UNIVERSITY OF AMSTERDAM

# UvA-DARE (Digital Academic Repository)

## Netherlands

Appelman, N.M.I.D.; Fahy, R.F.

**Publication date**
2020
**Document Version**
Final published version
**Published in**
Automated Decision-Making Systems in the COVID-19 Pandemic: A European Perspective

Link to publication

**Citation for published version (APA):**
Appelman, N. M. I. D., & Fahy, R. F. (2020). Netherlands. In F. Chiusi, S. Fischer, & M. Spielkamp (Eds.), *Automated Decision-Making Systems in the COVID-19 Pandemic: A European Perspective* (pp. 25-26). AW AlgorithmWatch gGmbH.

**General rights**
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

**Disclaimer/Complaints regulations**
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

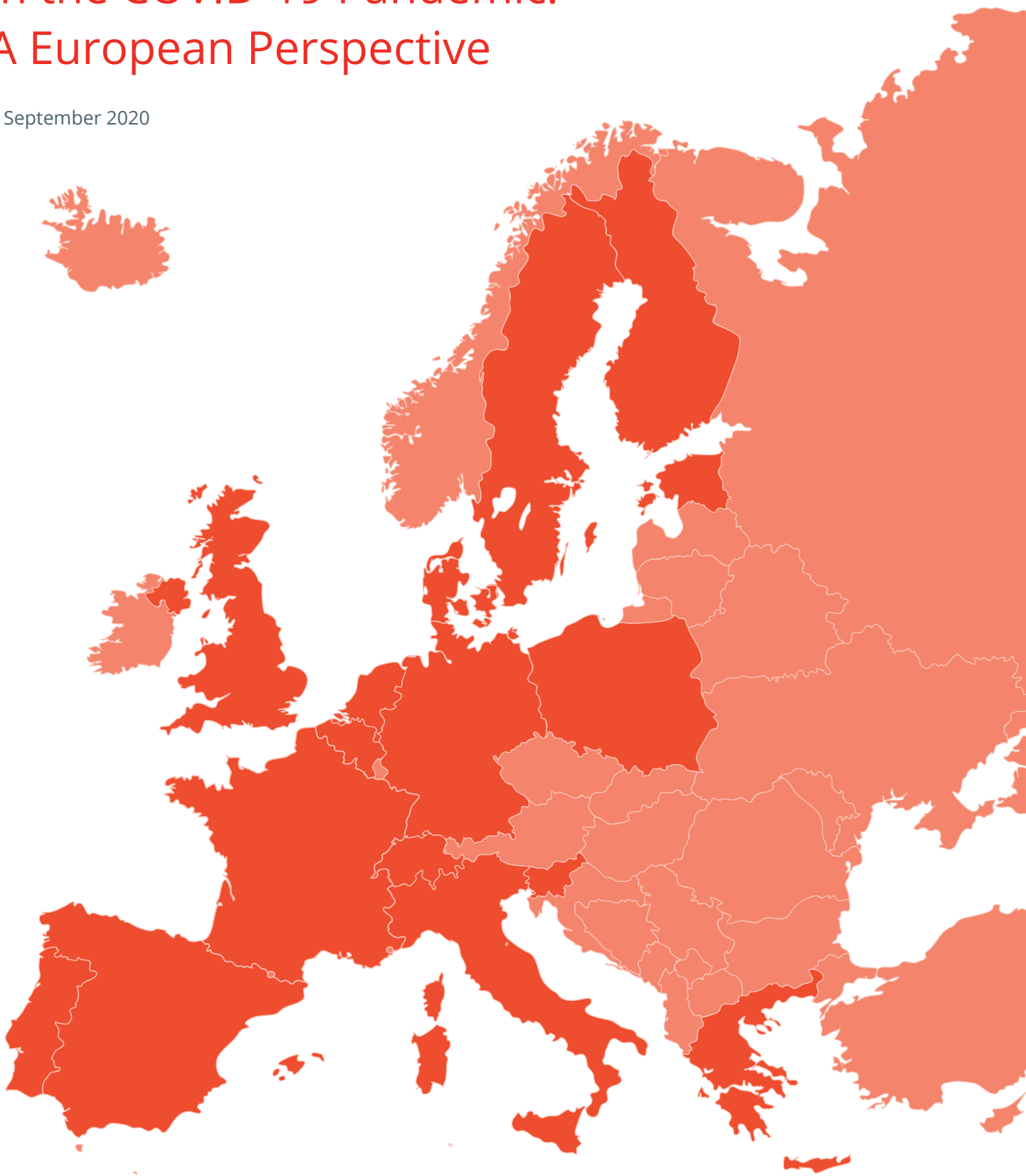
*UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)*

Download date:12 Feb 2025

AUTOMATING SOCIETY REPORT 2020 | SPECIAL ISSUE

# Automated Decision-Making Systems in the COVID-19 Pandemic: A European Perspective

1 September 2020



ALGORITHM WATCH

BertelsmannStiftung

# CONTENTS


INTRODUCTION ..... 3

What are we talking about when we talk about ADM in COVID-19 responses? ..... 3

Geopolitics of ADM systems in the pandemic ..... 4

/ Why "ADM", and not "AI" ..... 4
/ Mandatory and rights invasive ADM systems: the China model ..... 5
/ Echoes in Europe: geolocated selfies and bracelets ..... 6
/ WHO guidelines paint a different, and better, picture for ADM ..... 7
/ The EU alternative: public health, digital technologies and human rights are not incompatible ..... 8

ADM systems to complement contact tracing efforts ..... 10

/ Locations vs proximity: what data do ADM systems need to actually help with contact tracing? ..... 11
/ Does ADM in contact tracing and exposure notification work at all? ..... 12

Thermal scanners, face recognition, immunity passports: should this be our new normal? ..... 13

COUNTRY ANALYSES ..... 16

Belgium ..... 17

Denmark ..... 17

Estonia ..... 18

Finland ..... 19

France ..... 22

Germany ..... 22

Greece ..... 23

Italy ..... 24

Netherlands ..... 25

Poland ..... 26

Portugal ..... 27

Slovenia ..... 28

Spain ..... 29

Sweden ..... 31

Switzerland ..... 31

United Kingdom ..... 32

# INTRODUCTION

**BY FABIO CHIUSI**

The COVID-19 pandemic has spurred the deployment of a plethora of automated decision-making (ADM) systems all over Europe. High hopes have been placed by both local administrations and national governments in applications and devices aimed at containing the outbreak of the Severe Acute Respiratory Syndrome Coronavirus 2 (SARS-CoV-2) through automation, thus providing a much needed alternative to lockdown measures that limit personal freedoms and strain the economies.

Smartphone apps have been launched to help speeding up and complementing the manual contact tracing efforts put in place by health authorities, causing a heated international debate around how to best balance privacy and human rights with the urgent need to monitor and curb the spread of the disease. QR codes have been issued to enforce quarantine orders and log check-ins in shops and public places. Thermal scanners, at times powered by facial recognition technologies, are rapidly becoming the new normal to access venues as diverse as supermarkets, stadiums and museums. Artificial intelligence more generally — and vaguely — has been enrolled in the analysis of large masses of aggregate, anonymised population data, in order to get real-time insights on crowd behaviour, predict risk areas and model public policy interventions.

Several academic institutions and civil society organisations are keeping track of these developments, from the Ada Lovelace's Institute 'Digital Contact Tracing Tracker' to MIT's 'COVID Tracing Tracker' and Privacy International's 'Tracking the Global Response to COVID-19'. None, however, specifically concentrates on aspects related to automated decision-making within Europe. As they fall within the scope of AlgorithmWatch and Bertelsmann Stiftung's 'Automating Society' project, and with its 2020 edition due out in October, we felt that we could not miss out on such relevant developments.

This is why we decided to publish this "preview report", fully dedicated to an initial mapping and exploration of ADM systems deployed throughout Europe as a consequence of the COVID-19 outbreak. Especially given the uncertainties around the resurgence of the virus that are present at the time of writing, we felt it was necessary and urgent to provide a first snapshot of the socio-technical systems deployed against the virus in the 16 European countries investigated in the 'Automating Society' project.

It is, by all means, incomplete: too much is happening in the field on a daily basis, globally, to even try and claim exhaustiveness, and many such systems are still opaque and/or on trial. But it will provide a contextualisation of why so many ADM systems are being adopted, some explanation of their actual workings, and thoughts around their consequences in terms of human rights, democracy and public health.

Some comparison will also be drawn between the main features of ADM-based responses within the EU and outside of it, highlighting some significant differences in how the interplay of technology and rights is conceived in different parts of the world. At the same time, the report will show how and why "technological solutionism", a flawed ideology that conceives of every social problem as a "bug" in need of a "fix" through technology, is common to many such diverse endeavours instead — even in the face of scant evidence in favour of the effectiveness of existing anti-COVID ADM systems.

A more detailed country-by-country analysis is then presented in the second part of this report, thanks to the efforts of the outstanding network of researchers that has been working on the Automating Society project over the last year, thus providing unique on the ground insights from each of them.

## WHAT ARE WE TALKING ABOUT WHEN WE TALK ABOUT ADM IN COVID-19 RESPONSES?

Digital technologies have been touted as a solution to the COVID-19 outbreak since early in the pandemic. But while claims around "AI", a vague and much hyped term to which AlgorithmWatch has long preferred the more rigorous locution "ADM", being able to reverse the course of the disease have been quickly proven too enthusiastic in the face of available evidence, much of the attention in public discussions revolved around how to complement manual contact tracing efforts put in place by health authorities with automation.

The idea is simple: total or even partial lockdowns of the kind witnessed all around the world during the first wave

of the pandemic severely affect both individual rights and the economy, and therefore should be avoided, if possible, in the future. The most efficient and secure way to do so would therefore be, according to many in both government and academia, to deploy "smart" solutions to quickly spot virus carriers, both symptomatic and asymptomatic, and then more easily and reliably reconstruct their contacts over the last two weeks. This way, whoever has been exposed to the risk of contracting the COVID-19 disease is promptly warned through a notification on her/his smartphone, allowing potentially infected individuals to then immediately look for medical assistance (eg, by getting tested and, if necessary, quarantined).

Is this plan realistic? And how to translate it into action? Answers varied greatly, even within Europe. Sweden, for example, hasn't so far adopted a digital contact tracing app, and isn't planning to do so. Scotland also seriously considered not having one, even arguing that it might never be needed[1]. At the opposite side of the spectrum, Slovenia has developed a legislative framework for the creation of an app that is instead mandatory to both citizens who test positive and those who want to travel, even inside the country.

Ideas on the acceptable level of intrusion in the lives of European citizens by such apps has also been a divisive issue, leading to very different technological solutions. Some, more oriented on preserving individual privacy, resorted to Bluetooth low energy technology, either within a "centralised" or a "decentralised" architecture — a distinction that, although merely technical on the face of it, has actually embodied the gist of the public debate around the balancing of human rights and disease surveillance. Other applications have been more focused on making good use of epidemiological data gathered by health authorities, and in particular in the early spotting of risky locations or clusters, and therefore adopted GPS technology.

The former batch of applications is therefore based on proximity data, while the latter is based on location data, with very different implications not only for rights, but also uptake, actual functioning and efficacy.

1 After months of skepticism, at the end of July, Scotland finally announced the development of a contact tracing app which, according to the BBC, "it hopes to have ready for use in the autumn". The app will share the same software adopted in the Republic of Ireland and Northern Ireland.

In order to better understand this and other crucial distinctions, we need to first get a closer look at what ADM systems are, how they are institutionally and geopolitically framed in the context of the COVID-19 disease, and more specifically which processes and decisions are entailed by different types of ADM systems, to what degree of human involvement.

## GEOPOLITICS OF ADM SYSTEMS IN THE PANDEMIC

### / Why "ADM", and not "AI"

In the first edition of the 'Automating Society' report, we defined an "automated decision-making system" as "a socio-technological framework that encompasses a decision-making model, an algorithm that translates this model into computable code, the data this code uses as an input—either to 'learn' from it or to analyse it by applying the model—and the entire political and economic environment surrounding its use".

Contrarily to "AI", then, ADM systems are not mere technologies. Rather, they are ways in which a certain technology — which may be far less sophisticated or "intelligent" than deep learning algorithms — is inserted within a decision-making process[2].

In the context of COVID-19, for example, the same technology can be used for very different purposes, depending on the rationale behind it. Data collected through a Bluetooth LTE-based smartphone app can for

2 An interesting complication to the definition of "automated decision-making" in the context of the pandemic emerged during the editing process of this report. This introduction assumes that decentralised exposure notification apps should be considered ADM systems, as they automate the logging and — after user consent — sharing of notifications of potential exposure to an infected subject the user has been in proximity to. This is an (allegedly) essential component of a wider public health decision-making system, and the gist of what the digital could add to manual contact tracing efforts: a layer of automation to complement human efforts. But to some of the researchers who participated in the project (as apparent in the Belgium, Denmark and Portugal country analyses), this is not the case: DP-3T-based apps should not considered as including "automated decisions" or any ADM system, as they actually do not automate any decisions — a health professional and/or the user are always in the loop. This would however mean that such apps should not even included in a report on ADM in COVID-19 responses, and this would imply missing a crucial aspect of the broad, global debate happening around data, automation and the pandemic. We therefore decided to treat such systems as ADM systems, but at the same time reflect the fact that this assumption is contentious, at the time of writing.

example be voluntarily and anonymously shared either with a central server or with smartphones of potentially infected individuals, with no consequences or sanctions whatsoever in case a citizen decides not to download it. Or, the same technology can be adopted within a much more rights-invasive solution, working in tandem with GPS to continuously provide a citizen's location to the authorities, at times within mandatory schemes — and with harsh sanctions in case they are not respected.

Different governance models are therefore reflected in different ADM systems.

## / Mandatory and rights invasive ADM systems: the China model

Authoritarian countries made full use of the digital surveillance infrastructure they already had in place, and even added further equipment and devices, to deliver ADM solutions that strongly prioritise public health and safety concerns over individual rights. China, for example, employed a colour-based rating system, the Alipay Health Code, using big data "to draw automated conclusions about whether someone is a contagion risk", wrote the New York Times. Under this model of ADM, citizens have to fill a form with their personal details, to be then presented with a QR code in three colours: "A green code enables its holder to move about unrestricted. Someone with a yellow code may be asked to stay home for seven days. Red means a two-week quarantine". A scan is necessary to visit "office buildings, shopping malls, residential compounds and metro systems", according to a Reuters report.

Even without considering that 18 out of the 20 most video-surveilled cities in the world are in China (Comparitech), that this Moloch comprised of 54% of all CCTV cameras of the world is being repurposed with facial recognition technology "to scan crowds for fever and identify individuals not wearing masks", and that "non-contact thermal augmented reality" smart glasses supplied by AI start-up Rokid Corp are also being added to the surveillance apparatus to "enforce social distancing", it is easy to see how radical and extreme this view of ADM is.

The Alipay rating system is not only mandatory, but it also autonomously, and opaquely, decides the health status — and consequent rights — of individuals in a country in which the population is getting accustomed to having algorithmic credit scoring systems judge all aspects of their lives, both private and public.

An increasing number of countries is walking in China's footsteps. Face recognition, for example, has been adopted in Russia against COVID-19 since the beginning of the outbreak in the country. Late in March, the BBC reported that "Moscow police claimed to have caught and fined 200 people who violated quarantine and self-isolation using facial recognition and a 170,000-camera system", adding that "according to a Russian media report some of the alleged violators who were fined had been outside for less than half a minute before they were picked up by a camera."

Were it not enough, Moscow authorities also mandated download of a geolocation tracking app and registration of a government-issued QR code, similar to that in use in China: starting from April, it has been reported to be necessary "for each and every trip to the pharmacy, grocer, or even just to walk (a) dog", wrote Gizmodo. Going about without a QR code could mean jail time.

In the meantime, the app would also send push notifications to instruct quarantined and self-isolated citizens to take and send a selfie "as a proof of not having left the house without the phone", wrote Human Rights Watch. "If users miss a notification, they are automatically fined 4,000 rubles" — even when, according to "hundreds, if not thousands" of them, the fine is wrongly issued because of bugs and glitches in the software.

Mandatory and rights-invasive ADM systems largely concern countries outside of Europe. Around the same time, on April 11, the South Korean government announced plans "to strap tracking wristbands on people who defy quarantine orders", and "location histories" about individuals who tested positive were, and have so far, been regularly collected by the health authorities — and even published online, with serious consequences in terms of shaming of affected individuals.

When nightclubs in Seoul become potential hotspot for a new wave of COVID infections, the Guardian wrote that "lurid reporting, along with South Korea's use of the trace and test method, led to members of the gay community reporting feeling scared to get tested and even suicidal".

Also, the app to enforce quarantines was found to have "serious security flaws that made private information

vulnerable to hackers", according to New York Times reporting confirmed by the government. Crucially, "the flaws could also have allowed hackers to tamper with data to make it look like users of the app were either violating quarantine orders or still in quarantine despite actually being somewhere else."

India also made the download of its Bluetooth and GPS-based contact tracing app, "Aarogya Setu", compulsory for all workers in both the public and private sector on May 1st. With similar issues: a hacker claimed to be able to tamper with the app to always appear "safe", and several privacy hiccups occurred — all of this within a broader biometrics surveillance infrastructure in which, just like in China, facial recognition is rapidly becoming the new normal, and opaquely so.

The more intrusive the ADM system, the more severe the consequences. In Israel, contact tracing has been performed both through a location-based tracking app, Magen, and a digital contact tracing program run by the country's intelligence agency, Shin Bet. Both proved to have serious flaws: Magen showed inaccurate location records, while the intelligence programme has been renewed in July even after being widely criticised for forcing people in quarantine by mistake, with complaints reportedly going unanswered on a regular basis.

A 1-10 rating system based on mobile data analysis ("Coronameter") and even voice surveillance are being explored at the time of writing, showing a clear trend for countries that made digital mass surveillance an integral part of their public health response to the COVID-19 disease: no matter how invasive, it is never enough.

## / Echoes in Europe: geolocated selfies and bracelets

Even though this radical and ultimately repressive model of ADM systems deployment mainly concerns Asia and the Middle East, similarities can be found in some European countries as well. Strong analogies with the Russian selfie-based quarantine app can be found in Poland's "Kwarantanna domowa" app, that also uses geolocation and face recognition technology to ensure that relevant people are quarantined; and again, same as in Russia, the app download is mandatory.

In May, the same system has been adopted in Hungary, too.

Norway's contact tracing app, Smittestopp, has also been bundled in some unwelcome company: an Amnesty Tech investigation, in fact, showed it to be among the worst offenders in terms of users' rights on a worldwide scale, together with those by Kuwait and Bahrain, defined by the technical report as "highly invasive surveillance tools" — so much that Norwegian authorities had to suspend its deployment, after the country's Data Protection Authority issued a warning, raising concerns of a disproportionate impact on user privacy.

In an utterly dystopian turn, Bahrain even tied its app to a national television show, called 'Are you home?', which according to Amnesty "offered prizes to individuals who stayed at home during Ramadan. Using contact details gathered through the app, 10 phone numbers were randomly selected every day using a computer programme, and those numbers were called live on air to check if the app users were at home".

Lithuania's application has also been suspended by the country's data authority for failing to comply with the EU's privacy regulation, the GDPR.

Liechtenstein took a different path instead, giving priority to a pilot study that aims to investigate whether wearable devices can help with the early detection of COVID-19. For this reason, it has launched a study, called 'COVI-GAPP', in which 2,200 citizens are given a biometric bracelet to collect "vital bodily metrics including skin temperature, breathing rate and heart rate", and then have those data sent back to a Swiss laboratory for analysis. The idea behind an experiment that will ultimately involve all of the citizens in the country is that by analysing physiological vital signs "a new algorithm for the sensory armband may be developed that can recognize COVID-19 at an early stage, even if no typical symptoms of the disease are present" (AFP).

Anti-COVID bracelets are, again, more common outside of Europe, and namely in countries such as Hong Kong, Singapore, Saudi Arabia, the UAE, and Jordan — where, however, are mainly deployed to enforce quarantine orders and other COVID-19 restrictions.

Such and other uses are cause of concern to digital rights activists. The Electronic Frontier Foundation, for example, wrote that wearables, in the context of the pandemic, "remain an unproven technology that might do little to contain the virus, and should at most be a supplement to primary public health measures like

widespread testing and manual contact tracing". Also, and importantly, "everyone should have the right not to wear a tracking token, and to take it off whenever they wish".

This does not appear to be the case at Michigan's Albion College, where students are required to download an app that "tracks their location and ongoing health data" in an attempt to turn the campus into a safe "COVID bubble". In an email obtained by Newsweek, "the college told students (...) that they must have their location services on at all times".

And not just that: the app, called "Aura", also notifies "the school's administration if a student leaves the campus's bubble". And if a student is found beyond the 4,5 mile perimeter, the sanction is suspension.

Yet another echo of the Chinese model of ADM, heard in a democratic context.

## / WHO guidelines paint a different, and better, picture for ADM

But is this invasive model of deployment of ADM systems against COVID-19 supported by World Health Organisation principles? Not really.

For one, in its guidelines published on May 10, 'Contact tracing in the context of COVID-19', the WHO clearly states that adoption of "proximity tracing[3]" systems should not be mandatory, exactly because "such uses of data may also threaten fundamental human rights and liberties during and after the COVID-19 pandemic".

The concern here is the normalisation of mass surveillance, under the guise of an urgent and (allegedly) effective solution to the pandemic. "Surveillance can quickly traverse the blurred line between disease surveillance and population surveillance", writes the WHO. "Thus, there is a need for laws, policies and oversight mechanisms to place strict limits on the use of digital proximity tracking technologies and on any research that uses the data generated by such technologies."

Not only downloading any apps should be voluntary: users should also be free to delete them anytime, to avoid the risk of exacerbating existing inequalities. This is not the case in Hungary, for example, where the home quarantine app is only voluntary until one decides to download it, at which point it becomes mandatory. Failing to comply with geolocalised facial image and SMS authentication immediately amounts to an infringement that can be sanctioned by a fine.

This is also problematic in terms of WHO principles, as no benefits should be attached to the decision of downloading one such apps, and no discrimination should follow from that of not downloading them. Again, this is not the case with the Hungarian quarantine app: "If someone does not voluntarily agree to install the software, the police will go out more often to personally check that the house quarantine is being complied with", wrote Index.

The WHO then crucially warns against rushed deployments of solutions whose efficacy is still unproven. And yet, while "It is essential to measure the effectiveness and impact of these technologies", we don't really know how to fill the gap: «Currently, there are no established methods for assessing the effectiveness of digital proximity tracking," read the guidelines.

What can and should be done, argues the WHO document, is providing "transparency and explainability" of the adopted ADM systems. "Meaningful information about the existence of automated decision-making and how risk predictions are made" is included, and namely "the types of data collected, how data will be stored and shared, and how long data shall be retained".

Code of ADM systems should be open sourced, and "algorithmic models used to process data and assess risk of transmission must be reliable, verified, and validated". An independent oversight body should also be established to check for respect of ethics and human rights, according to the guidelines.

Importantly, download should be based on consent, and in particular notification that a user has tested positive should not be automatically transmitted by the app, but needs confirmation from a health professional.

3 The term is adopted to clearly distinguish ADM systems deployed to help contact tracing efforts from the contact tracing efforts themselves. "Proximity tracking is often conflated with 'contact tracing', although contact tracing is a broad public health discipline, and proximity tracking is a new technique for aiding contact tracing." The WHO document defines "contact tracing" as "the process of identifying, assessing, and managing people who have been exposed to a disease to prevent onward transmission".

In any case, the WHO warns against technological solutionism, arguing that digital proximity tracing is "not essential" and only meant to complement, not replace, manual contact tracing efforts: "This technology cannot capture all the situations in which a user may acquire COVID-19, and it cannot replace traditional person-to-person public health contact tracing, testing or outreach which is usually done over the phone or face to face. Digital proximity tracking applications can only be effective in terms of providing data to help with the COVID-19 response when they are fully integrated into an existing public health system and national pandemic response."

This is consistent with AlgorithmWatch's policy position on digital contact tracing apps.

## / The EU alternative: public health, digital technologies and human rights are not incompatible

The approach that most closely resembles the WHO guidelines arguably comes from the European Union. In a number of documents, EU institutions tried to combine the (alleged) benefits of automated decision-making systems with the respect of privacy, human rights, and democratic checks and balances, thus providing a much needed alternative to the China model, and giving criteria and principles that any technological response to the coronavirus outbreak should respect, if it has to comply with European laws and values.

As the European Data Privacy Board clarified since March, in fact, the processing of personal data to face the public health emergency caused by COVID-19 is not incompatible with the GDPR. However, as noted by EDPB Chair, Andrea Jelinek, "even in these exceptional times, the data controller and processor must ensure the protection of the personal data of the data subjects".

On April 8, 2020, the European Commission issued a Recommendation "on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data".

The document sets the stage for a EU-wide strategy on how to use data and technology in tackling the coronavirus outbreak, and hinges on two premises. First, that the pandemic is an issue that can't be properly tackled at national level: "a fragmented and uncoordinated approach risks hampering the effectiveness of measures aimed at combating the COVID-19 crisis", it reads, "whilst also causing serious harm to the single market and to fundamental rights and freedoms". Imagine a EU citizen travelling across borders and having to download different apps that are unable to communicate between each other.

The drawbacks of a fragmented approach are already apparent in the USA, where different and even competing views of how to deploy ADM systems, absent overarching strategies and principles, lead to a situation in which some States opted for decentralised Bluetooth-based "exposure notification" (South Dakota, Alabama, Virginia and North Carolina), others deploying their own solution (eg. Utah, using "a combination of GPS, WiFi, IP address, cellular location data and Bluetooth to identify contacts"[4]) and many not considering any ADM systems at all[5]. This resulted in a patchwork of non-interoperable solutions and contradictory health policies, with users showing legitimate concerns over fundamental rights and efficacy that mostly lead to confusion and low uptake rates.

In Minnesota, for example, officials "have been using what they describe, without going into much detail, as contact-tracing in order to build out a picture of protestor affiliations", wrote BGR, while a location-based app initially developed in North Dakota was found to be "sharing location data with Foursquare and an advertising ID with Google", according to Fast Company.

As a result, Harvard professor Jonathan Zittrain denounced "a plateau in visible activity on the tech side of the ledger", even wondering whether digital contact tracing in the US is "over before it began".

4 Later on, location tracking has been discontinued for Utah's "Healthy Together" app: "We've learned over the course of the past 3 months that location tracking isn't popular and, as a result, it hasn't really been helpful to our contact tracing efforts", said Dr. Angela Dunn, Utah State Epidemiologist. The app, costed $2,65 million, had in fact only been downloaded and activated by 56,000 users — "which translates to about $46 per active user", notes UtahPolicy.com (https://utahpolicy.com/index.php/features/today-at-utah-policy/24309-technological-boondoggle-utah-s-multi-million-dollar-coronavirus-app-will-no-longer-provide-contact-tracing)

5 "California, Colorado, Connecticut, Delaware, Georgia, Idaho, Indiana, Iowa, Louisiana, Maryland, Montana, New Hampshire, New Mexico, Tennessee, Texas, Vermont and Wyoming have all confirmed they aren't currently developing digital contact-tracing apps", wrote Lawfare on July 21 (https://www.lawfareblog.com/what-ever-happened-digital-contact-tracing)

This is exactly what EU principles — and interoperability specifications[6] — were meant to avoid.

The second premise in the EU Commission document is acknowledging that digital technologies and data "have a valuable role to play in combating the COVID-19 crisis" — but only assuming they meet certain conditions. This translates into a call for a "pan-European approach for the use of mobile applications, coordinated at Union level", while at the same time respecting privacy and fundamental rights.

In order to do that, reads the document, "preference" should be given "for the least intrusive yet effective measures, including the use of proximity data and the avoidance of processing data on location or movements of individuals, and the use of anonymised and aggregated data where possible".

The Recommendation also calls for "a common scheme for using anonymized and aggregated data on mobility of populations", to better predict the evolution of the pandemic, evaluate the effectiveness of Member States' responses and inform coordinated strategies — but again, "safeguards" must be "put in place to prevent de-anonymisation and avoid reidentifications of individuals".

Criteria for a democratic use of digital contact tracing apps detailed in subsequent EU documents are consistent with the rationale clearly expressed by European Data Protection Supervisor, Wojciech Wiewiórowski: "Humanity does not need to commit to a trade-off between privacy and data protection from one side, and public health, on the other. Democracies in the age of Covid-19 must and can have them both."

When a first iteration of the "common EU toolbox" was presented by the eHealth Network — a voluntary network created under article 14 of Directive 2011/24/EU — on April 16, digital contact tracing was in fact envisioned as "fully compliant with the EU data protection and privacy rules", voluntarily adopted and "dismantled as soon as no longer needed", based on proximity data (Bluetooth) rather than location data (GPS), cybersecure and interoperable.

Crucially, the eHealth Network reiterates — just like the WHO did — that digital contact tracing is a complement, rather than a substitute, for manual contact tracing, and calls for "monitoring the effectiveness of the apps": "Member States should develop a set of KPIs (Key Performance Indicators, ndr) to assess/reflect the effectiveness of the apps in supporting contact tracing".

While a heated debate among proponents of a centralised (ROBERT) versus decentralised (DP-3T) architecture for such apps followed among researchers, academics and lawmakers, with the PEPP-PT consortium[7] taking and rapidly losing center stage at EU level, important provisions on automated decision-making aspects of data-based responses to the pandemic have largely gone unnoticed.

The eHealth Network's toolbox, for example, reminds that fully automated processing of decisions concerning the warnings issued through apps should be prohibited, consistently with art. 22 of the GDPR[8]. Transparency is also key, as the document requires code of such apps to be open source, "public and available for review".

More generally, all interventions by EU institutions on ADM-related aspects of the COVID-19 crisis revolve around the idea of building trust between citizens and health authorities. This is only possible when privacy and fundamental rights are fully respected within Europe, they clearly state, while at the same time — again, similarly to what the WHO prescribes — preventing any discriminatory outcomes for those who freely decide to not adopt contact tracing apps: no "negative consequences" should follow from such decisions.

These are the pillars of a model of ADM systems deployment that is fundamentally different, and radically opposed to that adopted in China and, to a lesser degree, other countries in Asia and the Middle East.

6 Contained in a document published on June 16, 2020: 'Coronavirus: Member States agree on an interoperability solution for mobile tracing and warning apps', https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1043

7 PEPP-PT is an international effort "to assist national initiatives by supplying ready-to-use, well-tested, and properly assessed mechanisms and standards" for "privacy preserving proximity tracing", according to https://www.pepp-pt.org/

8 For an explainer, see: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/

## ADM SYSTEMS TO COMPLEMENT CONTACT TRACING EFFORTS

Nowhere has this fundamental clash between different models of ADM been more apparent than in the global debate around digital apps to complement contact tracing efforts. Born in the midst of the first, tragic wave of COVID-19 infections, it has been initially informed by a (mostly tech-solutionist) sense of urgency and necessity that seemed to justify unprecedented intrusions of government surveillance into the lives of millions of citizens living in democratic countries.

Tech enthusiasts the world over argued that privacy and other fundamental rights were to be somehow sacrificed — or at least could be sacrificed — to enable public health, and especially to avoid further total lockdowns. Some, for example in Italy, even theorised to do away with privacy altogether, as respecting it would have been an unnecessary burden on the ADM system, according to this view.

As previously said, a heated global discussion around which technology would better help speeding up contact tracing endeavours ensued, with two main camps: one in favour of using GPS tracking (Norway, Iceland and Bulgaria), and therefore location data (at times, as in the Czech Republic, integrated with bank and payments data, and data from apps downloaded by the user), and the other preferring Bluetooth Low Energy, and therefore proximity data.

Soon, this camp also split in two opposing lines of thought. Countries like France, the UK and initially Germany tried to develop "centralised" Bluetooth-based solutions, while Italy, Switzerland, Denmark, Estonia (and, ultimately, Germany itself) opted for a "decentralised" solution. In this latter case the "contact tracing" app is not doing contact tracing at all, but instead it is merely signaling that two phones have been close to each other for enough time to consider the encounter at risk, and therefore issue a notification of potential exposure to a positive subject, were one of the owners to be diagnosed with COVID-19 within 14 days — and willing to upload such data through the app.

The debate concentrated on what precise architecture to adopt to inform and shape the sought after anti-COVID-19 ADM systems, their pros and cons in terms of privacy and fundamental rights, but also of cybersecurity and (at least potential) effectiveness.

A game-changer was the introduction of "exposure notification" — a term adopted to avoid promoting the flawed idea that any apps could replace "contact tracing" altogether — APIs developed by tech giants Google and Apple, that are together responsible for the almost totality of operative systems installed on smartphones in commerce.

No location data would be collected, claimed the tech giants — even though a New York Times report argued on July 20, months after the protocol's announcement in April, that Google still asked for location data to be turned on, even though not collected according to Mountain View, to actually be able to notify users via Bluetooth.

This at the same time helped the debate going forward and posed, once more, the issue of extremely powerful private multinational companies mandating technical rules that policymakers and State technologists could not shape in any ways, but only follow and obey to, thus suggesting that ADM responses to the global public health emergency can be more easily and effectively decided by Big Tech CEOs than by democratically elected governments.

All apps developed by countries that chose a Bluetooth-based architecture but refused to adopt the one by Google and Apple ran into serious technical issues due to limitations and requirements imposed by the tech giants, in fact, even leading to countries fully reconsidering their ADM deployment strategy. The UK, for example, decided to ditch its own centralised solution after it was proven to be able to recognise just about 4% of iPhones during a trial on the Isle of Wight. France even asked the Cupertino giant to relax some privacy features, so that its "StopCovid" app could work when in the background, an issue that has been consistently found to plague apps with the same architecture, most notably in Australia, where the app has been deemed "a terrible failure" — and "by any measure" so — in a Sidney Morning Herald editorial.

Apple refused to comply, and on May 26, top digital affairs officials from five EU governments (Germany, France, Italy, Spain and Portugal) strongly criticised both tech giants in a joint op-ed published in several languages. They argued that the imposition of an exposure notification standard from private entities was "the wrong signal when it comes to promoting open cooperation between governments and the private sector", especially when one considers that "digital sovereignty" is arguably

the core principle that informs the EU's policy stance on digitisation strategies.

But this does not mean that GPS-based and "decentralised" Bluetooth-based apps are immune from bugs and glitches themselves. Qatar's app, 'EHTERAZ', for example uses both GPS and Bluetooth technologies, and yet an Amnesty Tech Security Lab investigation found "a critical vulnerability" in it "that would allow malicious actors to access sensitive personal information, such as names, national ID number, health status, and location data, for more than a million users in the country", wrote Access Now. This is all the more relevant given Qatar's model of ADM systems deployment, according to which download of the app is compulsory for all users, while those who don't comply "face a disproportionate penalty of up to three years in prison and a fine of approximately 55,000 USD".

Even Google/Apple-based, decentralised apps are not immune from inaccuracies and bugs, potentially leading to high rates of false positives/negatives, and not even knowing "the number of people warned by the app", as per a BBC investigation. This leads to serious questions not only in terms of efficacy, but of even being able to somehow measure that alleged efficacy.

A study[9] published at the end of June by Trinity College researchers in Dublin adds further concerns. By applying the proximity detection rules adopted by the German, Swiss and Italian exposure notification apps to the context of public transportation (a commuter tram), authors Douglas J. Leith and Stephen Farrell concluded that "the Swiss and German detection rules trigger no exposure notifications, despite around half of the pairs of handsets in our data being less than 2m apart".

As for the Italian one, it "has a true positive rate (i.e. correct detections of handsets less than 2m apart) of around 50%. However, it also has a false positive rate of around 50% i.e. it incorrectly triggers exposure notifications for around 50% of the handsets which are greater than 2m apart". What it means is that its performance is "similar to that of triggering notifications by randomly selecting from the participants in our experiments, regardless of proximity", authors conclude.

All of this leaves us with a question: what data do ADM systems need to actually help with contact tracing — if they can, at all?

## / Locations vs proximity: what data do ADM systems need to actually help with contact tracing?

The idea behind different contact tracing and exposure notification apps may be similar, but different decision-making processes are entailed by different app architectures.

By collecting location data, GPS-based apps can for example help health authorities reconstruct the web of contacts of an individual who tested positive to COVID-19, thus allegedly contributing to contact tracing efforts, by speeding them up and making them more effective and complete (logs are assumed here to be more reliable than human memory and judgment alone, here), while at the same time making it possible to realise that outbreaks are happening in precise spots and areas within a city or country.

Also, they can inform the understanding of trends in the population that are relevant for public health. For example, an intelligent analysis of the movements of a large number of people can reveal a population's attitudes towards social distancing rules. GPS is also adopted in the enforcement of quarantine rules.

On the other hand, Bluetooth-based apps do not collect location data, and are instead based on proximity. Therefore, under this model of ADM, smartphones on which a contact tracing or "exposure notification" app has been downloaded regularly emit a Bluetooth Low Energy signal that contains a random, and temporary, key. This is used to create an encrypted log of all other phones equipped with the same app that qualify as "contact"[10], i.e. potentially expose other smartphone owners in the log to infection, were one of them to be diagnosed with the COVID-19 disease.

9 Douglas J. Leith and Stephen Farrell (2020), Measurement-Based Evaluation Of Google/Apple Exposure Notification API For Proximity Detection In A Light-Rail Tram, https://www.scss.tcd.ie/Doug.Leith/pubs/luas.pdf

10 Definitions of "contact" in the context of exposure notification apps vary, but according to WHO guidelines a contact is relevant for a potential COVID-19 infection when "within 1 metre of a COVID-19 case for > 15 minutes", "from 2 days before to 14 days after the case's onset of illness".

This functionality is common to both centralised and decentralised Bluetooth-based apps. But then, the process differs. In a centralised app, such as Australia's 'COVIDSafe' app or in the UK's discontinued one, when individuals test positive for COVID-19 they may be asked by health authorities to share data collected through the app in a central database, that is then used to compute which contacts qualify as such in terms of potential coronavirus exposure, and actually track them down.

Instead in a decentralised model, such as Italy's 'Immuni' or Germany's 'Corona Warn-App', such computation is performed on each individual phone. If willing to share such information through the app, all "contacts" of a positive subject are then warned through the system, and they may decide to seek medical attention as a result.

This means that, contrarily to centralised apps, health authorities are not given the whole chain of contacts of an infected individual, even if anonymously. This is why such apps are correctly framed not as contact tracing apps, but as "exposure notification" apps: they only notify potential exposure to contagion to an individual, but authorities have no way to know who that individual is, who they have been in contact with over the last two weeks, and most importantly where, using app data only. As the BBC writes, these apps "operate more as a warning system" than a contact tracing system.

Difficult trade-offs need to be considered when evaluating pros and cons of such models of automated decision-making. GPS systems, for example, are much more invasive in terms of privacy and human rights, but at the same time may provide much more information that can be useful in tackling future outbreaks. Bluetooth systems, on the other hand, are less invasive, but arguably less useful, certainly less ambitious, and actually effective only when downloaded by large parts of the population and in combination with extensive, and readily deployed, testing programmes: what good is a notification that warns you of potential infection, otherwise?

## / Does ADM in contact tracing and exposure notification work at all?

Many pundits, institutions and civil society organisations weighed in on what data would actually be needed to at the same time maximise effectiveness and minimise the burden on fundamental rights. Answers are still provisional, as — even months after the first deployments — we still lack hard evidence on the effectiveness of all such ADM systems.

As a systematic review of the literature published in Lancet[11] on August 19 concluded after analysing 110 full-text studies, "no empirical evidence of the effectiveness of automated contact tracing (regarding contacts identified or transmission reduction) was identified".

In fact, what we do know casts several doubts over their efficacy, putting the initial enthusiasm around tech-based solutions to the pandemic to rest, and actually calling into question the very decision of deploying them in the first place.

An American Civil Liberties Union (ACLU) White Paper, for example, after having described all possible types of data collection (GPS, cell tower location data, Wi-Fi, Bluetooth and QR codes) concluded in April that "none of the data sources discussed above are accurate enough to identify close contact with sufficient reliability".

GPS technology has "a best-case theoretical accuracy of 1 meter, but more typically 5 to 20 meters under an open sky". Also, "GPS radio signals are relatively weak; the technology does not work indoors and works poorly near large buildings, in large cities, and during thunderstorms, snowstorms, and other bad weather".

This is especially important for ADM: "Even if we were to imagine a set of location data that had pinpoint accuracy", writes the ACLU paper, "there would still be problems translating that in any automated way into reliable guesses about whether two people were in danger of transmitting an infection". Case in point is Israel, where "one woman was identified as a "contact" simply because she waved at her infected boyfriend from outside his apartment building — and was issued a quarantine order based on that alone".

Cell tower location data also is not precise enough, especially in rural areas, and even China had to abandon it after trials did not return the desired results.

11 Isobel Braithwaite, Thomas Callender, Miriam Bullock and Robert W. Aldridge (2020), Automated and partly automated contact tracing: a systematic review to inform the control of COVID-19, https://www.thelancet.com/journals/landig/article/PIIS2589-7500(20)30184-9/fulltext

As for Bluetooth, even its own creators, Jaap Haartsen and Sven Mattisson, argued for caution: problems in terms of accuracy and "uncertainty in the detection range" are very real, they told the Intercept, "so, yes, there may be false negatives and false positives and those have to be accounted for".

Skepticism is confirmed in another study by Trinity College's Leith and Farrell[12], in which the researchers found that "the strength of the received Bluetooth signal can vary substantially depending on whether people walk side by side, or one behind the other. Whether they carry their phone in their back or front pocket, where they place it within their handbag, and so on." This might not be a problem for Bluetooth in general, but it surely becomes one in the context of containing the outbreak of the virus.

According to the paper, walls and furniture, especially metal objects such as shelves and fridges in a supermarket shopping aisle, or train or bus, could have "a significant effect" on this crucial component of decentralised, Bluetooth-based ADM systems, affecting the very core of their potential contribution in addressing the pandemic: notifying users that are actually in danger of contracting the COVID-19 disease.

"For example", argued prof. Leith speaking with the Irish Times, "for two people walking around a large supermarket we found that the Bluetooth signal strength is much the same when they walk close together and when they walk 2m apart. When sitting around a meeting table with phones in their pockets we measured the signal strength to be very low, even for people sitting next to one another." This fundamentally challenges the idea that exposure notification apps should be a pillar of effective broader contact tracing efforts.

The study therefore called for extensive testing prior to deployment of any such ADM systems, but — as previously noted — this is a complex endeavour in itself, as we don't really know even how to define and measure "success" and "effectiveness" of such apps.

What we know, both from actual deployments so far and available literature[13], seems to confirm this fundamental confusion over such crucial metrics. Can we define an app "successful" based on its actual downloads and active users? Would this mean that Germany's app, downloaded by more than 14 million citizens in just the two first weeks after launch, is a success story even if, for the first five weeks, it has been shown not to work properly in the background of millions of Android-based Samsung and Huawei smartphones?

Also, some countries made download of such apps mandatory, making comparisons moot. In fact, this would make India's Arogya Setu controversial GPS+Bluetooth-based app the most successful in the world, having been made mandatory for certain social categories, and therefore downloaded by some 127 million citizens in around 100 days — by far the most "popular" in the world. Does this mean that we should justify its many privacy and cybersecurity issues?

And what to make of the Indian app's developer claim of a 24% rate of effectiveness? How to actually make sense of — and audit, really — the assertion that "24% of all the people estimated to have Covid-19 because of the app have tested positive"? Is any percentage above zero a success?

Questions concern how to even measure these variables in a decentralised, Apple/Google-based, app: how to evaluate whether these apps actually work, when it is impossible for authorities to reconstruct who received an "exposure notification" through the app, in what contexts, and to what results?

## THERMAL SCANNERS, FACE RECOGNITION, IMMUNITY PASSPORTS: SHOULD THIS BE OUR NEW NORMAL?

The COVID-19 pandemic is severely affecting the economy on a world-wide scale. But the virus did not spell disaster for all commercial sectors. Some, on the contrary, are profiting from it.

12 Douglas J. Leith and Stephen Farrell (2020), Coronavirus Contact Tracing: Evaluating The Potential Of Using Bluetooth Received Signal Strength For Proximity Detection, https://www.scss.tcd.ie/Doug.Leith/pubs/bluetooth_rssi_study.pdf

13 Leonardo Maccari and Valeria Cagno, 'Do we need a contact tracing app?', https://arxiv.org/pdf/2005.10187.pdf

Take the latest forecasts for the thermal scanning and facial recognition technology markets, whose items are being aggressively repurposed and marketed as indispensable "anti-COVID" tools by a growing number of technology firms and startups, and deployed in supermarkets, theatres, cinemas, hospitals, stadiums, banks, public offices and of course private businesses.

"The global thermal-imaging market is estimated to grow to $4.6 billion by 2025 from $3.4 billion this year due to the coronavirus pandemic", Reuters reported at the beginning of July 2020. This means that "there are now 170 companies selling fever detection technology meant to detect people potentially suffering from the coronavirus, up from fewer than 30 companies selling similar technology before the pandemic", reported OneZero, citing an IPVM directory. Five out of the six biggest players are Chinese: Sunell, Dahua, Hikvision, TVT, and YCX.

The market for face and voice biometrics is also about to significantly expand thanks to the pandemic, with an expected leap to $22,7 billion in 2027 from a current estimate of 7,2 billion, more than tripling in value in just five years, according to Global Industry Analysts estimates.

This is both unsurprising and surprising. Unsurprising, given that face recognition is being widely adopted and deployed, both inside and outside the EU, with little to no meaningful democratic debate and safeguards in place.

Bur surprising also, given what we know about their scant usefulness in the battle against COVID-19. As a recent, and groundbreaking, US National Institute of Standards and Technology (NIST) study has argued, contrarily to what several developers claimed in PR material over the course of the pandemic, "wearing face masks that adequately cover the mouth and nose causes the error rate of some of the most widely used facial recognition algorithms to spike to between 5 percent and 50 percent".

Doubts abound around the accuracy and actual usefulness of thermal scanners too. According to the Electronic Frontier Foundation, thermal cameras "threaten to build a future where public squares and sidewalks are filled with constant video surveillance—and all for a technology that may not even be effective or accurate at detecting fevers or infection".

More precisely, "experts are now concluding that thermal imaging from a distance—including that in camera systems that claim to detect fevers—may not be effective. The cameras typically only have an accuracy of +/- 2 degrees Celsius (approximately +/- 4 degrees Fahrenheit) at best". Also, "human temperatures tend to vary widely, as much as 2 degrees Fahrenheit. Not only does this technology present privacy problems, but the problem of false positives can not be ignored. False positives carry the very real risk of involuntary quarantines and/or harassment".

Even perfect accuracy would not be enough in the context of fighting the COVID-19 pandemic, as many infected individuals are asymptomatic or have symptoms that are "mild enough to avoid triggering a "fever detecting" camera. For example, one might be positive to COVID-19 and not have a fever at all.

These issues are true of "AI" solutions for the pandemic more broadly. As a study[14] (not peer-reviewed at the time of writing) conducted by the WHO with universities in New York, Durham and Montreal concluded, "there is a broad range of potential applications of AI covering medical and societal challenges created by the COVID-19 pandemic; however, few of them are currently mature enough to show operational impact".

Some countries are experimenting with immunity passports too — from Estonia to the UK[15]. The rationale for their adoption, and the case for urgently doing so, is the same: when adopted as a digital "credential", as per Privacy International, an individual becomes able to prove his health status (positive, recovered, vaccinated, etc.) whenever needed in public contexts, thus enabling governments to avoid further total lockdowns.

And yet, the London-based NGO warns that, similarly to all the tools previously described, "there is currently no scientific basis for these measures, as highlighted by the WHO. The nature of what information would be held on an immunity passport is currently unknown."

What is already known, however, is that using immunity passports would entail several "social risks", serving "as

14 Joseph Bullock, Alexandra Luccioni, Katherine Hoffmann Pham, Cynthia Sin Nga Lam and Miguel Luengo-Oroz (2020), Mapping the landscape of Artificial Intelligence applications against COVID-19, https://arxiv.org/abs/2003.11336

15 More on this on both individual country sections.

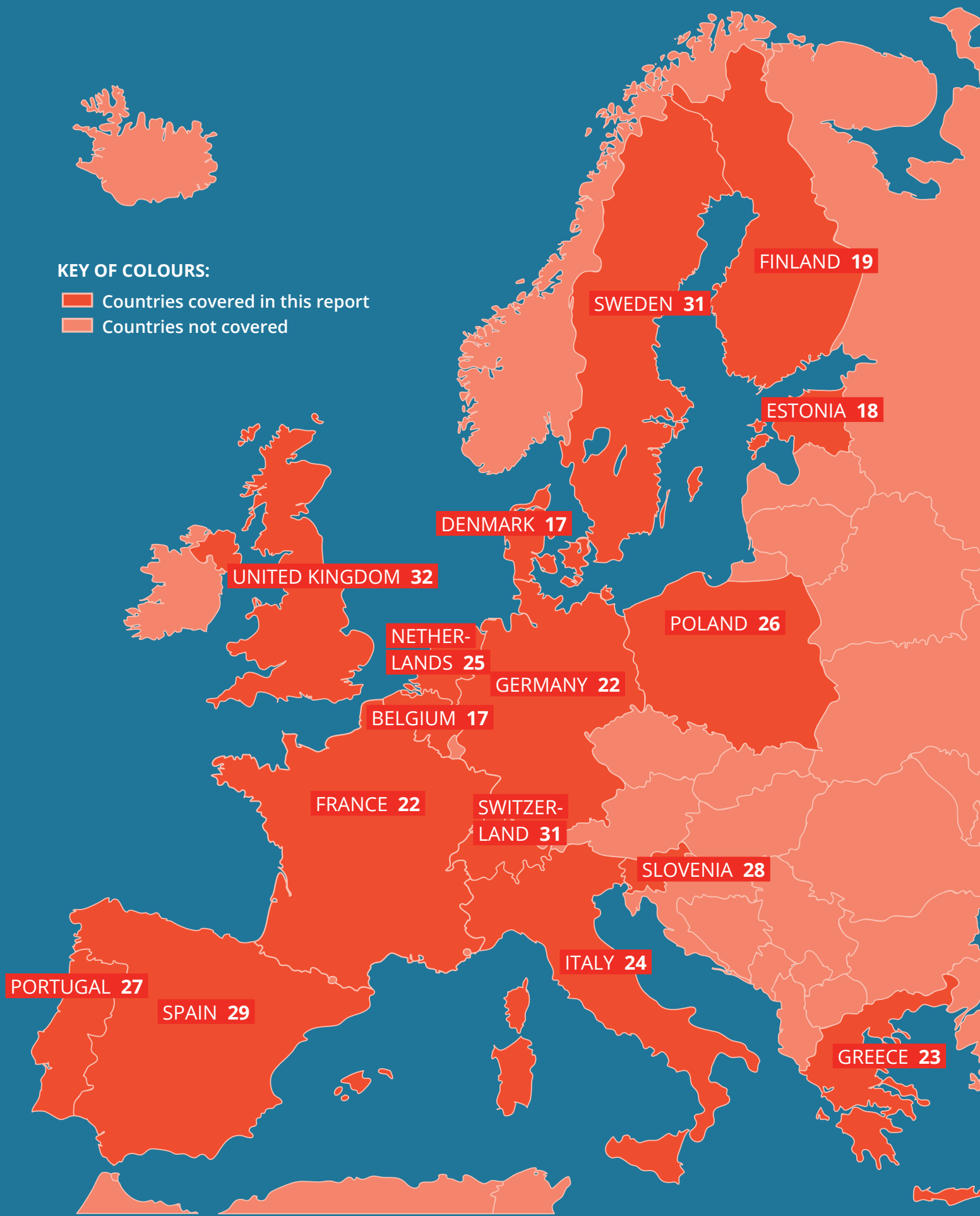
a route to discrimination and exclusion, particularly if the powers to view these passports falls on people›s employers, or the police".

A common theme emerges around all such tools: while marketed as necessary tools in "going back to normal", what they do in reality is trying to impose — with no evidence whatsoever as to their effectiveness — a new normal based on pervasive and health-based surveillance. This socio-technical apparatus — as shown in many examples already, most notably in the Chinese city of Hangzhou — may be born out of a public health emergency, but is definitely here to stay, adding to the already concerning arsenal of surveillance devices deployed before the SARS-CoV-2 outbreak.

Whether this "new normal" actually helps containing the spread of the COVID-19 disease is a question that can only be addressed at a later stage of the pandemic, when actual results of implementations of such ADM systems will (hopefully) become available, and with further and much more in-depth research. A rigorous approach on how to measure and evaluate such results will also need to be developed in the meantime, however — if possible, at all.

But no matter the evidence, a general conclusion can already be drawn from this early foray into the status of ADM in tackling public health emergencies: rushing to novel technological solutions to as complex a social problem as a pandemic can result both in not solving the social problem at hand, and in needlessly normalising surveillance technologies. These systems should, instead, be widely and openly discussed before adoption, if they truly are to be compatible with our fundamental rights and democracy.

# COUNTRY ANALYSES



# BELGIUM

**BY ROSAMUNDE VAN BRAKEL**

Belgium was hit hard by the COVID-19 pandemic, with a high number of deaths. The virus was confirmed to have spread to Belgium on 4 February 2020. It became significantly worse after people returned from spring holiday at the beginning of March. The National Security Council ordered a 'lockdown light' from Friday 13 March midnight onwards, which included the closure of schools, discos, cafes and restaurants, non-essential shops and companies, the cancellation of all public gatherings and the message that people need to work from home and leave the house as little as possible. Starting early May, the lockdown measures were removed in different phases.

## / Road to a contact tracing app

At the end of March, the Minister of Health and the Minister of Digital Agenda and Privacy launched a taskforce 'Data & Technology against Corona'. Members of the taskforce included representatives of the Ministry of Health, Sciensano, the e-health platform and the Belgian Data Protection Authority. The goal of the taskforce was to oversee and coordinate all health initiatives.

The possibility of developing a contact tracing app was explored but at the end it was concluded that this was not a decision for the Federal government to make but should be taken by the regional Flemish, Walloon and Brussels governments.

In June 2020, an inter-federal interdisciplinary working group was set up by Professor Bart Preneel from the University of Leuven who is one of the leading partners in the Decentralized Privacy-Preserving Proximity Tracing (DP-3T) app initiative. It is considered the most privacy-friendly app solution as no data is stored centrally by the government and, no use is made of automated decision-making[16]. The goal of the working group is to develop policy measures for the Belgian version of the app.

A cooperation agreement between the regional governments was finalized in a couple of weeks, which usually would take two years . The Belgian app will be based on the German app and will be built by Belgian company Devside. It is expected that the app will be operational by the end of September 2020.

## / ADM to enforce lockdown rules

Automated decision-making systems have been used by the government to enforce lockdown rules. For instance, mobile phone signals are used to track movements of people and indicate in real-time how busy certain areas get. With two to three minutes delay, the algorithms give a warning when the maximum number of people has been reached.

The algorithms can also distinguish between residents and passers-by, and was already tested when the Tour de France passed through Brussels.

Another example is the deployment of smart video surveillance cameras to monitor how crowded the shopping streets become. For instance, in Roeselare, telecom operator Citymesh installed smart cameras in one of the shopping streets. "The camera counts in real time how many people walk on the image in or out of the street," said Citymesh CEO Mitch De Geest. "These counts give the police, taking into account the available surface area and the diameter of one and a half meters, an insight into the occupation rate of the street. So that they can close it if necessary".

# DENMARK

**BY BRIGITTE ALFTER**

A few months into the COVID-19 crisis, Denmark started following a test and trace strategy. The first case of COVID-19 was registered on February 27, and the first death on March 16.

## / From location to proximity

From early on in the pandemic, a tech solution was envisaged, and in mid-April, the government commissioned a legal assessment of a contamination tracing app, based on geodata. At that stage, the government pondered the legality of such an app, including a legal

16 Cfr. Footnote n. 2, Introduction

basis in the law about epidemics (Kammeradvokaten, 2020).

Later, however, the government decided against geo-tracing and data storing and decided on a solution based on a decentralized software solution offered by Apple and Google.

Throughout May 2020, the Danish health authorities were able to open testing capacity to more of the population than before, when testing was restricted to selected groups who were tested in hospitals. It soon emerged that the authorities would store DNA information of those tested in a national database for up to ten years after the death of the person in question, while hospitals would destroy the DNA once the test had been carried out. This situation caused public controversy.

Neither the coronavirus app nor the testing question apply automated decisions[17]. Yet, the controversies around these tech-approaches in dealing with a health emergency are worth noticing and possibly studying as such.

### / Blocking websites without warrant

Another, little noticed, measure to react to COVID-19 was the right to block websites offering fake or overprized COVID-19 protection gear, notably to block them immediately and without warrant. A judge can then be asked to "approve" the blocking or otherwise the judge can inform the ministry of justice (L 157. 2020).

The bill introducing this and other measures were ad-hoc reactions to the COVID-19 crisis and is set to expire automatically in 2021. However, the minister of defense suggested to make the right to block websites without warrant permanent beyond the planned expiration date.

17 Cfr. Footnote n. 2, Introduction

## ESTONIA

**BY MARIS MÄNNISTE**

### / COVID-19 Contact tracing and warning app

Public and private sector consortiums have been called up by the government to discuss and plan the development of a contact tracing and warning app for Estonia. Different options are under consideration with a preference for privacy-enhancing solutions based on consent, such as PEPP-PT, emphasizing the need for cross-border interoperability.

The app is hoped to be ready to be used by August, and is based on Bluetooth technology, notifying users to turn on Bluetooth on their mobile phones. It will inform the user if they have been in close contact with someone for more than 15 minutes, who already contracted COVID-19. Users themselves will have to provide information about contracting coronavirus. However, it have to will be confirmed by data from other sources (for example, Health Board data or by data from a patient portal).

One Estonian entrepreneur, Keith Siilats, has already developed a contact tracing app for COVID-19, which he argues will conform to the national contact tracing app requirements in the future.

The technology behind the app is similar to technology used in Singapore; however, there is a difference when it comes to what the consortium plans to do with it. According to Priit Tohver, from the Ministry of Social Affairs, Estonia aims to develop an app where a lot of the data collection and analysis is happening inside the individual's phone, and citizens can voluntarily share this data with governmental Institutions.

Estonia, like many countries, is also planning to integrate its contact tracing app with Apple and Google's joint COVID-19 APIs for iOS and Android.

### / COVID-19 Travel app

The Estonian IT development company Nortal, in cooperation with a German company called Ottonova and inHealth, from the United Arab Emirates, aims to develop a system called the Corona Travel App.

It "matches the official immigration requirements of the traveler's final destination with the individual health data from the user", according to the company's own blog. If the user meets the conditions set for the final destination, a certificate will be sent to him or her, which will be accepted upon arrival by both transport companies and migration authorities. It is hoped that the app will be ready for use by travellers over the next few months.

### / Immunity Passport

According to Immunity passport homepage, it is an app that will allow people to access their various COVID-19 test results, get a probabilistic assessment of their immunity status and share this information either with employers and officials or family members. Test results are shared via a QR code created by the system to be used for a certain amount of time.

Once scanned, the system shows the necessary health information and a photo of the user for identification. ImmunityPassport aims to give frontline workers more confidence in safer workplaces, and let people who recovered from the disease help caring for older relatives. The project is still in pilot phase.

### / Data Management System for WHO and Immunity Wallet

A number of Estonian and Finnish software companies have formed a consortium to develop data management systems for the WHO based on the principles of distributed data exchange.

The first project for the WHO based on Estonian digital solutions is called the Immunity wallet and it is being developed by the data security company Guardtime. The project aims to connect databases from 15 to 20 countries and it could be helpful in tracking vaccinations by WHO-supported laboratories.

## FINLAND

**BY TUUKKA LEHTINIEMI AND MINNA RUCKENSTEIN**

The Finnish ADM-related efforts to mitigate hams from the COVID-19 pandemic include a corona symptom checker, maintained by a state-owned company, and two projects involving public-private partnerships.

### / Corona symptom checker

Once the pandemic started to spread in Finland, a corona symptom checker was added to the Omaolo ("MyFeel" in English) health service, maintained by a state-owned company SoteDigi. As a CE-marked service, the Omaolo is guaranteed to meet the requirements for medical devices, stated in three different European Union directives.

The COVID-19 symptom checker was compiled in collaboration with The Finnish Medical Society Duodecim and the Finnish Institute for Health and Welfare. After the publication of the checker, it has been updated 15 times, according to the state of the pandemic and changes in regulatory guidance.

The main purpose of the corona symptom checker is to assess the possibility and severity of a COVID-19-infection. In practice, the symptom checker asks yes-or-no, or multiple-choice questions, in order to evaluate the possibility of contagion and whether the condition needs medical care, or if self-care is sufficient.

The service is available for approximately 3,3 million Finns (the overall population in Finland is 5,5 million), with the possibility to send the symptom report to a health professional. According to SoteDigi, since March the corona symptom checker has been used over 600 000 times. In comparison, the amount of confirmed covid-19 infections in Finland is 7,362, with the number of tested samples being a little over 320 000 (23.7.2020).

The citizen using the Omaolo service is asked for informed consent and contact information, so that the medical personnel can communicate with the patient, if needed. One can also make a health appointment after using the corona symptom checker.

The Omaolo service has been used and tested extensively prior to the pandemic and it is a very good example of how existing digital infrastructures, which have already gained the trust of the citizens, can be mobilized for health care needs in exceptional times.

## / Crowd insights

As part of the pandemic-related efforts, the telecommunications operator Telia launched a service called Crowd Insights, tailored to the Government, at the beginning of April 2020 for three months.

Information gathered by Telia can be used to monitor the connections of mobile devices to the base stations of the mobile network. The aggregated data can aid in monitoring the presence of mobile devices in geographical areas and the mobility of devices e.g. between municipalities and provinces, so that the Government can use that information to survey people's whereabouts, movements and gatherings.

The collected data is anonymized and aggregated, and cannot be used to trace individual actions. While Telia's data covers only their own customers, it is computationally generalized to provide an estimate of the entire population.

Later in April, another telecommunications operator, Elisa, announced that they are providing a similar service to HUS Helsinki University Hospital. The service can, at least in principle, be used to monitor how pandemic-related restrictions are followed and how effective they are.

## / Exposure notification app

As part of the "exit strategy" from restrictions imposed due to the pandemic, the Finnish government is, much like the governments of many other countries, planning and preparing a smartphone app for coronavirus exposure notifications.

According to media reports, the app development got started as a public-private partnership effort in late March, when the IT consultancies Reaktor and Futurice teamed up, aided by the government's funding agency Business Finland, to examine whether the app used in Singapore, or the app concepts developed elsewhere in Europe could be employed in Finland. In early April, a government minister confirmed that the Finnish government supports the effort.

In late April, details of the app were outlined in a plan prepared by the Ministry of Social Affairs and Health. The app is based on using the smartphone's Bluetooth radio to determine the proximity of other smartphones running the app. Healthcare authorities determine criteria for exposure to the virus, such as Bluetooth-based estimation of contact distance and duration.

The app is of the decentralised variety: pseudonymous identifiers about proximate app users are stored on each device instead of a central database. Contact data is to be deleted after a period of a few weeks, and the app itself is to be discontinued after the epidemic ends.

A pilot version of the app was called Ketju (in English, Chain) and it was developed by the above-mentioned IT consultancies, Reaktor and Futurice, and the information security company Fraktal. The pilot was funded by the government-backed innovation fund Sitra. Pilot studies took place during May and early June, when the pilot app was used by healthcare workers in the city of Vaasa. The focus was on technical feasibility of Bluetooth-based exposure tracing. After the pilot, the app' source code was published in GitHub.

In early June, concurrently with the pilot phase, it was announced that Solita, an IT firm that had not been involved in the pilot, won the competitive tender for the final app. A number of public-sector organizations, including the Finnish Institute of Health and Welfare (THL) and the Social Insurance Institution of Finland (Kela), are now involved in the project. Temporary legislative amendments necessary for launching an app for public use, related to, among other things. the necessary personal data collection, were passed in late June.

The launch of the app for public use is expected to take place at the end of August. The goal of the Finnish Institute of Health and Welfare, the public authority responsible for the app, is that the app would have one million users during the first month after the launch. Around three million users, corresponding to 60 % app penetration in the Finnish population, has been cited as a longer-term target.

The expected benefits of the app are reliant on considerable voluntary action on part of citizens. First, install-

ing the app itself is voluntary. The hurdle of convincing citizens to install the app is thought to be diminished by the decentralized and therefore ostensibly more privacy-preserving design.

Second, if an app user is diagnosed with COVID-19, they receive a code from healthcare authorities. If the user chooses to input the code in the app, the app sends the pseudonymous identifiers of past potential contacts to the backend system. The backend system then notifies the potentially exposed users via the app.

Third, when the app notifies someone about potential exposure to the virus, they only receive information about next actions, such as taking a test or remaining self-quarantined. Nevertheless, in addition to providing information to app users, the app is expected to supplement manual contact tracing by healthcare authorities.

At least some health authorities have expressed hopes that the app will significantly help with this task. According to the Ministry's plan, however, any use of exposure information in manual contact tracing relies on app users voluntarily notifying authorities about potential exposure – that is, healthcare authorities will not have access to any information without explicit voluntary action from part of the app user. It is for this reason that we have referred to the app as "exposure notification" rather than "contact tracing" app.

In the Finnish public debate, the development of a national coronavirus exposure app has from the start been mainly taken as a given. The notion that an app should be built to help with a complex societal phenomenon has led to the typical debates around technological solutions: worries about privacy infringements and surveillance, technology choices to mitigate these worries, and complains about the public sector's decision processes being so slow that they prevent quick technological solutions to emerging problems.

## / Questions that need to be asked

There are, however, fundamental questions about the app that would merit asking, but have largely been absent from the public debate.

First, before delving into the technical minutiae of the app and its privacy-preserving features, we should carefully consider whether privacy-preserving, end-user-focused app-based exposure notifications are a feasible idea to begin with. Even if Bluetooth is the best available technological proxy for coronavirus exposure, this does not mean that it provides us with reliable information about exposure. Similarly, even if a decentralised design offers high guarantees for user anonymity, this likely makes the app less useful for supplementing manual contact tracing by healthcare authorities.

Second, we should consider the legitimacy of public health interventions when they are delegated to apps. Some of the challenges faced by the authorities are related to convincing enough citizens to install the app. A 60 % population coverage for a voluntary app is a very high target. Achieving it requires not only a high sense of responsibility on part of the citizens, but also a smooth use experience of the app. Even if a high number of people installed the app, under which conditions would they take the app and its suggestions seriously and continue its use? If, for example, using Bluetooth as a proxy for virus exposure leads to many false positives, would citizens voluntarily continue to use the app and follow its suggestions?

Third, and most fundamentally, even if we assume that large-scale app penetration is achieved and maintained, and exposure notifications become part of our everyday lives, we should ask what it is like to live in a society where public health is ensured and controlled by apps. How might our everyday lives change as a result? What are the consequences in terms of equality and justice in public health? Are there some groups whose lives will be affected negatively more than others?

Even if questions like these seem irrelevant, or hypothetical, amid the urgency to combat the pandemic, we should carefully consider technological solutions, instead of remaining fixated on the ones that are technologically most feasible.

# FRANCE

BY NICOLAS KAYSER-BRIL

## / Slow start for Stop Covid, the contact tracing app

In early April, the French government announced an automated contact-tracing app. The project, Stop Covid, is headed by the National Institute for Research in Computer Science and Automation (Inria), a public organization. It designed its own centralized, pseudonymized Bluetooth-based protocol, ROBERT.

Parliament voted to support the project in late May, with the government's party and parts of the right supporting it. Others voted against, citing concerns that the project brought little in way of health safety while opening the door to widespread government surveillance. The data protection authority published an opinion on 26 May, which stated that the project was legal.

A few hiccups happened as the app was developed. Orange, the historical telecommunications company, announced its own contact-tracing app before stepping back. Some people downloaded a Georgian app with the same name, Stop Covid, and complained that it was not available in French. The actual app was finally published on the App Store and Google Play on June 2.

Minor incidents followed the release, such as the government's forgetting to allow the app in France's former colony of Guadeloupe, which is now part of France proper. Overall, software security experts praised that the code was open-sourced and that a bug bounty program allowed for finding and fixing bugs early.

However, key aspects of the project remain blurry. It is unclear, for instance, whether or not personally identifiable information, such as IP addresses and user-agents, are stored centrally.

Adoption has been slow in the first week after launch, with 1.2 million users activating the app and about 350,000 daily running it daily.

## / Mask-recognition algorithms

DatakaLab, a Paris-based company, supplied several public institutions with a tool to automatically detect mask-wearing. It was used at least in Cannes (population 70,000) and at the Parisian metro station of Châtelet-Les Halles (800,000 daily commuters).

Both trials were suspended in June.

## / Fever controls

Several cities installed automated software coupled to infrared cameras to measure the temperature of visitors entering town halls, or of children leaving school. Roissy airport installed a similar system to screen passengers from some international flights.

La Quadrature du Net, a civil society organization, claims that such measures are likely illegal under GDPR.

# GERMANY

BY LOUISA WELL

When the COVID-19 crisis hit Germany, several digital tools were developed to combat the spread of the virus and to live through the prolonged lockdown.

## / A Hackaton against the virus

Inspired by the Estonian hackathon, the Federal Chancellery hosted the hackathon WirVsVirus (Us versus the virus) in March 2020. A staggering 27,000 people participated in the hackathon and 1500 innovative ideas on how to combat COVID-19 were developed, many of which include digital applications that range from organizing neighborly support, to managing hospital resources, or checking COVID-19 symptoms.

## / Criticism to sharing mobile location data with local health authorities

Early on, discussions in both the public arena and the government focused on how to use data-driven solu-

tions to combat COVID-19. In March, Jens Spahn, Minister of Health, intended to grant access to mobile phone location data held by telecommunications operators to local health departments. However, due to public criticism over privacy rights and the general ineffectiveness of the measure to trace the spread of the virus, Spahn withdrew the initiative from a draft proposal on protecting the population from the pandemic.

### / Making the most of health data through apps

As in many other countries, several apps were developed specifically for issues around COVID-19. One of the first was CovApp, which provides a questionnaire to identify people who should get tested for the virus. It was provided by the Charité hospital in Berlin, who feared that they would not be able to deal with a high number of people turning to them for testing. The app helps to ascertain who is most at risk of infecting others. It was developed using open source code and can be adopted by other hospitals all over the world.

In April, a voluntary data donation app was introduced by the Robert Koch Institute (RKI), the federal agency for infectious diseases. The app transfers health data from fitness devices such as smart watches and wearables to the RKI, who use the data to monitor the spread of the virus and the development of hot spots.

### / A U-turn on digital contact tracing

Debates in Germany are most contentious when it comes to contact tracing apps. While such apps were implemented early on in Asian countries such as Taiwan and Singapore and later also adopted in European countries like Austria and the UK, Germany went through a long period of quarrelling over the direction to take.

Things seemed to get moving when the European consortium Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) started working on a common standard for a tracing app that would be in line with the EU General Data Protection Regulation (GDPR) and provide open source software. Hence, each country could build their own app, all of which would be interoperable and contact tracing would be possible across Europe.

A dispute emerged over whether to store the data in a centralized database or to keep it decentral on the devices collecting the data. Apple and Google proclaimed that they would only support a decentralized structure and while the German government first tended towards a centralized app they eventually favored a decentralized app structure.

The Federal Ministry of Health and the RKI tasked T-Systems and SAP with building a contact tracing app for Germany. Since its roll out in June, the app was downloaded 17,2 million times, as of August 17.

## GREECE

**BY ELEFTHERIOS CHELIOUDAKIS**

During the COVID-19 pandemic, technology is being held up as a crucial component to support the fight against the spread of the virus. Its uses in Greece seem to have included support for different measures. We will briefly report on three such technological applications: i) tracking of self-reported symptoms to predict potential COVID-19 patients, ii) screening of individuals in order to predict those safe to travel, and iii) monitoring the movement of populations via the use of drones.

### / Assessing the risk of being infected by the coronavirus

In March 2020, the Regional Governor of Attica launched a platform that assesses the risk of being infected by COVID-19 and provides personalized advice for potential patients. The platform is called “COVID19 Symptom Checker” and it is powered by DOCANDU, a company offering digital health solutions. According to its official website, the platform is approved by two official health entities in Greece, i.e. the Medical Association of Athens and the Athens Medical Society.

Users respond to a series of questions related to biographical information (gender, age, height, weight), current symptoms (fever, cough, shortness of breath, myalgias, etc.), chronic health conditions (cardiovascular diseases, diabetes, respiratory diseases, malignancy, renal diseases, etc.), as well as their social whereabouts (social/professional history, travel, contact with patients, etc.).

According to the users' answers and based on statistical probabilities, the platform informs the users whether they belong to vulnerable groups, while also it predicts the risk of a user being infected by the corona virus. Finally, the platform provides instructions for further steps (stay home, avoid contact with people, contact a doctor etc.). During its first week of operation, the platform received about 12,000 visits.

### / Screening of incoming travelers

In July 2020, the Hellenic Government launched the "Passenger Locator Form (PLF)", a questionnaire that all incoming travelers must complete before entering Greece. The travelers shall provide input including their biographical information (name, age, gender, contact details), as well as information about the country of their permanent residence and their previously visited countries in the last 14 days. It is worth mentioning that the PLF does not include questions related to travelers' health. Furthermore, based on the PLF's privacy policy, the personal data of the travelers will be retained for twenty three days starting from the traveler's entrance in Greece, and then will be completely destroyed.

The purpose of collecting these data is to conduct screening of incoming travelers so that the Greek Authorities will assess upon travelers' arrival whether one should be tested for COVID-19 or not. More precisely, after analyzing the received input and based on statistical probabilities related to the traveler's country of residence and their previously visited countries, the PLF sends a special QR code to each of them. Then, when travelers arrive to Greece, screening personnel directs them, depending on their QR code, either to the screening area where they will be tested for the coronavirus or to the exit of the check-point.

From the description of the tool on its official website, it is not particularly clear how exactly the variables related to the prior countries of travel and the country of residence affect the risk assessment procedure.

### / Using drones to monitor compliance with physical distancing measures

In April 2020, the Greek Deputy Minister of Citizen Protection announced that the Greek Police will deploy drones during the Easter holidays in order to ensure compliance with the movement restriction measures related to COVID-19, while such actions were later confirmed by numerous media reports. It is worth mentioning that the use of drones was based on legal rules that were adopted just few months before.

The new legislation allows for an indiscriminate and blanket use of drones for any kind of policing and border management activities, opening the way for various kinds of drone operations. The Greek civil society organization Homo Digitalis claims that the new rules do not address the challenges arising from the applicable data protection and privacy legislation, and that the use of drones in public places raises profound fundamental rights issues.

For these reasons, Homo Digitalis filed an official query with the Ministry of Citizen Protection requesting more information about the deployment of drones by the Greek Police to ensure compliance with the lockdown measures against COVID-19, while it notified the Greek Data Protection Authority on this regard.

## ITALY

**BY FABIO CHIUSI**

### / "Immuni" exposure notification app

A Bluetooth-based, exposure notification app initially called "Immuni" was announced by the Italian government on April 16, 2020. The announcement followed a consultation between the Ministry of Innovation and a "task force" of 74 experts, divided into eight groups, each dedicated to a crucial aspect of the app — "technologies for governing emergencies", "Big Data & AI for policies" and "legal aspects of managing data related to the emergency" being the most relevant aspects here. The license to develop the application was awarded to Bending Spoons SPA, a startup which claims to have over 300 million downloads for its 20+ iOS apps.

Even though the application was deemed "not in contrast with data protection principles" by the Italian Data Protection Authority on April 29, a persistent lack of transparency over its detailed functioning fueled a heated debate, involving claims from several high profile figures — both in institutions and among leading experts

and virologists — that digital contact tracing through the app had absolute priority over privacy and human rights concerns, and that, therefore, these rights should be sacrificed in the name of containing the pandemic.

On April 30, general principles for the development of the app — officially referred to as an "alert system" — were formalized in a legal decree published the same month (Decreto Legge 30 aprile 2020, n. 28, art. 6). The application has to be voluntary, and no discrimination can come to anyone who chooses not to download it. Also, privacy principles and regulations must be strictly observed, meaning that GPS localization data must not be collected, and, in any case, all data gathered through the app must be deleted by December 31, 2020.

In May, after a thorough analysis by the Comitato parlamentare per la sicurezza della Repubblica (COPASIR, a body of the Italian Parliament deputed to survey and oversee the activities of the Italian intelligence agencies) highlighted several doubts in terms of efficacy, definitions (what is a "qualified contact"?), practices (are tests immediately available, in case of notification of exposure?) and even "non-reducible" geopolitical risks, "Immuni" has been initially piloted in four regions (Abruzzo, Liguria, Marche and Puglia; others, such as Veneto, Friuli Venezia-Giulia and Piemonte, opposed the rollout, claiming that the app is not effective, if not useless altogether, and should therefore not be downloaded) starting from June 8, with a nation-wide launch a week later that led to a million downloads over the first 48 hours.

On July 23, Innovation Ministry, Paola Pisano, said in the Italian Senate that 12% of smartphone owners in the country (4,3 million individuals) downloaded the app so far. Questions concerning its efficacy still remain, though, as only 46 subjects who tested positive for coronavirus actually gave consent to send an alert to potentially infected contacts over the first month of operations, with 23 individuals made "aware of having been potentially exposed to contagion".

According to Pisano, however, "this shows that the app is useful".

### / Local applications for symptoms reporting

Some regions in Italy also launched their own smartphone applications. Examples include "AllertaLOM" in Lombardy, and "LAZIODRCOVID" in Lazio, both gather self-reports about symptoms that could potentially reveal COVID-19 infections.

An app, "ROMA AL TUO FIANCO", allows every citizen in Rome to report illegal gatherings, and will inform heat maps on the virus that, according to major Virginia Raggi, could help visualise the dynamics of the outbreak, thus allowing for example to avoid crowded or at risk situations.

### / Face recognition against COVID-19

Face recognition technology is also being deployed and used to enforce social distancing in relation to COVID-19 in the municipality of Como, earning the city the label of "Big Brother-style Como" in il Giorno on May 2, 2020.

According to the same newspaper, the 260,000 euros contract with the Brescia-based A2A Smart City SPA included 32 security cameras to monitor the city, half of them equipped with face recognition capabilities. All security cameras in the city will upgraded with face recognition technology over the coming years.

"Augmented reality" helmets with thermal scanning and facial recognition capabilities have been adopted in Milan and Rome. The device is produced by a Chinese company, KC Wearable.

## NETHERLANDS

**BY NAOMI APPELMAN AND RONAN FAHY**

The already quite pervasive techno-optimism and techno-solutionism in the Netherlands has been clearly shown in the response to the COVID-19 pandemic. Centre stage takes the government's attempts to develop a contact tracing app.

### / A failed "appathon"

In April 2020, after a tender period of less than a week, seven possible apps were selected to participate in a so-called weekend-long "appathon". The goal of this appathon was to engage the public and experts to test and improve the apps in the hope one would be suitable

for use. The entire process was widely criticised by civil society groups such as Bits of Freedom and a group 60 academics sent an open letter condemning the process (Helberger et al., 2020). The appathon was widely deemed a failure, also as none of the selected apps were deemed safe and usable enough.

### / Contact tracing app

The government is, at the time of writing (August 2020), in the process of finalising the development and testing of its own app. Called CoronaMelder, and based on Bluetooth technology, it has been released for download on August 17, even though its alert system will only be working in the provinces of Drenthe and Overijssel, where it is being tested before a nationwide release planned for September 2020.

### / Proctoring software for exam-taking at Dutch universities

Among many others, another striking example of ADM in dealing with the fallout of the pandemic is the use of online proctoring software for exam-taking. Several universities across the Netherlands are obligating their students, if they see no alternatives, to download software that allows the monitoring of a student's webcam, microphone, web traffic, screen, mouse- and keyboard activity, and tracks movements to determine cheating .

Student unions have protested vehemently against the use of this software. Indeed, two student councils launched legal action over the use of such software. However, in an important judgment, the District Court of Amsterdam ruled that the use of such software was not an unlawful interference with the right to privacy (District Court of Amsterdam, 2020).

## POLAND

**BY NATALIA MILESZYK AND ALEK TARKOWSKI**

The techno-solutionist logic behind some actions of the Polish government in response to the pandemic is just more proof that ADM systems in Poland, if they exist, lack transparency, societal overview, and well-informed public discussion around the issue.

### / A mandatory home quarantine app, with face recognition

The Polish Ministry of Digital Affairs launched a Home Quarantine app on March 19 that uses GPS location, time-stamped photos, and face recognition to ensure that citizens stay at home. As per its terms of service, the government uses this app to ensure that people instructed to remain in quarantine do so.

The app routinely asks users to share their location which must match with their GPS location. They are also asked to take a photo at the location and complete a "task" within 20 minutes of receiving the message from the government. If this is not done, action could be taken against the person by the authorities.

From April 1, the app was made mandatory, which, in our opinion, is not proportionate (due to factors, such as, people sending images of themselves to government servers).

The Home Quarantine app most probably includes an ADM component, which uses automatic face recognition to confirm that the photos sent by users match the reference photo provided when creating an account. According to independent experts who have studied the application, the system most probably uses ADM components available as a component in the Azure cloud solution used by the app. No official documentation on this functionality (or lack thereorf) has been made available.

### / Bluetooth-based digital contact tracing

In June 2020, another application was launched – contact tracking ProteGO Safe app using Bluetooth technology

and Exposure Notification protocol. The application evaluates the risk for COVID-19 exposure by using three colors: green – low, yellow – medium and red – high – colors are only recommendations to contact health authority. The application evaluates the risk based on following criteria: the length of the contact, the distance from the COVID-19 carrier, the date of the contact and certainty of the contact.

At the time of writing, ProteGO Safe did not distribute a single key allowing users to find out that people with a confirmed coronavirus diagnosis were in the vicinity. Over the past two weeks, not one of the 4,000 new COVID-19 carriers has sent information about their social contacts to the ProteGO Safe server.

In response to the development of new apps by the Polish government, Centum Cyfrowe Foundation has participated in the co-creation of "The Seven pillars of trust" – a set of important standards and rules [PL] to which these applications should adhere. These rules, in particular, recommend minimizing the data collected and having strict time periods for its retention, which states must follow in order to comply with fundamental rights.

### / ADM in the business sector

Some Polish businesses have implemented ADM systems to help fight the pandemic. Since 2012, Infermedica has been developing artificial intelligence tools for patient triage, and symptom checking, and these tools were adapted during the pandemic.

A curated COVID-19 pre-screening solution for patients, compliant with WHO guidelines, was deployed. The goal was to shift the burden of triage from health care practices, government-organized assessment centers, and emergency departments while helping all patients to quickly and accurately self-evaluate their risk of infection, and properly send them to the appropriate venue for care.

The COVID-19 screening protocol was first deployed by Symptomate, and then by other platforms, including Call Center Triage and Infermedica API.

Another example is FeverGuard, which is an AI-driven solution that combines analytic models with thermal image recognition to monitor body temperature and detect anomalies. By applying deep-learning, object tracking, and a temperature correction model, it can successfully extract human body temperature in real-time.

## PORTUGAL

**BY EDUARDO SANTOS**

During the COVID-19 epidemic crisis in Portugal, as in Europe, there was much discussion on the use of technology as a way to fight the epidemic, namely the use of contact-tracing apps. The debate was particularly intense in civil society and also reached politics.

### / Decentralised proximity tracing app

In light of several solution models that other countries adopted, or were considering adopting, public actors, in general, defended solutions that do not need automatic decision mechanisms while highlighting privacy concerns. In April, the Portuguese government declared its support to a INESC TEC initiative of a contact-tracing called STAYAWAY COVID, which implements the DP-3T decentralized proximity tracing system.

The app makes use of Google's and Apple's APIs related to the usage of Bluetooth technology, yet the government has publicly criticized those companies. First, due to their imposition of technical standards, which was considered an attempt to question the right of democratically elected governments to assess and judge them as acceptable to their citizens and compatible with the European values; and at a later stage because the app needs the localization option to be active in order to use Bluetooth, even if it does not use localization services.

The app faced public criticism from civil society, and even though it has not yet received full approval from the data protection authority, legislation was approved by the Government. At the end of July the source-code of the app was made available. As of early August, the test phase is still ongoing, but the app is expected to be available to the public by the end of the month.

### / An app for the bathing season

In preparation for the summer bathing season, a website and an app were also announced by the government. The prime minister said that all persons planning to go to the beach should install this app, which will indicate if any given beach still has space or if it has already reached the maximum (reduced) capacity.

While the app itself does not seem problematic, it remains unclear how the information is being gathered in practice. The system accepts different kind of inputs, including manual inputs from the local beach operators, but it also supports an automatic machine learning system that relies on live video footage from the beach in order to calculate the density of people on a beach. Both details of the system and information around where it is being deployed are available to the public.

### / Smart screening of COVID-19 patients

On May 15, 2020, S. João Hospital in Porto announced that it would begin analyzing CT scan images from COVID-19 patients through an artificial intelligence system. This system will do a first reading and screening of the images, and select some features that it thinks may correspond to an infection, highlighting these facts to the doctor, who may or may not validate the findings. It was decided to use this system to try and speed up the process of reading the images, increase confidence in the diagnosis, and help the patients' prognosis by automatically quantifying the damage the disease does to the lungs.

The Program in Data Science and Artificial Intelligence in Public Administration for 2020 was also redirected specifically to the fight against COVID-19. This year the objective is "to support R&D projects and initiatives that can contribute to new responses to this and future pandemics, with an emphasis on supporting citizens and health care services".

## SLOVENIA

**BY LENART J. KUČIĆ**

### / A dramatic increase in police powers

In March 2020, the Slovenian government proposed a first draft of the Act on intervention measures to mitigate the consequences of the COVID-19 disease for citizens and the economy. The text was submitted to the National Assembly for consideration and adoption under an emergency procedure.

However, the Information Commissioner, the Ombudsman, and some privacy experts soon noticed that the proposed draft also included two articles that would dramatically increase the powers of the police.

Article 103 suggested that the police could use various methods to ensure that citizens respect the quarantine and the Communicable Diseases Act. Among other measures, they can also use face recognition to identify individuals they have stopped, enter their houses or apartments, limit their movements, and collect and process personal information such as medical data from the National Institute of Public Health.

Article 104 went even further by suggesting that the police could trace the location of an individual's mobile phone without a court warrant.

All the suggested measures were introduced using an emergency procedure – without any consultations or public debates. As a result, the Information Commissioner commented that the anti-COVID-19 measures were, potentially, an attempt to "establish a police state". The commissioner considered the new police powers to be too broad and, potentially, unconstitutional and undemocratic.

The Human Rights Ombudsman wrote that it is hard to believe that such measures are really necessary and proportional (both institutions were not consulted during the process). Members of the Institute of Criminology also published critical commentary, stating that mass surveillance is not compatible with European legal culture.

Article 104 was removed from the amended act because of strong criticism from the public and the opposition political parties. However, article 103 relating to the powers of the police remained in the "Corona-act" that was adopted in April 2020.

### / The looming spectre of a mandatory tracking app

Furthermore, the government insisted that contact tracing applications are necessary to help health officials stop the pandemic. They also suggested that citizens will have to install such an application in order to travel across the country (between cities and municipalities). The data from the application would be collected and used by the National Institute of Public Health, but the police would also be allowed to access the database and exchange the information with the Institute.

In July, the government adopted another package of anti-corona measures, which provided a legal basis for introducing the mobile application for contact tracing. According to the new law, the app is obligatory for citizens who are tested positive for the coronavirus or who are in quarantine. The legislation package was adopted before the application was even developed, introduced, and tested. The opposition parties said the obligatory use of the application could breach personal data protection rights.

The information commissioner as many other experts and activists criticized this decision as well.

The minister of Public Administration Boštjan Koritnik later said that the use of application will be voluntary for everyone, including those who have been quarantined or confirmed to be infected with COVID-19. But the law still required obligatory use at the time of his press conference.

The minister also said that the application will not use a GPS system and the storage of geolocation data will not be enabled. Also, Slovenia will use the open source solution that was first developed by Germany. But he did not address any criticisms regarding the police use of the data. The voluntary app, called #OstaniZdrav (#StayWell) has been launched on Google's Play Store on August 17, with 5.000 downloads over the first 24 hours.

### / Anti-government protests potentially in danger

The new legislation could also allow police to access other kinds of personal information and, potentially, curb future anti-government protests.

The expansion of police powers thus remains problematic, especially considering that the new Slovenian government, formed just before the pandemic, has used the virus outbreak to enforce emergency measures and limit citizen's rights.

When the first groups of citizens started protesting against the government in April 2020, the minister for interior affairs, Aleš Hojs, took to Twitter to demand that the police should use their new and existing powers to identify and prosecute protesters, e.g., to collect and analyze all available images from both traditional and social media.

## SPAIN

BY JOSE MIGUEL CALATAYUD

### / A controversial self-diagnosis application

On 18 March 2020, the Madrid regional government launched a website including a Covid-19 self-diagnosis application based on a simple algorithm composed of eight yes-or-no questions. Each question was assigned a number of points, and if a user got 30 or more points, the application told them they might be infected with the Covid-19 virus and what they should do next.

The application had been developed by the Madrid government and several private companies, including Google, Telefónica, Carto and Ferrovial. Its stated aim was to free up the emergency phone lines and to provide the authorities with information to manage the crisis situation, including a first assessment of individuals who might need medical assistance and follow-up.

To use the application, people had to submit quite a few personal details, including the national ID number, full name, birth date, full residential address and email address. Then the questionnaire asked about symptoms the person might have.

The privacy policy stated that the collected data could be shared with the national security forces, the judicial system and all the companies acting as suppliers or working with the Madrid government, including those acting as subcontractors. The data was to be stored and processed for statistical aims and for biomedical, scientific or historical research; and it would be "deteleted, anonymised and/or blocked" when "the period of keeping the data finishes, and according to the requirements established in the applicable norm", without any other specification on when exactly that would be.

This lax privacy policy was criticised on social media and in some media reports, and when on 22 March the Madrid government released the Android and iOS mobile versions, the application no longer asked for the user's email address and the terms and conditions and the privacy policy had been updated.

Now they specify that the data would be used both to describe the pandemic and to predict how it might evolve, and added that the companies would only get "temporary" access to the data under instructions by the authorities, and that the companies would not be allowed to use the data for their own aims. Users could opt out of giving their phone GPS location, but if they chose to do so, the application would use their residential address for geolocation purposes.

## / The same results, just without personal data

Shortly afterwards, the Spanish national government released its own version of the web and mobile applications, based on the code of the one developed for the Madrid region. In its privacy policy, this version detailed that the data would be stored for a maximum of two years, and that it would not be shared with any private companies but only with Spanish national and regional administrations, and with international authorities if needed.

Several other regional governments within Spain released their own applications, in some cases also based on the code of the Madrid one. Interestingly, an independent developer released an open source version of the Madrid application, using the exact same algorithm and therefore producing the same output, that people could use without giving any personal data.

## / Predicting the lifting of lockdown restrictions

On 14 April, the Spanish government announced a new study, run by the National Scientific Research Council (CSIC), that would gather and analyse mobile phone, map servers and social media data to predict different social distancing scenarios and help in the decision of when, where and how to start lifting lockdown restrictions. The data is to be collected by the operators and companies taking part in the project, and the announcement said that no information that could identify individuals would be accessed.

The project was described as using "artificial intelligence tools and data science, and (integrating) big data in real time on human mobility, geo-localised surveys and computational models", without going into more detail about what all that exactly meant.

The announcement also stated as a long-term goal "to establish the basis for a computational epidemiology network in Spain, as in other countries, and a series of interoperable analytical tools based on epidemiological theories, data science and artificial intelligence, to inform the decision-making process in future situations of epidemiological crisis". No further information on which precise data would be collected and on how it would be processed could be found.

## / Temperature screenings for the basketball league

From the 17th to the 30th June, the Spanish professional basketball league held its playoffs in Valencia. The ACB, the sports association that manages the league and is made up of the top-tier 18 clubs, set up an ADM system to check people's temperature before entering the premises where the matches took place.

Developed by Valencian company Sothis and known as Thermal Vision System, the device measures the person's tear conduct temperature (which is supposedly very accurate to determine's someone's temperature) remotely by combining a "thermographic camera and artificial vision".

The company says the system gets the temperature in less than a second and with a margin of error of ±0.3º. In the basketball playoffs, the limit for a person to be allowed in was set at 37º. The whole process is automatic and the inner working of the system is not public. Reportedly, the whole exercise is seen as a pilot in Spain and in the future could be used in other public events.

## / promising results from decentralised contact tracing app trial

Lastly, Spain announced its national contact tracing app, "Radar COVID". Available for download in late August, it is based on the Apple/Google decentralised Bluetooth protocol. The app has been trialed on La Gomera, an island in the Canary archipelago, where it has been downloaded some 60.000 times (against an initial objective of 3.000), with interesting results.

Over the one-month experimentation, concluded on July 31, the app has been "twice as effective as human tracers" in the pilot, simulated outbreak, Reuters reports. Ac-

cording to a statement by Carme Artigas, head of the state digital and artificial intelligence unit, "for every virtual positive diagnosis, the app identified an average 6.4 contacts with others (...), compared with an average 3.5 contacts identified by human tracers in the Canary Islands".

# SWEDEN

BY ANNE KAUN

The ADM initiatives developed in response to COVID-19 can roughly be described as either voluntary or involuntary.

## / COVID-19 symptom-checkers

Of the voluntary initiatives, at least three applications have been developed to document and map symptoms among the Swedish population. One of these apps was developed by a non-profit group—made up of private individuals who met at the fifth Hack the Crisis hackathon—and it maps the development and spread of COVID-19 based on the self-reporting of symptoms.

A second app, initially developed in the UK, is now used by a research group based at Lund University to similarly track COVID-19 symptoms and the development of the disease among patients. App users register voluntarily and are asked to report their health status on a daily basis.

The last initiative was based on a collaboration between the Swedish Civil Contingencies Agency (Myndighet för samhällsskydd och beredskap), the Public Health Agency of Sweden (Folkhälsomyndigheten) and the National Board of Health and Welfare (Socialstyrelsen). In collaboration with industry partners, the three public agencies worked on a digital tool to map experiences of symptoms among the population.

Although the tool was completed, it was never implemented. On 28 April 2020, Ander Tegnell – the state epidemiologist – announced that the initiative would be paused for now as it potentially does more harm than good by worrying and confusing Swedes with the collected information.

In the context of discussions around a similar application used in Norway, which has been downloaded by 60% of the Norwegian population, Tegnell announced that a similar tracking app might be useful, in some instances, at a later stage of the pandemic when there are few, individual cases left.

Journalists later explored several issues with the project. Firstly, the contracts with industry partners (mainly Platform24 Healthcare—which is owned by the Wallenberg investment company and Apoteket AB—which uses a cloud service solution provided by Amazon Web Services) were signed, without the necessary public procurement procedures. Secondly, the partners were continuously paid even though the project is on hold.

## / Analysing Telia's mobile phone data

One major initiative—not based on voluntary participation by the population—is the analysis of mobile phone data by Sweden's largest service provider Telia. The Public Health Agency of Sweden asked Telia to help analyze anonymized and aggregated data on mobility. This helped the public agency analyze how people moved during the pandemic. The data, and the mapping of the movement of people during the Easter break, were widely publicized in Swedish media.

# SWITZERLAND

BY NADJA BRAUN BINDER AND CATHERINE EGLI

## / Corona App

As in many European countries, Switzerland recently addressed the current COVID-19 situation with a digital contact tracing app.

The official launch took place on 25 June 2020. Upon installation of the so-called "SwissCovid App" (installation is voluntary), the smartphone sends encrypted IDs via Bluetooth at regular intervals. Other smartphones will monitor such reports and store all IDs they have received. The prerequisite is that they have come closer than 1.5 meters for 15 minutes during a day.

If a SwissCovid App user tests positive for the corona virus, he/she receives a code (Covidcode). Only if the

person who tested positive activates the messaging function by entering the Covidcode, the other app users are notified if they were in close contact with this person. This notification is automatic and anonymous after the Covidcode has been entered.

The app uses a decentralized approach to data storage. The information which devices have been encountered remains on the smartphones themselves. No personal or location data is sent to a central storage location or server. When the coronavirus crisis is over, or if the app proves ineffective, the system will be shut down.

Prior to the official launch of the SwissCovid App, the app was tested. The legal grounds for the app's pilot trial can be found in the federal ordinance published on 13 May 2020. The regulation of the pilot trial was repealed on 25 June 2020.

The legal basis for the SwissCovid App can now be found in the Epidemics Act. The legislation procedure was passed very quickly by Swiss standards. The Federal Council has submitted a corresponding bill to parliament on 20 May.

In its June session, parliament approved the legal basis for the App and made only minor adjustments to the draft law. It is based on the Data Protection Act and regulates the organisation, operation, processed data and use of the app. Parliament approved the amendment on 19 June 2020 .

# UNITED KINGDOM

**BY TOM WILLS AND FABIO CHIUSI**

## / Immunity passports

The Coronavirus pandemic has triggered a number of debates about the use of ADM-adjacent technologies in the possible future management and mitigation of the spread of COVID-19 in the United Kingdom. For example, it has been reported that the government has entered into talks with technology companies about the possibilities of using automated face recognition as part of a so-called 'immunity passport' app.

A company called Onfido has presented detailed plans for an app that would allow people to prove their COVID-19 status, as determined by an antibody test. The face recognition element would be used so that the test result could be attributed to a person to a higher degree of certainty than simple use of photo ID.

## / Movement maps, Big Data analysis and algorithmic scoring

The UK government has partnered with telecom operators — O2, BT — "to analyse anonymous smartphone location data to see whether people are following its social distancing guidelines", wrote Sky News on March 19. Only mapping of anonymous, aggregated ("movement maps") data would be involved. Also, according to the Guardian, "the information provided on geographical movement would be delayed by 12 to 24 hours rather than arrive in real time, but would still be able to show patterns such as whether people were avoiding the high street and heeding government advice to stay away from pubs, bars and restaurants" .

A "data platform" has been announced as "about to be revealed" around the same time. It would "allow decision-makers to see accurate information in real time and co-ordinate a truly national response to the pandemic", thus facilitating "the movement of critical staff and materials". Data is gathered "from across the health sector" to be then "presented in a dashboard, akin to the ones used for monitoring internet traffic", according to Sky News.

Controversial US firm Palantir has also been involved in mining medical data from COVID patients. As disclosed by the NHS to Byline Times, contracts with the firm and other technology companies have even been awarded "without being put out to competitive tender".

Starting in June, algorithms have been used by some of the largest hospitals in England and Wales to prioritise appointments through a "traffic light" or scoring system. DrDoctor, the company providing the software to hospitals such as the Nottingham University Hospital and the Christie in Manchester, "automatically rates patients' responses to digital questionnaires to assess the urgency of their medical need, giving each patient a red, amber or green score"

## / The digital contact tracing saga

A contact tracing app has been revealed to be in the works in April through reports in the Guardian and the

BBC. The app would be developed by the NHSX, the health service's digital innovation unit, together with epidemiologists and ethicists from the Oxford University, and represent a crucial element of the broader UK government's "Test and Trace" strategy.

Just days later, the BBC also revealed that its architecture had shifted from using "GPS location readings and scanning QR codes" to Bluetooth technology in a centralised system, "to provide users more privacy, which in turn could encourage take-up".

Previously, the government reportedly considered implementing a "health code" system similar to that adopted by China, which would have had major consequences for the debate around what kind of anti-COVID-19 ADM systems should be allowed in democratic countries. A memo proposing to give the government powers to "de-anonymise" users had also been rejected by the NHSX.

The app has then been trialed at the Isle of Wight, immediately showing serious technical limitations that would, in the end, prevent its deployment. In particular, while the app "worked well at assessing the distance between two users", according to results reported by the BBC it "was poor at recognising Apple's iPhones.

Specifically, the software registered about 75% of nearby Android handsets but only 4% of iPhones". These results are consistent with those from other experimentations of centralised contact tracing apps, e.g. in France and Australia.

A decentralised version of the app, also trialed, showed better results, but together with different problems. In fact, while 99% of both Apple and Google-operated smartphones were correctly logged through the companies' "exposure notification" architecture, "its distance calculations were weaker", notes the BBC, adding that "in some instances, it could not differentiate between a phone in a user's pocket 1m (3.3ft) away and a phone in a user's hand 3m (9.8ft) away".

Choice of the centralised model depended on contingent, as well as technical, factors. As the NHSX app would not have sent notifications based on a positive test, but on self-reports of symptoms by users, a well-functioning decentralised solution would have only been possible together with quick and extensive testing of the population — the only way to prevent "trolls" and malicious actors to flood the platform with fake reports of exposure to infected individuals.

Because this was not the case in the UK, health authorities decided that the NHS itself would perform the matching between information shared by the user and actual testing data on a central server — rather than by each phone individually — before sending out notifications to all potentially affected subjects.

The scant results obtained in the trial, together with the decision, in June, to now issue alerts based on actual tests and not on self reports by users, thus better aligning with manual contact tracing efforts, forced the government to backtrack both from the centralised approach adopted until then — now missing its whole rationale — and from initial claims that considered the app a "priority" within the Test and Trace strategy.Health Secretary Matt Hancock argued that people had a duty to download it and Transport Secretary Grant Shapps even suggesting to make it mandatory for travellers entering the country at airports.

The government ditched the centralised architecture developed at the cost of 11,8 million pounds in favour of a decentralised one, based on Google and Apple's "exposure notification" protocol.

But while the new app was being developed, with a second trial in mid August and a new QR barcode functionality ("so users can check in when they visit a venue and be told if others there later tested positive"), the UK government seemed to be growing more and more skeptical about digital contact tracing technologies.

Consequently, promises of a "world beating" test-and-tracing system by Prime Minister Boris Johnson gave way to a much more cynical digital realpolitik. As he himself claimed in June in Parliament, "Yes of course it's perfectly true that it would be great to have an app, but no country currently has a functioning track and trace app". When FullFact checked, it couldn't prove him wrong: "it's too early to say whether (such apps) will be effective in helping combat COVID-19".

Whatever the end result, the debate around the UK's contact tracing app clearly shows how ADM systems cannot be meaningfully deployed without a careful consideration of all remaining, "analogue" elements of the wider public health policy and strategy within which they must be inserted.

IMPRINT

**Automated Decision-Making Systems in the COVID-19 Pandemic: A European Perspective**

**Special Issue of the Automating Society Report 2020**

1 September 2020

Available online at algorithmwatch.org/automating-society-2020-covid19

**Publishers**
AW AlgorithmWatch gGmbH
Linienstraße 13
10178 Berlin
Germany
Contact: info@algorithmwatch.org

Bertelsmann Stiftung
Carl-Bertelsmann-Str. 256
33311 Gütersloh
Germany

**Editors**
Fabio Chiusi
Sarah Fischer
Matthias Spielkamp

**Project manager**
Fabio Chiusi

**Publication coordinator**
Marc Thümmler

**Copy editing**
Justin-Casimir Braun

**Layout**
Beate Autering, beworx.de

Published as part of the project Automating Society by

ALGORITHM WATCH | BertelsmannStiftung

Website: algorithmwatch.org/en/automating-society

This publication is licensed under a Creative Commons Attribution 4.0 International License
https://creativecommons.org/licenses/by/4.0/legalcode