. The FOI contained the questions set out by the Civil Liberties Union for Europe (Liberties):

- how many people downloaded the app;
- how many of them were active users;
- what kind of efficiency-related problems were detected and how they were resolved;
- how many positive cases were signaled through the app;
- how many of those notified as contacts self-quarantined or got tested;
- how many of them were actually infected;
- was there any sort of model calculation for the social costs of the app;
- whether there was a clear government plan for revoking the app.

The ITM refused to answer the questions citing that it did not accept the NAIH's notice and still did not consider itself a data controller.

Since turning to government bodies did not bring any results, the HCLU contacted Mr. Dániel Nemes, head of biztributor, the Hungarian company representing the app's North Macedonian developer, NextSense, to find out more about the app.

According to Mr. Nemes, the app has roughly 100,000 registered users, which corresponds with the lower benchmark of the figure shown in Google Play, which is presently at "100,000+" downloads. Mr. Nemes adds that it is not technically possible to tell how many active users there are, only the number of downloads and registrations. The difference between the latter two is thought to be a few hundred users, maximum.

Regarding the app's efficiency, the most obvious problem is the lack of users. A contact tracing application should cover the majority of smartphone users, which in Hungary would require several million active users, compared to which the figure of roughly 100,000 is minuscule. Among the reasons for the limited uptake, Mr. Nemes mentions the relative slowness of authorisation both by Google and Apple (as well as the fact that the app had to be pulled from the Apple Store because of technical difficulties), and by the Hungarian

authorities: the app was eventually launched in May 2020. This date corresponds to the end of the first wave of the pandemic in Hungary, which brings to light the second and more important reason for the app's limited penetration: the lack of communication on the government's part. Although quite enthusiastic at first, the government apparently lost interest in the application as the pandemic subsided – which is paradoxical, considering that contract tracing apps are only effective when:

- the number of new infections is low and the chains of infection are easier to track, and

- the app is widely used, covering a sufficiently large proportion of society.

Taking these criteria into consideration, the best time to advertise a contract tracing application is exactly between the waves of the pandemic. In the case of VírusRadar, this coincided with the app becoming available to the public. Nevertheless, the Hungarian government apparently abandoned the project precisely then.

It can be concluded that the almost complete lack of government publicity as well as the app not being available in the Apple Store are the main contributing factors to its minimal uptake.

As for the number of persons who (1) uploaded their positive test results to the central database (2) self-quarantined or took a test after being notified of a possible contact (3) actually became infected after a contact: these questions could only be answered by the data controller, but presently all possible candidates deny being one. Mr. Nemes has no data pertaining to these questions.

He also clarifies that he does not know of any data or model calculation relating to the social costs of the app during development, as it was developed on the initiative of the North Macedonian government by a local company, which then offered it free of charge to several other countries. Therefore, no analyses on the social impact could have possibly been made by the developer. Whether calculations were made before the implementation is a question that the data controller could answer; although, because of the relatively short time span between the development and making available of the app, the possibility that any such study has been carried out appears to be low. Whether a plan for revoking the application exists is unknown, but since it appears that the government has given up the project, it is probably safe to assume that in effect it has already been revoked. It is nevertheless unknown whether any plans for an official ending exist.

When asked about making the source code available to the public, Mr. Nemes points out that the source code is the intellectual property of NextSense, which would have probably been reluctant to disclose it publicly (although the question is hypothetical, because they received no such request). He also adds that they probably would have agreed to an audit, had such a request arrived.

The app and the social environment

As the app gained only slight attention and never became widely used, it is reasonable to believe that it did not have any meaningful social impact whatsoever. Nevertheless, as the implementation of the app is not without lessons regarding the social environment in which it was introduced, it is useful to discuss some of the phenomena encountered. It also makes sense to examine how the app could aggravate already existing social problems, should it ever be applied on a massive scale. To address these questions, the HCLU consulted Mr. Zoltán Kmetty, assistant professor and lecturer at the Department of Sociology at the Faculty of Social Sciences at Eötvös Loránd University.

Mr. Kmetty mentioned two areas where the effects of the app could be examined: data protection – or more precisely, people's attitudes towards data protection issues – and the possibility of social exclusion should access to certain services be restricted to those using a similar contact tracing app.

1. Data protection and transparency

According to Mr. Kmetty, a main sociological aspect in the case of the app (or any other technology for that matter) is people's fear of surveillance and new technologies in general. This could vary across societal groups, and less tech-savvy groups may be more wary of certain technologies. The groups potentially more prone to fear such technologies include the elderly and people living in poverty, which could lead to their exclusion from the app's benefits – which is paradoxical, since these groups are the most vulnerable to the virus.

In Mr. Kmetty's opinion, the most important issue is that Hungarian society is deeply polarised along political lines, which affects the public perception of any kind of data processing by the government. This means that people's trust depends primarily on who does the data handling, and not on its specific circumstances, safeguards or technical details. This leads to the adverse result that while it may be impossible to convince some of the safety of a certain data processing, others are going to be ready to accept it even if safeguards are not presented at all.

Both Mr. Nemes and Mr. Kmetty point to the COVID-registration website as an example: upon its introduction, the vaccine registration portal immediately raised suspicion among supporters of the opposition, who had reservations about sharing their personal data (name, address, telephone number, etc.), even though these did not include any data that the government was not already handling in at least one of its several other databases.

Since trust is dependent on political allegiance instead of the objective safety of technologies, transparency measures are expected to have little effect on the technologies' public perception. For example, publishing the source code of the app would probably do little to counter the distrust effected by the immediate triggering of ingrained political narratives. This is also because there are no organisations acknowledged across party lines to be

independent, whose "seal of approval" would be accepted by everyone. A possible solution to this problem, according to Mr. Kmetty, would be if governing and opposition parties campaigned alongside for the app – an admittedly unlikely scenario.

Mr. Kmetty adds that unlike some other countries – especially in Western Europe – Hungarians are not particularly concerned about data handling by corporations. That is unless a corporation can be tied to a political actor, in which case the above-mentioned reflexes activate.

2. Access to the app

It must be noted that in the case of accessing the app the most important divisions are along age and economic status. As with all apps, VírusRadar must be downloaded on a smartphone – which in turn excludes groups that do not have such devices. This mainly affects the elderly, but it must be added that even though smartphone use is prevalent among persons with a lower societal status, internet access is much less common. Aversion to new technologies can be higher than average in disenfranchised groups, which adds to these groups being less likely to use them.

Since contact tracing apps are most effective if they have a significant number of users, the problems outlined above can lead to an undesirable situation where precisely the groups most vulnerable to the virus are left out of the benefits of the app. This is especially alarming in the case of disadvantaged groups, as they are more likely to be in poor health and lack access to healthcare facilities. Therefore, it is to be expected that since contact tracing apps will have limited penetration in these communities, chains of infections will be traced and broken less effectively in an already underprivileged environment, adding to existing deprivation.

Exclusion may be exacerbated if the app is made compulsory or if it is made necessary to access certain services. Opportunities will be allocated to those accessing the app and divisions along economic lines may deepen. Inclusiveness may suffer if e.g. some are deprived of the opportunity to visit the same facilities as others. Such a situation would put a duty on the government to mitigate any such adverse effects and find alternative solutions to the use of the app under certain circumstances.

Technical accessibility is also of paramount importance: the needs of disabled persons should be taken into account when developing an app. Vision impairment can affect the elderly as well, which makes adequate technical solutions all the more necessary when considering accessibility issues.

Ireland: CovidTracker

Olga Cronin (Irish Council For Civil Liberties)

Privacy and the CovidTracker app

Tracking technologies can raise significant concerns about human rights, including the right to privacy. Privacy is a fundamental human right. It is central to the maintenance of democratic societies and it reinforces other rights, such as freedom of expression and information, freedom of association and freedom of thought and conscience. Data protection is a fundamental right set out in Article 8 of the EU Charter of Fundamental Rights. In addition, Article 5 of the General Data Protection Regulation (GDPR) sets out seven key principles related to the processing of personal data, which data controllers need to comply with when collecting and processing personal data. These principles are: (i) Lawfulness, fairness, and transparency; (ii) Purpose limitation; (iii) Data minimisation; (iv) Accuracy; (v) Storage limitation; (vi) Integrity and confidentiality: and (vii) Accountability.

To balance individuals' right to privacy, and other rights, with the collective right to health and life, such tools must be shown to be effective and show that they pass the tests of necessity and proportionality enshrined in international human rights law if they are to be used and continued to be used.

In late March 2020, it emerged in media reports[104] that Ireland's Health Service Executive (HSE) was planning to roll out a COVID-19 "tracking and tracing" app to assist contact-tracing in Ireland. It came days after the then Taoiseach Leo Varadkar gave his St Patrick's Day address in which he said the government believed the number of Covid cases in Ireland would rise to 15,000 by the end of the month.[105]

Over the next number of weeks, it was reported that the HSE said it would not publish the app's source code and/or Data Protection Impact Assessment (DPIA) until after the app was launched. There were also reports that the HSE had abandoned an initial plan to create a centralised app and, instead, decided to create a more privacy-respecting decentralised app.[106] At around the same time, Apple and Google had announced that they were joining forces to provide an application programming interface (API) and operating system that would enable interoperability between Android phones and iOS devices that public health authorities could use as a means for contact tracing.[107]

In addition, it emerged that a technology company based in Tramore, Co Waterford,

104 Business Post, *Phone tracking app set to be used as next step to fight Covid-19*, 29 March 2020.

105 RTE, *Ministerial Broadcast by Taoiseach Leo Varadkar about the Covid-19 pandemic*, 18 March 2020.

106 The Irish Times, *Lack of transparency will 'damage uptake' of contact tracing app*, 27 April 2020.

107 Apple, *Apple and Google partner on COVID-19 contact tracing technology*, 10 April 2020.

NearForm, would be creating the Irish app.[108] (NearForm has since outlined that, in the early stages of development, when considering what data sources could be used, "call data records from cell towers", "social media information", "ad identifiers" from ad platforms, or QR codes that people would use to check-in to locations had been considered. However, these considerations were ultimately abandoned.[109])

Privacy and data protection academics, experts and advocates warned against delaying publication of the DPIA, stating that any lack of transparency, or perceived lack of transparency, would harm the uptake of the app. This advocacy resulted in the writing and publication of an open letter in April 2020, signed by civil societies, including the Irish Council for Civil Liberties, Digital Rights Ireland, scientists, and academics.[110] The letter said the eventual app would need to respect the rule of law and human rights norms. It also called on the health authorities to ensure it would not create a centralised app; to follow the European Data Protection Board recommendations in respect of contact-tracing apps[111] and publish the app's design specifications, DPIA and source code ahead of its launch; allow for independent experts to scrutinise the same; and to ensure the app's purpose was limited so as to prevent mission creep, mandatory uptake, or discrimination against those who would not install the app.

On foot of this open expert letter, ICCL and Digital Rights Ireland, along with scientists, data protection experts, and academics, created a set of principles stating that they should be upheld by the government and legislators to ensure that any tech solution deployed as part of a public policy would be developed with human rights and robust privacy protections at the front and centre. Although the then pending COVID-19 app was the impetus for creating these principles, they were finalised with the view that they could be used to assist positive engagement with government and legislators on the implementation of any new technology developed in-house or in partnership with third parties.[112] One of the principles was that the technology would have to be effective with the experts noting that the necessity and proportionality of any technology is contingent on its effectiveness. The group insisted that the deployment of ineffective technologies erodes public trust and undermines efforts to implement solutions.

These principles included measures such as ensuring that any piece of new technology would be effective, have a clear and limited purpose, and be a necessary and proportionate

108 The Irish Times, *Why we should be slow to use tracking apps in coronavirus response*, 9 April 2020.

109 NearForm, *Total Solution to Contact Tracing*, 28 August 2020.

110 Irish Council for Civil Liberties, *HSE app: experts and public need to see details*, 29 April 2020.

111 European Data Protection Board, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, 21, April 2020.

112 Irish Council for Civil Liberties, *Principles for legislators on the implementation of new technologies*, 3 June 2020.

response to a problem. The publication of these principles led to an invitation being extended to the ICCL to meet with the Minister for Health to raise its concerns. ICCL was told that the DPIA and source code would be published before the app's launch and that ICCL and others would be given time to examine that material ahead of the launch. ICCL and Digital Rights Ireland, and others, were later invited to make a submission to a Special COVID-19 parliamentary committee specifically about the app.[113] That committee was later told that the Department of Health was confident that the expert principles were observed.

The HSE and Department of Health subsequently published significant documents on GitHub, including the app's DPIA, source code, and the feedback that the Data Protection Commissioner had sent to the HSE and department after it reviewed the DPIA. Such steps towards transparency were unprecedented and they will unquestionably be the model for all future DPIA processes by Irish authorities.

After examining this published material, ICCL and Digital Rights Ireland published a report giving the app an overall score of a C+. The report card also gave a score for how the app seemingly upheld each principle previously published by the expert group. For example, in terms of the principle of transparency, it received a B grade. For the principle that a new piece of technology would have to have a clear and limited purpose, it received a D grade. It also received a D grade for the principle of necessity and proportionality and a D grade for effectiveness.

Effectiveness

In respect of the principle of effectiveness, the report card noted that while the Chief Information Officer of the HSE said the app could "accurately detect 72% of close contacts using the Google Apple API",[114] no data had been published by the authorities to support this assertion. The report also highlighted the extensive research carried out by scientists Dr Stephen Farrell and Professor Douglas Leith, from Trinity College Dublin, showing that a 72% accuracy rate may not be possible; that it would be challenging for Bluetooth contact-tracing apps to discern whether contacts are closer or further than two metres away;[115] that app signals recorded between users can vary substantially depending on whether

113 Irish Council for Civil Liberties and Digital Rights Ireland, *Submission to the Special Committee on COVID-19 Response on the HSE/ Department of Health's COVID-19 contact-tracing/symptom-tracking app and contact tracing*, 16 June 2020.

114 Department of Health. *Department of Health and the HSE announce the publication of the Covid Tracker APp Data Protection Impact Assessment and source code*, 29 June 2020.

115 Dr Stephen Farrell and Professor Douglas Leith. *Coronavirus Contact Tracing: Evaluating The Potential Of Using Bluetooth Received Signal Strength For Proximity Detection*, 6 May, 2020.

people have their phones in a pocket, a handbag, if they are on a bus[116] or tram,[117] or if a person is standing in front of them or beside them; and that for Bluetooth apps using the Google/Apple API, false negatives, where people who have been in contact but are not detected as contacts, may be unavoidable.[118]

The report also highlighted concerns about the false positive rate, the rate at which people are falsely alerted as having been in contact with someone diagnosed with COVID-19. Given close contacts are advised to self-isolate, the report warned that the false positive figure negatively impacts the ability of people to work and visit family. It called on the health authorities to share the false positive rate detected during the app's testing and to explain how this figure was calculated.

Release and uptake

The app was launched on July 7 and, within 48 hours, it was downloaded more than one million times.[119]

Based on the decentralised Google and Apple's Exposure Notification (GAEN) system, the app is free and voluntary. When two users are within 2 meters from each other for at least 15 minutes, their devices exchange Random ID keys via Bluetooth. The keys are stored for two weeks on the memory of the respective smartphones. When a person is tested positive with the virus, they receive a code from the HSE which they can enter into the app. The users' keys generated in the previous two weeks are then sent to the app's server. Users who have been in contact with the infected person and whose phones saved one of the keys in its memory are notified of the exposure via a close contact alert. The app also has a symptom checking function. Users can decide whether they want to share real-time data on symptoms and location with the health services.

On July 21, ICCL issued a press release pertaining to new research by Professor Douglas Leith and Dr Stephen Farrell, of Trinity College Dublin, in respect of Android users of the app who must have Google Play Services – which sends highly sensitive personal data to Google servers – running in order for the app to work.[120]

The app was deleted almost 500,000 times over the following six weeks post-launch, amid

116 Dr Stephen Farrell and Professor Douglas Leith. *Measurement-Based Evaluation Of Google/Apple Exposure Notification API For Proximity Detection In A Commuter Bus*, 15 June, 2020.

117 Dr Stephen Farrell and Professor Douglas Leith. *Measurement-Based Evaluation Of Google/Apple Exposure Notification API For Proximity Detection In A Light-Rail Tram*, 26 June 2020.

118 Dr Stephen Farrell and Professor Douglas Leith. *Android COVID-19 Tracing App Pairwise Attenuations: Calibration Needed*, 15 June, 2020.

119 Irish Examiner, *HSE's Covid-19 tracing app passes 1m downloads*, 8 July, 2020.

120 ICCL, Serious privacy and data harvesting concerns about technology underlying HSE app, 21 July 2021

complaints about the app draining users' batteries,[121] but there are currently, according to the app itself, 1.3 million active users (from a population of 4.98 million). By the end of April 2021, the app states that just over 15,000 users who had tested positive had uploaded their Random IDs; and this has led to just under 25,000 users getting a close contact alert. It is not known how many people who got a close contact alert subsequently tested positive, but the HSE has repeatedly said in media reports that "some" of those close contacts have gone on to test positive. It's not known if the people who later tested positive could have been traced by any other means and/or if they were definitely traced more quickly by the app than by human contact-tracing? The app's false positive figure is also still unclear.

In September 2020, it was reported in Irish media that a school in Louth had to close to more than half its 1,200 students after more than 30 of its teachers received a close contact alert via the app.[122] Confusion ensued with some teachers getting tested and others being told that, in fact, they did not need to isolate after all, or get tested, and were free to teach. It was reported that, following an assessment of the situation, public health officials found that teachers contacted by the app were not close contacts after all. The situation led to the president of the Association of Secondary Teachers in Ireland calling for clarity around the app.

Some weeks later a "pause" function was added to the app which some healthcare workers[123] and teachers[124] were encouraged to use. Over time, the app has also brought in new features to show a breakdown of case numbers for each county; hospital admissions; hospital discharges; hospital confirmed cases; ICU admissions; ICU discharges; ICU confirmed cases; the number of tests completed over the previous seven days; and the positivity rate over the same. Since the vaccine roll-out, a new feature was included to show the number of first dose vaccinations given; and the number of second dose vaccinations given.

Data on efficacy sought

The Irish Council for Civil Liberties and Digital Rights Ireland has repeatedly sought statistics and figures from the HSE and the Department of Health about the efficacy of the app. As mentioned above, efficacy is crucial when one considers the human rights implications of any technological tool in a public health context. The necessity and proportionality of

121 Irish Examiner, Covid tracker app deleted 500,000 times, 26 August 2020.

122 RTE, *Concern over confusion surrounding close contacts at Drogheda school*, 17 September, 2020.

123 HSE, *Covid Tracker App advice for staff wearing PPE*, 28 October 2020.

124 The Irish Sun, *Teachers in schools with positive Covid-19 cases asked by HSE to turn off contact tracing app while in work*, 23 October 2020.

technological tool, such as a contact tracing app, is contingent on its effectiveness.

Specifically, the aforementioned DPIA of the app states that it collects the following 14 metrics on both a daily and cumulative basis as a means to monitor its performance and for analysis and modelling:

- Number of app downloads
- Number of app users with app active
- Number of app users who delete the app or select the 'leave' function
- Number of app users who drop out of the onboarding process
- Number of app users who have the Exposure Notification Services enabled
- Number of close contact notifications
- Number of close contact notifications who tap an in-app notification
- Number of app users within the "app contact tracing network" with a positive COVID-19 diagnosis
- Number of app users who, upon testing positive for COVID-19, uploaded diagnosis keys to other users
- Number of matched diagnosis keys per positive exposure notification
- Number of days between app notice of exposure and communication of positive test result Ratio of exposure notifications to positive cases
- Number of symptom check-ins
- Number of check-in no symptoms, check-in with symptoms

The same DPIA also states that an App Advisory Committee was to be set up tasked with overseeing the app. On 6 November 2020, the ICCL asked the Irish health authorities

(I) To outline

a. How is the Department of Health specifically measuring the efficacy of the app?

b. Of the number of people who have received close contact alerts, how many have subsequently tested positive?

c. Of the number of people who have received alerts, how many were later told, following a risk assessment, that they were not a close contact?

d. Could we please receive the minutes from all the App Advisory Committee meetings to date?

(II) The following data (or equivalent) to date in machine readable format:

a. Counts of Temporary Exposure Keys (TEK) uploaded.

b. Counts of the number of people who have requested a COVID-19 test solely as a result of an app close contact alert, and of those who are tested for other reasons.

c. Statistics on how many people test positive following a close contact alert compared to how many people test positive overall.

d. Whether or not (and if so how much) of a time difference there is between test results for those identified via manual contact tracing and those only identified as a potential close contact via the app.

e. Criteria for whether or not the app can be considered an effective tool in the dealing with the pandemic, (e.g. based on the above), and for actions to take (e.g. turning off the app) when/if it is shown to be ineffective.

As of 2 June 2 2021, answers to the questions above are still pending, despite numerous requests for the same since November. To give context to this lack of information surrounding the efficacy of the app, in April 2021, a public health doctor, who chairs the Irish Medical Organisation's public health committee, said she was not aware of a single COVID-19 case, among the 26,000 cases that had occurred in the counties of Cork and Kerry since March 2020 in which the app led to a detection of COVID-19.[125]

Meanwhile, new research on the effectiveness of the app has been carried out by Dr Farrell and Professor Leith. Based on data from the app, from October 2020 to April 2021, it shows that only a quarter of the expected number of tested-positive app users uploaded Random ID keys.

In their concluding remarks, Dr Farrell and Professor Leith write: "This data seems to further indicate that "technology-first" solutions may be ineffective and may be yet another indication that the overall process followed worldwide with BLE-based COVID-19 tracking apps was flawed, and could usefully be contrasted with the time-proven "test-before-deployment" strategy followed by those involved in vaccine development."[126]

In response to media queries, the HSE has since confirmed that "an app efficacy review" is under way and that this review will provide information on the app's performance within the entire Irish testing and tracing operation.[127] It has also confirmed that the app, as of May 2021, had cost €1.36 million to develop and maintain.[128]

Unfortunately, it's unclear if ICCL will receive answers to questions concerning the app put to the HSE, via a Freedom of Information request, because of a criminal cyber attack affecting the health service's computer systems[129] in May 2021. The request sought the minutes of each meeting of the App Advisory Committee in respect of the CovidTracker app from its first meeting in 2020 until May

125 Evening Echo, *No Cork cases from Covid App: Cork public health doctor critical of highly-publicised tracker, 7 April*, 2021.

126 Dr Stephen Farrell and Professor Douglas Leith. *Irish Covidtracker App Key Upload Shortfalls*, 14 April, 2021.

127 Irish Examiner, *Just 25% of positive Covid cases being uploaded to tracker app*, 2 June, 2021.

128 The Sunday Times, *Data scientists question €1.36m Covid tracker app*, 9 May, 20201.

129 HSE, *Cyber attack response*.

2021; all submissions provided to the committee during the same period; and any reports produced by the committee during the same period. However, for several months prior to this attack, and as stated above, ICCL has continually requested information concerning the app and the App Advisory Committee's meetings. At the time of writing, the app itself, in terms of figures showing vaccination doses and COVID-19 case numbers, has also not been updated since 11 May on account of the cyber attack.

Although we are living with a pandemic, human rights laws still apply and any interference with privacy must still be lawful, necessary and proportionate. ICCL has previously acknowledged the efforts made by the HSE and the Department of Health to create a privacy-respecting app and to also be transparent about the process. It is now time for the HSE and the Department of Health to be transparent and forthcoming about the efficacy of the app.

In ICCL's *Human Rights in a Pandemic*[130] report, published on 3 June 2021, ICCL has called for:

- The HSE and Department of Health to be transparent in respect of all aspects of the app.

- The publication of all available data related to the efficacy of the symptom tracker element of the app and outline the research methodology related to this data collection.

- The publication of details relating to the figures for the 14 metrics that the app has reportedly been collecting on both a daily and cumulative basis to date.

- The regular publication of the minutes of the meetings held by the App Advisory Committee.

- The publication of details relating to how and when the app will be wound down.

COVID-19 certificate proof of vaccination/recovery

In March 2021, ICCL wrote to the Minister for Foreign Affairs and Minister for Health to raise concerns about the potential introduction for a vaccination passport system in light of the plans at a European level for an EU COVID-19 Certificate for travel.[131] Our concerns focussed on people's right to privacy, bodily integrity, data protection, movement, and equality, and ICCL specifically called

130 https://www.iccl.ie/wp-content/uploads/2021/06/Human-Rights-in-a-Pandemic.pdf

131 ICCL, *Letter to Minister for Foreign Affairs Simon Coveney and the Minister for Health Stephen Donnelly*, March 18, 2021.

for no such vaccine certification system to be rolled out domestically.

We suggested that there was a risk that such systems would lead to mandatory vaccination by the backdoor. From ICCL's perspective, this would fundamentally reverse established Irish policy on voluntary vaccination. We called for any use of such a system to be banned within Ireland.[132]

ICCL welcomed the government's subsequent clarification in correspondence with ICCL, and in public, that Ireland's version of the EU COVID-19 Certificate, which provides for proof of vaccination, recovery or a negative test, would only be issued to those who wanted it and that there were no plans for any domestic vaccination certificate system.[133]

However, just before the Irish houses of parliament adjourned for the summer recess, this was reversed with the passing of legislation at the end of July 2021. The Health (Amendment) (No. 2) Act 2021 provided that indoor hospitality could only be accessed to people who could show proof of COVID-19 vaccination and /or recovery. A negative COVID-19 PCR or antigen test would not suffice. The Act does provide for the making of a regulation that could expand the definition of a "permitted person" to include someone who tested negative for COVID-19, but this provision has not been utilised. On 17 August 2021, ICCL wrote to the relevant minister and asked if and when such a regulation would be made. As of 17 September 2021, we still await a reply.

The bill passed without any pre-legislative scrutiny, without inclusion of amendments, and without any meaningful, democratic debate. By omitting testing, the legislation does not provide any exemption or accommodation for a person who cannot get such a vaccine for medical or other reasons including allergies; and/or people who have yet to be convinced of the benefits of the vaccine and do not wish to receive it.

Although limited by time, until 9 October 2021, at which point the government could extend the system for another three months, ICCL believes this was a significant legal change in a country that does not have mandatory vaccination. ICCL believes this legal change necessitated open, robust, transparent, democratic debate about legitimate purpose, proportionality, principles, laws and ethics but such a debate did not take place.

The main method for people to show their proof of vaccination is via the Irish version of the EU Digital COVID Certificate. However people can use the cardboard record that people receive following vaccination. People are also required to show photographic proof of identification to prove that the proof of vaccination or recovery relates to that person. It was subsequently widely reported that the certificates would be integrated into the Covid

132 ICCL, *Call for government to ban vaccine passports within Ireland*, 18 March, 2021.

133 Twitter, *Minister of State with responsibility for Public Procurement eGovernment Ossian Smyth TD*, 9 May, 2021.

Tracker app. The app's Data Protection Impact Assessment was updated to say:

"For people who want to store their DCC in digital form, the app provides a feature whereby people can choose to scan the QR code in the DCC and store its contents on their phone so they don't need to carry a paper copy of the certificates when they travel overseas. This 'DCC Wallet' feature as they are commonly known, is primarily a convenience feature and users can choose whether they want to use it or not. DCC data is held within the app and not shared."

The app currently now invites users to "register" their EU Digital Covid Certificate. ICCL and DRI have raised concerns about this and have been told that the storage functionality in the Covid Tracker app for the certificate remains separate and that there is no linking of personal data nor centralised storage of personal data deriving from the new discretionary feature on the app. However, ICCL and DRI have raised concerns with the Data Protection Commission.

Italy: Immuni and regional apps

Tommasso Scannicchio (CILD - Italian Coalition for Civil Liberties and Rights)

Introduction

Italy has been hit particularly hard by COVID-19 and in response has, throughout the pandemic, implemented some of the strictest confinement measures in Europe – sometimes aided by the use of unconventional enforcement measures, like the use of drones to monitor social distancing.

At both regional and national levels, several apps have been developed to assist in stopping the spread of COVID-19. The advent of these apps has brought with them a litany of concerns, including doubts around privacy for data supplied to each app and market crowding of apps leading to the displacement of the national Immuni app.

Regional apps

AllertaLOM

The region of Lombardy developed its own app, AllertaLOM, designed to collect data and identify potential outbreaks. Users are asked to repeatedly fill out a short questionnaire including questions about their gender, age, previous health conditions, location, if the user has been in contact with infected people and if they have symptoms. The questionnaire is anonymous, and the app does not provide for continuous location access. AllertaLOM continues to be available and has thus far been downloaded over a million times between GooglePlay and the Appstore. In Lombardy, the regional government has also obtained data from telco network operators and thus can analyse how many citizens have continued to leave their homes despite lockdowns in place.

LAZIODrCovid and others

The regional government of Lazio developed the LAZIODrCovid app that connects patients and prospective patients (those who have come into close contact with someone with COVID-19) with health professionals. COVID-19 symptom tracking apps have also emerged in the regions of Basilicata, Trentino, Valle d'Aosta, and Tuscany. In Sicily, an app originally designed to monitor people in quarantine was made available to tourists. In the event of experiencing symptoms, users could contact relevant health authorities. In Veneto, a health reporting app was created, enabling citizens to inform authorities remotely about possible symptoms. In Sardinia, another app was released and swiftly criticized for using explicit geolocation data of users.

Immuni – Italy's federal contact tracing app: Some important questions and answers

How many people have downloaded Immuni so far?

As of 27 July 2021, Immuni has been downloaded 12,168,758 times.

How many active users does this app have?

As of 27 July 2021, Immuni has approximately 20,125 active users.

What kind of operational hurdles have been encountered and how have they been overcome?

The exposure notification system is based on Bluetooth technology and thus cannot currently exclude instances of "false positive" proximity (for example incidences of people technically being within 2 metres of each other, but separated by an impenetrable barrier, like a wall, or being in separate cars alongside each other).

How many positive test results were uploaded by users of the app?

As of 27 July 2021, 101,618 positive test results were uploaded by users.

13 months into the app's operation, is there data on how many of those who received a notification either self-quarantined or got tested?

There is no official data available on this issue.

Similarly, is there any data available around how many of the people who received a notification were, in fact, infected with COVID-19?

If this information was collected, it has not yet been publicly disclosed.

13 months into the operation of the app, is there any data or modelling around the social costs around the app's use (for example, the costs of working-time lost as compared to chances of being infected)?

To our knowledge, there has been no official or unofficial attempt to calculate or estimate the social costs attributable to Immuni's operation.

Noting Immuni's challenges (lack of sufficient uptake and use for the desired impact), have any steps been taken in the direction of decommissioning the app? What are the conditions under which this process may be triggered?

Despite Immuni's challenges, it seems at present that the government intends to continue trying to revive app downloads and incentivise use by offering additional services to users via the app, similar to the approach utilized by the NHS and UK government as regards its app.

Immuni in-depth: inception and challenges

In March 2020, then Minister for Technological Innovation and Digital Transition Paola Pisano created the "Innova per l'Italia" initiative alongside the then Minister of Economic Development Stefano Patuanelli and then Minister of Universities and Research Gaetano Manfredi. Billed as a "call to the world of business and research" to find digital solutions to help stop the spread of the virus, it received hundreds of proposals, from which a group of experts, including from the WHO and the Italian Data Protection Authority ("the

Garante"), selected a proposal put forward by Milan-based start-up Bending Spoons. Bending Spoons, importantly, formed part of the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) project.

In April, a group of privacy experts and academics highlighted, in an open letter, the lack of transparency from the government around the development of Immuni, contracts around its creation and the app's information flows. The government subsequently published the source code and conducted a data protection impact assessment that it then sent to the Garante (more on this below in *'Immuni in-depth: Involvement of the Garante'*).

On April 30, the Italian government passed a legal decree that inter alia set out the rules regarding the adoption of contact tracing apps (Decreto Legge 30 aprile 2020, n. 28, art. 6). It also stipulated the Ministry of Health as the data controller. While the data processed through the Immuni app can only be used to contain COVID-19, aggregated or anonymised data can also be used for public health or scientific research purposes. In June the decree was converted into Law No. 70 of 25 June 2020.

After beta tests were conducted in the regions of Liguria, Puglia, Marche and Abruzzo at the beginning of June, Immuni was finally launched at the national level on 15 June.

This was followed by an awareness campaign launched by the national government in October to promote Immuni and encourage citizens to use the app. Many were (and are) reluctant to download the app, largely due to privacy concerns and doubts about the app's efficacy, however despite this, by 7 December 2020, Immuni had been downloaded over 9.9 million times and more than 6,000 users had shared their positive test results.

Immuni is expected to remain in effect until at least 31 December 2021, after an extension of its operation period in late 2020.

Subsequently, the Bending Spoons team concluded the free design, development and consultancy process and handed the project over to the two public Italian companies SOGEI and PagoPa under the supervision of the Extraordinary Commissioner for Emergency, the Ministry of Health and the Minister for Technological Innovation and Digital Transition.

Immuni in-depth: technical details

Immuni's system architecture is based on the decentralised Google/Apple API. The app generates temporary exposure keys (TEKs) for each user, which change several times per hour to prevent re-identification. When two users are within two metres for at least 15 minutes, their mobile devices exchange these encrypted keys via Bluetooth Low Energy (BLE).

When users test positive for the coronavirus, they receive a code from public authorities – albeit often after enormous delays of 30 days or more – which they can then upload to the app. This then triggers every person who has been in direct proximity in the last 14 days to then receive a notification advising them

of potential exposure. The app's algorithm assesses the risk of the encounter based on its duration and the distance between the two users.

The data is collected and stored on individual devices for 14 days. The app also sends, upon users' consent, epidemiological data (e.g. day and duration of exposure) and operational information (for example about the device's platform) to a central server (located in Italy and managed by SOGEI) to help the National Healthcare Service improve the app's accuracy and optimise resource allocation. The Ministry of Health then collects the data and decides for which purpose they will use it.[134]

The use of the app is completely voluntary and no personal information is required to install the app. To ensure transparency, the source code is publicly available on GitHub.

Along with those of Germany and the Republic of Ireland, Italy's contact tracing app was one of the first interoperable apps from the EU, meaning that Immuni also works in other countries with interoperable software.

Immuni in-depth: Involvement of the Garante

The Italian Data Protection Authority (Garante) was involved from the inception of discussions around the use of contact tracing apps as part of the response to the COVID-19 emergency. They formed part of the expert group that selected Bending Spoons' proposal and they were engaged in the development of the legal framework surrounding the use of contact tracing technologies. On 8 April 2020, the Garante made known its position on the use of new technologies to stop the spread of the virus at a parliamentary hearing; underlining the importance of voluntary use, data minimisation, the need for a well-defined data-retention period and a legally guaranteed purpose limitation. The Garante was also consulted by the government during the drafting of Law Decree no. 28 of 30 April 2020.

The Ministry of Health forwarded to the Garante a data protection impact assessment (DPIA) it had conducted, and based on this assessment, the Garante issued a decision on 1 June, arguing that the measures in place at the time sufficiently protected the rights of the data subjects, thus authorising the use of Immuni. It did, however, point out twelve critical issues that the Ministry would need to address within 30 days.

These included that users would need to be better informed about the functioning of the app's algorithm; better informed about the system's generation of exposure notifications that do not always reflect an actual risk (false positives), and allowed to temporarily deactivate the app. Additionally, the Garante advised that the DPIA would need more information on the data subjects' right of cancellation and that the role of Bending Spoons, Apple and

134 More details on which data is collected and stored on the central server can be found here.

Google would need to be clarified based on the accountability principle. More details on the twelve points then considered for rectification can be found here.

A lack of response from the Ministry of Health then prompted the Garante to issue a reminder that any processing of personal data without the requisite legal basis would be illegitimate and violate both European and national data protection law. Subsequently, on 19 October, the Garante announced that the Ministry of Health had still failed to address five of the twelve points.

The Ministry of Health delivered a second DPIA to the Garante on 16 October, as is necessary to guarantee interoperability. In February 2021, the updated version of the impact assessment prepared by the Ministry was finally assessed as compliant per the requirements of the Garante during informal discussions held with representatives of the Ministry, the Ministry for the Economy and Finance, the Department for Digital Transformation and SOGEI. The Garante's focus was concentrated largely on measures adopted to protect the security of the COVID-19 alert system and on new features introduced by the Ministry to simplify the use of the Immuni app by users who test positive for COVID-19, making it more effective in sending exposure notifications to close contacts.

National Rollout Progress and Concerns

The app enjoyed success right out of the gate, being downloaded 10,387,432 times between its launch and the end of March 2021. By July, the app managed to reach 11,602,915 downloads, but still, disappointingly was issuing only a few dozen notifications per day – underwhelming noting that the nation was still recording many thousands of confirmed positive cases per day. In June, only a meagre fraction of the confirmed positive cases utilised Immuni – 177 out of tens of thousands of positive cases across the nation in the same month. This confirmed what was acknowledged on Immuni's official website – that it had unfortunately become a "ghost" service.

The lack of commitment to continued promotion supporting the adoption and use of Immuni was likely at least in some part influenced by changes in government and stakeholder involvement during the rollout period. While this national incentive was driven and authorized by then Minister of Innovation Paola Pisano and developed by Bending Spoon, as aforementioned, former Minister Pisano was replaced in Mario Draghi's new cabinet, and, having handed over the project to SOGEI and Pago Pa, Bending Spoon is no longer directly invested in the project. In June 2021, in a desperate attempt to revive the public's interest in Immuni, it became possible to store the EU's digital COVID-19 vaccination certificate, the "*Green Pass*" on the app, an attractive prospect for users as the Green Pass will soon become necessary for individuals' access to Italy's recreational establishments.

This initiative has gone some way in rekindling interest in the app in that it triggered one million additional downloads within a month.

According to Luca Ferretti, an Oxford researcher specializing in contact tracing apps, who followed the progress and development of the NHS/UK app, the missing link in Italy's rollout of Immuni was a close and cooperative connection between the app and the public health system: "Without massive testing and without positive exposure codes these tools are useless. The health care system needed to track positive subjects but during the pandemic, many Italian counties have simply stopped entering codes. Without the codes, many people were not tracked, and the app did not affect the epidemic".

This much needed, but presently lacking, coordination between the health care system and the app has been made infinitely more difficult to achieve noting that, in Italy, health welfare services are provided locally by counties as a feature of a decentralised system that is coordinated by an overarching Health Ministry.

Troubling developments and emerging risks to freedom

During the first week of July, a national news item, which in typical circumstances would not have garnered much notice, managed to capture the attention of numerous law and IT contact-tracing experts and generated much-animated discussion.

The subjects of the news item were two migrants convicted of a robbery. Discussion amongst experts centered around the fact that it was the Immuni app, active on the victim's mobile phone, that had provided critical details of the exact movements of one of the convicted subjects during the commission of the crime. Specifically, it tracked him as he moved between different ATMs to make withdrawals, while his accomplice held the victim. Representatives for the subsequently convicted subjects, during their trials, raised objections about the use of data extrapolated from the app, created exclusively for public health purposes, for criminal justice purposes. Regardless, the presiding court accepted the position of the prosecutor that there was no regulation in place prohibiting the use of data from Immuni in court for criminal justice purposes. It is as yet unknown if this relatively fresh ruling has been appealed.

Poland: STOP COVID - ProteGo Safe

Krzysztof Izdebski, ePaństwo Foundation

Introduction

The STOP Covid app[135] history began in mid-March 2020 when a group of IT specialists started to work voluntarily on the technology which would support the fight against the spread of the virus.[136] The first version was released in the last days of March and contained only basic COVID information and a health diary. In parallel, the process of elaborating the actual contact tracing features started with the support of the IT community and in an open-source manner and continued as an initiative of the Ministry of Digital Affairs.[137] The first version was released in the end of April 2020. It was planned as a centralized system and was heavily criticized by IT experts and civil society organizations (CSOs). Most of their arguments referred to privacy issues.[138] It is also worth noting that already in March dozens of experts were supporting recommendations issued by a group of Polish non-governmental organizations (NGOs) on how to build tracing tools without infringing the right to privacy.[139]

Unlike with the model proposed by Google and Apple,[140] under the first versions of STOP COVID (then under the name ProteGo Safe), user identifiers were not generated locally on devices but downloaded from the Ministry of Digital Affair's server. That is, the identifiers, which were "anonymous" in concept, could be linked to an IP address - and this can point to a specific person, as the government servers have the appropriate mechanisms to request this type of data from operators. Additionally, *"while the app was advertised as 'data-free', this was not entirely true. If someone marks themselves as infected, they will have to (according to suggestions on the app's github) verify their phone number, which will also deprive them of anonymity"*.[141]

Together with releasing the first (centralized) version of the app in the end of April 2020, the Ministry of Development proposed a regulation aimed at loosening restrictions in shopping centers in which it described some privileges for persons using the app.[142] These are:

135 https://www.gov.pl/web/protegosafe
136 https://mobiletrends.pl/jak-powstawala-aplikacja-stop-covid-protego-safe/
137 https://github.com/ProteGO-Safe
138 https://panoptykon.org/protego-safe-ryzyka
139 https://epf.org.pl/pl/2020/04/06/technologia-w-walce-z-koronawirusem-7-filarow-zaufania/
140 https://www.google.com/covid19/exposurenotifications/
141 https://github.com/ProteGO-Safe/specs/issues/123
142 https://github.com/ProteGO-Safe/specs/issues/119

- A 10% higher number of people may be admitted to the premises at the same time if they have the Stop COVID (formerly ProteGo Safe) application. Such persons receive queuing privileges if there are no large crowds in the shop/ lounge.

- Placing a device with installed Stop COVID application (formerly ProteGo Safe) at the entrance to the facility in order to register by the device the customer who is a user of the application entering the facility. In the absence of the possibility of issuing such a device – printing a QR code generated from the Stop COVID application (formerly ProteGo Safe) to be scanned by entering customers.

Following protests, the Ministry of Development deleted the proposal from their website. Also in April 2020, the Ministry of Digital Affairs confirmed that new versions of the application will be built on Exposure Notification principles and finally released the application based on this principle on the 9 June 2020.[143] First only for Android users, and a few days later for iOS.

Just after the launch, we witnessed social media activity which was conducted to promote use of the application. The campaign was conducted mostly by trolls and fake accounts which praised the app and the government – and were exposed almost immediately.

According to research conducted by niebezpiecznik.pl,[144] some accounts were also active during the 2020 Presidential election campaign in Poland supporting the candidate connected with the governing party. This campaign has again led to undermine the trust in the app and relatively small number of users. For an application of this type to work, it would have to be activated by at least 60% of the population, i.e. at least 20 million Poles. It wasn't even close to 10% of this number.

How does it work?

The current application released in June 2020 is based on the Exposure Notification system. The phones of users with the contact tracking application are constantly broadcasting random IDs over the Bluetooth channel. At the same time, they are also scanning the environment, and remembering IDs of other devices that are within a distance of several meters. In this way, the devices register that they have "seen" each other. The IDs broadcast are random and changes every quarter-hour, so the owners of these devices remain anonymous.

When a user of the app is diagnosed as carrying the coronavirus, they will receive a PIN code that will allow them to upload their "sick IDs"

143 https://www.gov.pl/web/protegosafe/wszystko-w-twoich-rekach--pobierz-zainstaluj-i-korzystaj-z-aplikacji-protego-safe

144 https://niebezpiecznik.pl/post/porazek-aplikacji-protego-safe-ciag-dalszy/

to the ministry's server. Other users' phones will automatically download these "sick IDs" and check whether they have appeared in the list of IDs heard in the past two weeks. If so, the user will be notified that they have previously been in contact with someone who has been positively diagnosed.

Basic data[145]

As of 6 May 2021, the STOP COVID - ProteGO Safe application had been downloaded 2,001,470 times. Due to the design of the application and to ensure the anonymity of users, the Chancellery of the Prime Minister (acting also as the Minister of Digital Affairs since January 2021) is unable to provide the number of people who have downloaded the application. It is possible that the same person downloaded the app more than once.

As of 6 May 2021, based on data from the Google and Apple stores, the STOP COVID - ProteGO Safe application was installed on 678,504 devices. Authorities are unable to provide the number of active users, which is due to the fact of anonymity of users and "by design" lack of mechanisms to collect and download data about users of the STOP COVID - ProteGO Safe application.

Specific data obtained from users

The application by definition does not receive information about "being infected with a virus or disease caused by it".

The user is anonymous, so it is not possible to pass on information about the test result to the relevant user. The purpose of STOP COVID - ProteGO Safe is to voluntarily warn about possible contact with a person with a positive SARS-CoV-2 test result. Therefore, it is only possible to warn about a close contact (as defined by WHO and the Polish Chief Sanitary Inspectorate) with a person infected with SARS-CoV-2. Information about other diseases is not supported and available in this application. Moreover, the application does not provide information about the infection as such. However, a user who tests positive for SARS-CoV-2 may voluntarily send an anonymous warning to other users of the STOP COVID - ProteGO Safe application and similar applications used by citizens of other EU countries. The user in this case sends an anonymous Diagnostic Key. These keys can only be sent by a user who has received a PIN code from the Chief Sanitary Inspectorate (through the Contact Centre) allowing them to send the warning. This mechanism protects against false warnings being sent by people who are not infected with the SARS-CoV-2 virus.

For reasons of user anonymity, authorities can only provide the number of PINs used to send

145 Data presented in this and the following chapter was obtained from the Ministry of Digital Affairs via a Freedom of Information request sent on 6 May 2021.

a warning about close contact with a person infected with SARS-CoV-2 and the number of Diagnostic Keys sent. As of 6 May 2021, these numbers are respectively: PINs 6,951, Diagnostic Keys sent 75,599.

Diagnostic Keys are downloaded by all devices with the STOP COVID - ProteGO Safe application on which they were installed. Then an algorithm, using the data available on the device, calculates the risk of close contact with an infected person. Thus, there is no possibility of giving the number of people warned about actual close contact with an infected person.

The only information available that indicates the number of people who have been warned and have taken a virus test is the number of PINs to sign up for the test by app users. As of 6 May 2021, 4,078 such codes have been issued.

The cost of the application

As of 6 May 2021, the cost of implementation and operation of the STOP COVID - ProteGO Safe application stood at 5,944,344 PLN (about 1,316,664 EUR)

Portugal: Stayaway COVID

Ricardo Laufente (D3 - Defesa dos Direitos Digitais)

Introduction: Stayaway Covid

While many similar experiments were deployed around Europe, Portugal's case was remarkable in that the government, faced with exponential case growth, declared the app to become mandatory, breaking the EU-wide stipulation that these apps could only be voluntary. This significant measure, withdrawn five days later, was very likely a factor in diminishing the public's trust in apps controlled by government, and was followed by a remarkable nosedive in app usage in October 2020, blocking the chance for the app to have any effect on the devastating third wave that followed Christmas. There are other highlights in the app's lifetime – such as the blaming of doctors for low numbers, or the constructive feedback loop in the app's code repositories – that make the Portuguese experiment a relevant case study, which will hopefully provide good insights into if and how the adoption of similar future efforts should take place.

We start with a technical outline of the app and its development, followed by a review of factors and episodes that may help shed light on its disappointing results.

In April 2020, Portugal announced a plan to launch a coronavirus tracing app to help combat the spread of COVID-19 in the country, with a planned launch date of May 2020. The app would be named Stayaway COVID and was eventually released on 1 September 2020.

The project was brought together by:

- the Institute of Computer Systems Engineering, Technology and Science (Inesc Tec or Inesctec), leading the project;

- the Public Health Institute of the University of Porto (ISPUP), advising on ethics and health matters;

- the public Foundation for Science and Technology (FCT), financing;

- the startups Ubiwhere (specialised in IoT, smart city and urban tech) and Keyruptive (data security and cryptocurrencies).

HypeLabs, a startup in Porto, also developed a coronavirus contact tracing app, which was deployable in April 2020. There was also an announcement of another app by PricewaterhouseCoopers (PwC), along with a few other similar efforts that were not heard of again. The government favored Inesctec's digital tracing solution, as it followed the DP-3T protocol. Out of this project emerged the Stayaway COVID app.

Before Inesc Tec, the developer, rolled out the app in September 2020, the Portuguese data protection authority, Comissão Nacional de

Proteção de Dados (CNPD), recommended the adaptation of a legal framework concerning the operation of Stayaway. On this account, a legal decree was passed which laid down the Directorate-General of Health (DGS) as data controller. It also set out that the DGS regulates doctors' intervention in the app (11 August 2020).

Technical details

The app's system was based on the DP-3T protocol and later embraced the Google-Apple Exposure Notification (GAEN) API. No personal data is required to run the app. Stayaway generates temporary exposure keys (TEKs) which are transmitted via Bluetooth to other devices. Rolling Proximity Identifiers (RPIs) are generated from the daily renewed TEK. The data is stored locally on the mobile devices for a maximum of 14 days.

When a person tests positive for COVID-19, a code should be generated by National Health Service doctors, which is to be input into the patient's app; after this, people who were in close contact with the patient will be anonymously notified. For privacy reasons, once the code is inserted, the app stops tracing close contacts. After recovery, the user needs to reinstall the application to restart monitoring.

The public health system created the so-called TraceCovid system to address general IT needs for the pandemic response. As part of Stayaway's development, an add-on to TraceCovid was implemented which would allow doctors to request a code for a confirmed patient to input into their app. This system is a re-implementation of the Swiss CovidCode-UI and uses the same CovidCode-Service backend. The process is straightforward: the physician is asked to input the patient's date of initial symptoms, the date of the positive test result, and a code is generated which can be forwarded to the patient in an automated SMS message.

Both the app and the code generation server's source code is available on GitHub. The Github page was home to lively discussions between developers, critics and contributors, with comprehensive responses by the app developers.

Like other GAEN-based apps, Stayaway also depends on a closed-source API provided by Google and Apple, yet until July 2020 it was advertised as a "fully open-source project" – in August, a security report by Inesctec concedes (p.62) that there are closed parts. Concerns about the closed source nature of part of the framework were raised by CNPD and by Deco (consumer defense association); Inesctec dismissed these concerns with weak arguments; those concerns were revealed to be on point after the disclosure of the Google vulnerability in April 2021.

Support for Huawei devices without Google services (the most recent models, since Huawei stopped including the Google App Framework in their handsets) was announced, but as of the date of this report, Stayaway's FAQ still has a note promising developments, with an indication to keep checking "Huawei news".

The project's cost was 400,000 EUR, as reported by Inesctec. It was initially self-funded, but the amount was later fully covered by the public Institute for Science and Technology (FCT).

Its initial launch date was May, but deadlines kept slipping until it was finally released in early September 2020.

Key moments and takeaways

We produced a chart to depict the timeline of the application's lifetime, in order to help us – and now, the reader – better understand the progression of events. The data comes from the TACT project from Trinity College Dublin.

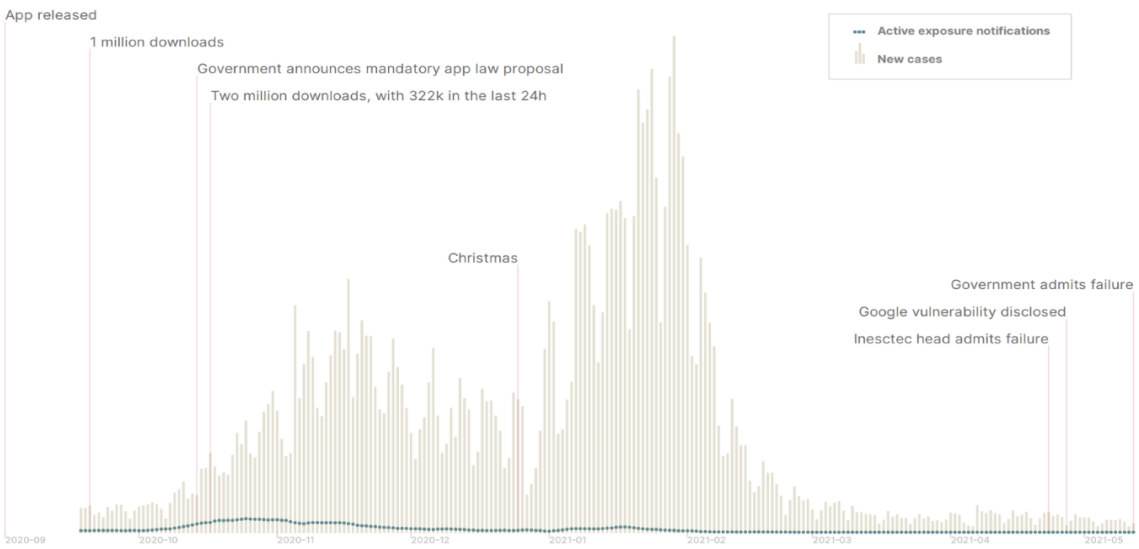
The vertical bars show the progression of the second and third waves through the count of daily new cases. The blue dots represent the active exposure notifications; each notification (activated when a COVID-19 positive patient inputs the code in the app) is active for 14 days, so this line represents the total number of notifications (not individual cases).

We will now move to a faceted analysis of key events and statements, hoping to provide a useful interpretation to help understand what exactly went wrong.

The mandatory app law turned Stayaway into a political episode.

After the government's unexpected announcement that it would put forward a law proposal to parliament to impose mandatory usage of Stayaway, confusion was immediately set. Many entities including the CNPD expressed strong reservations about the implications of this: would citizens be obliged to carry their phones? If one's phone battery ran out, would they be fined?

Public trust was further eroded by the break of a clear promise that the app would be voluntary. The other promises made beforehand – full data privacy, decommissioning the app



on pandemic end – suddenly became harder to take for granted. This episode severely hurt Stayaway's projected image of an endeavour of national/European unity and concern for each other. More importantly, Stayaway became irremediably politicised, and yet another bullet point in daily pundits' criticisms of government overreach.

While conservative and liberal (in the European sense of the word) politicians and analysts were once among the most enthusiastic public defenders of a contact tracing app in its early stages, the government's move remarkably flipped their positions into vilifying the app as yet another sign of an overreaching state – in this sense, the mandatory app incident was a godsend to any agenda critical of the current government. The government, with little political support, was facing headlines that highlighted manual contact tracing shortages (which would later require emergency reinforcements) and reports of delays and system errors in Stayaway's code generation by the public health service.

The mandatory app debacle was shelved by the announcement, five days later, that the law would not yet be put forward to parliament, and that there would be a round of consultation of civil rights organisations to measure next steps. Such consultations never took place. This move of leaving a proposal in limbo is not uncommon, since it makes more sense to try and let the issue fade from public perception rather than making an explicit statement of defeat by withdrawing the proposal – and it worked, as there were no follow-up measures and no further media interest.

Exposure code generation was a defining issue.

Shortly after the launch of Stayaway, it quickly emerged that very few exposure codes – the code that is given to COVID-19 positive patients to input in the app, to warn anyone who was close to them – were being generated, and many of those that did faced delays. Complaints appeared on social networks, with even public figures publicly protesting that they did not receive a code to activate Stayaway.

Stayaway's proponents were quick to assign blame to doctors, or the public health system in general, for the low count of exposure codes. Inesctec floated this line, remarking "People are losing trust in the app because there's no codes. Doctors are badly informed about how the apps work and where codes can be found. Since the app was launched we have doctors contacting us for help. It shouldn't be like this."

Testimonials from doctors indicate that the user interface of the code generation system was trivial to use and work with. Those testimonials also pointed to other reasons:

- Other tasks had higher priority, such as patient care, supervision and medication.
- Aversion to the mandatory app measure.
- Failure to promote the app with professionals, no support from medical associations and little training by the Minister of Health, with a few webinars to remind doctors that the tool existed.
- Unlike other TraceCovid features, Stayaway did not present any operational benefit to doctors – such as the ability to

automatically mark transmission chains – which made it into a lower priority compared to other tasks and processes.

At the same time, there were reports of code generation system downtimes, including a corroborated news story highlighting recurring server failures.

Finally, official numbers published in the press highlight a decreasing pattern. The percentage of input codes in relation to the total number of codes generated is a good measure of the public's intention to follow through in marking themselves as positive, fulfilling Stayaway's purpose. While the ratio was at 35% in early October, reaching 41% later that month; it was at 24% in January to a low of 21% in late April 2021 (we don't have complete data to have a better notion of progress).

It became evident to the layperson that the app was not fully functional.

Public messaging eliminated any reference to the app's technical workings, as the communication strategy focused around projected optimism around the app. A significant media campaign was launched with TV, print and web advertisements highlighting the need to install the app and follow its guidance. The ads' art direction was glossy, featuring relieved citizens with floating shields nodding at each other. The slogan "Stay away from covid with a single click" worked as further reassurance that the app worked.

Glowing statements about future repurposing of the system for other diseases, or employing the app to avoid full-scale school quarantines, conveyed an adamant belief in the app's full effectiveness. Such optimism remained even after the app's numbers were dwindling. As the third wave subsided, "What went wrong?" articles started appearing in the media in December, along with other critical perspectives by former advocates.

It is now clear that people ought to have been better informed of the app's technical limitations. Those existed and were well known:

- Stayaway and similar apps are ineffective inside trams and other public transports.
- Many false positives and negatives are to be expected, since crowds make signal detection harder, the Bluetooth easily penetrates barriers and is easily smothered by specific materials, such as a metal purse.
- Even with perfect usage, detection might not happen: keeping a "positive" phone centimeters away from a "negative" one might not trigger the activation of the "negative" one, due to wildly varying environmental factors such as reflective wall materials or signal interference from other devices.

This last point was discovered when several identical cases appeared on social media networks: a member of the family was positive and input their code, but the family members (who had verifiably stayed in close contact to the infected person) did not receive an exposure notification. Meanwhile, the media campaign concentrated on an abstract positive outlook

instead of preparing people for a sometimes imperfect experience.

A false sense of security caused by the app's interface metaphor.

The user interface relied on a "green light" / "yellow light" system to display whether any exposure signal was detected. However, while there was a text message that "green light" only meant that the app did not detect any positive case (as there might well have been many actual exposures that the app did or could not identify), the use of the green light interface metaphor contributed to a false sense of security – a hypothesis that is neatly underscored by the Prime Minister's remarks on 18 September 2020: "I use [the app], and it is with great satisfaction that, every morning, I have verified that until today I have not been close to anyone that could be a contact risk".

It is reasonable to argue that employing the familiar metaphor of traffic lights, with green meaning "safety", was not only unnecessary but detrimental to the app's effectiveness in properly informing people.

Blame was liberally assigned yet missed the target.

There were ample complaints by Inesctec about how doctors were the reason for the low number of exposure codes that were generated. Fingers were also pointed at data protection authorities. And so far, no party has explicitly admitted responsibility in the app's failure. The government's admission only went as far as to recognise that the app did not work as expected. Stayaway's health and ethics advisor (Henrique Barros, a highly regarded doctor and researcher) still held that the app "must continue", remarking that "health professionals cannot keep on being a source of problems".

In the interview where the app's failure was admitted, Inesctec lead Rui Oliveira justified the low code generation with two factors: insufficient mobilisation around the app inside the public health system, and excessive privacy concerns blocking both the involvement of private testing labs in code generation, and the automatic issuance of codes without physician input. In the same interview, Oliveira claimed that only a third of generated codes were actually shared by patients – a proportion that official numbers reveal to be less than one fifth, as outlined above. The explanations by Inesctec focused on bottlenecks in code generation, but it's in code input numbers that one can find clear insufficiencies.

This was not the only persistent issue that went unacknowledged. Another one was the effect of the app's technical limitations, that the public came to understand by first-hand experience. There was also no mention of the social effect of the move to make Stayaway mandatory.

No serious analysis of the Stayaway experiment can ignore both of these as likely causes of heightened public distrust in the app as demonstrated both by the dwindling numbers of exposure codes shared by people, and the insignificant usage numbers throughout the third wave. Without public trust to sustain

mass adoption, even a functional app would fail.

It was never clear who was ultimately responsible for the app.

Over the project's lifetime, there was confusion as to whom was operating the app – Inesctec, the Government or the Ministry of Health. Many public announcements concerning the app were made by Inesctec's directors or the Prime Minister himself, instead of the Health Minister or General Director of Health, whose statements on the matter focused mostly on reporting usage numbers and encouraging widespread adoption.

This confusion was exacerbated by the announcement of mandatory use. While the Prime Minister was the public face of this move, Inesctec's directors quickly distanced themselves, describing the move as "a political decision" and having been "taken by surprise", with the app's health and ethics advisor himself joining the protests.

Finally, the Google Play Store app page has an account named "FCT FCCN" (a division of the FCT, the project funding institution) officially responding to the many user comments, adding to the mix of entities with public roles in the project.

During the Stayaway experiment, manual contact tracing efforts faced severe shortages.

Stayaway was persistently sold as a secondary measure to reinforce manual contact tracing efforts – especially when addressing shortcomings and problems with the app.

However, manual contact tracing had ongoing human resource shortages even before the third wave: in November, the national army joined the contact tracing efforts, along with special measures to involve nursing college students and high school teachers without experience in health care. It will probably remain unknown whether this situation could have been mitigated if part of the available budgets and public attention were not diverted to a contact tracing app.

Two relevant vulnerabilities with varying reception.

In April 2021, a significant vulnerability in Google's Contact Tracing API was disclosed by researchers from AppCensus. The risk of working with black-box APIs controlled by external entities was articulated by the CNPD as early as June 2020. The incident also suggests that Google's API code was not audited by Portuguese authorities, nor was any independent supervision in place to assess the vulnerability's impact – only Google could now shed light on whether there was any leak or exploit, we found no sign that they've done so.

On 10 May 2021, another security vulnerability was published, discovered by Henrique Faria, a Cybersecurity Masters student at the Polytechnic Institute of Viana do Castelo. It affected the Google Exposure Notification framework itself, affecting Stayaway and all other identical apps around the world. The practical consequences of the Faria

vulnerability are, however, very limited: the discovered flaw "allows an attacker to interrupt the Bluetooth transmission of GAEN (…) with a malicious application installed on the same device". This means that there seem to be no practical risks other than disrupting beacon transmissions – no beacon or PII leaking, for instance. Moreover, the requirement for a malicious app implies active exploiting by bad players, which is a weak scenario to serve as an example of these apps' fragilities.

Nevertheless, the story gained traction on social networks, fuelled by the angle of national academic excellence along with the "student finds flaw in government app" trope, which again fed into critical narratives around the app's effectiveness. Many news outlets, including prime time TV news, featured this vulnerability, whereas the previous Google flaw saw minimal airtime. The story broke a day before the government finally admitted that the app did not work as expected.

The data protection authority's risk scenarios were accurate.

The CNPD was not given much space to have a say on matters; right from the start, the formal request by government for CNPD validation was done in the same day that the law was approved, with the commission politely arguing that there is much less of a point to get a data protection evaluation for a law that was already passed.

Even having been mostly sidelined, with its feedback sought only when legally mandated, the CNPD's input was key to ensure that only doctors could validate infection status, clarify data protection insufficiencies in the early proposals, and set voluntary adoption as an essential requirement. Three months before the app's release, the commission clearly identified the GAEN dependency as a major issue, pointing out that "there is a crucial part of the application that isn't controlled by its authors", a point validated by the later discovery of the vulnerability in Google's framework which leaked active exposure notifications.

It is reasonable to argue that, along with a health and ethics advisory entity, Stayaway (and any similar future endeavours) could have integrated at least one person, ideally from CNPD, to advise on data privacy matters. The current feedback loop of working inside closed doors and only asking for feedback when the application is almost done leads to obvious inefficiencies; instead, such concerns must be present at the planning stage, long before the first line of code is written down.

Slovenia: #OstaniZdrav

Iza Thaler (Peace Institute)

Introduction

The Slovenian contact tracing app #OstaniZdrav, launched on 17 August 2020 for Android and since the beginning of September 2020 for iOS users, alerts active users if they have been in contact with a person who tested positive for the SARS-CoV-2 virus. Smartphone devices with the installed application, which are located close to each other, communicate with each other using unique codes. If one of the exchanged codes belongs to a user who has indicated in the app that he is infected, the owner of the other code will receive an alert that he was in the vicinity of an infected person. The app does not disclose either the location or the time of the meeting.

Even though the app does not only process personal data, but particularly sensitive personal data, Slovenian government did not conduct a Data Protection Impact Assessment (DPIA)[146] before creating a legal basis for the app and did not involve the Information Commissioner (IC) in the process of drawing up the bill or in the process of introduction of the app in any way. The public was excluded as well. For a long time, it was unclear what type of an app will even be introduced and with what purpose. The idea of massively tracing individuals' locations was abandoned very late, generating frustration and distrust in the public. Meanwhile, the Prime Minister tweeted: "*Opposing the digital application is the same as opposing compulsory vaccination against infectious diseases. It endangers everyone's health*",[147] shutting up voices calling for inclusion of civil society and experts and a reflection and careful introduction of untested technological 'solutions'.

Months after the introduction, the experts mainly agree that the app is technologically sound, but they seriously question the efficiency of the app[148] and warn of technological solutionism.[149]

146 Article 35, GDPR: "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."

147 Ivan Soče, Covid aplikacija ni rešitev, je težava, Večer, 2. 8. 2020, available here, accessed on 20. 7. 2021.

148 Mladina, Je aplikacija #OstaniZdrav res učinkovita?, 10. 10. 2020 ; Metina lista, Meta PHoDcast 124: Pika Šarf, 11. 2. 2021, both accessed on 20. 7. 2021.

149 Aleš Završnik, Pika Šarf: Social Surveillance in the Time of COVID-19. Journal of Criminal Investigation and Criminology, available here, accessed on 20. 7. 2021. Metina lista, Meta PHoDcast 124: Pika Šarf, 11. 2. 2021, available here, accessed on 20. 7. 2021. Kristina Božič, Aleš Završnik: Zelo hitro smo od skrbi za posameznika, ki zboli, prešli k temu, da ga moramo nadzirati, Večer, 24. 4. 2020, available here, accessed on 20. 7. 2021.

There are plenty scenarios where the app can't help. If we don't have a phone with us. If we don't have Bluetooth turned on. If the app is not installed by enough users. It also depends on the people who have tested positive receiving and uploading their TAN codes.[150] False positive results are also possible. Bluetooth signal can travel through the walls, but viruses cannot; a turned-on phone can be left in another room, etc. It is not to be overlooked that Bluetooth was not initially created for this purpose. Monitor magazine commented already in September 2020: "T*he app records the duration and proximity of contact with other phones that have the app. Anything more is a matter of discipline in use and interpretation. The app will not secure us against anything individually, but it can contribute a very small piece to the mosaic of measures. Much smaller than hand washing.*"[151]

In the report we will further analyze and discuss issues of efficiency, protection of fundamental rights and how the introduction and operation of the Slovenian version of the contact tracing app fits to the concept of responsible governance.

Methodology

In the process of drawing up the report, we have filed FOI requests with the Ministry of Public Administration, which is the state institution, competent and responsible for the contact-tracing application. Further, we have filed a FOI request with the National Institute of Public Health (NIJZ), which is competent to advice the government in situations of epidemiological crisis and regularly participates at the daily government press conference, urging the public to install the app. We have interviewed a public official at the Slovenian Information Commissioner.

Pika Šarf, Junior Research Fellow at the Institute of Criminology in Ljubljana, directed us to her article, which she wrote together with Aleš Završnik, PhD, the Director of the Institute, "Surveillance in the time of COVID-19". The article complemented and contextualized our desk research of scarce sources on the topic of the contact tracing app in Slovenia.

How the app #OstaniZdrav works

The app #OstaniZdrav alerts users if they have been in contact with an infected person. The app uses Google's and Apple's Exposure Notification system, relying on Bluetooth Low Energy (BLE), without recording the users' location or identity. The Exposure Notification system generates a daily Temporary Exposure Key (TEK), from which it generates a transmission code (Rolling Proximity Identifyer - RPI) every 10 minutes. This code is a condensed value of the daily key and is

150 Per example in November 2020 about two third of issued TAN codes were uploaded into the app.

151 Monitor, Z aplikacijo nad korono, 30. 9. 2020, available here, accessed on 20. 7. 2021.

additionally encrypted along with the time interval.[152] This is a precaution because a unique daily key is still only pseudo-anonymous, and it would theoretically be possible to track the moving of a phone (through a chain of exchanges of keys).[153] When two persons are close to each other (approximately 1.5 meters) for 15 minutes or longer, their mobile phones exchange the encrypted transmission codes via BLE. The distance between the devices is estimated based on the strength of the Bluetooth signal.[154]

When a person tests positive with the virus, they receive a Transaction Authentication Number (TAN) code from the National Institute of Public Health, either together with the test result in a message or call or they can request it via an online form. They must enter the TAN code into the app within 3 hours.[155] Once the code has been entered into the app, users who have been in close contact within the last 14 days are notified about the risky exposure.

Optionally, the user can enter the date of the onset of symptoms so that the app can determine the level of risk more accurately. If not, the daily keys are assigned a default value of infectivity.[156] The transfer risk is the lowest 14 days from entry of TAN code and then escalates and is highest on the second, third and fourth day before the entry of the confirmed infection. The app also considers the length and proximity of the contact, using these three factors to calculate whether the risk is high enough to issue an alert.[157] If a user is alerted of an exposure, this information is not shared. The exposed contacts are not tested or quarantined, but the person can opt for self-isolation and pay more attention to the symptoms. Thus, there are no concrete consequences for the user whose phone has been exposed to a risky contact.[158]

It was prepared by the National Institute of Public Health (NIJZ) and the Ministry of Public Administration (MJU), with NIJZ taking care of the content part of the application, and MJU for the technical. Both are common data controllers.[159] The app was adjusted from a German version of the contact tracing app by a company RSteam and the difference with the German version is in fact only in language.[160]

152 Ministry of Public Administration, The workings of the app, available here, accessed on 20. 7. 2021

153 Monitor, Z aplikacijo nad korono, 30. 9. 2020, available here, accessed on 20. 7. 2021.

154 Ministry of Public Administration, The workings of the app, available here, accessed on 20. 7. 2021.

155 Ministry of Public Administration, The workings of the app, available here, accessed on 20. 7. 2021

156 Ministry of Public Administration, The workings of the app, available here, accessed on 20. 7. 2021.

157 Covid-19 sledilnik, Aplikacija #OstaniZdrav, available here, accessed on 20. 7. 2021.

158 Matej Kovačič, OstaniZdrav - Slovenska aplikacija za sledenje stikom. Telefoncek.si, available here, accessed on 20. 7. 2021.

159 Notice on data protection, available here, accessed on 20. 7. 2021.

160 Monitor, Z aplikacijo nad korono, 30. 9. 2020, available here, accessed on 20. 7. 2021.

But a data security expert cautioned that the adapted version of the German app was not the most secure amongst all the versions.[161] Since 10 February 2021, the updated Slovenian version of the app is connected to the European server and thus includes the ability to share codes with all apps using the Google's and Apple's Exposure Notification system. In practice, the app still communicates only with the Slovenian server, which is synchronized with the European server once a day.[162] In May 2021 the app was updated with two new features: statistics, which show data on how many users have entered their TAN codes and a diary of meetings, where the user may enter information about the people they met and the places they visited. The purpose of the latter is to serve as a digital aid in the event of a confirmed SARS-CoV-2 infection, so that the user can better remember his contacts and inform them of the exposure. The meeting log also shows the user's risk status on each day. The data entered in the meeting log is only accessible to the user.[163]

As described above, the app follows a decentralized approach, the keys are stored only locally on users' smartphones, preventing authorities or other parties from accessing the data. The application's source code is published on Github.[164] Installation is free of charge and voluntary, although, as it will be shown below, the latter could be up for debate.

Efficiency under question

There were 383,769 downloads of the app by 22 July 2021.[165] There is no data on the number of active users of the app,[166] but if we counted each download as one user, the percentage of the population that has installed the app after almost a year would be only about 18 percent. The percentage is likely even lower, because surely there are users who have downloaded the app more than one time. Besides, the above numbers and percentages are silent about active usage of the app, seeing that for a person to actively use the app several conditions must be met. First the mobile device must be turned on and carried around on the user's body, exposure logging must be enabled, and Bluetooth must be turned on.

161 Matej Kovačič, OstaniZdrav - Slovenska aplikacija za sledenje stikom. Telefoncek.si, available here, accessed on 20. 7. 2021.

162 Monitor, Aplikacija #OstaniZdrav podpira tudi druge evropske države, 13. 2. 2021, available here, accessed on 20. 7. 2021

163 Ministry of Public Administration, Mobilna aplikacija #OstaniZdrav odslej v različici 1.14.3, dodano spremljanje statistike in dnevnik srečanj, 21. 5. 2021, available here, accessed on 20. 7. 2021.

164 Available at: https://github.com/si-covid-19/ostanizdrav-android

165 Goverment Communications Office, Mobilna aplikacija #OstaniZdrav, 30. 7. 2020, available here, accessed on 23. 7. 2021.

166 Ministry of Public Administration answer to FOIA request on 28 May 2021.

The data controllers only started to count the number of entered TAN codes (uploaded positive test results) on 7 April 2021, and in the period between April and July 2021 around 2,000 TAN codes were entered into the app.[167] In the same period, around 31,900 TAN codes were issued by NIJZ, which means only around 6 percent of app users upload the fact that they have been infected.[168]

The Ministry of Public Administration explained that due to the decentralized approach, they do not collect data on how many users received an alert about a high-risk contact and what did they do after the alert (whether they have self-isolated or got tested).[169] They also do not collect data on how many users received the alert and later tested positive.[170] The Ministry as well reported that data on the social costs of the app cannot be gathered due to the decentralized model of the app; therefore, there is no model calculation on the social costs of the app (the costs of working-time lost vs. chances of being really infected, etc.).[171]

It is therefore difficult to assess the effectiveness of the app, beyond the fact that less than 18 percent of the population has downloaded the app and that apparently even its users do not use it the way they are supposed to. It is the position of the Ministry that "*[a] mere one active use of the #OstaniZdrav app, which would break the chain of possible SARS-CoV-2 virus infections, means that the app, [...] has achieved its purpose.*"[172] NIJZ, on the other hand, reflected that there should be more support in development of new functionalities (e.g., location check-in) and more support in the development and promotion of voluntary use of the app: "*Only in this case, the application will play a relevant role as an additional tool in limiting the spread of the virus.*"[173]

Statistically relevant data that would allow for an assessment of the efficiency of the app could have surely been gathered through other means than only a centralized server. For example, people who test positive could have been surveyed by NIJZ epidemiologists during the standard call, whether they were tested due to an app alert; a nationwide survey could have been done by the Ministry to gather data

167 Detailed and continuously refreshed data can be accessed on OPSI - Slovenian Open data hub, available here, accessed on 23. 7. 2021

168 Statistical data of the app #OstaniZdrav, National Institute for Public Health. Available here, accessed on 23. 7. 2021

169 Ministry of Public Administration answer to FOI request on 28 May 2021

170 Ministry of Public Administration answer to FOI request on 28 May 2021

171 Ministry of Public Administration answer to FOI request on 28 May 2021.

172 Ministry of Public Administration answer to FOI request on 28 May 2021.

173 National Insitute of Public Health answer to FOI request on 5 May 2021.

on practical use of the app to understand what hinders its use, etc. The issues of (in)efficiency were brought up by experts as well[174] and they closely relate to the notion of responsible governance.

How the introduction and operation of #OstaniZdrav fits to the concept of responsible governance

The United Nations Human Rights Council has identified *transparency, responsibility, accountability, participation*, and *responsiveness* (to the needs of the people) as the key attributes of good governance.[175] According to United Nations Economic and Social Commission for Asia and the Pacific, good governance is measured by the eight factors: participation; rule of law; transparency; responsiveness; consensus oriented; equity and inclusiveness; effectiveness and efficiency; and accountability.[176]

Introduction of a new technology, with discussion or even introduction of obligatory use, evident data protection issues coupled with lack of transparency immediately invite doubts about rule of law, right to privacy, but also dignity of a person or a community of people.

Leading Slovenian experts have identified requirements for the ethical use of apps for digital tracking. These requirements are, for example, monitoring the operation of the app (via an inclusive and transparent advisory committee comprising representatives of the public), unfolding the ethical principles that underpin the measure, explaining its costs and benefits to the public, ensuring equal access to the application and equal treatment in case of infection, the use of a transparent algorithm and thus subjection to auditing, periodic evaluations and research of interventions to better inform app operators, oversight and effective remedies.[177]

Some of the most prominent issues with the introduction and operation of the app #OstaniZdrav

The Information Commissioner (Slovenia's data protection authority - DPA) had issued an opinion on several discussed options of apps that could be used to help limit the spread of the corona virus already on 9 April 2020, highlighting the importance of a DPIA and transparency for the introduction of a contact tracing app.[178] Nevertheless, on 9 July 2020, the Slovenian parliament adopted the

174 Metina lista, Meta PHoDcast 124: Pika Šarf, 11. 2. 2021, available here, accessed on 20. 7. 2021.

175 OHCHR, About Good Governance, available here, accessed on 20. 7. 2021.

176 UNESCAP, What is Good Governance? 2009 Report, available here, accessed on 20. 7. 2021

177 Aleš Završnik, Pika Šarf: Social Surveillance in the Time of COVID-19. Journal of Criminal Investigation and Criminology, p. 47-48. Available here, accessed on 20. 7. 2021.

178 Reich et al., COVID-19 Technology in the EU: A BITTERSWEET VICTORY FOR HUMAN RIGHTS?, Civil Liberties Union for Europe, May 2021, available here, accessed on 20. 7. 2021.

Act Determining Intervention Measures to Prepare for the Second Wave of COVID-19 (Fourth COVID-19 Act), creating the legal basis for the use of a contact tracing app without including the DPA in the procedure and without conducting a DPIA.[179] The IC learned of the introduction of the app through media.

What is more, according to the law, people who tested positive with the virus or were currently in quarantine were obliged to download and use the app.[180] Not only did this measure only confirm the suspicions of many, that epidemiological measures were being used to turn Slovenia into a police state, such a measure is also completely useless as active use of the app makes (limited) sense only if we use it before we become infected, not when we are already infected and quarantined.

A DPIA was in the end conducted in July, but only after the adoption of the legal basis.[181] Public Administration Minister Boštjan Koritnik announced that the app would be voluntary for everyone and in the government's communications the voluntary aspect of the app has been consistently brought up. But the IC warned in its opinion on 31 July 2020, it is unclear how the infected person will be obliged to act in practice if a government representative publicly says that the use of the app is voluntary, and at the same time a law has been passed stipulating that as an infected person he must install the app and enter the code (with fines of 100 - 600 EUR).[182] The law has not been changed since.

In December 2020, the government introduced measures that seriously disputed the notion of voluntary nature of the app. At the time, movement was restricted to municipalities. However, on proposal of the Ministry of the Interior, the government decided that residents of four regions are allowed to move within their region if they prove to the police that they are using the contact tracing app. The Minister for Interior Aleš Hojs once again caused confusion when he made conflicting statements at press conferences as to whether a fine would follow in the event of non-compliance with the measure.[183] This case again showed an utter lack of an understandable and clear legal bases, where residents would be able to figure out how to adjust their conduct to the law. The measure was repealed after a few weeks in December

179 Reich et al., COVID-19 Technology in the EU: A BITTERSWEET VICTORY FOR HUMAN RIGHTS?, Civil Liberties Union for Europe, May 2021, available here, accessed on 20. 7. 2021.

180 Article 28, Act Determining Intervention Measures to Prepare for the Second Wave of COVID-19, available here, accessed on 20. 7. 2021.

181 Reich et al., COVID-19 Technology in the EU: A BITTERSWEET VICTORY FOR HUMAN RIGHTS?, Civil Liberties Union for Europe, May 2021, available here, accessed on 20. 7. 2021.

182 Upravljavec.si, Informacijski pooblaščenec ponovno opozarja na neustrezne pravne podlage za delovanje aplikacije covid, 31. 7. 2020, available here, accessed on 20. 7. 2021.

183 RTVSlo, Hojs: Če vas v sosednji občini zasačijo brez mobilne aplikacije #OstaniZdrav, sledi kazen!, 14. 12. 2020, available here, accessed on 23. 7. 2021.

2020, whereas the Communicable Diseases Act was repealed by the Constitutional Court in June 2021.[184] The measure of conditioning movement across municipality borders with installation of the app discriminated against people who do not use or have access to smartphones with the required hardware and software. In addition, this part of the population was often the most vulnerable, as it was above average exposed to infection due to its age or material status.[185]

In early September, another data protection issue popped up and it seemed as if the authorities would be completely oblivious to the notion of right to privacy and data protection. NIJZ suddenly launched a massive SMS promotion campaign, inviting people to install and use the app, even though citizens never agreed for their phone numbers to be revealed to NIJZ and used for the purposes of promotion campaigns.[186] In response to complaints, the IC emphasized that oversight of such measure falls within the competencies of the Agency for Communication Networks and Services of the Republic of Slovenia (AKOS).[187]

The app was created by the company RSTEAM, which was the most successful bidder amongst six bidders at the government's call for tender. The company charged only 4,026 EUR for the creation of the app. Questioning its efficiency and responsible use of public resources might therefore sound too meticulous, but the Ministry of Public Administration later concluded further agreements with the company, allocating first 32,000 EUR to it for updating the app[188] and more recently, in July another contract, worth 166,000 EUR for upgrading and maintaining[189] an application that is used by a negligible percentage of people in Slovenia and for which there is no study that would in any way justify its use and maintenance. Plus, as mentioned above, there is no data or model calculation on the social costs of the app and the competent ministry does not seem to find this as relevant. Such an approach is counter to the GDPR principle of data minimisation and seriously questions the general principle of proportionality already at the point of questioning the mere suitability of a specific measure to reach a specific goal.

184 Constitutional Court, Decision no. U-I-79/20-24, dated 13. 5. 2021.

185 Aleš Završnik, Pika Šarf: Social Surveillance in the Time of COVID-19. Journal of Criminal Investigation and Criminology. Available here, accessed on 20. 7. 2021.

186 Siol.net, NIJZ s SMS-sporočilom vabi k prenosu aplikacije #OstaniZdrav, 10. 9. 2020, available here, accessed on 20. 7. 2021.

187 Reich et al., COVID-19 Technology in the EU: A BITTERSWEET VICTORY FOR HUMAN RIGHTS?, Civil Liberties Union for Europe, May 2021, available here, accessed on 20. 7. 2021.

188 had.si, Vlada sklenila vzdrževalno pogodbo za 32.000 evrov za šest mesecev za aplikacijo #OstaniZdrav, 15. 1. 2021, available here, accessed on 24. 7. 2021.

189 24ur.com, Ministrstvo sklenilo pogodbo v vrednosti 166.000 evrov za nadgradnjo aplikacije #OstaniZdrav, 8. 7. 2021, available here, accessed on 24. 7. 2021.

It often seems the app was introduced due to the technology-solutionist approach and the fact that many European states introduced some sort of digital measures to try to contain the spread of the virus. But at the same time the app is often not embedded in the whole mosaic of measures, as per example in the period of peak infections in late October 2020, when according to the new testing protocol only persons for whom a more severe course of the disease was expected and those in exposed workplaces were tested. Many infected people were therefore presumed to be ill without testing, in which case they could not obtain a TAN code.[190] This undoubtedly limited the usability and efficiency of the app, but it was never brought up and reflected.

What is more, there is no clear governmental plan for revoking the app. When asked about the conditions under which it will happen, the Ministry of Public Administration answered that the app will be revoked, "...when the epidemiological service will come to the conclusion, that it is not needed anymore".[191]

Conclusion

The above analysis shows the app was introduced without involvement of competent state institutions (DPA), experts or the civil society, who were not only ignored but rather attacked for speaking out and questioning the non-transparent process and ambiguous goals of the authorities. It is not superfluous to conclude that such an approach, where the authorities refuse to consider and respond to people's fears and doubts, also affects the use of such a 'voluntary' solution.

Furthermore, in the processes of securing a legal basis for the app, there was no regard for EU and national data protection laws and regulations, the reasoning behind them and the established processes of drawing up laws that encroach on the right to privacy. There is no sunset clause for the app. Technology has inherent limits, but they are not discussed or recognized by the authorities. There is absolute refusal to analyze effects of an introduced measure and to take on responsibility for inefficient solutions.

190 COVID-19 Sledilnik, Skrivnosti aplikacije #OstaniZdrav, 28. 10. 2020, available here, accessed on 23. 7. 2020.

191 Ministry of Public Administration answer to FOI request on 28 May 2021.

Spain: Radar COVID

Sergio Carrasco Mayans (Rights International Spain)

Introduction

In order to analyze the efficiency and governance in the implementation of the Spanish contact tracing app Radar COVID, it is important to be familiar with the competent institutional framework. The Spanish case is peculiar, as health competences are transferred to the seventeen autonomous communities and two autonomous cities it is divided into. This circumstance, together with the lack of coordination between these bodies in decision-making processes (despite the existence of specific bodies to coordinate and cooperate between these administrations), has led to a series of delays and affected the efficiency of the proposed system, as will be analyzed in the different sections of this document. Significant divergences have been detected in critical elements such as the criteria for providing the code to enter the app, which makes it difficult to carry out general awareness campaigns to facilitate citizens' request for the necessary codes.

Regarding transparency, we found transparency deficiencies in the different phases that led to the contracting process for the development of the Radar COVID app. For example, by using the urgency procedure, neither the specifications and justification report, nor the economic offer were provided.

Several requests for information regarding the contract were made before the amounts and anonymized documents were provided, revealing an initial cost of 273,171.50 EUR for development of the app. Additionally, a contract was formalized before the end of 2020 for 1.4 million EUR for the maintenance and upkeep of this app for two years.

Even though the website created to inform citizens of the statistics relating to the Radar Covid app[192] provides a series of information, there are still some blank sections whose content is necessary to analyze the efficiency of these types of applications. This information was compiled through a series of right to access information requests, as well as information obtained gradually in collaboration with various media. Thus, a combination of strategic litigation in the strict sense and collaboration with the media has been used to put pressure on the administrations to provide the unpublished information on the corresponding platforms.

With respect to the model used, Spain opted for a decentralized and non-mandatory model. Using Bluetooth Low Energy (BLE), mobile terminals store a series of ephemeral identifiers. In positive COVID cases, a code is provided which, once entered, allows the uploading of the identifiers into the server. This makes it possible to track the contacts exposed while

192 Available on the app statistics website at https://radarcovid.gob.es/.

guaranteeing the privacy of the users. In this way, the impact on rights and associated risks – as well as the possible bias – is less than if its use was mandatory.

Development

Regardless of the development of other apps – such as those for self-diagnosis or mask usage time – in the case of contact tracing, Spain opted for the development of a new application using the decentralized GPT-3 system. However, it did not use the codebase already developed by other countries. This decision led to an unnecessary lengthening of the period needed before its introduction to the market, which was further delayed by the implementation of a pilot program to test it in June 2020 on the island of La Gomera in the Canary Islands.

Apple and Google allow only one single integration of their API per country, subject to authorization by the competent health authorities. In the case of Spain, this authorization is granted by the Ministry of Health for the implementation of Radar COVID, thus becoming the only application authorized for use. Later, agreements had to be made with the different autonomous communities for its integration,[193] which explains the differences in the dates of connection to the system, ranging from 19 August 2020, for Andalusia to 27 October 2020, for Catalonia. This means that while the codes were generated by the state, the autonomous communities were the ones to make the request and transmit them to those affected.

After consulting with technical managers in different autonomous communities, it can be concluded that these autonomous communities did not have the technical information needed to integrate the application into their systems until after the signing of the different agreements. This – in addition to the fact that the source code of the app was not previously accessible (either for citizens or for other public entities) – meant an additional delay in the integration within the health systems in the different regions.

Even though the initial announcement assured the app would be open source, general access to it was delayed under the pretext that it should first be integrated into the systems of all autonomous communities. In fact, the creation of the repository in GitHub was launched on 9 September 2020,[194] well after the app was already available and integrated in the first autonomous communities.

The alleged justification appears in the FAQ section of the app's website:

193 https://www.eldiario.es/tecnologia/si-descargas-app-radar-covid-no-esperes-avisos-riesgo-contagio-necesita-integracion-autonomica-operativa_1_6158485.html

194 https://github.com/RadarCOVID/radar-covid-android/commits/develop?after=211392ae3e3b1bb06b271a4c3b9a6e42f44782f9+349&branch=develop

> "*The main reason to wait before launching the app was to ensure that all the autonomous regions that had requested it had integrated the app into their systems. This decision was always based on the preservation of the public's common interest in the context we are experiencing, never due to a lack of transparency*".

In analyzing these circumstances, no real reason related to the preservation of the common interest could be found to justify not opening the code earlier. Additionally, access was subsequently granted before all the autonomous communities had been integrated into the system. This allegation thus appears to respond to a principle of security by obscurity, which must be rejected as it is a practice that only creates a false perception of security.

During this development, the Secretary of State for Digitalization and Artificial Intelligence (SEDIA) claimed to have collaborated with the team responsible for DP-3T since March 2020. Thus, it was stated: "*with the people of the DP-3T consortium there has been contact and meetings at different levels, not only with Carmela Troncoso, until the pilot program started at the beginning of June*". However, Carmela Troncoso denied these statements, declaring that the collaboration was limited to exchanged experiences of deployment and sending copies of documents.[195]

With regards to the personal data processed, the app's privacy policy[196] provides insight. As we know, this is a decentralized application that seeks to ensure the principle of privacy by design. For this reason, the personal data retained is limited, communicating to the server only temporary exposure codes generated by users diagnosed as positive for COVID-19. These are deleted from the server after 14 days. The same applies to temporary exposure codes and ephemeral Bluetooth identifiers, which are stored on the device for a period of 14 days, after which they are deleted.

No data retention periods are indicated for statistical or research purposes, nor are objective indicators established in order to proceed to the future withdrawal of the app.

Launch

As indicated, the Spanish government decided not to launch the application directly to the public after its development was completed, but instead carried out a pilot program on the island of La Gomera to test the effectiveness of a contact tracing solution of this type. For this purpose, three waves of contagions were simulated on 10, 13 and 17 July. These waves "*will be monitored on a daily basis to follow the evolution of the test and detect relevant milestones*".

The results of this pilot test were not made public until 26 January 2021, when they were

195 https://www.newtral.es/radar-covid-app-rastreo-espana/20200810/

196 https://radarcovid.gob.es/politica-de-privacidad

published in *Nature*,[197] despite requests for access to information from both citizens and the media. Regarding the access of the app during this testing phase, it should be noted that it was distributed during the pilot test in the Android and Apple Marketplace to the public, having detected a total of 31,892 downloads in June and 42,694 downloads in July 2020. However, given that the data is not geolocalised and that the population of the island of La Gomera, in which the test was conducted, is 10,000 people, it is hard to know how relevant this is. This circumstance is expressly considered in the research published by Nature, since certain data had to be calculated from indirect methods:

> *"(…) in relation to adoption, note that we could not use the number of downloads directly from the Apple and Google online stores (over 61k during the course of the experiment) as these are not geolocalised. Using indirect methods we estimate a 33% adoption, only using the amount of verifiable downloads directly performed offline by promoters, downloads from the Canary Island government, and assuming a 2% spontaneous adoption percentage and a few other assumptions".*

On the other hand, the same principle of privacy by default made it difficult to study the various KPIs in depth:

> "Since Radar COVID embraced a privacy-by-design approach, *the data that could be retrieved from the API to analyse the KPIs was limited, and indirect evidence had to be sought via extensive follow-ups and online surveys, which nonetheless were always anonymous and privacy-preserving".*

Therefore, we can conclude the pilot program was not only unnecessary and caused a significant delay in the population's access to the app, but also that its implementation did not prove to be useful or justified. The lack of a need to prove effectiveness is further reinforced by the fact that the cases where it was used could have been immediately analyzed in other countries that opted for other similar solutions. That said, a pilot project was also carried out in Guadarrama by the Community of Madrid[198] meant to last approximately three weeks and which again meant a delay in the launch in this autonomous community.

It should be noted that during the launch of this pilot test in the Community of Madrid, the application code was unnecessarily obfuscated, and no prior access was given to the source code, the impact assessment, nor risk analysis documentation.

197 https://www.nature.com/articles/s41467-020-20817-6

198 https://transparenciagov2020.github.io/

Transparency in the Operation of the Application

When analyzing transparency during the development process and operation of the application, it is important to take into account the recent manifesto in favor of transparency in public software development,[199] which was signed by people such as Carmela Troncoso, the researcher who leads the team that developed GP-T3.

In the Spanish case, and with respect to the aspects requested, we can indicate the following:

- The company in charge of the development (INDRA) opened a repository to give access to the application code, where we can track the different Pull Requests and changes produced. Thanks to this, vulnerabilities were detected, including false traffic in connection to the servers. However, we must remember that this repository was created after the first version was available in the mobile stores, so it does not include the development history from the early stages.

- This repository includes information about the mobile app but not about the rest of the system, back end applications, or security measures. Although basic principles are applied (such as those related to the Spanish National Security Scheme), transparency requires more information about the interconnection systems.

- There is no detailed report on app monitoring mechanisms beyond the existing one in the privacy policies.

Regarding the data protection impact assessment and risk analysis associated with the application, we must emphasize various aspects that have been detected due to the strategic litigation activities that were carried out.

Firstly, these documents were not accessible to the public in the repository, nor were the media, citizens or civil society[200] granted access to them under the excuse of possible changes and future general publication. Moreover, the updated version of the document published later did not correspond to the one existing at the launch, and which failed to indicate the changes that were made despite including (at least in appearance) a version control. These documents were also produced by the company in charge of developing the app.

Following a request for information,[201] access has been obtained to the original impact assessment and risk analysis, which were carried out on 12 August 2020, after the launch

199 https://www.xataka.com/aplicaciones/nadie-supo-darme-codigo-caos-radar-covid-codigos-que-no-llegan-notificaciones-retraso-mucho-trabajo-hacer

200 Including Rights International Spain.

201 *Idem.*

of the application (not to the integration with the different applications). We must emphasize that these documents, to which access was finally granted, have not been included in the public repository accessible to the public. There is also no record of any version control of the changes that have occurred, beyond the change of version numbering, and thus citizens, in general, only have access to the latest version of the document. In addition, none of the documents published has an electronic signature, which makes it difficult to know when they were actually created. That said, the impact assessment includes in its metadata that the PDF document was created in January 2021, and not in 2020 as could be extracted from the version control and date indicated.

The Spanish Data Protection Agency was informed of these circumstances and has recently initiated a sanctioning procedure due to the circumstances highlighted in this document, which represent a potential data protection infringement. At present, this procedure is under investigation.

Application effectiveness

The analysis of the effectiveness of the app, as well as certain data (such as the number of actual users) is complex because of the safeguards incorporated into the system by privacy by design principles. Therefore, such analysis must be carried out based on the figures provided both on the app's statistics website and those obtained as a result of requests for information.

The latest data provided show 7,431,238 downloads (including Android and iOS versions), which represents a penetration rate of 18% of the population. It should be noted that this number reflects downloads – not installations – and includes devices on which it has been downloaded several times, as it is not possible to discriminate by unique associated users. Furthermore, as we shall see, the effectiveness has been very low in terms of actual use and the introduction of codes provided by the health authorities.

In an effort to boost the low number of downloads, advertising initiatives have been carried out, such as an agreement with LaLiga to promote the use of the app during sporting events broadcasts, for example during the popular Clásico Barça-Madrid football match[202] (October 2020). An intense promotional campaign has also been carried out on social media, first by former players such as Fernando Morientes, Fernando Sanz or David Albelda, and then with advertising messages during the Clásico. As a result of this initiative, there were nearly 100,000 downloads of the app on the Sunday of the match.[203] This boosted the daily average achieved by Radar COVID tenfold from previous weeks. Other initiatives to extend the

202 https://twitter.com/SEDIAgob/status/1320002767029735425?s=20

203 https://www.elconfidencial.com/tecnologia/2020-10-26/radar-covid-la-liga-app-rastreo-contactos_2806188/

use of Radar COVID have been agreed upon with the High Council of Sports.[204]

In April 2021, a new investment of 1.5 million EUR[205] in advertising was announced to try to increase its use. This includes *"the development and implementation of a media plan to promote Radar COVID in digital environments, social media, radio and written press"*. This decision was based on the low penetration that Radar COVID has obtained so far.

It is even more complex to analyze the number of codes entered, given the disparity of criteria for providing them to the different autonomous communities. If we look at the cumulative number of codes requested, we find that the autonomous communities have requested a total of 971,138 codes, however, only 64,031 codes have been entered into the application. This represents 6.59%, i.e., less than 7 out of every 100 codes requested have been entered into the Radar COVID application.

In order to identify possible reasons for this, we can begin analyzing the codes requested to SEDIA by the autonomous communities for confirmed cases with active COVID-19 infection, where we find ratios of both requested codes and confirmed cases that range from a striking 169.7% in Cantabria, 153% in Asturias, or 120.1% in Galicia, to 0.5% in Extremadura or 0.8% in the Murcia or Valencia. This responds to the disparity of criteria between the different autonomous communities, with cases in Asturias, Galicia, Cantabria, the Basque Country or Castilla y León, which have requested a larger number of codes than the number of confirmed positives. These regions decided to incorporate in their pandemic protocols an expediting of codes to all users, with or without the app, whether or not they request them.

However, the mechanism for providing the code has not been uniform. Some communities sent short messages to a mobile terminal, while other communities provided them directly in the COVID-19 test results.

In addition, the codes generated by SEDIA include the percentage of active users who decided not to enter them in Radar COVID, as well as those that were delivered to people who were not users of the app and those that, for one reason or another, were sent to the communities but not bounced back to the citizens. Therefore, there may be duplicates that justify these high percentages, but which cannot be broken down because of existing privacy protection measures.

With regard to the ratio of codes entered in the application to the number of positive cases detected —and despite the initial affirmations that in some cases the percentages would have similar rates to other European countries— at the moment the accumulated percentages are

204 https://fep.es/website/18-13245-el-gobierno-se-apoyara-en-el-deporte-y-los-deportistas-para-generalizar-el-uso-de-la-app-radar-covid.htm

205 https://www.vozpopuli.com/economia_y_finanzas/radar-covid-gasto-gobierno.html

very low. Only Asturias with 6.7% and the Basque Country with 5.7% maintain this similar rate, and then decline from 4.2% in the Community of Madrid, to percentages below 1% in the case of La Rioja (216 codes out of 25,407 positives), or the particularly striking case of Extremadura, with less than 0.10% (70 codes entered out of 71,846 confirmed cases). In fact, nine of the seventeen autonomous communities and the two autonomous cities have a ratio of less than 1% codes entered in relation to confirmed cases.

The consultation with healthcare staff in Extremadura revealed that this autonomous community decided to request COVID codes from the Ministry after asking the patient directly. Therefore, presumably, the person with a detected contagion was offered the possibility of requesting this code if he/she considered it appropriate, as opposed to other communities that offered it by default. This explains the low number of codes requested (only 330 out of a total of 71,846 confirmed cases, of which, as we have indicated, only 70 codes were entered).

In the case of the Balearic Islands, which was one of the first regions to start using Radar COVID on 24 August 2020, the initial low volume of codes was justified by initial technical problems in obtaining them, and subsequently by the lack of adoption by citizens. That said, the media echoed the case of a positive patient who spent a whole day trying to obtain the code (despite actively requesting it) because neither the doctor, nor the trackers, nor the helpline knew the protocol for providing the code to be entered in Radar COVID, and this patient's close contacts took up to eight days to receive the notification[206] despite the importance of rapid action. In other autonomous communities there have been cases of healthcare staff who turned to social media to find answers about the code,[207] which proves the existence of deficiencies and lack of coordination when it comes to providing Radar COVID codes.

No information has been compiled as to how many people have been identified thanks to the tracking tools, nor has statistical data been provided on the cost and efficiency of the solution, although the Radar COVID's technical document mentions the implementation procedure[208] in the section on operational evaluation. Initially, some territories provided information in this regard to promote the effectiveness, as is the case of the Basque Country where it was indicated that as a result of 24 alerts, three people were confined.[209] However, this information has not been updated

206 https://www.elconfidencial.com/tecnologia/2020-09-28/coronavirus-radar-covid-covid19_2759416/

207 https://www.elconfidencial.com/tecnologia/2020-09-14/radar-covid-app-aplicaciones-coronavirus-covid19_2744252/

208 https://www.mscbs.gob.es/profesionales/saludPublica/ccayes/alertasActual/nCov/documentos/COVID19_Procedimiento_RADAR.pdf

209 https://www.elcorreo.com/sociedad/salud/radar-covid-ofrece-20201002143505-nt.html

periodically and does not figure on the app's website.

Consultation with people who went to the health services after receiving a message from the app reveals that there is no evidence of statistical forms being used in a generalized manner to obtain this information anonymously or to analyze the effectiveness of the measure. Furthermore, there is no section on the app's website that would allow us to conclude that this data is available for evaluation of the effectiveness of the application. Information has been provided on cases confirmed through contact tracing following requests for information,[210] but insufficient information is provided to evaluate the effectiveness of the Radar COVID app alone.

Regarding the total number of notifications, this information is not provided in the statistical data on the app's website. However, based on the averages mentioned before (three notifications on average for each positive infection uploaded to the app[211]), we can say that the potential number of infection alerts is approximately 192,000. That said, we should mention that the Nature report indicated that the application can alert an average of 6 close contacts for each confirmed case, which could potentially raise this number.

Conclusions

In view of the above, there are grave deficiencies, especially regarding coordination between the different Spanish autonomous territories. It seems difficult to establish criteria to be able to use the app effectively in the future. However, there is a series of criteria that can help to reinforce the confidence of citizens, and thus its use:

- Reinforcement of communication campaigns, especially on the importance of contact tracing.

- Establishing that all the autonomous communities will provide the code to the positive cases detected, as well pamphlets and other resources to inform about the use of the application and its benefits. This should be emphasized so as to facilitate all the information directly to the user, both to communicate the existence of the application and to obtain the code. Given the low numbers, it would be advisable to carry out campaigns in healthcare facilities to encourage those who may not know about the app or to install it.

- Greater code transparency, providing a true version control of all associated documentation, including risk analysis and impact assessment.

210 https://www.newtral.es/radar-covid-ventana-tecnologica-perdida-con-la-pandemia/20210421/

211 https://www.diariodesevilla.es/tecnologia/personas-avisadas-contagio-Radar-Covid_0_1556546448.html

• Complete the statistics, which currently still have blank spaces that make it difficult to detect efficiency.

• Include data from the app in all speeches related to the fight against the pandemic, in order to increase awareness of its existence.

For future similar initiatives, it is particularly important to reduce implementation periods, to coordinate the development of applications at European level, and unify efficiency study procedures. The way in which the different applications have been developed is inconsistent, both from the point of view of the time required and economic efficiency, as well as taking into account that in the future it will be necessary to provide an interoperability platform for the exchange of information.

The Civil Liberties Union for Europe (Liberties) is a non-governmental organisation promoting and protecting the civil liberties of everyone in the European Union. We are headquartered in Berlin and have a presence in Brussels. Liberties is built on a network of national civil liberties NGOs from across the EU. Unless otherwise indicated, the opinions expressed by Liberties do not necessarily constitute the views of our member organisations.

Website:
liberties.eu

Contact info:
info@liberties.eu

The Civil Liberties Union for Europe e. V.
Ringbahnstr. 16-20
12099 Berlin
Germany

Subscribe to our newsletter
https://www.liberties.eu/en/subscribe

Reference link to study
Please, when referring to this study, use the following web address:
https://www.liberties.eu/f/Nv4A36

Follow us