COVID-19 Technology in the EU:

A BITTERSWEET VICTORY FOR HUMAN RIGHTS?

May 2021

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

Nikolett Aszodi (Austria, England & Wales, France, Greece, Luxembourg, Malta, Portugal)

Jascha Galaski (Belgium, Bulgaria, Croatia, Germany, Italy, Ireland, Lithuania, Poland, Slovenia, Spain, Sweden)

Oleksandra Konoplia (Czechia, Cyprus, Denmark, Estonia, Finland, Latvia, Netherlands, Slovakia)

Orsolya Reich (Introduction, Hungary)

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 European AI Fund, NEF or European AI Fund's Partner Foundations.

A grant from **Digital Freedom Fund** allowed initial research to be conducted in twelve EU member states for the purposes of deciding over possible future strategic litigation actions.

Table of contents

Introduction 4
The risks of tracing apps 4
Key findings one year into the pandemic 5
GAEN: A laudable outcome? 6
Efficacy, social impact, future expectations 7
Other technologies 7
Country reports 8
Belgium 8
Bulgaria 14
Croatia 16
Germany 18
Hungary 22
Ireland 26
Italy 29
Lithuania 32
Poland 35
Slovenia 41
Spain 45
Sweden 51
Memos 53
Austria 53
Czechia 54
Cyprus 56
Denmark 58
England & Wales 60
Estonia 63
Finland 64
France 66
Greece 68
Latvia 68
Luxemburg 70
Malta 70
Netherlands 72
Portugal 74
Slovakia 75

Introduction

In trying to stop the COVID-19 pandemic, governments have tried to balance preserving public health and life with keeping their economies going and maintaining their citizens' freedoms. To help them navigate the pandemic, after the first few weeks of the 2020 Spring lockdown(s) in Europe, EU governments decided one after another to make contact-tracing, symptom-tracking, exposure-notification and quarantine-enforcing applications available and, in certain cases, mandatory for their populations.

The COVID-19 pandemic is the first global pandemic where personal technological devices are well-spread and "smart" enough to make mass surveillance of the population through their own devices possible. There is a risk not only that governments would introduce technology that allows for mass surveillance, but also that these temporary measures might become permanent. This is particularly concerning given that democracy is declining in a number of EU member states.

Liberties has partnered with twelve of its member organisations to monitor developments in coronavirus-related technology in their respective countries in 2020 and early 2021, and where necessary, start litigation. This publication documents the findings of this monitoring. Liberties members contributed to the in-depth country reports covering Belgium, Bulgaria, Croatia, Germany, Hungary, Ireland, Italy, Lithuania, Poland, Slovenia, Spain and Sweden. The publication contains a further 15 country memos, based on desktop research by Liberties staff.

The risks of tracing apps

Governments have are obligations to protect the health, lives and livelihoods of people in their jurisdiction. Fulfilment of these obligations can justify restrictions on other rights, such as privacy or the freedom to move around. However, such limitations must not go beyond what is strictly necessary to achieve legitimate aims, like the protection of health and life. Deploying technologies such as contact tracing applications (apps) may create a risk of mass surveillance. Such a deployment may be a disproportionate interference with the right to privacy with knock-on effects for civil and political rights in general, such as freedom of expression and information and freedom of assembly and association.

The risk to privacy and related civil and political rights would be most pronounced if governments were to use apps that collect GPS data and/or Bluetooth on (re)identifiable users and store them on central servers. Collecting GPS data on (re)identifiable users through the national contact tracing apps would have allowed governments easy access to the geographical movements of citizens. Collecting Bluetooth data on citizens would have allowed governments to obtain a clear picture of an individual's social networks.

Were governments to make such contact tracing apps mandatory or a pre-requisite to access certain communal spaces or the workplace this would have resulted in a system of mass surveillance that governments could exploit, for example to monitor and harass political opponents and activists.

Key findings one year into the pandemic

After more than a year into the pandemic in Europe the worst-case scenario outlined above has not materialised. Contact tracing apps were not used for mass surveillance, the apps (with the exception of some quarantine apps) have not become mandatory to use and, to the best of our knowledge, even where data was collected on a central server, the data has not been (mis)used by governments to harass opponents and critics. Although this is good news for human rights, the country research highlights a number of concerns.

First, in many European countries there was no public debate on whether such apps were needed or desired as a means to protect public health. While governments may be justified in taking swift action to deal with a public health emergency, there has been ample time since the apps were launched for public debate. This lack of public discussion may well undermine trust in the apps as well as other measures to protect public health, such as vaccinations.

Second, it seems that governments have not consulted experts on the expected efficacy of such apps, on the social impacts of their widespread use and on the ways potential harmful effects can be mitigated. While this may have been justified in an emergency situation, and/or in relation to apps that were launched in the Spring of 2020, it is hardly acceptable that governments kept introducing/running apps later on without investigating their costs and benefits.

Third, while a number of countries eventually published the source codes of their apps and made a data protection impact assessment available, many of them did so months after launching the apps, and some never did.

Fourth, in a number of cases data controllers did not consulted the data protection authorities before launching the app. Given that it is highly unlikely that e.g., processing contact data and storing them on a central server would not result in a high risk "in the absence of measures taken by the controller to mitigate the risk", in our view a number of governments breached their obligations set by the General Data Protection Regulation (Article 36.1)

Fifth, hardly any country adopted the most worrisome digital solutions. Rather most of them launched 'decentralized', Google/Apple Exposure Notification-based apps registering Bluetooth chatter between devices on the devices only (without sending this data to a central server). However, this outcome was effectively forced on governments by big tech companies.

Sixth, after a few months, most government silently abandoned efforts to convince their populations to download and use the apps offered. However, if COVID-19 becomes endemic (e.g. if a significant part of the population decides not to get vaccinated) tracing apps – either in their current forms or in revised forms – may come back to the stage.

GAEN: A laudable outcome?

In early 2020, an international consortium was formed of researchers concerned about the potential for misuse of contact-tracing technologies. Their aim was to create a decentralised open protocol and codebase (called the DP-3T) to enable smartphone users to be notified if they had been exposed to the coronavirus without needing a centralised database to store contact data or persistent identifiers. Without a centralized database, governments cannot reconstruct the social graph of users. Without persistent identifiers the apps cannot be easily turned into immunity certificates or used in enforcing quarantine (such repurposing is called ‘function creep’).

European governments were moderately enthused by DP-3T. Many favored the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) solution. PEPP-PT would not have retained data on handsets; instead, it would have sent contact data to a central server, thereby giving more data and more access on sensitive personal data to governments. According to the developers of DP-3T, PEPP-PT involved a high potential for function creep, and the transformation of a coronavirus contact-tracing tool into a surveillance tool.

However, tech giants Google and Apple decided to take a stand and to stand by (and build on the ideas of) the DP-3T team. On 10 April 2020, they announced a system later known as the Google Apple Exposure Notification (GAEN) system and effectively killed off almost all governmental attempts to centralize data. GAEN-based apps cannot collect data on the users (not for the governments, in any case) as contact data never leave the users’ devices. National contact tracing apps using the GAEN application interface could use Bluetooth even when the app is off-screen (this is generally not possible on iOS phones). This is very important, for not being able to use the app off-screen means that the app should be open and in the front at all times when people want to use them – on public transportation, in the office, etc. Having to run the app in the front makes it impossible for people to do whatever they used to use their phones for. It also drains the battery. The countries not willing to bow to the tech giants either developed major technological workarounds to resolve (or at least limit) this problem (see e.g., our report on France) or launched an app that works on iOS system very sub-optimally (see our report on Hungary).

While the GAEN system saved many European citizens from the worst privacy and centralization risks, this story, we believe, is not to be celebrated. Tech giants that have no democratic accountability have overwritten the will of democratically elected governments. On this occasion, they effectively forced governments to 'do the right thing' and not build systems that are easy to misuse. But there is no guarantee that corporations will always act benevolently, and any entity wielding power over the public should be accountable to that public.

Efficacy, social impact, future expectations

In April 2020, Oxford University researchers argued that if about 60% of the UK population would actively use the national contract tracing app, the country could reach a 'digital herd immunity' and effectively suppress the spread of the disease. For various reasons, as of February 2021 none of the European apps reached this threshold. In a number of countries, either the national contact tracing app silently disappeared from the app stores (e.g., Slovakia) or simply provoked almost no interest in the population (e.g., Croatia, 2% as of February 2021). The highest adoption rates (between almost 30% and 60%) could be observed in England and Wales, Ireland, Finland, Denmark and Germany.

To date, we do not know much about how many cases were discovered via these apps. Similarly, we know little about how many false-positive encounter notifications were sent out asking people to self-isolate. We also do not know whether and what social impact the widespread use of the apps had. Liberties' members and partners intend to publish findings on these questions in the second half of 2021.

Other technologies

While the present report is focused on contact tracing apps from 2020, the country reports provide interested readers with information on other corona-related technologies developed and/or used in 2020. At the time of writing, a new technological solution meant to control the pandemic is at centerstage: the vaccination/recovery/test certificate. As the European certificate is not yet developed and member state vaccination passes were launched after closing the manuscripts, this collection of essays does not contain information on them. However, we do conduct advocacy on the European pass and plan to monitor the upcoming national passes in the future. You can read about our work on these passes on our webpage, www.liberties.eu.

Country reports

Belgium

Introduction

Belgium was hit particularly hard by the coronavirus, with one of the highest death rates in the world. The government announced a lockdown from 17 March 2020, closing schools, universities and non-essential shops, encouraging home office, prohibiting non-essential travel and banning large gatherings.

Belgium's Federal Public Service (FPS) created a website that provides the latest figures and news and gathers general information on the virus. The National Public Health Institute Sciensano also has a website with a dashboard that gives an overview of the number of cases, hospitalizations, deaths, tests, and latest trends. The data is updated on a daily basis.

Data Against Corona Taskforce

At the end of March 2020, Minister of Health Maggie De Block and the Minister of Digital & Privacy, Philippe De Backer, established the 'Data Against Corona' taskforce, composed inter alia of data scientists, data privacy experts and epidemiologists. The taskforce used telecom data from the providers Proximus, Telenet and Orange to map population movements in order to help the federal government get a better understanding of the spread of the disease and adopt more effective measures. The first results showed that since the start of the lockdown, Belgians reduced their mobility by more than 50% and stayed at home or within the limits of their postal code 79% of the time.

An ethics committee was put in place by Maggie de Block and Philippe De Backer to supervise the activities of the taskforce. The Belgian Data Protection Authority (APD) issued a positive opinion after a prior data protection impact assessment (DPIA) was conducted, showing that only aggregated and anonymized data would be used and that it could therefore not be traced back to an individual. However, the reliability of that assessment was questioned after several experts, including from the APD itself, criticized the independence of the data protection authority (more in 'involvement of APD'*).*

Manual contact tracing and establishment of centralized database

In its deconfinement strategy, the federal government confirmed that contact tracing would play an important role. But Belgium's complex political system, with its nine health ministers and competences spread between federal, regional and communal authorities, has led to confusion over roles and responsibilities, making contact tracing of COVID-19 patients difficult.

Instead of digital contact tracing, for example via an app, the government opted for manual contact tracing, by setting up hundreds of call centers and hiring 2,000 "contact tracers". The tracing works as follows: persons who show symptoms call their general practitioner (GP), who assigns them a test, if necessary. The persons are then asked to fill in a form and draw a list of people that they have met in the last 48 hours. This form is sent to their GP, who can enter the data into a database. The call center agents, who have access to the database, are responsible for contacting the persons tested and informing them of the results. If the result is positive, the call center will call all the contacts to invite them to take a test or go into quarantine. The call centers are supported by health professionals who can assess potential symptoms remotely. There are also agents in the field for those people who do not pick up the phone or whom the call center agents deem to be "non-compliant". The operation and training of call center staff were delegated to regional authorities. Local media later questioned the efficiency of the call center operation, which allegedly cost €100 million.

The government commissioned Sciensano to create and manage a huge centralized federal database of COVID-19 patients to support the call centers, as well as to use the data for scientific, statistical or policy support studies and to give the regional health prevention inspectorates more information as to measures which would be most effective in limiting the spread of COVID-19. The database includes information on the patients' GPs and people with whom these patients had been in contact.

Regulatory framework for manual and digital contact tracing

In April, the government drafted a decree, Royal Decree of Special Powers No.18, that would form the legal basis for the creation of the database. The draft decree provided that the personal data would be communicated to Sciensano by GPs, hospitals, laboratories and call centers. It did now, however, include any provision for digital tracing applications.

The APD stated on 29 April that adoption of the draft would breach European data protection law. For example, doctors would be obliged to communicate their patients' data, a breach of medical confidentiality. The APD also questioned why Sciensano should collect sensitive data, such as national register numbers, and highlighted the risks of storing personal data in a huge central database. Despite this criticism, the government adopted the decree on 4 May.

The government said that it took the APD's opinion into consideration. However, the APD issued another opinion on 25 May, noting that its main complaints (e.g. clarification about the data retention period or the data controller) had not been addressed and demanding that the bill be restructured. The APD also said that regional authorities should provide a plan on how they would manage and store the data and guarantee that citizens who do not want to pick up the phone are not harassed or forced to isolate.

On 15 May, at the initiative of the Belgian NGO Human Rights League (LDH), more than 300 academics, legal experts, data protection specialists and civil society actors addressed a letter to the Speaker of the Chamber of Representatives (the lower house) and the heads of the different political groups, criticizing the manual tracing via call centers. They argued that the decree "does not comply with fundamental rights", insisting that if the government wanted to trace its citizens, "serious guidelines" had to be put in place to protect the rights and freedoms of the population. In their letter, they advocated a minimization of data collection with a clear time limit (more here).

The decree was amended a month later by Royal Decree No. 25, which, the APD noted, improved the bill. However, it still highlighted issues, such as the lack of justification for collecting massive amounts of sensitive data on a central database or that GPs were forced to breach medical confidentiality when they communicated their patients' data. It also criticized the provision allowing call center agents to carry out home visits, calling it a "disproportionate intrusion".

On 1 July, the decree was replaced by Royal Decree No 44, which, besides regulating manual contact tracing, also set the legal basis for the creation of a digital contact tracing app. The decree deals mainly with the technical aspect of the app, including its functionalities and operations, technical specifications and interoperability, as well as the responsibilities and obligations of its developers. The text also includes control measures, such as regular monitoring and evaluation, and subjects the app to an information security audit.

Royal Decree No. 44 was later replaced by a Cooperation Agreement between the federal state and the federal entities. In an interview with the national magazine Le Vif, the Director of the APD's Knowledge Center, Alexandra Jaspar, criticized the government for not consulting with them previously and said that the "text lacks clarity and readability".

Contact tracing app Coronalert

A federal contact tracing app was initially not considered in Belgium. A Reuters' article quotes Philippe De Backer saying on Belgian television channel VRT that "there is no need for an app for contact tracing, it can be done manually and it has been around for years." On 7 July, however, the government announced that a national contact tracing app would be ready in September.

The small Brussels-based company Devside, which specializes in mobile applications, was selected to develop the app, with the help of the software publisher Ixor as a subcontractor. The tender was led by the public company SMALS. Its choice to commission the development of the app to an almost unknown startup with only five employees, including the CEO, Frank Robben, who also worked at the APD, met with surprise from experts in the field. Costs were estimated at around

€850,000. The company Nviso was commissioned in a second tender to check whether the app meets all safety standards. The app is based on the German Corona-Warn-App and has been adapted to fit the Belgian health protocol (see main differences between the apps here).

Devside held a public consultation from 5 to 31 August, in which it asked privacy experts, civil society, municipalities, academics and 'concerned citizens' for feedback about the use of the app. Specifically, it asked questions about how to make the app as inclusive as possible, how to increase user-friendliness and trust in the app and who should be included in an oversight committee. Some of the changes adopted following the feedback included lowering the minimum age to use the app from 14 to 13 years. A conclusion of the consultation can be found here.

Ahead of the launch, the app developers conducted a 10-day test phase with 10,000 volunteers, recruited by Colruyt, KU Leuven, Ernst & Young and hospitals. On 30 September, the contact tracing app Coronalert was available for download.

Coronalert – technical details

Coronalert is based on the decentralized Google/Apple Exposure Notification (GAEN) system. The use of the app is voluntary and the source code is available here. Sciensano is responsible for the server infrastructure and also acts as data controller. The app alerts users if they have been near a person who tested positive with COVID-19.

Upon installation, the app generates temporary exposure keys (TEKs), which are renewed every day. When two users are physically close, their devices exchange pseudorandom IDs (derived from the TEKs and refreshed every 10-20 minutes) via Bluetooth Low Energy (BLE). The IDs are then stored on the devices for a period of 14 days, together with the date, the signal strength and the duration of the encounter.

When users are tested for COVID-19, they receive a code composed of 17 digits that they or the test center (upon consent) can upload to the app. The code is stored on the Sciensano servers. The app then regularly checks the test results on the server. Once the result is available, the app notifies the user whether the result is positive or negative. If the result is positive, the app will alert people that have come within 1.5 meters or less for at least 15 minutes in the last 14 days of the risky exposure.

In November, the app was updated. The new version addressed in particular the problem of test tracking. For various reasons, e.g., mistakes by patients or doctors, the randomly generated codes were not always uploaded onto the app. As a result, other users were not always notified. The second version therefore made the device more flexible, allowing users to upload the code at different times, such as when booking the test on the website masante.be.

The second version also brought new functions. For example, users can now obtain a quarantine certificate via a call center if the app reports that the user is at high risk, facilitating home office requests. The app developers announced in January 2021 that the app is now interoperable in 10 other EU countries.

Two weeks after its launch, Coronalert already passed the milestone of one million downloads, which translates into a penetration rate of around 15% of the Belgian population. By mid-November, two million Belgians had already downloaded the app. However, the number of downloads significantly dropped thereafter. By mid-February 2021, Coronalert had been downloaded less than 2.5 million times. And between the launch in September and mid-February, only 15,700 infected people used the app to alert their contacts, which represents 2.5% of all positive test results during that period.

Reaction of the Belgian Data Protection Authority

On 28 April, the Belgian Data Protection Authority (APD) issued an opinion on the use of contact tracing apps to contain COVID-19. The APD highlighted the importance of the right to privacy, the principle of proportionality and the need for the app to be less intrusive than other measures that would achieve the same result.

Following the request from 15 May for an opinion by the President of the Chamber of Representatives on the draft decree no 44 , the APD stated on 26 May that the draft was not yet compliant with EU data protection law and provided a list of recommendations, including the obligation of the app's developers to prepare a data protection impact assessment (DPIA) and share it with the APD and the installation of further data protection safeguards. The DPIA was made and published in September (French & Flemish version).

Conflict of interest within the APD

On 9 September, Alexandra Jaspar (who is behind most of the APD's opinions mentioned in this report) and Charlotte Dereppe, two directors of the APD, sent a ten-page letter to the Belgian Parliament, in which they stated that the APD had become "unworkable" and "is no longer able to fulfil its mission independently" due to "serious" actions of its president, David Stevens.

Stevens was notably part of the Data Against Corona Taskforce. Under normal circumstances, the decisions of this task force had to be submitted to the opinion of the APD. Jaspar and Dereppe argued that this placed the body "in an obvious situation of conflict of interest". In their letter, the two directors called on Parliament to remove the mandate of Stevens. They also requested two external audits, one of the psychosocial environment within the DPA and the other of its expenditure.

The online newspaper Brussels Times reports that one of the issues was related to the corona tracing app. In July, Jaspar posted a message on LinkedIn in which she "feared for our democracy" regarding the Royal Decree of 26 June, which set the legal basis for the app, but which had never been submitted to the APD for observations on the privacy aspects. On 19 December, Jaspar wrote on her LinkedIn: "If you are interested in our summaries of some of our opinions on sensitive draft bills and implementing measures, hurry up ... someone is apparently putting pressure on LinkedIn to get them removed .."

Another representative of the APD, Frank Robben, has also been accused of conflicts of interest. Besides his work for the APD, Robben is a member of the Corona taskforce and the initiator of the Information Security Committee (CSI), responsible for defining who is allowed to tap into the data. In an investigation by the magazine Wilfried that made national headlines, the virologist Emmanuel André argued that Frank Robben's mandate at the APD was in fact illegal because he is also a civil servant.

Bulgaria

Introduction - National Information System for Combating COVID-19

In April 2020, the Ministry of Health introduced the 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. Since 7 April, Bulgarians have been able to download it for free from the Apple Store and Google Play. 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, and 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 high 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, as reported by the Bulgarian Helsinki Committee. There is no information available on its website; no reactions, comments, statements or press releases.

Croatia

On 19 March, the Croatian government passed a new bill amending the Law on Electronic Communications, which would legalize the widespread monitoring of citizens' mobile devices in order to contain the spread of the virus. This caused concerns among privacy experts about possible surveillance issues. The Croatian Parliament did consult with the Croatian Ombudsman Lora Vidović, who highlighted that the government should respect the principle of proportionality, that the measures implemented must be clearly defined and that it must provide information on "the beginning and duration of the measure, with an explicit prohibition on retroactivity." The amendment was finally withdrawn before its second reading in the Parliament.

Official coronavirus website and chatbot Andrija

In order to counter misinformation and centralize information around COVID-19, the government launched a website in mid-March. It provides the latest news on the country's pandemic situation, information on the measures implemented by the government or recommendations on how to deal with the pandemic regarding issues such as stress or job loss.

In mid-April, the Ministry of Health presented the WhatsApp chatbot Andrija, named after famous Croatian doctor Andrija Štampar, that allows people to do a health self-assessment online. The chatbot was donated to the Ministry by a coalition of Croatian companies specializing in artificial intelligence. Although the project was a good example of how technology can help contain the virus, it did have serious data protection issues, including a lack of information on what data it collected, for what purpose and the absence of prior consultation with the Croatian data protection agency.

Contact tracing app Stop COVID-19

On 27 July, Croatian Health Minister Vili Beroš, the CEO of the APIS IT Support Company, Saša Bilić, and the epidemiologist from the Croatian Institute of Public Health, Tomislav Benjak, presented the contact tracing app Stop COVID-19. It was developed to alert users about risky exposures and prevent the spread of the coronavirus. The user interface was donated by the company Bornfight. On 28 July, Stop COVID-19 was available for mass download.

Stop COVID-19 – technical details

The app is based on the decentralized Google/Apple (GAEN) API and uses Bluetooth Low Energy (BLE) technology to alert users if they were in close contact with people who tested positive for the virus. Upon installation, the app generates a temporary exposure key (TEK) which is then changed several times every hour. When there is an encounter between two users within 1.5 meters for more than 15 minutes, their smartphones exchange these keys and store them on the device for 14 days. After that they are deleted. An infected user receives a unique verification code from a healthcare professional, which can be uploaded onto the app. Every user who has been in close contact within the last 14 days will then receive an alert about the potential danger, including the day of the exposure and recommendations on the procedure to follow.

The Ministry of Health is the data controller and is responsible for data processing. The user's consent is required for the processing of personal data. Installation and use of the app do not require registration. The app also does not request or record any personal data, such as the name, date of birth, mobile phone number or e-mail address of the user. Installation and use of the app are voluntary and the source code is available on GitHub.

Since 19 November, the app has been interoperable across borders through the European Federation Gateway Services (EFGS).

Despite the efforts of the developers to respect the users' privacy, the penetration rate of the app is very low. Local media report that after four weeks, fewer than 50,000 people had downloaded Stop COVID-19, only two users received a verification code and only one of the two uploaded the code onto the app. Four months later, the app has not become more attractive. Statistics on the app's official website show that by February 2021 only 83,191 people had downloaded the app and only 56 infected persons entered a code into the app to warn others of a potentially risky exposure.

Involvement of the Croatian Agency for the Protection of Personal Data (AZOP)

On 20 July, AZOP representatives held a teleconference with the Croatian company APIS IT and representatives of the Ministry of Health. AZOP was presented with the app's functionality and introduced to its technical characteristics and was able to assess compliance of the app with EU data protection law. The three parties also agreed on further cooperation (summary of the meeting here).

AZOP published a summary of the data protection impact assessment (DPIA) of the Stop COVID-19 app.

Germany

In spring 2020, following the outbreak of the COVID-19 pandemic, Germany had a relatively low number of infections and deaths compared to its neighboring countries. In the months that preceded the 'first wave', it was often praised as a success story. Starting from October, this changed, with tens of thousands of infections reported every day.

Emergence of data-driven solutions to contain the virus

To stop the spread of COVID-19, Germany hosted a gigantic hackathon in March 2020 with about 28,000 participants, working together on innovative solutions on topics such as childcare, symptom tracking and neighborhood support. From this, hundreds of projects were supported, such as a contact diary app and a heat map that warns of an overload of intensive care unit (ICU) beds, enabling decision makers to react quickly and efficiently distribute patients.

The Robert Koch Institute (RKI), Germany's federal agency for infectious diseases, introduced a data-donation app that collects health data (e.g. temperature, blood pressure, pulse, stress levels) from fitness devices such as smart watches. It also asks users to enter their socio-demographic data (e.g. age, height, gender, weight) and postal code. This enables the RKI to identify possible symptoms and monitor the spread of the virus, including detecting possible hot spots. According to the Federal Data Protection Commissioner (BfDI), more than 500,000 citizens voluntarily shared their data. A report published in April by the hacker association Chaos Computer Club (CCC) questioned whether the sensitive health data – stored on a centralized server of the fitness tracker provider – of the app's users was sufficiently protected. The BfDI criticized that it was not involved during the development of the app.

In March 2020, the company Deutsche Telekom voluntarily transmitted telecommunications traffic data to the RKI, enabling the institute to track the movement of mobile phone users. The information helps the RKI understand which measures could effectively help to contain the pandemic. Deutsche Telekom assured that the data was aggregated and anonymous and could not be traced back to individuals. The German civil liberties NGO Gesellschaft für Freiheitsrechte (GFF) wrote that the move was legitimate as long as the data remained anonymous. However, they also questioned whether traffic data can ever be completely anonymous, since there were signs that a re-personalization remained possible. GFF concluded that "the transmission was burdened with both legal and factual uncertainty" and demanded that a formal legal basis be created for the transmission.

On 25 March 2020, the German Parliament passed amendments to the Infection Protection Act (*Infektionsschutzgesetz*) in a fast-track procedure. The amendments mainly transferred more powers to the Federal Ministry of Health (BMG). Originally, it contained a clause that would oblige telecommunication operators to share sensitive personal data – so, not anonymized – with health authorities, but it was removed after public criticism. There were several incidences where German authorities unlawfully transmitted health data to law enforcement.

Digital contact tracing

In talks about introducing a contact tracing app, the Federal Minister of Health, Jens Spahn, initially favored the common standard developed by the European consortium Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT). It would fall in line with European data protection law, provide open source software and be interoperable across Europe. However, that approach required the data to be stored on a centralized database. On 20 April, a letter signed by over 300 academics was published strongly supporting a decentralized approach. It argued that it could be problematic to have so much sensitive data on a central server, in particular in countries where fundamental rights are not well secured. Four days later, the CCC sent a letter to the government advocating a decentralized approach. Around the same time, the two tech giants Google and Apple developed the Exposure Notification (GAEN) framework and stated that they would only support a decentralized approach. The government decided to change course and opt for the Decentralized Privacy-Preserving Proximity Tracing (DP-3T).

The Ministry of Health and the RKI entrusted Deutsche Telekom and SAP with developing a contact tracing app – without a cost estimate and a public tender, which such large projects usually require. Following a request from a politician from the Left Party, the Federal Ministry of Finance revealed that the cost of the project could amount to more than 69 million euros by the end of 2021.

The Corona-Warn-App (CWA) was rolled out on 16 June 2020 after two months of development. Ahead of the launch, the government urged the German population to download the app *en masse*. It commissioned its in-house advertising agency with a big promotion campaign to convince sceptics and increase the app's popularity, with success. Within the first 24 hours of its launch, the app was downloaded 6.5 million times. It is the first government app that has ever made it to the top of downloads in the major app stores.

Corona-Warn-App

The CWA's system architecture is based on the decentralized Google/Apple (GAEN) API. It uses Bluetooth Low Energy (BLE) technology to log encounters on an anonymous contact diary. Registration or personal information is not required to install the app. Once installed, the app generates a random key, which is updated every day. When two users are within 1.5 meters of each other for a period of at least 10 minutes, their devices exchange these anonymous codes. The data is then stored on the device for a period of 14 days. When a person tests positive, they can upload the test result by scanning a QR code that they receive from the testing laboratory. Other users are then notified of the risky exposure. If a laboratory cannot generate a QR code, people who were diagnosed with COVID-19 can have their test verified via a telephone hotline. The hotline staff will then generate a teleTAN after performing a plausibility check to prevent misuse. The teleTAN can be used to confirm a positive test result in the app.

Since December 2020, the app has a contact journal where users can note whom they have met in the last two weeks. In January 2021, the CWA received new functionalities, including statistics provided by the RKI on confirmed new infections, warnings by app users or the 7-day incidence rate.

The usage of the CWA is voluntary. Since 19 October 2020, it supports the European interoperability gateway service, allowing it to interact with other European apps. The CWA is open source and the code can be viewed on GitHub. Independent IT experts, including the CCC, which is usually highly skeptical of governmental IT projects, reviewed the source code and found no significant data security or privacy risks. In accordance with Art. 35 GDPR, a detailed data protection impact assessment (DPIA) was released. It can be viewed here (in German). The Federal Commissioner for Data Protection and Freedom of Information (BfDI) and its executive, Prof. Ulrich Kelber, supported the CWA project from the start in an advisory capacity.

A debate sparked around the voluntary aspect of the app. The DPIA highlights that the app's usage is based solely on voluntary consent (Art. 6 GDPR). However, it fails to address the fact that there could be factual circumstances and incentives – such as the government's possible decision to impose further lockdown measures if not enough people use the app – which could render the app's usage *de facto* compulsory. For this reason, civil society actors such as the GFF advocate a formal legal basis for the app's usage, which explicitly prohibits 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 Green Party drafted a new law in June to prevent such measures. However, the ruling coalition did not consider it necessary to establish a legal basis, arguing that the use of the CWA is voluntary, and the processing of personal data is based on the consent of the app's users.

The GFF observed no significant, far-reaching attempts by state or powerful private actors to render the app *de facto* compulsory. While the app suffers from some bugs, no security breaches have been detected. By 11 March 2021, it had been downloaded 26.1 million times and more than 10 million test results (positive and negative) had been shared by the RKI with the users. Since the app's launch, 277,545 users uploaded their positive test results onto the app. There are no statistically significant scientific evaluations, however, about the app's contribution to containing the pandemic.

Several politicians, including Bavaria's Minister President, have claimed that the app is failing to fulfill its role because of high data protection standards. Some went as far as to demand remodeling of the app into a GPS tracking device. BfDI exectuvie Prof. Ulrich

Kelber has rejected those claims. In a piece for *Spiegel Magazine*, he argues that the app was deliberately not developed as a geo-tracking app and that its purpose is to warn people quickly if they were exposed to an infected person. He writes, "what is the added value of the information whether I met an infected person in the supermarket or in the bookstore? It is not the location that transmit viruses – but people". Independent IT experts have suggested adding further updates to the app to improve its effectiveness. These include connecting more testing sites and laboratories to the app, since it remains a big problem that too little users receive and share their tests results through the app. Other proposals include offering automatic cluster detection in cooperation with Apple and Google.

Hungary

Introduction of the apps and (the missing) public debate

Contact tracing app

The first two months 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, Virus Radar, was launched on 13 May.[1] The technology was given free of charge by the Northern 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 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 the ministry's announcement.

As of mid-March, Google Play shows that more than 100,000 users downloaded Virus Radar. 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.

[1] The app was released only for Android at first. At a press conference held by ITM on 13 May, the Ministry promised that the iOS version would become available soon. The iOS version was indeed released a few weeks later, but, presumably because certain problems related to screen lock and battery depletion could not be solved, in mid-September it became unavailable.

Quarantine enforcement app

On 4 May, Government Decree 181/2020 was published. The Decree made it possible for the relevant authority to check the compliance with the official home quarantine rules electronically and modified the procedure for violating epidemiological regulations. The public was not previously informed about the government's plans to issue such an application.

On 7 May, 24.hu reported that a new home quarantine system app became available on Google Play, developed by a Hungarian firm. This app turned out to be the app later used by the police, first on a (somewhat questionably) voluntary basis, then, from 28 October, on a mandatory basis.[2]

The Házi Karantén Rendszer (HKR, Home Quarantine System) application was developed by a Budapest-headquartered software company, Asura Technologies, in cooperation with the Ministry of the Interior, the National Police Headquarters (ORFK) and IdomSoft Zrt. They worked on the map data display with GLI Solutions Kft. The development of the health questionnaires was carried out in cooperation with the National Healthcare Service Center (ÁEEK). According to the official government corona webpage, the license of the completed application was offered to the Hungarian government free of charge.

At the end of May, the authorities reported 1,715 registrations with the app and approximately 1,000 active users. Interestingly, even in late November, when electronic quarantine surveillance was already mandatory by law for people who have the necessary devices, only about one in ten people in quarantine registered with the app. As of mid-March 2021, Google Play showed that more than 100,000 users had downloaded the HKR application.

Technical details

Contact tracing app

The Virus Radar 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,

[2] The use of the app is mandatory only if the subject does own a smartphone device that can run the app. If the subject does not own such a device, the police will visit the subject at the place they quarantine to check compliance. However, it seems that in practice, the police do not enforce the mandatory use of the app.

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.

Quarantine enforcement app

The Home Quarantine System (HKR) app is connected to the police database on quarantine status information. Once a user registration is activated, the user can expect remote monitoring requests sent at random times several times a day through SMS. After receiving such a request, users have 15 minutes to start the app and let it take pictures of the user. The system uses these pictures to verify the location of the user and identify them. Automatic identification is done by Asura Technologies' artificial intelligence-based face recognition algorithm. Upon registration, the user takes a photo of themselves, which is then compared to their photo in the official quarantine database (these photos in turn are acquired from government databases, e.g. pictures on ID cards). If the two pictures match, a biometric template is created based on the picture taken upon registration, and during subsequent check-ins, the selfies taken by the user are compared to this initial template on the user's phone. If the remote control location does not match the home quarantine location specified at registration or the system cannot identify the user on the photo, the case goes to a human operator who decides on the next steps. If the user may have left the quarantine location, the ORFK regional duty officer may decide on a personal inspection.

Reaction of data protection authorities and privacy watchdogs

Contact tracing app

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.

Quarantine enforcement app

In connection with the Home Quarantine System, NAIH issued no opinions or statements either. The watchdog Amnesty International Hungary, however, criticized the authorities for discriminating against those who cannot or do not want to use the app. In their view, although the app was supposed to be voluntary (at that point), the voluntariness is undermined by the fact that the potential fines are higher for those who do not opt in. Those who do not use the app and are found to breach of the rules of home quarantine can expect a fine of up to HUF 500,000 and the police cannot issue a verbal warning only. In contrast, if someone agrees to the electronic control, but violates the rules, they can expect a maximum fine of HUF 300,000 and the police may simply warn them verbally.

Ireland

Corona App Ireland Report

At the start of the COVID-19 pandemic, Ireland reported relatively few infections. In March 2020, the Dáil, Ireland's lower house, passed a controversial emergency legislation that allowed, *inter alia*, medical officers to order the detention of a person believed to be corona positive. Restrictions, including the closure of schools, were relaxed in summer. With rising infection numbers in October, the government announced more restrictions with hopes of a 'meaningful' Christmas. The lockdown ended in December. Soon after, infections surged. In January 2021, Ireland recorded the world's highest infection rate.

Ireland's Health Service Executive (HSE) has a website that contains information related to symptoms, how to protect yourself and others, testing, as well as advice on how to stay mentally sane while confined at home. Together with the Health Protection Surveillance Centre (HPSC), the HSE also developed a data hub that provides comprehensive COVID-19 data in Ireland, such as the total number of confirmed cases, the number of vaccines administered or the incidence rate by local electoral area.

Contact tracing app

In March 2020, the HSE commissioned the Irish tech firm NearForm to develop a contact tracing app. Cost were estimated to be around 850,000 euros. The developers initially planned to build a centralized app. Pressure from privacy activists and Google and Apple's Privacy-Preserving Contact Tracing project, which only supports a decentralized approach, convinced them to change course.

In April, the government officially announced that it was working on the COVID Tracker App. The app's primary purpose is to enable health services to improve the speed and effectiveness of contact tracing and map and predict the spread of the virus in order to contain the pandemic.

A national survey of attitudes conducted in May and published in the Irish Journal of Medical Science revealed that Irish citizens expressed high levels of willingness to download a contact tracing app.

Field trials were conducted in June with members of the An Garda Síochána, Ireland's national police service. Testing results suggested that the app was able to accurately detect 72 per cent of close contacts. In May, however, researchers from Trinity College Dublin conducted a measurement study which demonstrated the unreliability of Bluetooth signal strength for contact tracing, casting doubts about the efficacy of the technology.

On 7 July 2020, COVID Tracker App was launched. The government launched a national communications campaign to make sure that the app had a high uptake. More than 862,000 people downloaded the app within the first day. By mid-January 2021, the app had about

1.3 million active users and sent close-contact alerts to more than 20,000 people.

In August, users with the Android operating system complained that the app was draining their phones' batteries. HSE officially apologized and the issue was later fixed with the help of Google.

COVID Tracker – technical details

The COVID Tracker App is based on the decentralized Google and Apple's Exposure Notification (GAEN) system. Its use is free and voluntary. Users do not need to register or provide personal information when they install the app. They can, if they wish, provide their phone number. The app generates random keys for each and renews them every 10 to 20 minutes. When two users are within 2 meters from each other for at least 15 minutes, their devices exchange these keys via Bluetooth.

The keys are stored for two weeks on the memory of the respective smartphones. When a person tests positive for the virus, they receive a code from the HSE, which they can enter into the app. The users' keys that were generated in the last 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 on its memory are notified of the exposure. If the user provided their phone number, they can also receive a phone call from the HSE.

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. To respect the users' privacy, the app would not record the exact location. With this information, public health services could more easily monitor and manage the virus at national level.

The app is available for people aged 16 or older, the age of digital consent. On 19 October, COVID Tracker App was linked with the contact tracing apps from Italy and Germany. Since February 2021, the app also includes the vaccination headline figures – something a lot of people were calling for on Twitter.

Involvement of civil society and national data protection authority

In April, civil society organizations, including the civil liberties groups Digital Rights Ireland (DRI) and the Irish Council for Civil Liberties (ICCL) advocated the need for transparency and a privacy-by-design approach. Demands also included that the HSE publish the source code and the data protection impact assessment (DPIA).

Similar comments came from the national data protection authority (DPC). In its DPIA review, it recommended regular monitoring and evaluation of the app's efficacy. In case the adoption rate did not "reach a sufficient threshold, the necessity and proportionality of continuing to process the data of those who do use it should be reconsidered."

On 26 June 2020, the HSE released the DPIA and source code of the COVID-19 Tracker App.

Italy

Summary of Corona apps

Status of regional apps

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

Throughout the country, several apps were developed to stop the spread of COVID-19. This brought a multitude of problems, including securing privacy protection for each app or people ignoring or forgetting about the national Immuni app.

Lombardy developed an app designed to collect data and identify potential outbreaks. Users are asked to fill in a short questionnaire (gender, age, previous health conditions, location, if you have been in contact with infected people, if you have symptoms). The questionnaire is anonymous, and the app does not provide for continuous localization. It is still up and running and has more than a million downloads. In Lombardy, the regional government also obtained data from network operators and could thus analyze how many citizens continued to leave their homes despite the lockdowns.

The regional government in Lazio developed an app that connect patients with health professionals. Symptom tracking apps 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 symptoms, they could contact the 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 particularly criticized for using explicit geolocation data of the users.

Federal contact tracing app Immuni

In March 2020, the Minister for Technological Innovation created the initiative "Innova per l'Italia", 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 (Garante), selected the Milan-based startup Bending Spoons, which is part of the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) project.

In April, a group of privacy experts and academics highlighted the lack of transparency in an open letter. The government subsequently published the source code and conducted a data protection impact assessment that it sent to Garante (more on this in 'Involvement of Garante').

On 30 April, Italy's 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 stipulates that the Ministry of Health is the data controller. While the data processed through the Immuni app can only be used to contain COVID-19, aggregated or anonymized 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 in the beginning of June, the app Immuni was finally launched at national level on 15 June. By February 2021, it had been downloaded more than 10 million times, and more than 12,000 users uploaded positive test results.

The government launched an awareness raising campaign in October to encourage people to use the app. Many citizens are reluctant to download the app because of privacy concerns and doubts about the efficacy.

On 7 October, the operation period of Immuni was extended by a year, until 31 December 2021. 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 of Innovation

Immuni – technical details

Immuni's system architecture is based on the decentralized Google/Apple (GAEN) 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 meters for at least 15 minutes, their mobile devices exchange these encrypted keys via Bluetooth Low Energy (BLE).

When users are diagnosed positive with the virus, they receive a code from the public authorities – often after enormous delays of 30 days and more – which they can upload to the app. Every person who has been in direct proximity in the last 14 days will then receive a notification of the risky 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 the individual devices for 14 days. The app also sends, upon users' consent, epidemiological data (e.g., day and duration of exposure) and operational information (e.g., the device's platform) to a central server (located in Italy and managed by SOGEI) in order to help the National Healthcare Service improve the app's accuracy and optimize resource allocation. The Ministry of Health collects the data and decides for which purpose to use it.[3]

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

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

With Germany and the Republic of Ireland, Italy's contact tracing app is one of the first apps from the EU that became interoperable, meaning that it also works in other countries with interoperable software.

Involvement of Garante

The Italian Data Protection Authority (Garante) was involved from the start in discussions about the use of contact tracing apps. They were part of the expert group that selected Bending Spoons' proposal and they helped develop the legal framework surrounding the use of contact tracing technologies. On 8 April, Garante presented its position on the use of new technologies to stop the spread of the virus at a parliamentary hearing. It underlined the importance of voluntary use, data minimization, the need for a well-defined data-retention period and a legally guaranteed purpose limitation. Garante was also consulted by the government for the Law Decree no. 28 of 30 April 2020.

The Ministry of Health sent Garante a data protection impact assessment (DPIA). On the basis of the impact assessment, Garante issued a decision in June 1, arguing that the measures sufficiently protect the rights of the data subjects, and thus authorizing the use of Immuni. It did, however, point out twelve critical features that the Ministry must address within 30 days. These included that users must be better informed about the functioning of the app's algorithm; that they must be informed that the system can generate exposure notifications that do not always reflect an actual risk (false positives); that users must be allowed to temporarily deactivate the app; that the DPIA needs more information on the data subjects' right of cancellation; and that the role of Bending Spoons, Apple and Google must be clarified on the basis of the accountability principle. More details on the twelve points can be found here.

A lack of response from the Ministry of Health prompted Garante to reiterate that any processing of personal data without a proper legal basis is illegitimate and violates European and national data protection law. On 19 October, Garante declared that the Ministry still had failed to address five of the twelve points.

The Ministry of Health delivered a second DPIA to Garante on 16 October, as is necessary to guarantee interoperability. By the time of writing, Garante is still assessing the second DPIA – including whether it addresses the five missing elements.

Lithuania

Lithuania Corona App

On 16 March 2020, the Lithuanian government reacted to the outbreak of the COVID-19 pandemic by declaring a nationwide quarantine. Virus-containment measures included border closures and prohibitions on gatherings. The quarantine was extended several times, while new measures, such as mandatory mask-wearing in public, were introduced. Restrictions were gradually eased starting in May and the quarantine was fully lifted on 17 June. Due to rising numbers, the government imposed a second quarantine on 7 November 2020.

Location tracing app

On 7 April, the government introduced the app Karantinas, designed to monitor the movement of people in mandatory self-isolation. It also has a symptom-reporting function and provides personalized information on preventive action. The app is the product of a joint effort of several actors, including the government, the National Center for Public Health (NVSC), who acts as data controller, and the Kaunas Clinic. It was developed by the start-up Lympo and the municipality of Vilnius. Later, the head of Lympo complained that NVSC never paid for the services. NVSC replied that it lacked funds and never promised to pay. On 15 April 2020, however, the Lithuanian government passed a resolution that allocated 3.5 million euros to the Ministry of Health to purchase various equipment, including the Karantinas app.

Persons diagnosed with COVID-19 received an SMS from the NVSC suggesting that they download the app. Those who decided to use the app had to enter their personal data (name, surname, email, phone number and gender). If they activated the function “mandatory self-isolation monitoring”, the app would record their isolation location via GPS data. Users could be contacted at any time and asked to send photos to prove that they had not changed their location.

In exchange for information about their health status, users of the app were rewarded with points that could be exchanged for awards and discounts in the app store. There were more than 5,500 users by mid-April, according to local news website 15min.

In May, the State Data Protection Inspectorate (VDAI) suspended the app due to possible breaches of European data protection law. It found that it was not clear who the data controller was and therefore that the processing of personal data may have violated the principle of accountability (Art. 5 (2) GDPR). In February 2021, the VDAI imposed two fines on the NVSC and UAB IT Solutions Success, the company that developed the app. The NVSC was fined 12,000 euros for violating Articles 5, 13, 24, 32, 35 and 58 (2) (f) GDPR and UAB IT Solutions Success 3,000 euros for violating Articles 5, 13, 24, 32 and 35 GDPR.

Amendments to Electronic Communication Law to allow location tracking

In March 2020, Lithuanian Transport and Communication Minister Jaroslav Narkevič proposed amendments to the Law on Electronic Communications that would oblige phone service providers to share location data from people subject to mandatory self-isolation. Narkevič said the bill was necessary because some people did not follow quarantine rules. Opposition politicians criticized the move, arguing that this would legalize mass surveillance and violate people's right to private life.

Organizations representing Lithuanian physicians appealed in a letter to members of the Lithuanian Parliament to reject amendments to the Electronic Communication Law, arguing that they would be illegal and unjustly impose mass surveillance on the Lithuanian people. They also signaled that the amendments would "not improve the epidemiological situation". Criticism as to incompatibility of the proposed legislation with the principle of proportionality and European standards on data protection was also expressed by the telecommunications service provider Telia.

The proposed amendments failed to pass in a parliamentary vote on 21 April 2020.

Contact tracing app

In June, the Minister of Health, Aurelijus Veryga, said in an interview that the government plans to purchase a contact tracing app. He announced that the app is scheduled for August. However, it took until 6 November until the Ministry of Health (SAM) announced the launch of the contact tracing app Korona Stop LT. The app is based on the German Corona-Warn-App model. NVSC and SAM commissioned the company Dizaino Kryptis to adapt it to Lithuania for an estimated 19,000 euros. The Ministry of Health is the data controller.

As of 11 February 2021, the app was downloaded by around 300,000 people, which corresponds to about 10 per cent of the Lithuanian population. At the same time, more than 1,000 users reported a positive test result via the app, notifying other users of a potential risky exposure. In order to encourage the population to use the app, the NVSC regularly organizes presentations of the app to municipalities, educational institutions and representatives of various organizations.

Korona Stop - Technical details

Korona Stop is based on the decentralized Google/Apple Exposure Notification (GAEN) system. During the installation process, the app generates unique random keys that are anonymized, also called temporary exposure keys (TEKs), and renewed every day. When two users are within two meters for a duration of at least 15 minutes, their smartphones exchange a pseudorandom ID, which is derived from the current TEK and renewed every 10-20 minutes, via Bluetooth. The IDs, also called rolling proximity identifiers (RPI), are then stored on the devices' memory for 14 days.

When a user tests positive for the coronavirus, they can decide to alert others by entering a 10-digit diagnosis code, which they receive upon request from the NVSC. The app then uploads all the person's TEKs of the last two weeks onto a central server. The app from other users who the infected person has been in contact with in the last two weeks and whose devices saved the IDs are automatically notified of the risky exposure. As the keys are anonymous, users won't know who the identity of the infected person with whom they were in contact. The only time a person must identify themselves is when they give their consent to upload their diagnosis keys via TeleTAN. The identification is necessary to avoid false positives. The use of the app is voluntary.

There has been criticism as to the efficacy of the app. In an interview with the news portal *Delfi,* the software engineer Džiugas Baltrūnas explains that the success of the app was "already buried before it appeared", given the fact that people have to actively request diagnosis codes to the NVSC.

According to Robertas Petraitis, head of NVSC, the National Cyber Security Center performed a data protection impact assessment ahead of the launch of Korona Stop. However, the document has not been published.

Poland

Introduction of the apps and public debate

Contact tracing app

In spring 2020, shortly after the pandemic hit Europe, the Polish Ministry of Digital Affairs declared that it would start work on a mobile contact tracing application to help limit the spread of COVID-19. This triggered a public debate, with critics concerned about privacy and surveillance issues, as well as the efficacy of such an app.

The government made the source code publicly available from the start, enabling Polish programmers, software testers, graphic designers and data protection experts to discuss the best outcome of the app.

On 20 April, the Ministry of Digital Affairs announced the first version of the ProteGo Safe app, which initially only provided information and health monitoring functions. Only nine days later, it produced a newer version that made use of Bluetooth technology and allowed for contact tracing. On 9 June, after a series of controversies surrounding the previous versions (e.g., here, or here), the Ministry produced yet another version – this time using the decentralized application programming interface (API) developed by tech giants Apple and Google (previously it had used the BlueTrace centralized approach).

The application is the result of the work of a coalition of Polish IT companies at the request of the Ministry of Digital Affairs in cooperation with GovTech Polska, under the supervision of the Chief Sanitary Inspectorate. Local media reported about fake Twitter accounts, mostly profiles of doctors and professors, who praised the app on the day of the launch, shared pro-government content and criticized opposition leaders. There was also an idea to prioritize customers in shops who use the app, but the government quickly withdrew that idea after facing public criticism.

Quarantine enforcement app

On 19 March, the Ministry of Digital Affairs launched the quarantine enforcement app Kwarantanna domowa. At first it was voluntary, but on 31 March the Polish Parliament adopted the "Act on special solutions related to the prevention and combating of COVID-19 and other infectious diseases and crisis situations they caused", with Article 7e making it mandatory for people under home quarantine to install the app. The obligation applies to anyone who is subject to mandatory quarantine or potentially infected (e.g., people returning from risk zones abroad), has no visual impairment and subscribes to a telecommunications network or has a mobile device enabling the use of the software.

In July, the Ministry of Digital Affairs concluded a new 12-month contract with the Warsaw-based company TakeTask for the development and implementation of the Kwarantanna domowa app. The costs are estimated at around 2.5 million Polish zlotys (around €555,000).

ProteGo Safe and Kwarantanna domowa – technical details

Protego Safe (now STOP COVID)

The ProteGo Safe application notifies its users about a potential contact with a COVID-19 infected person. The app is controlled and managed by the Ministry of Digital Affairs. It uses Google/Apple Exposure Notifications (GAEN) API, giving it access to the mobile phones' operating systems. Upon installation, the app generates a temporary exposure key (TEK) that is randomly assigned to the user and renewed every 30 minutes to prevent re-identification. When two people meet, their phones exchange the encrypted keys using Bluetooth Low Energy (BLE). Following the decentralized approach, the keys are then stored locally on the devices for 14 days. When a user is diagnosed with COVID-19, they receive from the control center where they tested positive a PIN code, which they can upload to the app. The app then notifies other users who have been in close contact in the last 14 days about the risky exposure.

The app also allows users to monitor their health by providing a risk assessment test and encourages users to keep a health diary. Finally, it provides up-to-date information on the current situation, on local health authorities, such as telephone numbers and addresses of infectious disease hospitals throughout Poland, and informs people about COVID-19 transmission and protective measures.

Despite intensive promotional activities, the population has shown little interest in the app – partly due to poor ratings on Google's and Apple's app stores. By September 6, fewer than 725,000 people had downloaded the app – less than 2% of the population. In September, the government rebranded the app from ProteGo Safe to STOP COVID. In November, the government said that there were almost one and a half million users and announced that people notified by the app of exposure to corona-positive persons could now sign up for a test via the app without having to contact a general physician.

Regarding the efficacy of the app, Tomasz Zieliński, the author of the blog InformatykZakladowy.pl, points out in an article in October 2020, that in the four previous weeks, out of 166,000 Poles diagnosed with the virus, only 241 uploaded their test results on the app.

In early March 2021, the newspaper RMF24 reported that the app had been downloaded fewer than 1.9 million times, adding that it was impossible to know the number of active users. The newspaper highlights that only 3,800 users uploaded positive test results onto the app.

Kwarantanna domowa

The quarantine enforcement app Kwarantanna domowa uses GPS data, and the data is stored on centralized servers from the Ministry of Digital Affairs. It collects users' names and surnames, telephone numbers, declared addresses of residence, photos, citizens' locations and the end dates of quarantine. According to the Polish privacy watchdog Panoptykon, once installed, the app also has permission to see what Wi-Fi network users are connected to, has access to the camera and microphone and can read, modify or delete the content of the device's memory.

The app automatically creates accounts for people who have to quarantine. From 1 April 2020, when it was made mandatory, while in quarantine, users have to take a daily selfie and upload it on the app to prove that they are at home. The app uses geolocalization and a face recognition system so that authorities can make sure that the person taking the selfie is really the person in quarantine. Users have to keep their phones charged and unmuted and regularly check whether they have received an SMS. Once they receive an SMS, they have 20 minutes to complete the task, i.e., send a selfie. If they fail to do so, the police are notified and can visit the user's home to check whether they are respecting confinement.

People who do not install or use the app may be reprimanded or receive fines of up to PLN 5,000 (about €1,128). Local media report (here or here), however, that people can easily avoid the installation of the app by simply stating that they don't possess or have an outdated mobile device. Further, the efficacy of the project is questionable because many persons who are infected do not conduct COVID tests.

Nevertheless, it has become a nuisance. There are reports of SMSs coming before 8am, forcing users to wake up before to check their devices. The app has terrible reviews on Apple and Google, unsurprisingly considering that the government created the app in only three days. In interviews with the media company Politico, Polish citizens report of daily police visits, although the users uploaded selfies on a daily basis, or the app not understanding that the mandatory isolation had ended. The president of TakeTask responded that such issues occur because of problems with the devices, not the app.

The app's privacy policy indicates that the following have access to the data: police headquarters, provincial police headquarters, voivodes (Poland's provinces), the Central Information Technology Center from the Ministry of Digital Affairs, the app's developer Take Task and the Healthcare Information Systems Center from the Ministry of Health. The data is retained for six years, with the exception of the selfies, which are deleted when the account is deactivated.

Unlike the contact tracing app, the Ministry of Digital Affairs decided not to release the source code of the Kwarantanna domowa app.

Reaction of data protection authorities and privacy watchdogs

ProteGo Safe (now STOP COVID)

Early on, many experts were skeptical of the government's plan to launch a contact tracing application. In April 2020, Panoptykon formulated a list of key factors, 'seven pillars of trust', that such an app would have to fulfill if it wanted to gain social trust. These include, a) data minimization and correctness; b) limitation of data storage time; c) data stored on the citizen's device; d) security, encryption and anonymization of data; e) clear information for citizens; f) open code and transparency of algorithms; and g) public control of tools.

On 30 April, the Office of the Polish Data Protection Commissioner (PUODO) drew the attention of the Ministry of Digital Affairs to three problems related to the ProteGo Safe application:

- The need to organize the privacy policy and regulations. PUODO signaled that it was unclear who was responsible for the operation of the application, the Ministry of Digital Affairs or the Chief Sanitary Inspector.
- There was reference to the legal basis for data processing. According to the PUODO, consent is the only acceptable basis for the processing of data of users. It criticized the application's failure to provide in advance reliable information to its users about the data processed.
- The lack of a data protection impact assessment (DPIA).

On 4 June, the government appointed a team of experts with a range of competences: epidemiologists and scientists dealing with risk modelling, data security experts, lawyers (including from civil society), whose task is to observe the work on the application.

Following the launch of the app on 9 June, the government published a series of documents, including the DPIA. The authors of the impact assessment have indicated several potential risks connected with the ProteGo Safe app (translation provided by the Polish Helsinki Foundation for Human Rights):

- possible access to the device's data by unauthorized persons;
- possible use of collected data for other purposes;
- the risk that the backend server would be able to identify persons suffering from COVID;
- possible access to non-personal data at the backend server;
- possible disclosure to other persons that the device's user is using the app;
- possible disclosure to other persons that the device's user is suffering from COVID;
- possible unauthorized modification of the app's code;

- possible suspension of Bluetooth communication with other devices;
- possible loss of statistical data at the back-end server;
- possible fake notification concerning COVID infection;
- lack of users' possibility to access app's content;
- failure to send the notification to the device user regarding its exposure to COVID-19 infection;
- limitation of freedom of people who are not using ProteGo Safe.

According to the Polish Helsinki Foundation for Human Rights (HFHR), the Minister of Digital Affairs tried to consult PUODO about the DPIA, but the latter refused, arguing that the Ministry had not officially initiated the process of consultation under Article 36(1) of the European General Data Protection Regulation (GDPR).

In August, Panoptykon wrote that the app "seems fine" and complies with the principles of good design the privacy watchdog had laid out in April, i.e., the seven pillars of trust. Panoptykon did, however, voice concern over Google's and Apple's role as public service providers, and that the app may give users a false sense of security, making them forget about other precautionary measures.

Kwarantanna domowa

Following the launch of the quarantine enforcement app and in particular the decision by the government to make it obligatory for people potentially infected with the coronavirus, civil society actors and the general public expressed alarm. In April 2020, the Polish Ombudsman, Adam Bodnar, asked the Data Protection Commissioner (PUODO) for an evaluation on whether the app violated the personal data of Polish citizens, referring to the importance for the government to meet the requirements of the GDPR. PUODO replied on 19 June that they did not see the need to take additional actions and rejected the Ombudsman's request to have a closer look at the app. Instead, PUODO provided a list of its activities, such as participation in the work of the European Data Protection Board (EDPB), and consultations that it participated in and simply redirected the Ombudsman to its website, where the latter could find more information.

Meanwhile, according to Mr. Bodnar, citizens have continued to express their privacy concerns. In particular, citizens are worried that for the proper functioning of the app, as users must allow it to access the Internet connection, the camera, photos, location and the microphone. In addition, the information about the application's operations are insufficient. These concerns were already raised by Panoptykon in March. As a result, Mr. Bodnar wrote a letter to the Prime Minister and the Minister of Digital Affairs on 12 November, asking them to evaluate the application's operations. The Ministry of Digital Affairs responded on

30 November, saying that a DPIA had been developed by the Ministry and that the app complies with GDPR requirements. However, as of 15 March 2021, the DPIA has not been published.

Slovenia

Introduction

More police power

On 2 April 2020, the Slovenian Parliament passed the Intervention Measures to Contain COVID-19 Epidemic and to Mitigate its Consequences for Citizens and Economy Act in order to stop the spread of the virus – in a fast-track procedure without any consultations or public debates. The new legislation significantly increased the power of the police. Article 103 enables police to use personal data obtained by the National Institute for Public Health (NIJZ). The information includes the name, identification number (EMŠO), and address of a user as well as information on their general practitioner and on the decision by which the person is ordered to be quarantined, information on the type and duration of the quarantine and more. In its first draft proposal, the government had also suggested to give police the power to trace the location of an individual's mobile phone without a court warrant (Article 104).

The national data protection authority, the Information Commissioner (IC), subsequently issued an opinion criticizing the proposed draft. Specifically, Article 103 could potentially confer enough power to the police to cover the entire Slovenian population and establish a 'police state'. Article 104 constituted "serious interference with the fundamental constitutional rights of individuals" in regard to privacy and data protection, as per Article 37 of the Constitution, which requires a court order for such interferences. The IC also remarked that the government had not consulted with them nor informed the general public and had failed to make a proper data protection impact assessment (DPIA) of the proposed provisions.

The draft proposal also received criticism from the Human Rights Ombudsman, who voiced their concerns over Article 104, questioning the necessity and proportionality of the interference. As a result, the government removed Article 104 from the bill – but Article 103 was retained.

Digital tools to contain COVID-19

In a report commissioned by the European Union Agency for Fundamental Rights (FRA), the Slovenian Peace Institute identified two major web-based initiatives that collected data on the spread of the pandemic. The first collects and analyzes publicly available data to provide the general population with information on the spread of COVID-19. The second initiative, Koronaštevec, is a health reporting website, where people can voluntarily report their symptoms. The collected data is then used to calculate the population's immunity and reproduction rate by looking at the ratio of persons who contracted and recovered from the virus. This allows the website operators to give an estimation about the course of the pandemic.

After its launch on 25 March 2020, the IC received a series of complaints about Koronaštevec and identified two major data protection weaknesses: a) a lack of proper encryption (i.e. the data was not anonymized); and b) the collection of personal data identifying the subjects (i.e. the website collected the personal identification number [EMŠO] and the location of their residence). Accordingly, although it recognized the "noble initiative", the IC asked the project team to ensure the lawfulness of the data processing, inform data subjects, and conduct a DPIA. As a result of the IC's intervention, the website was shut down. However, after the project team complied with the IC's requirements and submitted a DPIA, the website opened again in April.

Introduction of a contact-tracing app

Contact tracing apps were initially not considered. Only in late April 2020, following a video conference of EU Interior Ministers, did the Slovenian Interior Minister, Aleš Hojs, evoke the possibility of an app, commenting that if it was to be effective, it would have to be presented well to the people. On 9 April 2020, the data protection authorities (DPA) had already issued an opinion, giving general remarks, highlighting the importance of a DPIA and transparency for the introduction of a contact tracing app.

On 9 July, the Slovenian Parliament adopted by 50 votes to 23 to pass the Act on Intervention Measures in Preparation for the Second Wave of COVID-19 (also called Fourth COVID-19 Act), creating the legal basis for the use of a contact tracing app, as Reuters reported. According to the new law, people who tested positive for the virus or were currently in quarantine are obliged to download and use the app, cementing concerns about the creation of a police state. Opposition parties and the IC said that the mandatory use of the application was unconstitutional and would breach personal data protection rights. In a press conference a few days later, the Public Administration Minister, Boštjan Koritnik, announced that the app would be voluntary for everyone. However, the law has not been changed since.

On 12 July, the government announced a call for tender for the creation of an app. Six bidders responded to the invitation, and it was the company RSTEAM that ended up signing the contract, with a bid of only 4,026 EUR, as reported by local media. It proposed to develop an app using the open source solution from the German Corona-Warn-App. #OstaniZdrav (#StayHealthy) was finally launched on 17 August for Android, and, since the beginning of September, also for iOS.

#OstaniZdrav – technical details

Like the German Corona-Warn-App, the #OstaniZdrav app alerts users if they have been in contact with an infected person. The app uses Google's and Apple's Exposure Notification (GAEN) system, relying on Bluetooth Low Energy (BLE), without recording users' location or identity. Upon installation, the application generates a temporary exposure key (TEK), which is renewed every 30 minutes. When two persons are close to each other (approximately 1.5 meters) for 15 minutes or longer, their mobile phones exchange the encrypted keys via BLE.

Following a decentralized approach, the keys are stored locally on the devices, preventing authorities or other parties from accessing the data. When a person tests positive for the virus, they receive a code from the National Institute of Public Health. 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. The application's source code is published on GitHub. Installation is voluntarily and free of charge.

The app did not enjoy much interest from the public. One week after the launch, only about 37,400 people had downloaded it. In early September, the government launched a massive SMS promotion campaign, inviting people to install and use the app. The IC received numerous complaints and questions concerning the legality of this campaign, but the IC emphasized that it was not its responsibility, as it falls within the competencies of the Agency for Communication Networks and Services of the Republic of Slovenia (AKOS). The government is also regularly promoting the app via television advertisements and at press conferences.

By 11 February 2021, almost 371,246 users had installed the app, according to the application's official website. For a population of about 2 million, this translates into a penetration rate of around 19 per cent. In February 2021, the number of codes issued by the National Institute of Public Health varied between 213 and 1,297 per day. However, it is unclear how many codes are uploaded onto the app.

In mid-December, the government adopted a decree that *inter alia* made downloading the #OstaniZdrav app a condition for crossing municipal borders. As a result, the number of downloads increased sharply in the days following the decree. However, the move caused great controversy. Legal experts came forward calling it unconstitutional and discriminatory against people who do not own a smartphone. On 25 December, the government backtracked and decided that the use of the app to cross municipal borders would no longer be mandatory.

Involvement of the Slovenian Information Commissioner

The Slovenian government did not involve the IC in the introduction of the app or in the bill that provided its legal basis. On 26 June 2020, the IC issued a statement that it was informed through the media about the upcoming Fourth COVID-19 Act and about the government's intention to make a contact tracing app mandatory for people forced to quarantine. In the statement, the IC listed a series of key points – already published in a general opinion in April – that must be considered when introducing a contact tracing application. They include that location tracking is excessive; that collected data must be minimized (i.e., only relevant data should be collected), properly encrypted and stored on local devices (and not on a central server); that the upcoming bill must precisely define the purpose of the app and clarify that its use is voluntarily; that a data controller is defined; and that a DPIA is carried out before the introduction of such an app.

A few days later, the IC sent an opinion to the National Assembly, calling on it not to adopt the mandatory use of a contact tracing app. It sharply criticized Article 24, which enables authorities and various providers of telecommunication to monitor the location of citizens who use the contact tracing app. A similar measure was proposed in the first COVID-19 Act in April – Article 104, mentioned earlier in this report – but was not adopted due to the strong reaction from the IC.

In July, after the Act was adopted by the National Assembly, the Ministry of Public Administration prepared a DPIA. The IC reacted on 30 July, objecting that the DPIA, which is supposed to point out the risks in the protection of personal data of contact tracing apps, was made *after* the law had passed. The IC argued that even though a government representative publicly stated that the app would be voluntary, the law still said that it is mandatory, with fines between 100 to 600 EUR if people did not use it, creating a contradiction. It also highlighted that no data controller had so far been identified and that there had been no clarification as to the purpose limitation of personal data.

In October, Andrej Tomšič, Deputy of the IC, said at a virtual roundtable at the Faculty of Law in Ljubljana that he did not have major safety concerns but questioned the effectiveness of the app.

Spain

Introduction

Spain was hit particularly hard by the first wave of the pandemic. As a result, the government declared a state of alarm on 14 March 2020, introducing a number of strict measures and a mandatory lockdown, extended several times. Spain also adopted a series of new regulations. The most relevant in terms of collecting and processing people's data is Order SND/297/2020, approved on 27 March. The State Secretariat for Digitalization and Artificial Intelligence (SEDIA) of the Ministry of Economic Affairs and Digital Transformation was given more competences to manage the health crisis, including the development of technological solutions and mobile applications for data collection and the launch of a mobility study (see *DataCOVID below).* An analysis by the foundation Hay Derecho found that the Order is in line with European and Spanish data protection laws.

DataCOVID mobility and lockdown evaluation study

One measure was the launch of a population study called DataCOVID, which analyzed the mobility of people during confinement through anonymous and aggregated data from mobile phones, provided by Spain's main telecommunication operators, including Orange, Telefónica and Vodafone, and presented by the National Institute of Statistics (INE). The study allows authorities to get a better understanding of population movements and take informed decisions to contain the virus (more on the methodology and data collected here). INE's website offers publicly available data, showing to what extent Spaniards followed the confinement orders. On 21 April, for example, almost 90% of Spaniards stayed at home. The study was carried out between March 16 and June 20.

On 14 April, the government announced another study to be run by the Spanish National Scientific Research Council (CSIC). The research team used mobile data obtained by telecommunication operators to study the effectiveness of lockdown measures.

AsistenciaCOVID-19 and Hispabot-Covid19

On 6 April 2020, the government launched the app AsistenciaCOVID-19, which provides its users with reliable information and a questionnaire for self-diagnosis to find out if they are infected with the virus. The purpose, as stated in its privacy policy, is to "reduce the volume of calls to the emergency health center and address doubts about the infectious disease COVID-19". The data collected includes the user's name, phone number, personal ID, address and postal code, birthdate, gender and geolocation (both optional), as well as the health information reported by the users. The data is stored as long as the health crisis lasts, or for a maximum of two years for statistical, research or policy purposes. Users can fill out a form to request the deletion of their data. Local media warned about a possible "permanent surveillance" of citizens, as the app allows for geolocalization. The app was based on the code of the app of the Madrid region launched in March (*see CoronaMadrid below*).

The government also created a chatbot on WhatsApp called Hispabot-Covid19 that offers up-to-date information and advice on the coronavirus pandemic. As with the AsistenciaCOVID-19 app, the objective of the bot is to reduce the pressure on health care telephone lines.

Digital tools developed by Spain's autonomous communities to contain COVID-19

Following the outbreak of COVID-19, Spain's autonomous communities (CCAA), who have the competences in health matters, developed a series of web and mobile phone apps in parallel to the government's AsistenciaCOVID-19. While all provided users with reliable information and advice on the health crisis, some have additional functions, such as self-diagnosis tests, chatbots or heat maps that help authorities understand population movements. Examples include Castilla y León's SACYL CONECTA; Andalusia's SaludResponde; Aragon's Salud Informa; Catalonia's STOP COVID19 CAT; Navarra's CoronaTest Navarra; the Community of Valencia's GVA Coronavirus; the Community of Madrid's CoronaMadrid; and the Basque Country's COVID-19.eus.

In addition, Catalonia introduced in October its own tracking app ContactCovid.cat, which enables people who tested positive for the virus to immediately alert their close contacts and cut the transmission chain by sending an SMS via the app. People who receive such an SMS can then schedule their own PCR test and monitor their symptoms via the app. For more details click here.

The multiplication of apps sparked a privacy debate, as several of them violated data subject rights. For example, in the first version of the web and mobile app CoronaMadrid, which collects personal data from its users, such as the name, birth date, address and email address, the privacy policy stated that the Autonomous Community of Madrid (CSCM) could share the data with national and international security forces, the judicial system, as well as private companies working with the Madrid government. Privacy expert Sergio Carrasco explains that the app requests too much data and access to mobile GPS.

In 22 March, for the new version 2.0, CSCM updated the privacy policy, clarifying what data is collected and for what purpose, i.e., to describe the pandemic and predict how it may evolve in the future. It also clarified that the private companies involved would not be allowed to use the data for their own purposes and would only receive temporary access. Finally, the new privacy policy assured that geolocation would be optional, and would not be used to monitor whether people quarantine or not, as is done for example in Hong Kong.

In October, Xunta de Galicia launched PassCovid, an app that allows users to register at a restaurant or a hotel via a QR code. If a person visits an establishment and is later has a diagnosed case of COVID-19, other visitors can be notified via the app. In February 2021, Castilla-La Mancha reopened its hospitality industry. Bars and restaurants can reopen, but only under the condition that they force their customers to check-in via a QR code.

Contact tracing app Radar COVID

The development of a contact tracing app, for which the Secretary of State for Digitalization and Artificial Intelligence (SEDIA), headed by Carme Artigas, is responsible, took relatively long. Talks about such an app started in April but it was only in June that concrete plans were made.

On 15 June, SEDIA concluded a contract with the company Indra Sistemas SA for about €330,000 to develop the contact tracing app Radar COVID, designed to alert users if they have come into contact with a person diagnosed positive with the virus. Several irregularities were later discovered relating to the contract SEDIA concluded with Indra, approved under the emergency procedure and therefore without a tender. Amongst others, the contracting agreements were published too late, according to the country's Public Sector Contract Law (LSCP).

On 23 June, the Council of Ministers approved the launch of a pilot project on the Canary island of La Gomera. Authorities simulated four waves of fictional COVID-19 outbreaks to test the efficiency of the app. The pilot test ran from 29 June to 31 July. The objectives were to measure a) the adoption rate, i.e., the number of people who download the app; b) the retention and engagement rate, i.e., the number of people who keep and actively use the app; and c) the app's performance in tracing risky exposures.

On 3 August, the government declared the testing phase a success. The first target, to reach 3,000 downloads (for a population of about 22,000), was exceeded (there were about 3,200 downloads). The second objective was also satisfactory, as 83% of users kept the app on their phones and 61% communicated the fictitious positive results by entering a simulated code on the app. Finally, the app's performance was also deemed a success, as it detected on average 6.4 risky exposures – compared to an average of 3.5 when done manually. The government also pointed out the favorable user reviews.

However, it took a while before the app was introduced across the country, as the regions (CCAAs) are responsible for integrating the app into their health system. For it to work, they must complete a technical process that then allows the health centers or private doctors to provide diagnostic codes to people who tested positive for the virus. On 26 August, SEDIA announced that eight of Spain's 17 CCAA had activated Radar COVID. People living in Madrid and Catalonia, the two communities with the highest numbers of infections, had to wait until 8 and 27 October, respectively, to be able to use the app.

In the beginning of September, a group of more than 200 leading researchers criticized the lack of transparency from the government, and in particular SEDIA, and demanded the publication of the app's source code so that experts could analyze it and guarantee its reliability. In their open letter, they argue that "without an open procedure that enables the involvement of the entire community and the recipients of the app, [the Radar COVID app] will not enjoy the trust necessary for its mass adoption."

When on 9 September the government finally released the code external experts found it "incomplete and confusing" and discovered several issues. First, the code was obfuscated, a common practice to prevent copying, but senseless if it is made public, as was the purpose. Second, the code's version was not the same as the one that millions of Spaniards were currently using, but a trial version.

Further questions arose about the app's use of Firebase, a software from US tech giant Google, which is not mentioned in the app's privacy policy, as required by EU data protection law. Firebase serves to detect bugs, but it also collects information on the use of the app, such as how long people use it, how often it is opened or the type of phone of the users. Firebase data is shared with Google.

In October it was revealed that the app had a security breach. Unlike most other European contact tracing apps, Radar COVID did not generate 'dummy traffic', which protects people who upload positive results from being identified by those who can observe the traffic between the app and the server – including Amazon, which provides the software to upload results onto the server, and internet service providers (ISPs). SEDIA later fixed the vulnerability, although, according to national newspaper El País, it took longer than announced.

On 9 December, SEDIA concluded a new contract with the company Indra Sistemas SA for about €1,740,101 to continue with the maintenance and update of the app for a period of 24 months, approved again under the emergency procedure, and therefore without a public tender.

Figures about how many people downloaded or are actively using Radar COVID are not provided by SEDIA because it devolves this responsibility to the CCAAs. Local newspapers reported about 4 million downloads by mid-September and a study conducted by the consulting firm Smartme Analytics reported of a penetration rate of 14.4% in November (about 7.2 million). In mid-November, El País reported that only about 1.45% of positively diagnosed persons uploaded their results onto the app. By the end of January 2021, 6.8 million people had downloaded the app and 42,000 positives had been registered in the app, according to El País.

Another issue regarding efficacy arose from the fact that not all health centers or private doctors knew how to issue diagnostic codes to people with positive test results. While the app detects a high level of exposures, users do not receive the expected number of diagnostic codes that they can enter into the app to alert others who have been in close proximity. SEDIA blamed the CCAAs for poorly managing the distribution of codes.

Radar COVID has its own Twitter and Instagram account, which SEDIA uses for promotional purposes and to regularly assure people that the app is in line with Spanish and European data protection laws. In November, Radar COVID joined the club of interoperable apps.

Radar COVID – technical details

RadarCOVID is based on the decentralized Google/Apple API system (GAEN). It uses Bluetooth Low Energy (BLE) to log encounters on an anonymous contact diary. The app is free of charge and installation is voluntary. It does not require users to enter personal information. Upon installation, the app randomly generates a temporary exposure key (TEK), which is changed several times an hour.

When two persons meet within less than two meters and for a minimum of 15 minutes, their mobile devices exchange the current TEKs via BLE. These are then stored locally (on the mobile devices) for 14 days. When a person tests positive for the virus, they receive a code from the public health service that they can enter into the app. The app then assesses the infection risk based on the duration of the encounter and the distance between the two devices and alerts other users about the potential risky exposure.

The app is owned by the General Secretariat for Digital Administration (SGAD), which is dependent of the SEDIA. Its code is publicly available on GitHub. More details can be found on the website's privacy policy.

Involvement of the Spanish Data Protection Agency (AEPD)

Following the outbreak of the pandemic, the Spanish Data Protection Authority (AEPD) issued a series of communiqués to raise awareness of potential dangers and position itself about the use of new technologies to limit the spread of the pandemic.

On 16 March 2020, it warned about unofficial web and mobile apps that proliferated and collected sensitive health data, pretending to be from the Ministry of Health.

On 26 March, AEPD issued a statement on COVID-19 self-assessment apps and websites, in which it states that the current situation "cannot imply a suspension of the fundamental right to the protection of personal data. But, at the same time, the regulations for the protection of data cannot be used to obstruct or limit the effectiveness of the measures adopted by the competent authorities, especially the health authorities".

On 30 April, it warned about the possible risk of discrimination and creating a false sense of security regarding the use of infrared cameras to measure temperature at specifically designated public spaces, such as shopping malls.

In May, AEPD published a study in which it analyzed the different technologies developed to fight against COVID-19 and the risk they pose to the privacy of data subjects. It focused on seven different technologies, including geolocation through data collected by telecommunication operators, self-assessment and symptom-reporting apps and websites, and Bluetooth contact tracing apps. Regarding the latter, it specifies that risks come inter alia from re-identification, the collection of data from third parties and the storage of data on central servers. The full report can be accessed here.

On 21 May, AEPD indicated in a tweet that it would be launching an investigation into the government's plans to launch a contact tracing app (what would become Radar COVID): "The AEPD begins investigative actions to obtain information on the app for tracking possible COVID-19 infected [persons] announced yesterday by the Vice President and Minister of Economic Affairs, project of the Secretary of State for Digitalization and Artificial Intelligence".[4]

On 23 June, the government announced the launch of Radar COVID's pilot project and SEDIA indicated that AEPD "participated in the process prior to the launch of this pilot and will also participate in the evaluation of the results in order to propose improvements that guarantee privacy to users at all time".

AEPD reacted to the press release by clarifying that its involvement in Radar COVID was actually very limited and complained about the poor collaboration with SEDIA, in particular the latter's unwillingness to provide enough information to assess whether it complied with the EU's General Data Protection Regulation (GDPR).

On 8 September, the non-profit organization Reclamadatos filed a complaint with the AEPD against the SGAD, the body in charge of the implementation of Radar COVID App, to investigate whether the app complies with EU data protection laws. Reclamadatos asked AEPD to confirm that the app falls in line with the principles of lawfulness, fairness and transparency (Article 5 GDPR) and pointed out that the SGAD still did not publish a data protection impact assessment (DPIA), although this is expressly indicated in the guidelines of the European Data Protection Committee (EDPB). Further, Reclamadatos pointed out that the app's privacy policy had not defined the functions and responsibilities of the health authorities of the CCAAs (Article 13 and 14 GDPR). AEPD incorporated the complaint into its on-going investigation of the Radar COVID app.

[4] *Translated from Spanish by author*

Sweden

Introduction

Sweden has stood out from other countries in the European Union, in that it did not adopt early strict measures to contain the spread of the virus. Instead, Sweden encouraged the population to be responsible and provided guidance on distancing and other measures individuals could take.

Analyzing mobile phone data

In April 2020, Sweden's Public Health Agency received access to customer data of Sweden's largest mobile phone operator, Telia, in order to study people's movements during the pandemic. Telia assured the public that the data collected was aggregated and fully anonymized and could never be traced back to an individual. The Minister for Digitalization supported the phone tracking measure.

COVID Symptom Study

Sweden does not have a contact tracing app. Instead, several digital tools were developed to help stop the spread of COVID-19. One of them is the symptom tracking app COVID Symptom Study, a research project by Lund University and Uppsala University, which aims to get a better understanding of the epidemic and map the spread of the virus in Sweden. The research team says that participants should enter their symptoms into the app on a daily basis for it to make sense. Upon installation, participants have to give their email address, which remains disclosed. The location of the user is based only on the first two digits of the postal code. The publicly available data is intended to help predict outbreaks and enable a good allocation of resources and testing capacities. It was launched on 29 April. By November, almost 200,000 people had participated in the study. The app was developed by British health company ZOE Global Ltd.

Corona App

A collaboration between the Swedish Civil Contingencies Agency (MSB), the Public Health Agency of Sweden and the National Board of Health and Welfare saw the emergence of another digital tool, the so-called Corona App. It consisted of a questionnaire that would be used to map the spread of COVID-19 and study behavioral changes of Swedes as a result of the pandemic.

However, the project was plagued with a series of issues. On 9 April, MSB contracted the private health technology company Platform24 to develop the app, without a public procurement procedure. MSB justified the decision because of the urgency and the necessity "to protect people's lives and health". The argument was rebutted by Andrea Sundstrand, professor of public law at the Stockholm University, and the Swedish Competition Authority launched an investigation to check the legality of MSB's decision.

Human rights defenders and IT experts also pointed out privacy risks, as Platform24 used the cloud service solution Amazon Web Services (AWS), owned by US tech giant Amazon. Under US legislation, this gives the US the right to request information and data from the servers.

The project was finally canceled on 8 May and MSB took full responsibility. Local news reported in May that the scrapped project cost Swedish taxpayers around SEK 6.5 million (almost €620,000); others noted that the costs could even be as high as SEK 15 million (about €1.5 million).

Involvement of the Swedish Data Protection Authorities

On 27 March 2020, the Swedish Data Inspectorate published their position in regard to digital tools that make use of mobile phone data to track the spread of the pandemic. Following the development of the Corona App, the Swedish Data Protection Authority (DPA) warned about storing sensitive data on Amazon's cloud service. It did not, however, see the need to conduct a data protection impact assessment (DPIA), as the processing of data "is unlikely to lead to a high risk for the rights and freedoms of natural persons". Despite this assessment, MSB decided to contract the law firm Delphi to make a legal risk and vulnerability analysis regarding the use of a single-cloud service solution. In its report, Delphi highlighted inter alia that the terms of agreement between Amazon's cloud service AWS and Platform24 were very favorable to AWS.

Memos

Austria

Austria was among the first countries in Europe to launch a contact tracing app when it did so in March 2020. Being in the vanguard of contact tracing apps, there was much public debate concerning data protection and the voluntary basis of the "Stopp Corona App".

The Austrian Red Cross (ÖRK) commissioned the development of a coronavirus tracing app to help break the chain of coronavirus infections. While the Stopp Corona App was being developed, the Austrian National Data Protection Authority (DSB) pointed out key elements to consider in the development of the contact tracing app, including the principles of privacy by design and privacy by default (Art. 25 GDPR) and data minimization.

The ÖRK's Stopp Corona app was endorsed by the Austrian government. The ÖRK serves as the data controller of the tool. Accenture, a private consulting firm, developed the app and the project was financed by the UNIQA Foundation, which donated EUR 2 million.

Increased transparency due to published source code, data protection evaluation and an official online platform

In order to increase transparency and trust in the tool, the source code was published for independent groups of privacy experts and academics. Experts from epicenter.works, noyb.eu, SBA Research and Armin Ronacher (independent) reviewed the source code of version 1.1. and found that *"additional requirements and technical limitations on the smartphone operating systems of Google and Apple led to an architecture that has certain problems"*. Subsequently, out of the 25 recommendations, 16 were quickly implemented by a hotfix, while the remaining recommendations were solved with the new release and ultimately with the new architecture of the app. More on this can be found here.

As of today, the Stopp Corona App is based on the decentralized Google Apple Exposure Notification System (GAEN). It logs encounters via near-field sensor technology using Bluetooth Low Energy. The pseudorandom ID, derived from random UUID (temporary exposure key), is stored for 14 days on the smartphone. In case of an infection, the Red Cross records the user's phone number for 30 days to prevent abuse and to be able to contact the person for any necessary assistance. The use of the app is completely voluntary. No personal information is required for the installation of the app. The data is exchanged in an encrypted form so that users cannot identify the infected person.

The ÖRK conducted a data protection impact assessment (DPIA) on the Stopp Corona App. On the basis of the assessment, 32 risks were identified including: discrimination on the basis of the processed data, especially on the account of health status and behavior; the potential that unauthorized persons can access data; and fear that social distancing measurements will be thwarted. For the minimization of these untenable risks, technical and organizational measurements were identified and adopted. These included: data minimization, such as disabling the server from knowing who had contact with whom; sick reports being recorded anonymously; and the establishment of an authorization concept for accessing the data. A more detailed list of the risks and adopted measurements can be accessed from here. Nonetheless, this DPIA did not touch upon which measurements were eventually implemented and whether they were effective.

Low popularity blamed on loss of trust

As of February 2021, the app had been downloaded more than 1.36 million times (about 16% of the total population). Around 10,000 users warned their contacts via the app, according to estimations of Federal Rescue Commander Gerry Foitik.

Many citizens are reluctant to download the app because of privacy concerns and doubts about the efficacy. The Vienna Center for Electoral Research found that half a year after the Stopp Corona app was launched, skepticism still prevailed among the public. Many fear that if they receive a red warning they will be submitted to quarantine and surveilled via their smartphone.

Public insecurity and distrust increased when Interior Minister Wolfgang Sobotka invoked the possibility of making it mandatory. In order to build confidence and convince the general public to use the tool, the government created a website to provide transparent information on the app.

Czechia

Emergence of the contact tracing app

The development of the contact tracing app "eRouška" (Czech for "eMask") in the Czech Republic is the result of a joint activity of Czech technology companies and IT enthusiasts, who united in an initiative called COVID19CZ. The app is part of the "Smart Quarantine" strategy, which has been developed by the same Initiative. The strategy intends to limit the spread of the virus, trace and quickly isolate infected individuals, and assure wide availability and distribution of medical supplies. Apart from the app, the "Smart Quarantine" includes other technological solutions such as "Maps.cz" (where people may voluntarily save locations they have been to and declare themselves as being infected once they receive a positive test) and "Memory Map" (based on the interview between the health care worker and infected person, where the latter voluntarily names individuals he/she has been recently in contact with). The founders of COVID19CZ from the data operations platform Keboola said that the initiative *"wasn't just some 'hackathon' where something was done to throw it in the trash. Our projects are being taken over by the state and will be better prepared for the next crisis."*

The first version of the application, launched on 20 April 2020, is covered by a 6-month free cooperation agreement between Keboola and the Ministry of Health, which confirms Keboola's voluntary assistance. The second version of the app has been in operation since August 2020, following an agreement between the Ministry and the National Agency for Communication and Information Technologies (NAKIT). The Agreement was concluded on the basis of Governmental Resolution No. 576 of 25 May 2020, which defined a joint task to implement the Smart Quarantine strategy 2.0 through mutual cooperation between the Ministry and NAKIT. The application is currently supported by the NAKIT employees and a group of individual NAKIT contractors that includes members of COVID19CZ.

As of February 2021, the app had been downloaded more than 1.5 million times (approximately 14% of the Czech population). 60,803 individuals who tested positive notified others through the app and 236,512 users were notified about risky encounters.

eRouška - Technical Details

The contact tracing app generates a random ID every 10-20 minutes and exchanges it via Bluetooth Low Energy (BLE) technology with other active eRouška apps. The keys of other apps encountered by the app are stored on the respective device for 14 days, after which they are automatically deleted. The app calculates that there has been a risk of the infection when two users are in a proximity of 2 meters for a period of 15 minutes at least. The app uses measurement algorithms such as the length of the encounters set up by the Google/Apple Exposure Notifications Application Interface (GAEN).

If a user tests positive for COVID-19, they will be contacted by a healthcare provider and notified about further steps. Test results are sent by the laboratories to the central information system of the Ministry of Health. All individuals who provided healthcare services with a phone number will receive a one-time random verification code from the health office's system via SMS. This code is valid for a period of 4 hours and needs to be typed in the app in order to notify other users. After that, infected individuals and the users who have been in close contact will receive instructions on how to proceed.

eRouška - Data Protection

The earlier version of eRouška was reviewed on the basis of data protection several times by the Czech IT Agency Ackee, faculty of the informational technologies of the Czech Technical

University and the independent think-tank IDEA (The Institute for Democracy and Economic Analysis). The latter had confirmed that eRouška offers a high degree of privacy protection and follows the principles of decentralisation and data security. The external ethics expert from the European Commission, Ondřej Veselý, described the app as *"only working with the data it really needs"* and being *"an exemplary fulfillment of the principle of data minimization."*

The Czech Association for Personal Data Protection made a statement in September 2020 indicating overall satisfaction with the technical solution chosen by the Ministry. The Association concluded that technical features of the app minimise the scope of the processed personal data and significantly reduce the potential risk of its misuse.

However, the national data protection authority - Office for Personal Data Protection (hereafter "the Office"), was not fully satisfied with the app in the first stages. On 1 July 2020, the president of the Office, Ivana Janů, expressed criticism towards the Ministry of Health, claiming that it failed to consult on the Smart Quarantine Project, which includes the introduction of the app, with the Office. The President pointed out that they *"did not receive all the data on the basis of which the Office could evaluate the entire process of processing personal data."* She added, however, that *"it wasn't something they didn't want to give us. It was more like liquid sand, the project was constantly changing and to this day it does not have a basic shape that could be checked."*

On 6 October 2020, the next president of the Office. Jiří Kaucký, confirmed that it was not possible to dispel the ambiguities around the app as they did not receive the data protection impact assessments (DPIAs) of the two versions of eRouška (1.0 and 2.0) from the Ministry of Health. On 27 October 2020, the Ministry of Health issued a letter indicating that the DPIAs would soon be finalized. In an interview with a local newspaper, the founders of eRouška praised the Ministry for its flexibility and ability to work under pressure.

Cyprus

Emergence of the contact tracing app

The contact tracing app in Cyprus was developed voluntarily and free of charge by the former Research Centre of Excellence RISE (now CYENS Centre of Excellence). The RISE (CYENS) is a joint venture between the three public universities of Cyprus, the Municipality of Nicosia, the Max Planck Institute for Informatics (Germany) and the University College London (UK). The app was created as a response to the call of the Deputy Minister for Research, Innovation and Digital Policy to find quick and innovative solutions to the COVID-19 pandemic.

The app, called "CovTracer", which was based on GPS technology, was launched on 5 April 2020. The Deputy Ministry of Research, Innovation and Digital Policy supported and promoted the widespread use of the app, emphasising at the same time that the primary target group of the CovTracer are *"mainly doctors, police officers, firefighters or other citizens who are out on the street and working. If you are at home, you do not need to download it."* To facilitate the management of the pandemic, users of the CovTracer were able to share with CovTracer the information about their location for the previous 2 weeks.

At the same time, another tracing app, based on Bluetooth technology, was developed, but it was not launched in 2020 due to privacy concerns. The Deputy Ministry of Research, Innovation and Digital Policy has explained that they needed more time to adapt the app to the laws on personal data. CEYNS and KIOS Research Centres perform the function of data processors of the app, the Ministry of Health as the national data controller, and the Ministry of Research, Innovation and Digital Policy as an advisor. The app was released on 12 January 2021, and since 1 February it has been the only official app of Cyprus. The former app CovTracer was removed from Google and Apple stores.

CovTracers - Technical Details

The former CovTracer was designed on the basis of Safepaths technology, developed by the Massachusetts Institute of Technology. The Safepaths technology was created to maximise the effectiveness of contact tracing, enabling at the same time a high level of data protection. The CovTracer was using GPS information to trace a person's movements during the course of a day. If the person was tested positive with COVID-19, the one may have chosen to share the geolocation data of the movements of the last two weeks with a contact tracer. The contact tracer then could check the information and take actions (e.g., to evacuate areas, perform cleaning or to inform people who were in close touch with the corona-positive person).

On 16 March 2021, the government presented the contact tracing app CovTracer-EN, which replaced the original app. The CovTracer-EN's privacy notice, last updated on 15 December 2020, states that it does not collect any location data and works via Bluetooth Low Energy (BLE) technology. The app generates random IDs every 10-20 minutes and exchange them through BLE between the other users. The keys of other apps encountered by the app are stored on the respective device for 14 days and are automatically deleted after this period. The app calculates the risk of infection when two users were in proximity of 1.5 meters for a period of 15 minutes at least. The app uses other data such as the length of the encounters set up by the Google/Apple Exposure Notifications Application Interface (GAEN).

If a user has been tested positive for COVID-19, they will be contacted by a healthcare provider and notified about further steps. The data controller is the Department of Epidemiology (DoE) of the Ministry of Health. Individuals who tested positive will receive a one-time random verification code from the health system via SMS. This code needs to be typed into the app in order to notify other users. After that the users who have been in close contact with affected individual will receive instructions on how to proceed. By the end of March 2021, CovTracer-EN was downloaded by less than 8,000 people (about 8,5% of Cyprus's total population).

CovTracers - Data Protection

Regarding data protection concerns, the Deputy Minister for Research, Innovation and Digital Policy assured on 6 April 2020, that the first app CovTracer fully respects the provisions of the Law No. 15 of 2018 on the Protection of Individuals Against the Processing of the Personal Data. He has added that *"the data are recorded exclusively and belong to the user, are not transmitted anywhere else. Only the user has access to this data and it remains exclusively on his device"*. The Deputy Minister emphasised that they were in contact with the Commissioner for Personal Data Protection (hereafter "the Commissioner") in order to provide a proper implementation of the app.

On 6 May 2020, the Commissioner stated that even though the CovTracer is based on the legal basis of the user's consent, it must also comply with all legal principles of personal data processing. The Commissioner emphasised that the Bluetooth-based apps impose a lower risk to users' privacy than those that map and track users' paths. This notice was taken into account and resulted in the development of the Bluetooth-based app CovTracer-EN.

On 12 January 2021, the Commissioner said that implementation of the app *"has followed the guidelines of the European Commission and the guidelines given by the Commissioners of the Member States."* The source code of the CovTracer-EN is publicly available.

Denmark

Emergence of the contact tracing app

The development of a contact tracing app in Denmark was one of the solutions of the government's strategy to ensure a controlled and responsible reopening of society, starting in April 2020. An app "Smittestop" (Danish for "infection stop") was developed free of charge by the Danish IT services company Netcompany on its own initiative in collaboration with the Ministry of Health and the Danish Agency for Digitisation. Netcompany was also involved in the creation of the Danish app COVIDMeter, launched in the beginning of April 2020, through which citizens can complete weekly questionnaires about their health status and contribute to the work of the health authorities.

To ensure a better security and privacy protection of the app, the Ministry of Health created an Advisory Board that included five experts from the related fields. The main role of the Advisory Board was to contribute its knowledge, advice and assessments concerning the protection of privacy and technological choices. On 15 May, the Danish government entered into a political agreement on the principles, purpose and technological solution for the Danish contact tracing app. The government determined the principles on which the app should be developed, among which the voluntary usage, decentralisation of data and compliance with security requirements.

Smittestop was launched on 18 June 2020. As of January 2021, the app had been downloaded more than 2.1 million times (approximately 34% of Denmark's population). More than 53,000 users reported being infected in the app. According to the Ministry of Health, almost 88,000 people made an appointment on the official Danish COVID-19 test booking platform after being notified of a risky exposure via the app.

Smittestop - Technical Details

The contact tracing app is based on the DP-3T (Decentralised Privacy-Preserving Proximity Tracing) implementation protocol and uses the Exposure Notifications Application Interface provided by Google and Apple (GAEN). Smittestop works via Bluetooth Low Energy (BLE), which allows phones to exchange signals between each other. The phone calculates that there has been a risk of the infection when two users were in a proximity of 2 meters for a period of around 15 minutes. Tracking codes and details of encounters are stored on the respective devices and are removed automatically after 14 days.

If a user has tested positive for COVID-19, they can find their result on the official portal for the public Danish Healthcare Services. If the person chooses to notify other users, they need to log into the app using NemID (special personalised code used in Denmark) to confirm a positive result. After that, the Danish Microbiology Database (MiBA) detects whether an notice concerning the positive COVID-19 PCR test has been sent by the health care provider. If yes, the system confirms an infection on the app's server. After that, infected individuals and the users who have been in close contact will receive instructions on how to proceed.

From November 2020, Smittestop is interoperable with several other European contact tracing apps. When a person receives an alert in the app, they cannot see whether it comes from the user of Smittestop or another European contact tracing app. To share a notice of infection directly with Smittestop, the person needs to have tested positive in Denmark.

Smittestop - DPIA and further development of the app

In June 2020, the Danish Agency for Patient Safety prepared a data protection impact assessment of the Smittestop app. The Data Protection Adviser for the Ministry of Health has also been involved in the preparation of the DPIA and commented on the various versions of the document. The DPIA identified the risks to the data subjects, such as the possibility of the users' personal data loss, and set out measures aimed at countering these risks. The Danish Agency for Patient Safety mentioned in the DPIA that *"in accordance with Article 36 of the Data Protection Regulation they are not obliged to conduct a prior consultation* *of the Danish Data Protection Agency, as there is no high risk for the data subjects after implementation of the recommended measures".*

Prior to the launch of the Smittestop app, the Danish Data Protection Agency (Datatilsynet) published an announcement identifying basic data protection considerations that, in their opinion, should have been kept in mind during the development of the app. This included the principles of the voluntary usage of the app, transparency and the secure storage of information. The agency emphasised that the data controller must keep the necessary balance between the needs for solutions to the "extraordinary situation", such as coronavirus pandemic, and the rights of individual citizens. This reflects the idea of a "minimum medium principle", according to which "*no measures should be implemented that could have been achieved by using solutions that are less intrusive for the individual citizen.*" Therefore, one of the tasks of the health authorities is to consider the time during which the collection of the information is necessary and to ensure that the information collected is deleted after the respective period.

In contrast with some other European contact tracing apps, the developers of Smittestop decided not to make the app's source code available to the public. They believe that it would "*increase the risk of security breaches as persons or organisations with malicious intentions will be able more easily to hack or otherwise attack the solution*".

The current contract between the Danish Agency for Digitisation and Netcompany expired on 31 March 2021. Further development, maintenance and operation of the Smittestop was sent by the Danish Health and Medicines Authority for a tender with a deadline for applications on the 3 February 2021.

England & Wales

Within the UK, England and Wales, Scotland, Northern Ireland, Jersey, and Gibraltar have their own separate contact tracing applications. This document reports only on the NHS COVID-19 app in England and Wales.

As COVID-19 unfolded, the UK's National Health Service (NHS) set up official tracing programs to monitor and control the spread of the virus. The NHS COVID-19 app, operating in England and Wales, held to play a key role in England's NHS Test and Trace service and the NHS Wales Test, Trace, Protect program, supporting the traditional contact tracing apparatus.

The NHSX, the NHS's digital healthcare innovation unit, started building a contact tracing app in April with support from VMware Pivotal Labs. The app's first design followed a centralized data collection structure, which received much criticism due to concerns over whether the tool would be effective provided an insufficient user uptake and whether the centralized nature would lead to privacy breaches. Research institutes – the British Computer Society and Cass Business School – urgently called for testing before the app would be launched. Due to the pressure, a trial test took place on the Isle of Wight in May, which revealed that the app could only recognize 4% of Apple devices and 75% of Google Android phones – meaning the app went to sleep quickly when it was not used and therefore the server could not trace the device anymore.

After the revelation of the technical mishap, Matt Hancock, Secretary of State for Health and Social Care, announced that the NHS would turn to the decentralized Google-Apple Exposure Notification (GAEN) API. Silkie Carlo, director of the privacy charity Big Brother Watch, commented, "*This just shows what a mess the centralized data-hungry approach was. Government was wrong to waste precious time and millions of pounds of public money on a design that everyone warned was going to fail, and now we're back at square one.*" Eventually, the postponements of numerous scheduled launch dates – which in the end added up to a 4-month delay – further undermined the tool's public image.

The official NHS COVID-19 app was eventually launched on 24 September. The UK Department of Health and Social Care (DHSC), the data controller of the app, conducted a data protection impact assessment (DPIA). The DPIA stresses that principles such as privacy by design and default, data minimization, user protection, and secure data processing were fundamental to the app's design.

The role of the national data protection authority

In the UK, the role of data protection authority – the data regulator – is played by the Information Commissioner's Office (ICO). Elisabeth Denham, the UK Information Commissioner, noted that from the beginning, the ICO was included in discussions around data protection and contact tracing apps and was consulted on the app's development from the start of the project. In April 2020, the ICO published a formal opinion on the Google-Apple Exposure Notification API, which concluded that the contact tracing framework "*is aligned with the principles of data protection by design and by default" and called for the clarification of app users about who is responsible for data processing*". In the next steps, the ICO developed a detailed 'expectations document' which served as a reference point throughout. This document "*sets expectations on how contact tracing solutions may be developed in line with the principles of data protection by design and default, and includes a series of best practice recommendations*". The ICO's feedback, centered around the transparency, legality and fairness of the app, prompted changes, which were carried out by the DHSC before the app was launched in September. These included: improved privacy information towards the app users; clearer information on automated decision-making, including the reasoning behind the algorithm; further transparency measurements; and greater clarity on data flows and security considerations.

Technical details

The app, which was fundamentally rebuilt from the first version tested on the Isle of Wight, has two major changes. First, it is based on the decentralized Google-Apple (GAEN) API. Second, it has a check-in functionality: app users are asked to scan a QR code, in order to mark their presence when entering venues such as restaurants, pubs and hairdressers. This function aims to help contact tracers in cluster-busting, which is the pinpointing of all those people who might have been exposed to a super-spreader event. The digital check-in is not mandatory and venues must offer a paper-based form, too.

Once the NHS COVID-19 app is downloaded, a code will be generated to identify the app's existence on the device. This code changes every day to prevent user identification. The app produces rolling proximity identifiers (RPIs) every 15 minutes. These RPIs are gathered by another user's NHS COVID app, provided the devices are within 2 meters from each other for at least 15 minutes. Bluetooth Low Energy is used to log encounters. This data is stored locally on the phone for 14 days. When installing, app users are asked to provide their postcode district to help the NHS with finding out more about the impact of coronavirus on the community services, to manage local hospital services and monitor the effectiveness of the app. For privacy reasons, only the first part of the postcode is shared with the NHS.

Using the app is voluntary. To incentivize its adoption, major network providers agreed to not deduct any data used by the app from subscribers' monthly mobile fees. Zühlke, a Swiss software engineering firm, participated in the building of the NHS's decentralized version. The source code is available on Github. Self-isolation, advised by the app, is voluntary. The NHS COVID-19 app has a self-isolation countdown timer function that lets users know when the confinement is over and shares a link with further advise. Both England and Wales provide a self-isolation support scheme – those who were advised by the app to self-isolate and meet the eligibility criteria can apply for financial support.

Penetration rate

According to the DHSC, as of 12 February 2021, the app had been downloaded almost 21.7 million times. The number of active users amounts to 16.5 million. To this date, 1.7 million notifications were sent via the app to tell people to self-isolate. Researchers from the Alan Turing Institute and Oxford University claim that the app prevented approximately 600,000 cases. In an analysis for the BBC, Rory Cellan-Jones stated that "*areas where take-up of the app was high, the infection spread more slowly than in places it was lower*".

Estonia

Emergence of the contact tracing app

The development of the contact tracing app in Estonia has a unique background that does not include a public tender from the government or any other sort of "competition" between tech companies. The app was created free of charge by a consortium - an association of 12 Estonian companies that united voluntarily. This resulted in a public-private partnership, a part of which became the Ministry of Social Affairs, the Estonian Health Board and the Health and Welfare Information Systems' Centre (TEHIK), both in the area of responsibility of the Ministry. The consortium concentrated specialists in design, marketing, security and software development, among which the leaders were Iglu, responsible for the design of the app and technical lead, and Mobi Lab, which was in charge of the development of the mobile application.

Resulting from the partnership, the coronavirus contact tracing app HOIA, which means "to take care" in Estonian, was launched on 20 August. The managing director of Iglu, Kristjan Aiaste, said that to their knowledge, *"this was the first time such a large-scale endeavour has been successfully undertaken in such a form. As we needed to act quickly and many IT companies were willing to participate, there was no time nor a need for a complicated, time-consuming procurement process."*

Between August 2020 and February 2021, HOIA was downloaded 265,093 times (almost 20% of the population). Through the app, 3,596 individuals reported themselves as having been infected.

HOIA - Technical Details

The contact tracing app is based on the Decentralised Privacy-Preserving Proximity Tracing (DP-3T) implementation protocol and uses the Exposure Notifications Application Interface provided by Google and Apple (GAEN). HOIA works via Bluetooth Low Energy (BLE). When two users are within 2 metres of each other for a period of at least 15 minutes, their smartphones exchange signals. Tracking codes and details of encounters are stored on the respective devices and are removed automatically after 14 days. Users can delete their data from their phone at any time within the app.

The app's server, which generates and exchanges codes between devices, is located on the Estonian Government Cloud administered by TEHIK. If a user reports their positive corona test result via HOIA, other individuals receive an alert of the potential exposure. To prevent false alerts, the app redirects the user that reports an infection to the national Patient Portal, where the individual must authenticate themselves (e.g. through Mobile-ID). The Health Information System then detects whether a notice concerning the positive COVID-19 PCR test has been sent by the health care provider within the last 14 days. If yes, the Health Information System

Patient Portal confirms an infection on the app's server, which allows the app to upload the individual's non-personalized code. Infected individuals and users who have been in close contact will then receive instructions on how to proceed.

In contrast to many other international contact tracing apps, HOIA cannot communicate with other applications, even though it is potentially interoperable.

HOIA - Legal framework and Data Protection

In July 2020, the Estonian government introduced an amendment to Regulation No. 138 Statutes of the Health Information System, which entered into force on 21 July. The purpose of this amendment is to ensure the protection of the users' personal data. In particular, the amendment calls for data providers to perform their obligations in such a way that the app will not reveal users' personal data. The Estonian data protection authority, Data Protection Inspectorate, has considered HOIA suitable for use by the general public due to the app's safety, transparency and absence of the excessive data processing.

Later, at the end of August 2020, the developers of HOIA together the Ministry of Social Affairs and TEHIK conducted a Security Review, which reported on how the security requirements and measures of the HOIA application have been met in the first published version. They concluded that even though 31 security requirements out of 33 were met, "*partially met requirements or security measures were reassessed in terms of risk and found not to preclude the release of the 20 August 2020 version.*"

Finland

Emergence of the contact tracing app

Unlike other European countries, Finland is considered to have kept the pandemic under control, in many respects thanks to a swift government reaction. Finns also did not hesitate to develop and introduce a coronavirus tracing app in quick terms.

The main roles in this process were divided among several institutions: the Finnish Institute for Health and Welfare (THL), responsible for providing an information system based on mobile technology, the realisation of the competitive tendering procedure and determination of the candidate; DigiFinland Oy, which implemented a separate interface to the Omaolo service (Finnish national digital service that helps people assess their need for health care), which allows healthcare professionals to create and send unlock codes to those with a positive coronavirus infection; the Social Insurance Institution (Kela), responsible for a proper functioning of a back-end system; and the National Cyber Security Centre, for maintaining data security of the app. In the beginning of June 2020, THL selected the company Solita Oy, which was in charge of the technical implementation of the app. Solita Oy won THL's tender for the development of a COVID-19 tracing app as the most cost-effective project.

After creation of the app, 500 people tested Koronavilkku on their phones between 4 and 14 August in the cities of Helsinki and Tampere to help the developers to ensure proper functioning of the information system before the official launch. Users were supposed to report imaginary infections through the app, and the latter had to send notifications of potential exposure to the coronavirus. On 31 August 2020, the app Koronavilkku (CoronaBlinker) was officially launched. By February 2021, Koronavillku had been used by more than 2.3 million people (almost 42% of Finland's total population), making it one of the most downloaded contact tracing apps in the world relative to population size. More than 11,000 infections were reported via the app.

Koronavilkku - Technical Details

Koronavilkku is based on the DP-3T (Decentralised Privacy-Preserving Proximity Tracing) implementation protocol, which ensures a quick notification of contact individuals who are at risk. The app uses the Google/ Apple Exposure Notifications Application Interface (GAEN) to create identification codes and close contact information. When two users are within 2 meters of each other for a period of at least 15 minutes, their mobile devices exchange regularly updated Temporary Exposure Keys (TEKs) via Bluetooth Low Energy (BLE). Tracking codes and details of encounters are stored on the respective devices and are removed automatically after 21 days.

If a user of the app tests positive, the healthcare provider (which is THL) sends the person a single-use unlock code via text message, which is valid for 4 hours from the receipt of the message. Once the person types the code into the app, other Koronavilkku users will receive an alert of the potential exposure that cannot be traced back to the person who uploaded the code.

Since September 2020, Koronavilkku is available for download in neighboring countries too, and it is interoperable with several European contact tracing applications.

Koronavilkku - Lawfulness and DPIA

The development and functioning of the Koronavilkku has its legal basis. In July 2020, the Finnish Parliament introduced temporary amendments (Chapter 4a) to the Finnish Law on Contagious Diseases, which entered into force on 31 August. These amendments set up rules of the use and transfer of data, such as receipt of the user's consent for data processing inside the app, as well as a requirement to delete the collected data within 21 of registration.

The force of the temporary amendments expired on the 31st of March 2021. Shortly before the expiration date, the Ministry was to consider the question of further necessity of the amendments.

In August 2020, the Office of the Data Protection Commissioner, in cooperation of the Cyber Security Center, made an assessment of the data security of Koronavilkku, according to which *"no deficiencies were identifies in Koronavilkku that would pose significant risks related to data security or user monitoring"*.

Apart from that, in July and August 2020, the THL assigned Privaon Oy, the leading Finnish company operating in the fields of Privacy and Data Protection, to carry out a data protection impact assessment (DPIA) focusing on privacy risks of the Koronavilkku project. Following the DPIA, the CEO of Privaon Oy, Ville Sarja, concluded that *"The Koronavilkku project has successfully achieved its objectives, without problems related to respect for privacy, which have occurred in many other countries. Data protection has been a central principle guiding the project from the start"*.

France

In the end of May 2020, the majority of the French Parliament voted for the deployment of a contact tracing app to help break chains of coronavirus infections. Minister of Justice Nicole Belloubet insisted that principles of temporality, voluntary installation, non-identification and transparency must be guaranteed in the project. In order to protect technological sovereignty from foreign tech giants, France, contrary to most European countries, did not wish to rely on the Apple-Google API and therefore built its own, centralized architecture.

StopCovid, the first version of France's contact tracing app, was launched on 2 June. Four months later, the app had been downloaded only 2.6 million times. President Emmanuel Macron acknowledged the failure of StopCovid, saying, *"It did not work"*, and announced the launch of a new version. This unpopularity was considered to be due to data privacy reasons, the fact that some French people believed the end of the pandemic was imminent, or the government's inability to fully launch its communication campaign before the app was available.

A new, more interactive version: TousAntiCovid

After the bumpy start, on 22 October France introduced the new, updated version of StopCovid re-named as TousAntiCovid (everyone against COVID). If someone has already downloaded StopCovid, just by updating the app it would become TousAntiCovid. Technologically, no change was made. Besides keeping the core functionality of the app – which is to facilitate contact tracing and to monitor chains of infection – the new version was enriched with new informative services. These include information on the epidemiological situation in France, a map of screening centers with information on waiting time, customized advice and easy access to curfew exemption forms. INRIA, the French National Research Institute for Digital Sciences and Technologies, which was involved in the development of StopCovid from the beginning, is leading the TousAntiCovid project.

Technical details

The centralized system to collect data was created by INRIA and the server is hosted by Outscale. The server assigns a permanent ID (pseudonym) to each user and sends a list of ephemeral IDs to the user's device derived from that permanent ID. The app does not collect location data such as GPS, but relies on Bluetooth Low Energy to log encounters by collecting ephemeral IDs of users which were nearby another user's device. Encounters are logged anonymously between app users closer than 1 meter for at least 5 minutes and 2 meters for more than 15 minutes. As opposed to the decentralized approach, proximity logs are exchanged between the user of the app and the central server. If a user tested positive, they can voluntarily enter a one-time code received from the Ministry of Health and Solidarity into the app, which will anonymously notify other users about the potential exposure. Once the code is uploaded, the proximity history is shared with the central server and will be retained for no longer than 2 weeks after being shared.

Using the app is voluntary. In case someone decides to uninstall the app, it can be done at any time and will result in the deletion of all recorded data after 14 days. The app is available in six languages.

Involvement of the French data protection authority

Before StopCovid was launched, the French National Commission for Informatics and Liberty (CNIL) delivered two opinions related to the legality and data protection features of the app. In the first assessment, the CNIL delivered an opinion on the principle of implementing a contact tracing application and set out a number of recommendations, such as the principle of data protection by design and default. In the second opinion, the CNIL affirmed that the app respected the aforementioned principle and set out additional recommendations, such as the improvement of communication about the app and publishing its source code. The team that developed StopCovid was composed of state officials and two private companies. The data controller is the General Health Directorate of the Ministry of Social Affairs and Health.

The public's response

StopCovid, the first version of the app, received criticism on various levels. First, privacy advocacy groups and the public raised their concerns about France adopting a centralized contact tracing protocol, which stood in stark contrast to the choices most EU members made. ROBERT, which stands for "ROBust and privacy-presERving proximity Tracing protocol", was developed through a collaboration between France's INRIA and Germany's Fraunhofer Institute, which participated in the Pan-European Privacy-Preserving Proximity Tracing project (PEPP-PT). The specification of the protocol highlights that "*it might use collected information for purposes such as to re-identify users or to infer their contact graphs*". TechCrunch, an American online newspaper, interprets it as "*designed in such a way that it protects your privacy as long as you trust the government/the health ministry/whoever is in charge of running the central server*". A researcher also noticed that the app collected information on all people who crossed each other and not just those encountering for more than 15 minutes, as it was announced. Second, having followed a centralized approach, StopCovid gave a headache to the European Commission in terms of figuring out how to make it interoperable with other decentralized systems. Third, favoritism was suspected in the absence of a call for public tender for the maintenance of the application. Although the development of the app by the involved companies was on a *pro-bono* basis, for hosting StopCovid they set a price well above the market average. Anticor, an anti-corruption association, reported a "risk of overbilling" in the absence of a public market.

As of 2 February 2021, the TousAntiCovid had been downloaded by more than 4 million users and it had sent out 1,100 notifications. These numbers include the downloads and notifications of StopCovid.

Greece

In June 2020, Kyriakos Pierrakakis, Minister of Digital Governance of the Hellenic Republic, said, "*Tracking technologies [across Europe] are still being tested for accuracy and usefulness. We want to make sure that they work well, and that people can embrace them like our other initiatives. If we are convinced, we will move forward*".

In early March 2021, the European Commission's dedicated corona app webpage stated that Greece was currently working on the development of an app to monitor the spread of COVID-19. The app was meant to be interoperable with other contact tracing apps in Europe.

Latvia

Emergence of the contact tracing app

In the European Union, Latvia is considered to be the country with the third-lowest incidence of COVID-19 and a relatively low level of mortality, thanks to the rapid and effective response from the government. Latvia was the first country to declare a state of emergency right after the WHO's announcement of the beginning of the pandemic in early March 2020. The Latvian prime minister from early on declared the country's approach as "test, track and isolate". In order to contribute to the effective realisation of the approach, a contact tracing app was developed.

The creation of the contact tracing app Apturi Covid (Latvian for "Stop Covid") in Latvia is the result of a joint activity of Latvian ICT industry and science, experts from the University of Latvia, in collaboration with medical professionals, scientists and epidemiologists. The app was developed voluntarily, free of charge and became one of the first after Singapore's and Australia's apps, using a Google/Apple Application Interface GAEN. Among the creators of the app are the country's largest mobile operator, LMT, software development companies MAK IT, Autentica, Zippy Vision, software testing service TestDevLab and IT security consultancy IT Centrs.

By mid-February 2021, the app had been downloaded 300,000 times (about 16% of the total population) and 2,976 people reported positive test results through the app. The recent updates of Apturi Covid allow it to work together with several other European apps that are based on the GAEN application interface.

Apturi Covid - Technical Details

The contact tracing app generates a random ID every 10-20 minutes and exchanges it via Bluetooth Low Energy (BLE) technology with other users of the app. The exchanged keys from the encounters are stored on the respective devices for 14 days, after which they are automatically deleted. The app calculates that there has been a risk of the infection when two users were in a proximity of 2 meters for a period of at least 15 minutes. The app uses measurement algorithms such as the length of the encounters set up by the Google/Apple Exposure Notifications Application Interface (GAEN).

If a user has tested positive for COVID-19, they can voluntarily enter a code in the Apturi Covid. The activation code can be provided by the Latvian Center for Disease Prevention and Control (SPKC) in two ways: 1) the infected person can write an e-mail to the SPKC asking for a code; or 2) receive the code after being contacted by the SPKC contact tracer. When the code is entered in the app, encrypted data about the infected user's contacts are delivered to the SPKC server. The server automatically checks the information about the risky encounters and sends notifications to the individuals who have been in close proximity to the positive-tested person.

Apturi Covid - Data Protection and Lawfulness

In April 2020, prior to the development of the app, its creators signed a Memorandum of Understanding on Public Participation in Limiting COVID-19, in which they defined the basic principles and conditions of the app's functioning. Among them are principles of proportionality, transparency and safety of the data. In the Terms of Use, developers have also emphasised data protection as their main priority, identifying the types of data the app should not record and process (location data, personal information etc).

According to the Latvian national data protection authority, the Data State Inspectorate (DSI), Apturi Covid is considered to be safe. It does not identify a specific person, track a person's location, or process private information such as messages, photos, videos etc. on a user's device. The DSI noted that it has provided support in the process of developing the app and will continue to monitor compliance with people's right to privacy. The source code of the app is publicly available.

The Privacy Notice on the app's official website explicitly describes the purposes of the data processing, one of the main highlighted is *"epidemiological safety to protect public health against Covid-19."* The basis for data processing constitutes the Law on the Management of the Spread of COVID-19 Infection, which defines, above all, purposes of the contact tracing and warning information system. The types of data collected by the app together with the period of storage is described by the Cabinet's Regulation No. 360 Epidemiological Safety Measures for the Containment of the Spread of COVID-19 Infection.

Luxemburg

As many countries across the globe adopted digital contact tracing apps to monitor and help contain the spread of COVID-19 as it unfolded, Luxembourg favored and stayed with the manual tracing approach.

Members of the Luxembourgish Parliament pressed the government not to create a contact tracing app. In case it would be unavoidable, they insisted on four conditions to keep in mind: "the app should protect privacy, disclose the source code, communicate with other European apps and not allow data identifying individuals to be collected centrally". Delano, a news outlet, reported that Xavier Bettel, Luxembourg's prime minister, was skeptical about adopting a contact tracing app due to data privacy, effectivity and interoperability reasons. The latter played an important role as a significant amount of Luxembourgers work in neighboring countries, where such app would need to be interoperable with those countries' apps. Bettel preferred manual contact tracing which, according to Health Minister Paulette Lenert, has been "*more effective at this point*". Lenert added that such contact tracing app could be launched "*within a short time if we wanted to, if it was decided politically*". Bettel noted that if having such a tool would mean an "entry ticket" to travel abroad, he would consider it – to ensure Luxembourgers travelling would not be affected by not having such an app.

Malta

On 18 September 2020, Malta's national contact tracing app was launched after a spike in cases towards the end of summer.

The COVID Alert Malta App was introduced as national health authorities were struggling to keep up with the increase in the number of cases, and there were issues with volunteer contact tracers facing abuse from COVID-19 positive patients. The app is run by the Maltese government and was developed by the Malta Information Technology Agency (MITA), in collaboration with the Ministry of Health and the Malta Digital Innovation Authority.

As of 15 January 2021, the app had been downloaded by 91,215 people, which amounts to nearly 19% of the population. The COVID-19 Public Health Response Team of Malta was notified 1,071 times by individuals who were informed by the app to seek testing (between November 2020 and January 2021). 505 codes were sent via the app to users who tested positive with COVID-19, out of which 305 people entered the code into the app to anonymously warn app users they were in contact with.

Technical details

The app follows a decentralized approach and uses the Google-Apple Exposure Notification API. Once it's installed, the COVID Alert Malta App sends signals containing random codes via Bluetooth Low Energy. Temporary Exposure Keys (TEKs) are generated daily, using a cryptographic random number generator. Rotating Proximity Identifiers (RPIs) are generated from these TEKs every 10 minutes. These data are stored on the devices for 14 days after which they are deleted. If a user tested positive, they can voluntarily insert a code received from the Public Health Authority. Based on this authorization code, users who were in close contact with the positive person will be anonymously notified and recommended to get tested.

Privacy and Transparency

The processing of personal data is in line with the General Data Protection Regulation (GDPR) the Data Protection Act (Cap 586 in the laws of Malta). In case of a confirmed infection, the TEKs, the date of each key, the authorization code, the data on which the first symptoms appeared, the time at which this data is to be deleted and the transmission level will all be recorded by the central servers. These servers are under the control of the Superintendent of Public Health and operated by the MITA. The total data retention period on the data server is 21 days, including a 7-day backup for the data sent to the server. In a privacy policy statement, the Superintendent of Public Health explained in detail what kind of data is collected by the app, how it is processed and where it is stored.

A data protection impact assessment (DPIA) was carried out by the Maltese Information and Data Protection Commission (IDPC) before the app was launched. On the basis of the legal and technical analysis, Commissioner Saviour Cachia of IDPC asserted that the Superintendent of Public Health, the data controller, "*mitigated any possible risks with the appropriate measures*". The assessment, among others, checked whether the developers were "*providing the necessary information to users, ensuring that the use of the app will be on a voluntary basis, providing reasonable retention* *periods and adopting a data protection by design and default approach*".

As a response to the public's fear concerning mass surveillance through the app, Superintendent Charmaine Gauci asserted that the app "*does not name users who log as positive and it does not track movements or other unnecessary user data*". The app is available both in English and Maltese and is used on a voluntary basis. The source code is available on GitHub.

Netherlands

Emergence of the contact tracing app

Shortly after the outbreak of COVID-19 in Europe, the Ministry of Health, Welfare and Sports (VWS) of the Netherlands launched a public tender for smart digital solutions for COVID-19 tracing to be submitted by 14 April. From the 750 proposals received, officials of the Ministry and representatives of the National Institute for Public Health and Environment selected 7 of the providers to participate in the public test in the form of an "appathon" on 18 April, a digital event during which authors of the applications presented their products to teams of experts in efficiency and use, privacy and information security. Interested parties were able to follow the sessions via a live stream and submit their questions or suggestions to the providers. After reviewing the results of the appathon, the Ministry concluded that none of the presented applications were satisfactory in all areas, especially in the field of privacy and information security.

In addition to that, during the apathon experts invited by the VWS from worldwide advisory firm KPMG, Bureau ICT Toetsing (BIT; advises the government on the information and communications technology projects), the Dutch Data Protection Authority (AP) and the State Attorney could not identify a proposal that fully complies with the formulated principles of privacy and information security. The Ministry also concluded that proposals did not meet all the previously mentioned requirements and that they would continue to work towards the introduction of a contact tracing app.

However, the apathon revealed 'blind spots' and inaccuracies of the applications, which gave information sufficient to allow the Ministry, working groups of the National Institute for Public Health and Environment (RIVM) and the municipal health services (GGDs) to launch on 10 October the official COVID-19 tracing app, called "CoronaMelder". Practical tests of CoronaMelder were conducted in July in the region of Twente. A call for participation was made among Twente civil servants in local media. A total of 3,900 people registered to participate in the test in Twente, from which, as a result of a random selection and on the basis of people's questionnaire responses, 1,440 were selected to take part in testing. The participants remained positive about CoronaMelder, which allowed government to introduce the corona notification app to the general public in October. As of February 2021, 4.5 millions people (around 26% of the population) had downloaded the app. Among them, 112,089 warned others by reporting a positive test result. After receiving a notification of a risky exposure, 106,126 individuals scheduled an appointment to get tested.

CoronaMelder - Technical Details

CoronaMelder works via Bluetooth. It allows the system to recognise other mobile phones on which the app is installed and to notify users whether they have been in the proximity of a person who has tested positive with COVID-19. The app is based on Google/Apple Exposure Notifications Application Interface (GAEN) and uses two types of codes: Rolling Proximity Indicators (RPIs) that renew every 10 to 20 minutes and are generated from a second type of code - Temporary Exposure Keys (TEKs). The latter are regenerated daily and stored on a device for 14 days. When an app is installed on both smartphones that are within 1.5 to 2 meters of each other, their RPIs are exchanged and stored on the respective devices. If the user of the app tests positive and reports this information in CoronaMelder, everybody who was in close proximity to the infected person will receive a notification regarding the risk of infection and advice on next steps. This notification process is voluntary, not automatic and happens only when a user, together with the Dutch Municipal Health Service (GGD), has confirmed such transmission of data with a validation code. It is up to infected persons whether to warn other people in the app and about the time they were around somebody who has tested positive for coronavirus.

Since November 2020, CoronaMelder is interoperable with applications from other European countries, and the exchange of information between them happens in the same way as between two users of CoronaMelder.

CoronaMelder - Data protection assessment

The VWS Information Policy Directorate raised issues in their data protection impact assessment (DPIA), which were later summarised by the Dutch Data Protection Authority (Dutch DPA) in its letter to the Ministry of Health, Welfare and Sports in August 2020.

The VMS Information Policy Directorate (and later the DPA) advised the Ministry:

1) to complete agreements with Google and Apple considering the fact that it is not clear how exactly those tech giants will use the data provided by the user of IOS and Android that download CoronaMelder;

2) to create a specific and clear legal basis for the usage of notification application, including the prohibition of the involuntary use of the app (for example by employers, shops or catering services);

3) to arrange properly the “backside” of the app, so as to identify an actor responsible for a server through which the transmission of data takes place.

The Ministry took into consideration the DPA's instructions and entered into contractual agreements with Apple and Google. According to the agreement, Google and Apple do not use personal data for their own purposes, the Ministry does not share personal data that are processed within the app with Google/Apple and the personal data collected via the app may only be used to combat COVID-19. In addition, the Temporary Act on notification application COVID-19 was approved, which regulates the legal basis for the use of the CoronaMelder app (in particular, the voluntary basis of the application usage was secured). Furthermore, it was clarified the transmission of data on the "backside server" is managed by the GGD from one side and the smartphone user from the other; once both sides confirm a validation code, data are available for a download.

The Temporary Act is supposed to be in force until 10 April 2021. Shortly before the expiration date, provided that the CoronaMelder will still be deemed necessary, the Ministry will consider prolonging its force.

Portugal

Portugal announced its intent to launch a coronavirus tracing app in April 2020 to help combat the spread of COVID-19 in the country. The project brought together several national laboratories including the Institute of Computer Systems Engineering, Technology and Science (Inesc Tec), Inesc I&D, the Public Health Institute of the University of Porto, the Telecommunications Institute, and the Robotics and System Engineering Laboratory. Meanwhile, HypeLabs, a startup in Porto, had also developed a coronavirus contact tracing app, which was deployable in April 2020. The government favored the Inesc Tec'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, Stayaway COVID had to go through a data protection impact assessment (DPIA) and pass a test by the National Cybersecurity Center. The DPIA was carried out by the Portuguese Data Protection Authority (CNPD). On the basis of the DPIA, the CNPD recommended the adaptation of a legal framework concerning the operation of Stayaway COVID. On this account, a legal decree was passed that made the Directorate-General of Health (DGS) the data controller. It also set out that the DGS regulates doctors' intervention in the app. Besides this, the DPIA identified the main risks of the app, such as the re-identification of users. It set out recommendations including data minimization as well as the adaptation of a clear and simple language towards the users.

Shortly before the app's launch, national authorities were appealing to everyone in the country to download the app, saying it was "fundamental" in the fight against COVID-19. As cases grew exponentially in October, Prime Minister Antonio Costa attempted to make the app mandatory – "I hate to be an authoritarian but we have to get the pandemic under control," he said. The CNPD argued that this "would pose privacy and ethical issues". A Portuguese member of the watchdog European Digital Rights (EDRi), the Defesa dos Direitos Digitais (D3), condemned the move as authoritarian and one that does not belong to a democratic Europe. As a result of mounting pressure, the government postponed debate on mandatory use.

By March 2021, the app counted almost 3 million downloads (about 30% of Portugal's total population). However, a majority of those were not active users. In January 2021, the newspaper Publico reported that 60% of users already uninstalled the app, as confidence in the app's effectiveness vanished. In addition, fewer than one in four infected people use the code issued to them by the test center or family doctors to alert others of risky exposures.

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 COVID generates temporary exposure keys (TEKs) that are transmitted via Bluetooth to other devices. From the daily renewed TEK, so-called Rolling Proximity Identifiers (RPIs) are generated to handle logging. The data is stored locally on the mobile devices for a maximum of 14 days.

The installation of the app is voluntary. If a person tests positive for COVID-19, they are requested to insert a code into the app, after which users whom they were in close contact with will be anonymously notified. Once the code is inserted, for privacy reasons the app will stop tracing close contacts. After the recovery, the user needs to reinstall the application to restart monitoring.

The source code is available on GitHub.

Slovakia

Emergence of the contact tracing app

In order to contribute to the improvement of the epidemiological situation in Slovakia, the Slovak IT company Sygic developed a contact tracing app on their own initiative.

The app, ZostanZdravi (Slovak for "Stay Healthy"), was one of the earliest to launch in Europe, on 19 March 2020, and was downloaded more than 90,000 times during the first month. The developers offered ZostanZdravi to all countries free of charge as a tool to overcome the pandemic faster.

The app is functioning under control of the National Health Information Center (NCZI), and the operator of ZostanZdravi's personal data processing is the Public Health Authority of Slovakia.

ZostanZdravy - Technical Details

Due to the early launch, the contact tracing app uses its own designed protocol and not such known protocols such as DP-3T, PEPP-PT NTK or ROBERT, which came later than ZostanZdravy. The app asks its users to allow access to both Bluetooth and GPS. The app generates a random ID and exchanges it via Bluetooth Low Energy (BLE) technology with other users of the app. The app calculates that there has been a risk of the infection when two users were in a proximity of 2 meters for a period of at least 5 minutes. Such a short duration of a contact has been criticized by experts. The data about encounters is automatically deleted after 21 days. Phone number information is automatically deleted after 180 days at the latest.

When the contact exceeds a particular time duration, the application records the GPS position and an anonymous log of both encountered devices to the server. The developers explained that *"dissipated GPS position is essential for healthcare workers to analyze the spread of the disease."* Users are also able to mark the quarantine location directly in the app, which will allow the latter to monitor the GPS location of the device for the next 14 days, and notify the user in case quarantine rules are violated.

If a user has tested positive for COVID-19, they can voluntarily enter a code, provided by a healthcare worker, in the app. All the devices which were in contact with the infected person for the last 14 days will receive a push notification or SMS.

The developers have also planned to use the Innovatrics Face Recognition feature in the app, to ensure that infected people stick to the quarantine rules. The health authority would randomly send a push notification or SMS asking to check whether the person is in the place. The latter would need to perform face recognition through the app, which is then sent to the secure server with current GPS coordinates. If the person does not reply, or if the coordinates are false, the system notifies health care workers. However, there is no evidence that this system has actually been used.

ZostanZdravy - Data Protection and Lawfulness

The National Health Information Center (NCZI), which is listed as an official developer of the app in the national Google and App Stores, has published a Privacy Policy for ZostanZdravy, according to which the processing of personal data occurs under the general EU Regulation on data protection, and the national Act on Personal Data Protection, Act on Electronic Communications and the Public Health Act. The NCZI assured the public that the app is not used as a tool for monitoring citizens, justifying GPS tracking as the only way *"to statistically monitor citizens' compliance with mandatory domestic quarantine"*. The source code of the app has been released on 19 March 2020 and is available here.

Since its launch, the app has been an object of a multiple criticisms. One of the experts points out that ZostanZdravy lacks any proper specification of the contact-tracing protocol, of the API (application programming interface) or any other documented components, which makes it impossible to conduct a proper security analysis of the system or make a contribution to the project. Moreover, the absence of any prior testing of the app is another serious issue, as the chance of multiple errors in the code that has not been tested is extremely high.

The Slovak internet service provider DSL emphasises the high risk of deanonymization of users. The app automatically sends all identified contacts of all users for longer than the current 5 minutes to the state together with information on the profile ID of the user, the profile ID of the detected contact, the exact start time of the contact and the exact length of the contact. All of that raises the likelihood of identity exposures several times over.

After a few months, ZostanZdravy disappeared from the application stores.