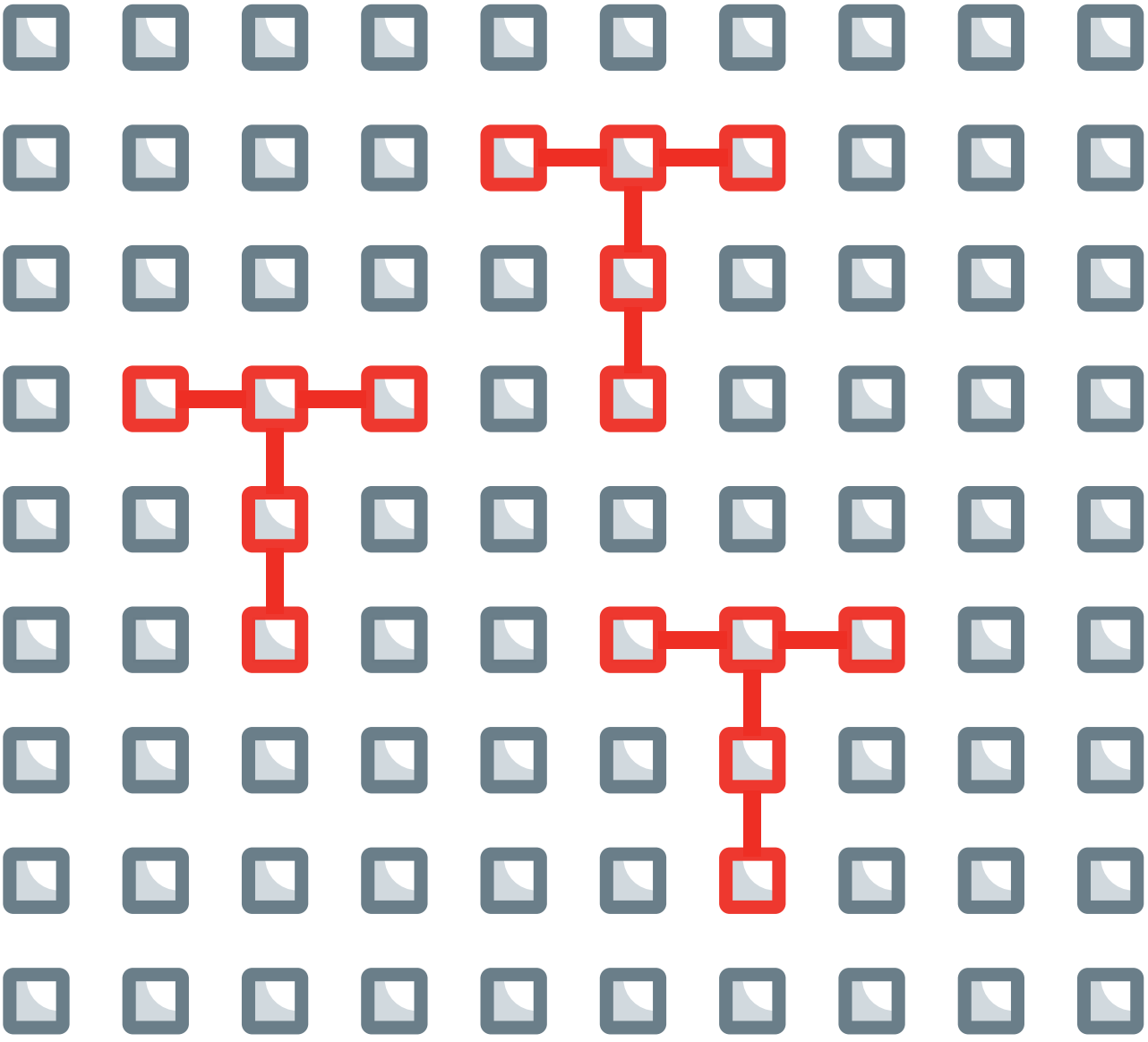
Automating COVID responses: The impact of automated decision-making on the COVID-19 pandemic

Tracing The Tracers 2021 report

Appelman, N.; van Brakel, R.; Calatayud, J.M.; Chelioudakis, E.; Chiusi, F.; Izdebski, K.; Kaun, A.; Männiste, M.; Ó Fathaigh, R.; Toh, J.; Visser, B.; Wladdimiro Quevedo, C.

Automating COVID responses. The impact of automated decision-making on the COVID-19 pandemic

Tracing The Tracers 2021 report



Published by

ALGORITHM WATCH

Funded by

EUROPEAN ARTIFICIAL INTELLIGENCE FUND

CONTENTS

EXECUTIVE SUMMARY.
HOW AUTOMATION DID NOT SOLVE THE PANDEMIC — BUT STILL SAVED LIVES 3

RECOMMENDATIONS.
ELEMENTS OF A BETTER, MORE DEMOCRATIC ALGORITHMIC STATUS QUO 4

SCENARIO.
THE GLOBAL QUEST FOR AUTOMATED SOLUTIONS TO THE PANDEMIC

/ The solutionist promise: automation will solve the pandemic 6
/ Solutionism is wrong, but influential 7
/ ADM did not solve the pandemic. But did it help? 8
/ The controversy over the role of AI in the pandemic 10
/ How COVID-19 normalized digital surveillance 11
/ There is no stopping biometrics, not even during a pandemic 13
/ Surveillance we wear and always bring with us 14
/ If ADM systems are solutions, they are faulty ones 15
/ We must make a better, more democratic use of ADM systems in a pandemic 16

BELGIUM
/ Context 19
/ Cases 19
/ Analysis 22

CYPRUS AND GREECE

CYPRUS
/ Context 24
/ Cases 24
/ Analysis: Limited uptake leads to a new approach? 24

GREECE
/ Context 25
/ Cases 25
/ Analysis: Openness, transparency, and public trust in challenging times. 26

ESTONIA
/ Context 28
/ Cases 28
/ Analysis 30

THE NETHERLANDS
/ Context 31
/ Cases 31
/ Analysis 33
/ Conclusion 34

NORDIC COUNTRIES
/ Context 36
/ Cases 36
/ Analysis: the overall contribution of ADM against COVID-19 in the Nordic countries 38

POLAND
/ Context 39
/ Cases 39
/ Analysis 41

PORTUGAL AND SPAIN
/ Context 42
/ Cases 42
/ Analysis 44
/ COVID-19 tracing technology in Portugal: when the government wants to force citizens to install a tracing app 44

EXECUTIVE SUMMARY. HOW AUTOMATION DID NOT SOLVE THE PANDEMIC — BUT STILL SAVED LIVES

BY FABIO CHIUSI

In an unprecedented global social experiment in health surveillance, a plethora of automated decision-making (ADM) systems — including systems based on artificial intelligence (AI) — were deployed during the COVID-19 pandemic. They were supposed to tackle fundamental public health issues. Nonetheless, too often, they were adopted with almost no transparency, no evidence of their efficacy, no adequate safeguards, and insufficient democratic debate.

This report is the result of yearlong monitoring of the rollout and use of such systems, documented in our Tracing The Tracers project. In this final report, we will provide an early overall assessment of the main trends and developments concerning ADM-based responses to COVID-19.

Many of our findings are consistent with those highlighted in previous AlgorithmWatch publications, such as the 'Automating Society 2020' and 'ADM Systems in the COVID-19 Pandemic: A European Perspective'. Opacity, lack of evidence, oversight, and substantial debate about the deployment of ADM systems preceded the pandemic. The response to COVID-19 only served to confirm these trends. Now, the situation is even worse than before COVID-19 because ADM systems include potentially life-saving tools.

Technological solutionism — i.e., reducing complex social issues to technological issues in need of a technological solution — emerged as the clear ideological background to most deployments of ADM pre-COVID. This kind of solutionism was on full display again during the pandemic and strongly influenced both public health policymaking and public perceptions.

Some ADM tools (digital contact tracing (DCT) apps and digital COVID certificates (DCCs)) have been hotly debated, but not in an evidence-based fashion and mostly based on contradictory, faulty, and incomparable methods, and results. And, while the use of these tools is partly acceptable in an emergency, too often it resulted in unfounded promises and marketing-oriented hype.

When it comes to the contribution of ADM systems in tackling some of the most pressing issues of the pandemic — containing infections, alleviating pressure on hospitals, allowing safe travel and social gatherings, prioritizing vaccines for those most in need — a somewhat mixed and provisional judgment must be given. Even though some ADM-based responses did help tackle COVID-19, there is so far no sufficient scientific evidence to back the conclusion that DCT apps, DCC schemes, AI, and/or algorithms have been central, fundamental, or even necessary to effectively respond to the pandemic.

DCT apps and DCC schemes — particularly in their "Green Pass" version for domestic uses — proved controversial, including per their effectiveness. However, the contribution of AI-based ADM approaches adopted in response to COVID-19 was, arguably, even more controversial and polarizing. Some argued in favor of an enthusiastic, solutionist future for public health thanks to AI. Others were more pragmatic and showed that, so far, the actual results produced by AI have been wildly overblown, subject to hype, and even exploited in dangerous, Cold War-style propaganda among conflicting superpowers.

Extremes abounded. On the one hand, dystopian applications of ADM have been repeatedly tested and/or deployed throughout the pandemic — mostly outside of Europe, according to our (incomplete) survey of the field. On the other hand, some promising applications have been adopted, including those used in vaccine research, distribution, and prioritization, in providing early COVID-19 diagnosis, assessing the risk of severe outcomes, creating "smart", efficient testing strategies, and assisting doctors with decision-making. Some of these uses might have saved lives, even though it is impossible to quantify their contribution.

As millions of lives were — and still are — at stake, a blunt, ideologically-based assessment should not be allowed in any informed discussions on the actual contribution of ADM systems in the fight against COVID-19.

The single, most worrying trend the Tracing The Tracers project was able to document throughout the pandemic was how it was exploited as an excuse to further entrench and normalize the surveillance, monitoring, measuring, and prediction of an increasing number of daily activities — now essentially including public and personal health purposes. This is even more concerning given the high degree of bugs, fakery, data leaks, and function creeps witnessed in the ADM tools deployed both in and outside of Europe. For example, some law enforcement authorities could access contact tracing data for criminal investigations.

In the 'Automating Society 2020' report, we concluded that the algorithmic status quo was untenable, and needed to change profoundly. Even though new normative frameworks in Europe and beyond are about to expand governance approaches to ADM systems on an enormous scale, so far, the pandemic has only perpetuated that status quo.

Now that ADM systems contribute to potentially life-saving decisions, it is even more urgent to open the health surveillance 'black box'. If we are to tackle both the current and future pandemics effectively and democratically, we must build a more transparent, evidence-based, and democratic algorithmic status quo.

RECOMMENDATIONS. ELEMENTS OF A BETTER, MORE DEMOCRATIC ALGORITHMIC STATUS QUO

To bring about a more democratic and evidence-based governance of ADM systems in the pandemic, some major trends need to be reversed, some cautions applied, and some basic principles respected. The Tracing The Tracers project highlighted the following elements, to be considered to facilitate a change toward a better algorithmic status quo:

— **Show us the evidence!** Now that the pandemic has raged for almost two years, there is no more justification for opaque impositions — with no clear end in sight — if there ever was one in the first place. Future ADM deployments must be evidence-based, transparent, clearly limited in scope and duration, and more democratically discussed. This will help remove abusive systems and make the most of those which promote public health.

— **Protect our rights!** The pandemic must not be treated as an excuse to normalize vague and undefined exceptions to principles of EU law and international human rights law in relation to the use of ADM systems, such as necessity, proportionality,

data minimization, privacy, respect of human rights, fairness, and equity.

— **Technology (alone) is not a solution.** The pandemic is a complex issue, with enormous economic, societal, normative, technological, and public health consequences. Therefore, it should not be treated as an eminently — or worse, exclusively — technological issue, to be "solved" by a technological tool. Not all technological innovations can be put to good use in society. Some of them should be banned altogether, including during a public health emergency — for example, biometric recognition in publicly accessible space that amounts to mass surveillance.

— **Make sure mass health surveillance does not become the new normal!** While many outcomes of COVID-related ADM tools are controversial, one is not: the pandemic has further accelerated the ongoing process of normalizing pervasive, in some cases mass surveillance — even in democratic countries and the EU, where digital ID schemes, biometrics (at the borders), and tracking schemes risk composing a complex "surveillance infrastructure" that many see as problematic. There must be a clearly defined post-pandemic return to a normal in which mass surveillance is and remains banned from societies.

— **As EU decision makers, provide more leadership in the next pandemic, and learn from the current one!** The EU contributed fewer cases of dangerous COVID-related ADM systems to our database, compared to Asia and Africa, for example. However, the EU failed to properly govern important developments throughout the pandemic. EU guidelines and principles were needed and were welcomed when — as in the case of digital contact tracing apps and digital COVID certificates — they arrived. However, contact tracing apps were arguably standardized by Google and Apple more than by the EU. The EU's interoperability efforts on a global standard for individuals to prove their COVID status digitally before traveling internationally were also needed and important, but domestic COVID certificates have been left to the whims of Member States. Precise rules and limits to AI-based applications are still absent.

— **Avoid an AI arms race!** This is especially true of the US and China. As Bloomberg notes, "by miscalculating the others' abilities, both superpowers risk overestimating their adversary's strengths and overcompensating in a way that could lead to a Cold War-style AI arms race." Steering toward an evidence-based approach to ADM systems in public health and beyond can assist in avoiding yet another global conflict based on mistrust, manipulation and ideology.

— **Gather more evidence! (Too) much is still not understood** on how ADM systems impacted the pandemic. Further research is not only needed, but vital to better inform future public health responses. In this field, the work of academia and civil society is key, and should be supported well after the end of the COVID pandemic.

SCENARIO. THE GLOBAL QUEST FOR AUTOMATED SOLUTIONS TO THE PANDEMIC

BY FABIO CHIUSI

/ THE SOLUTIONIST PROMISE: AUTOMATION WILL SOLVE THE PANDEMIC

For 2021, the Tracing The Tracers project documented the testing and deployment of a plethora of ADM systems, both in Europe and outside, to assist public health responses to the COVID-19 pandemic in several important ways.

Or at least, they promised to do so. As our yearlong monitoring endeavor clearly showed, most of them revealed a concerning lack of transparency, oversight mechanisms, and appropriate safeguards, were based on contradictory or faulty evidence — when provided at all — and were not the result of an informed and participatory democratic debate.

Nonetheless, in an unprecedented social experiment in health surveillance, manual contact tracing schemes were augmented all over the globe by digital apps using Bluetooth and/or GPS technology, digitized COVID status certification, and made into a prerequisite to both safely reopen international travel routes and grant access to public venues and events in several countries — many of them in Europe.

Thermoscanners and surveillance cameras, at times equipped with biometric recognition capabilities and with the help of drones and robots, helped enforce social distancing rules and quarantines. Algorithms were adopted to inform the authorities who to vaccinate first, and how to avoid wasting any leftover doses.

AI also played its part, which — as expected — had to be that of the protagonist. AI would — among other promises — help us understand the virus and predict its evolution, provide reliable early diagnosis of infection, make COVID-19 tests "smart" and more efficient, and predict the risk of severe outcomes. Not even the pandemic could subtract AI from the hype and solutionist assumptions in which it was shrouded before COVID-19, as we will document thoroughly in this report.

This global drive to fulfill the promise of ADM systems, which too often translated into an impossible quest for automated solutions to the pandemic, was not only concerned with public health and freedom of movement. It also profoundly changed how fundamental human activities, such as learning and working, took place.

It is clearly and unequivocally recognized that the pandemic further accelerated the subtle, ongoing normalization of pervasive digital surveillance in both the education system and the workplace. This has led many to fear that rights-invasive responses born out of the pandemic will continue after it and possibly remain in place indefinitely. After all, the attraction of systems that automatically prevent students from cheating or employees from slacking off will not stop after the pandemic.

Dangers concerning biometric surveillance have previously been highlighted, and yet its promise — however factually incorrect — not only survived the pandemic, but benefited from it. Even though issues with the automation of welfare and related benefits were known and documented well before the first COVID-19 outbreak, ADM systems have been instrumental in distributing unemployment benefits, providing

anti-fraud solutions, and in the distribution of other welfare services during the pandemic.

Even though, as thoroughly documented in the Automating Society 2020 report, the costs and perils of an "automated society" are much more evident than the benefits, the pandemic seems only to have further entrenched the solutionist assumption — according to which, every complex social problem, including COVID-19, requires a quick, user-friendly technological fix. Consequently, innovation in COVID ADM systems was frequently hailed as crucial and something to be welcomed by both governments and mainstream media.

No matter how many times the promise is broken: solutionists will always renew it.

/ SOLUTIONISM IS WRONG, BUT INFLUENTIAL

Does this mean that ADM systems should not have been adopted, or even experimented with? And does rejecting solutionism in the response to COVID-19 amount to condemning the role of technology and innovation in the context of the pandemic altogether?

Not at all. First, lives have been saved thanks to ADM systems, however imperfect the systems might have been. And second, rejecting a solutionist attitude toward such systems does not amount to a rejection of technology; rather, it is precisely the precondition to make good democratic use of it in the interest of public health. As the extraordinary scientific breakthroughs obtained with the COVID-19 vaccines show, technology can indeed provide solutions to some problems (e.g., that of significantly reducing the risk of severe outcomes).

The point here is that not even vaccines would have been enough to contain COVID-19, without a well-funded, accessible public health system, and a well-developed public health plan to make the right use of its resources and skills during an emergency. As writer and essayist Cory Doctorow put it, "The problem with solutionism isn't that technology is irrelevant to problem solving – it's that technology developed in a vacuum by people who will never have to use it will only ever make problems worse."

Unfortunately, this is what we witnessed repeatedly during the pandemic, with an endless number of startups and tech companies boasting to have found the algorithmic solution to fix the pandemic bug affecting the world — and several governments and local administrations were more than happy to blindly follow the narrative.

This is all the more evident in the debate and controversy surrounding the contribution of AI in the fight against the pandemic, and especially in how it was constantly framed as the ultimate game-changer. In this respect, mainstream media provided several examples. For example, "Artificial Intelligence and COVID-19. Can the machines save us?," asked the Washington Post. Not according to Wired magazine: "Artificial Intelligence won't save us from coronavirus", it argued, while the MIT Technology Review promised to further explain "Why tech didn't save us from COVID-19".

Some academic literature also adopted a similar framing. In 'The prospective of Artificial Intelligence in COVID-19 Pandemic', published by Health and Technology in September 2021, author Chandana Mohanty and colleagues argue that "it is believed that AI has a solution to every problem". Even The Lancet, in a paper published in January 2021, asked whether we should consider AI "saviour or saboteur" in respect to COVID-19 — evidently assuming that the choice must necessarily be between one and the other.

At times, European institutions seemed to closely resemble the same ideological posture toward the

pandemic. For example, "Artificial intelligence is now establishing itself as a key player in the fight against coronavirus, thanks to EU funding," boasted the EU Commission, arguing that, "Europe should aspire to lead in AI solutions for health systems."

It is not by chance then that both the OECD and WHO explicitly warned against the perils of solutionism in pandemic responses. "Recognise that AI is not a silver bullet," warned the former in its recommendations drafted as early as April 2020. "There are risks of overstatement of what AI can accomplish, unrealistic estimates of what could be achieved as AI evolves and uptake of unproven products and services that have not been subjected to rigorous evaluation for safety and efficacy," echoed the latter in June 2021. "This is due partly to the enduring appeal of "technological solutionism", in which technologies such as AI are used as a "magic bullet" to remove deeper social, structural, economic and institutional barriers," the WHO added.

Solutionist policies can result in an "overestimation of the benefits and dismissal of the challenges and problems that new technologies such as AI may introduce," warned the WHO, producing "unbalanced health-care policies and misguided investments," while at the same time diverting "attention and resources from proven but underfunded interventions that would reduce morbidity and mortality."
While solutionism only thrives in abstractions, the consequences are all too real.

/ ADM DID NOT SOLVE THE PANDEMIC. BUT DID IT HELP?

After two years of continuous monitoring of ADM-related responses to COVID-19, AlgorithmWatch can safely claim that the pandemic has once again proven solutionism wrong. Or, in simpler (unsurprising) terms: no automated technology or process "solved" the pandemic.

Once this ideological posture is finally off the table, a rich complexity of ideas, technologies, and justifications can be scrutinized. And while we cannot claim to have gained an exhaustive view of automated systems deployed in response to the pandemic — we are not even close —, we may have gathered enough examples to corroborate a more pragmatic hypothesis: that certain ADM systems did help address some of the most pressing issues posed by the pandemic, and did save lives.

This is not to say that we could gain open access to all such systems, and transparently check their workings or corroborate their results. On the contrary, most features — even those of the most promising applications of ADM used against COVID-19 — remain shrouded in mystery. However, it does mean that there is some degree of scientific evidence to justify such hopes in specific circumstances and contexts. For example, the positive contribution of DCT apps in containing infections during phases 1 and 2 of the pandemic in England and Wales.

Other applications just seem less controversial, intended to solve actual contingencies — rather than *everything* — and deployed in real-life contexts with no noticeable or known issues. For example, algorithms used to distribute and/or assign leftover doses of COVID-19 vaccine in countries such as Germany, France, Estonia, and the US may have avoided wasting vaccines by providing better, more efficient systems to match bookings and availabilities in real-time.

Algorithms to predict severe COVID-19 outcomes were also deployed in several countries — from India's "COVID Severity Score" to Italy's "SuperLearner" approach, and many others. Results are impossible to assess at present due to a lack of data. However, it is safe to say that, among these, the UK's "QCOVID" algorithm is possibly the one that received the most attention — including some controversy within the scientific community as to its reliability. Nonetheless,

the algorithm had a massive impact on the country's vaccination campaign: 1,7 million individuals considered to be at high-risk of developing severe COVID-19 outcomes by QCOVID — but who were not previously identified as such by the health authorities — were asked to shield. Some 820,000 of them were eventually prioritized for vaccination as a result.

Promising applications also incorporated AI to detect COVID-19 outbreaks early on and to better understand the dynamics of the virus and even predict its evolution . In Canada, for instance, several municipalities might be about to adopt an algorithm developed by professors at the Universities of Toronto, York, and the MIT to "help identify COVID-19 outbreaks in neighborhoods using wastewater data," CTV News reported.

The New York Times also wrote about an algorithm, detailed in a paper that has yet to be peer-reviewed. This algorithm is, allegedly, able to register "danger 14 days or more before case counts begin to increase", and that, according to authors from Harvard, could consequently work "as a thermostat, in a cooling or heating system, to guide intermittent activation or relaxation of public health interventions."

Wired UK described the predictive models based on machine learning deployed in the Spanish municipality of Valencia as a (rare) success story. According to Wired, the models would allow the authorities "to forecast the prevalence of Covid-19 in a given area at a given moment, (...) analyze wastewater from baths, basins, washing machines, and showers, and hunt down anomalies that might reflect changes in local infection rates."

AI is also being trialed as an additional, intelligent support to human doctors. In Singapore, it helped doctors prioritize attention to urgent COVID-19 cases recovering at home. In the UK, it was developed "to support doctors to decide what action to take on the front-line, such as giving oxygen and medications, before patients reach a critical stage." And in the US, Epic's (proprietary) "deterioration index" was "designed to help physicians decide when to move a patient into or out of intensive care," wrote online publication Undark. A paper by researcher Karandeep Singh and colleagues found that the index was "implemented in over 100 U.S. hospitals," even in the absence of an independent evaluation.

"Smart" testing software "Eva" was touted as life-saving when deployed at the Greek borders to help border agents "predict which travelers have the highest likelihood of testing positive," and subsequently only test them — thus making more efficient use of the scarce resources available to the health authorities.

All of this might not be enough to justify a solutionist posture, but it could well be enough to justify experimenting with AI and automated systems, and possibly imagine interesting future uses once they are more strictly regulated by law in the EU and elsewhere. Professor Thomas J. Fuchs, Dean of Artificial Intelligence and Human Health at the Icahn School of Medicine at Mount Sinai, may have a point when he argued that "while we must continue to vigorously oppose dystopian misuse of artificial intelligence for surveillance and propaganda, it is clear that within the health care arena, patients are dying not because of AI but because we are not using it."

Indeed, when surveying the uses of AI to help in the search for a COVID-19 cure, the Council of Europe argued that "the predictions of the virus structure generated by AI have already saved scientists months of experimentation."

However, what is still problematic is that, given the vagueness and the opacity surrounding most AI products deployed both in and outside the scope of the pandemic, it is hard to strike an informed balance and provide evidence-based assessments of what works and what does not — and precisely why.

As a result, foundational questions about the use of AI in public health crises remain unanswered.

Is the catalog of promising uses detailed here enough to justify booming investments — so much so that, according to Euobserver, the EU Commission decided to stick to its objective of attracting 20 billion euros for AI annually for the next decade even in the face of the pandemic?

Is this enough to justify the fact that "AI platforms have taken on an unprecedented role in healthcare," as Wired put it in a December 2020 article?

And has AI actually "proved to be an indispensable tool in the fight against the coronavirus pandemic"? as claimed by the European Centre for the Development of Vocational Training.

To provide a coherent answer, let us look at the evidence we were able to gather and consider what it could mean.

/ THE CONTROVERSY OVER THE ROLE OF AI IN THE PANDEMIC

AI is not the solution to every problem and it did not solve the pandemic. Nonetheless, should we consider it a key player in the fight against COVID-19?

Well, many have tried to put this claim to the test, and they have concluded that no, we should not. For example, in Nature Machine Intelligence, Cambridge researcher Michael Roberts and colleagues, published a systematic review of the uses of machine learning "to detect and prognosticate for COVID-19 using chest radiographs and CT scans" — one of its most advertised applications — and the conclusions were dismal. Roberts summarized the findings in a New Scientist op-ed ('Artificial Intelligence has been of little use for diagnosing COVID-19') that included this remarkable passage:

"There are hundreds of papers claiming that machine-learning techniques can use chest scans to quickly diagnose covid-19 and to accurately predict how patients will fare. My colleagues and I looked at every such paper that was published between 1 January 2020 and 3 October 2020 and found that none of them produced tools that would be good enough to use in a clinical setting. Something has gone seriously wrong when more than 300 papers are published that have no practical benefit. Our review found that there were often issues at every stage of the development of the tools mentioned in the literature. The papers themselves often did not include enough detail to reproduce their results. Another issue was that many of the papers introduced significant biases with the data collection method, the development of the machine-learning system or the analysis of the results."

No real-world application. No practical benefit. Issues at every stage. Non-reproducible results. And biased datasets.

This sounds like a recipe for disaster, especially considering that these drawbacks are not limited to such uses of AI against COVID-19, according to other literature reviews. For example, in 'A State-of-the-Art Survey on Artificial Intelligence to Fight COVID-19', authors from both the Taipei Medical University and the University of Sydney found that, while "the application of AI in pandemic control has shown great potential in various ways, including predicting epidemic trend, patient tracking, stratifying asymptomatic patients, and finding potential repurpose drugs," such efforts were plagued by fundamental issues.

"All of the studies," wrote the authors, "had a lack of sample size, and external validation and inappropriate model evaluation; therefore, using these findings would be an optimistic decision." And a bad one, really: "The finding of our study does not suggest using these prediction models for diagnosis, disease progression, and mortality risk," they concluded.

A general feeling of overpromising was shared throughout the pandemic, both in academia and in mainstream media coverage. This is consistent with a trend that preceded COVID-19, argued a Washington Post investigation summarizing AI-related experiments in healthcare: "those efforts wildly overpromised, and the second machine age, as scholars called it, failed to materialize". Throughout the history of AI, overpromising seems to be foundational.

This comes with additional — and actual — risks, during a public health emergency: "Overpromising on the benefits of technology or relaxing ethical requirements, as has sometimes happened during this crisis, both risk undermining long term trust in the reputation of the entire sector," wrote authors Stephen Cave and colleagues in 'Using AI ethically to tackle COVID-19'. Dr. Kevin Vigilante, Chief Medical Officer at consulting firm Booz Allen Hamilton, told Healthcare IT News that we might even be "at risk of another AI winter in healthcare due to several AI solutions falling short of their initial hype."

According to a growing body of literature, discrimination and inequalities could be the by-product of such rushed, uncritical deployments of AI systems against COVID-19. "Issues of inequality and exclusion related to data science and AI arose during the pandemic," wrote the Alan Turing Institute; 'Covid-19 driven advances in automation and artificial intelligence risk exacerbating economic inequality', argued a research paper published in the British Medical Journal, while another paper, 'Does "AI" stand for augmenting inequality in the era of covid-19 healthcare?' shared similar concerns:

"The widespread sense of urgency to innovate (...) should be tempered by the need to consider existing health inequalities, disproportionate pandemic vulnerability, sociotechnical determinants of algorithmic discrimination, and the serious consequences of clinical and epidemiological AI applications. Without this consideration, patterns of systemic health inequity and bias will enter AI systems dedicated to tackling the pandemic, amplifying inequality, and subjecting disadvantaged communities to increasingly disproportionate harm."

For all its uses, reminded the Council of Europe in a balanced assessment of the use of AI during the pandemic, we should not forget "the limits of what can currently be achieved by this very technology, which we cannot expect to compensate for structural difficulties such as those experienced by many health care institutions around the world."

Once again, technology — per se — is not enough.

/ HOW COVID-19 NORMALIZED DIGITAL SURVEILLANCE

And yet, in typical solutionist fashion, it is in technology, and automation, that many looked to for answers to the complex, multifaceted issues raised by the pandemic. While this produced a flurry of research, ideas, and tools, some of them useful or even life-saving, it also — and most importantly — fundamentally normalized the uncritical adoption of digital surveillance systems in contexts where they were previously controversial — and rightly so.

One such example concerns the mass and sudden adoption of exam monitoring software in the education system, which sparked protests from remotely surveilled students all over the globe, from Switzerland to India, from the United States, and Canada to Australia.

Protests targeted several companies and tools in the booming industry for "online proctoring". The Swiss "University Conference of Students Associations" rebelled against software, produced by French start-up TestWe, that was used to take "a snapshot every three seconds during the exam to see if the student has left the room, is distracted, or is engaged in

searching for information on the Internet or on the hard drive."

In the US, a campaign against Proctorio, a tool that adopts machine learning, "to record students through their webcams while they work on their exams and monitor the position of their heads," led the University of Illinois Urbana-Champaign to discontinue its use after the 2021 summer term.

However, pushback from students — a "global revolt", according to Reuters — was generally insufficient to reverse the broader trend toward indiscriminate adoption, which was soon identified by many as a clear concession to mass surveillance. Fears of an unprecedented and unjustifiable level of intrusion into the lives and homes of millions of students worldwide led to publications, like Inside Higher Education, referring to a '1984'-style dystopia from as early as May 2020.

And such fears spread everywhere. During the same month, Recode argued that "Paranoia about cheating is making online education terrible for everyone", while an Educause poll found that — even though "54 percent of institutions were using online or remote proctoring services, while another 23 percent were considering or planning to use them" — "over half of the institutions polled said they were concerned about cost, as well as student privacy."

The rise of the "surveillance State of education" and the "surveilled student" was described in Wharton Magazine and The Chronicle of Higher Education, respectively. The former denounced the tools: "these facial recognition technologies disproportionately flag students of color, students with disabilities, and those who wear religious garb," and the latter raised the (rational) worry that such "new ways of monitoring health and academic performance won't just disappear when the pandemic subsides."

Similar worries were echoed in workplace settings, where surveillance and monitoring devices have a much longer tradition — reaching as far back as the Taylorist roots of the "scientific management" of labor and "the idea that people need to be constantly observed if they are to work efficiently," as Rachel Connolly put it in the Guardian.

The pandemic acted as a catalyst in this respect by providing new potential use cases. For example, at Amazon, where social distancing among workers was enforced with the company's "AWS (Amazon Web Services) Panorama" computer vision technology. Or, as many companies did to monitor workers while "smart working" from home.

Employers did not hesitate to make the most of the new monitoring opportunities. In September 2021, the Washington Post wrote that "the number of large employers using tools to track their workers doubled since the beginning of the pandemic to 60 percent", before adding that, according to a Gartner expert, "that number is expected to rise to 70 percent within the next three years."

Companies working in this field have seen global demand skyrocket. In June 2020, CNBC reported that one such company "has seen a 600% increase in interest from prospective customers since the pandemic hit," while another, "has seen a 500% spike in users month to month."

As Eurofund wrote at the end of 2020, the pandemic has fast-tracked us to "a new era of employee surveillance", in which an updated version of Taylorism, augmented by AI, is increasingly treated as the new normal. "What has happened already to us as web users may increasingly apply in the workplace," the Foundation warned. "Intrusive employee monitoring may become normalised and the enmeshing of private and work life accepted as an inevitability".

Unsurprisingly, surveys of workers have revealed that they are not happy about it. For instance, a TUC survey found that "only 28 per cent of workers were comfortable with the use of technology to make decisions about people at work". According to a report published in August 2020 by consumer rights advocacy group Public Citizen, technologies "marketed as workplace surveillance tools to combat COVID-19" multiplied, amounting to at least 50. Some of these technologies go as far as "identifying people who may not spend enough time in front of a sink to note inadequate hand-washing," France 24 reported. This led the group to the conclusion that "the invasion of privacy that workers face is alarming, especially considering that the effectiveness of these technologies in mitigating the spread of Covid-19 has not yet been established."

/ THERE IS NO STOPPING BIOMETRICS, NOT EVEN DURING A PANDEMIC

In our Automating Society 2020 report, we recognized that the sudden, seemingly unstoppable rise of biometric surveillance was one of the defining features of the rapidly emerging 'automated society'. Once again, the pandemic only confirmed and magnified this pre-existing trend.

Biometric surveillance technologies built into online proctoring software and workplace monitoring tools are only part of the story. For example, the pandemic was instrumental in advancing biometric controls as a precondition for safe international travel. As TechRepublic put it, "to mitigate the spread of contagion and assess passenger flows, airports have... incorporated a vast suite of technologies including thermal imaging, artificial intelligence, and more."

Certain countries even required biometric checks as a mandatory precondition to obtaining a "vaccine passport". In the United Arab Emirates (UAE), biometric surveillance is mandatory in order to obtain a 'UAE Pass' — which grants access to almost all forms of social life — and provides a "key" marker in the establishment of an AI-infused "digital lifestyle" in the country, the authorities claimed. In the UK, the NHS app — which is used to access medical records, book appointments, and prove one's COVID status — was reportedly "collecting and storing facial verification data from citizens in England in a process which", according to the Guardian, "has fuelled concerns about transparency and accountability."

In India, face recognition was adopted to verify vaccine beneficiaries, even though the Ministry of Health and Family Welfare "failed to provide any legislative or legal order that authorised the use of such technology," wrote the Hindu, and "no privacy impact assessment of the use of facial recognition technologies was conducted prior to its deployment." A similar scheme was also trialed in Ghana, one of many African countries in which the push toward national biometric identification schemes is increasingly apparent — and worrying, given that "gaps in Africa's legal and regulatory ecosystem leave citizens, including vulnerable LGBTQ communities, exposed to privacy abuses," wrote Al Jazeera, citing activists and experts.

At times, confinement was also tackled with biometric surveillance. Recently, several states in Australia decided to implement face recognition in their quarantine apps. For example, South Australia's "Home Quarantine SA" app "will undertake random location check-ins using live facial verification three times a day, while South Australia State Police will conduct at least one random physical check-in on each participant between 8:00pm and 8:00am nightly during the trial period," wrote ABC News at launch. A similar scheme was also adopted — unsuccessfully — in Poland, earlier in the pandemic.

This leads us back to India and the city of Nagpur, where the authorities decided to bring the concept to the next level: by applying face recognition to the

3,800 CCTV cameras installed in the city. The authorities claim that they can recognize positive patients violating quarantine restrictions in real-time, wherever they are. "CCTVs will detect the patient automatically and create an alert", argued Civic chief Radhakrishnan B in the Times of India. "Zonal civic staff then visit the home of the violator immediately, levy a fine of Rs 5,000, and admit the person in an institutional quarantine."

However, Nagpur may have a strong competitor in the Chinese city of Yunnan, where face recognition was "linked to personal health codes" resulting from China's extensive health surveillance apparatus, deployed as a form of social control. According to an AFP report, "this is the first publicly reported instance of facial recognition being used to track a person's movements and health status as they enter and exit residential areas, supermarkets, transport hubs and other public places."

By now, concerns about biometric technologies that are abundantly clear in the literature and widely shared in mainstream media were somehow not enough to dissuade both public and private entities from advancing trials and upcoming projects, even in established democracies.

For example, Canada is in the process of developing new "biometric plans" in response to the pandemic, to try and "standardize the collection of biometric information on potentially inadmissible travellers". Canada is also investigating the potential for new uses of voice recognition and geolocation technologies.

In Denmark, several gyms adopted face recognition to allow customers to enter their premises — with the alleged additional capability of checking the person's mood — while at the same time checking that the customer's COVID status and gym subscription are valid.

/ SURVEILLANCE WE WEAR AND ALWAYS BRING WITH US

The pandemic magnified another pre-existing trend regarding the social impact of technology: the quantification of the self, and its every activity, through wearable devices.

And again, the use of wearable devices in workplace settings is only part of the story. According to Gartner estimates, published in January 2021, "worldwide end-user spending on wearable devices will total $81.5 billion in 2021, an 18.1% increase from $69 billion in 2020". Ear-worn devices and smartwatches have seen "particularly robust growth" not just for remote work, but also for self-health tracking and monitoring purposes.

However, could wearable devices help fight COVID-19? Research is ongoing and, at times, it is conducted by the very companies that deploy wearable tools. Therefore, as might be expected, some of the research presents wearable devices as "solutions" — for example, to the issue of "unequal access" to DCT apps. "Contracting wearables are a clear solution to this problem," argues a paper that is "supported in part by a grant from the Social Science Research Council (Ministry of Education, Singapore)", the one country which most notably used tokens to increase the reach of DCT apps.

At times, the discussion about wearable devices is overly enthusiastic, bordering on solutionism: "This study highlights the future of digital health," said Robert P. Hirten, co-author of a Mount Sinai study on wearables to detect COVID-19 symptoms. And the reductionist philosophical posture that is associated with the "quantified self" is also at times dangerously assumed in public health contexts — with experts in the field arguing that "just like a car dashboard monitors car health, a smartwatch will track a person's physiology." You may not be a gadget, as Jaron Lanier

famously claimed, but, apparently, you can be measured as one.

Even when the science is not clear, the tone is favorable. A Nature Medicine study, published in October 2020, ('Wearable sensor data and self-reported symptoms for COVID-19 detection') seemed to confirm the usefulness of wearable devices, "individual changes in physiological measures captured by most smartwatches and activity trackers are able to significantly improve the distinction between symptomatic individuals with and without a diagnosis of COVID-19 beyond symptoms alone."

However, at the same time, the authors themselves warned that "results are based on a relatively small sample of participants." Also, according to the Medical Device Network, "the majority of physicians and medical professionals are sceptical of wearable tech's functionality and usefulness." Concerns around privacy and accuracy remain, "combined with the general lack of an adequate medical record infrastructure". Finally, "physicians often do not know what exactly to do with the data presented to them by wearables and are often reluctant to make decisions based on data that has yet to be proven effective." Rightly so, given what we have learned about the effectiveness of contact tracing apps and "Green Pass" schemes'.

Nonetheless, according to TechReview, the use of wearable devices was "dramatically scaled up" in several hospitals across the US. TechReview adds that there is an assumption that health surveillance should be worn and carried with us at all times, wherever we go. This assumption is consistent with turning each smartphone into a contact tracing and COVID status certification device.

As we have thoroughly shown with our Tracing The Tracers analyses throughout 2021, these efforts remain controversial from an evidence-based perspective — in terms of efficacy and rights.

/ IF ADM SYSTEMS ARE SOLUTIONS, THEY ARE FAULTY ONES

We have seen several ways in which surveillance is being normalized by the pandemic. But even assuming we should be willing to accept it, is this enormous surveillance apparatus working as intended? Before we ask whether it produces effective results, can we say that it is operational?

Well, mostly yes — but not without serious issues in terms of recurrent bugs, outages, data leaks, persistent forgeries, and other privacy and security failures. Had motivated attackers exploited them, some of these issues could have been critical.

Think of the bug that potentially affected "exposure notification" apps — those built on the Google/Apple protocol — that was found by a Portuguese cybersecurity student. We reported on this bug in our Tracing The Tracers database. The bug could have allowed the malicious interruption of Bluetooth transmission and, therefore, exposure notifications, effectively rendering the apps moot. Or, take the vulnerability found in the controversial, centralized German check-in app, Luca, that could have allowed attackers to "paralyze" entire health departments. According to the Bangkok Post, Malaysia's contact tracing application even sent "unsolicited one-time passwords to random phone numbers" as a result of "malicious scripts"; this meant that "some users, including lawmaker Fahmi Fadzil, received emails saying they've tested positive for Covid."

At times, bugs and leaks concerned millions of individuals. In Indonesia, a suspected security flaw was discovered in the national DCT app, PeduliLindungi. In August 2021, Reuters reported that the flaw "left exposed personal information and the health status of 1.3 million people,", potentially allowing hackers, "to access the app directly and change data on passengers, including their COVID-19 test results".

Even President Joko Widodo's vaccine certificate was leaked due to this flaw.

Contact tracing logs were mistakenly exposed to pre-installed apps on Android devices. According to The Markup, Google failed to address the issue when alerted to it by privacy analysis firm AppCensus. Furthermore, it was common to witness temporary service interruptions to DCT apps. This happened in countries as technologically mature as Switzerland and Japan. The Japanese government admitted an overall "digital defeat" due to the inadequacy of the tech tools that have been deployed in response to COVID-19. In the UK, outages left travelers stranded in airports, or delayed, due to a malfunction with the NHS app.

Instances of fakery and forgery were quickly spurred in response to the widespread adoption of COVID-19 certificates. When New York adopted its "Excelsior" pass, Albert Fox Cahn, founder and executive director of the Surveillance Technology Oversight Project (S.T.O.P.), claimed in a Daily Beast article to have been able to forge the pass "in 11 minutes." Similarly, Richard Nelson, a software engineer, was able to do so in just 10 minutes for Australia's Express Plus Medicare app for vaccine certification.

Unsurprisingly, a "black market" for digital COVID-19 status certification also arose in several countries. In Canada, fraudulent websites impersonated the government promising "to deliver fake COVID-19 exposure notification applications, designed to install malware on users devices", wrote CBC. In Germany, news outlet Handelsblatt managed to pose as a made-up pharmacy — with a photoshopped operating license — and received credentials to issue vaccine certificates in a matter of hours. Even in Israel, home to the first "Green Pass" scheme, more than 100,000 users joined Telegram groups in which counterfeit vaccination certificates were sold — with Haaretz and other outlets repeatedly reporting how easy it was to fake a certificate, so easy that "anyone" could do it.

Flaws also produced ill-informed results that affected vaccine logistics and distribution algorithms. For example, the American Civil Liberties Union of Northern California found that the State's algorithmic vaccine distribution system "left out numerous small, hard hit neighborhoods located outside of priority zip codes," while Stanford's algorithm for vaccine prioritization famously failed to include most of the frontline workers who were actually at greater risk of exposure to the virus.

According to the Los Angeles Times, these were not isolated blunders — affecting, for example, California's "Blue Shield" program, "hammered (…) by complaints of glitches and compatibility issues." More broadly, a much greater degree of transparency is needed for such algorithms, a New York Times investigation found, while at the same time noting that "some prioritization formulas also conflict with one another or impose such prescriptive rules that they hinder immunizations."

/ WE MUST MAKE A BETTER, MORE DEMOCRATIC USE OF ADM SYSTEMS IN A PANDEMIC

AlgorithmWatch previously — and repeatedly — documented that the deployment of ADM systems mostly happens opaquely, with insufficient checks and balances, scarce oversight, and mostly in the absence of a properly democratic debate. Unfortunately, our yearlong Tracing The Tracers monitoring clearly shows that the pandemic confirmed such trends, and only made them worse.

What we defined as an untenable status quo in Automating Society 2020 is even more so when potentially life-saving applications are involved, as in the context of the pandemic.

Evidence, transparency, inclusion, participation, and clarity should be the hallmarks of sociotechnical

systems aimed at massively impacting the dynamics of a pandemic and the public health strategies put forward to address it. As the WHO put it in its 'Ethics and governance of artificial intelligence for health' report, "an emergency does not justify deployment of unproven technologies."

Even though to a different degree, and in different normative frameworks and cultural contexts, most ADM systems remain "black boxes" even when deployed to face a public health emergency. And this is extremely concerning, especially when married to a solutionist ideological posture that claims a priori justification for whatever technological deployment, no matter how opaque or arbitrary.

This leaves us with several difficult questions on how to make a more democratic, evidence-based use of automated systems for public health purposes, and especially on how to obtain the change we need, to best govern current and future pandemics.

First, a general trend toward mass opaque deployments is bad news for democracy. As authors, Antónia do Carmo Barriga and colleagues, put it in 'The COVID-19 pandemic: Yet another catalyst for governmental mass surveillance?', "all over the world, in many countries, the pandemic has been the engine (or pretext) for deteriorating the quality of democracies and undermining human rights compliance, including in those with a strong democratic tradition."

Paradoxically, COVID ADM surveillance raised the international standing of authoritarians. As the Lowy Institute wrote in 'Digital authoritarianism, China and COVID', the pandemic has not only "allowed China to expand the use of its digital authoritarian mechanisms at home": it also "provided an opportunity for the CCP (the Chinese Communist Party) to showcase the effectiveness of its tech-enabled authoritarian approach abroad, to counter negative perceptions of its inadequate handling of the initial outbreak." After all, "with democratic and authoritarian countries alike under unprecedented restrictions and surveillance, the stigma usually associated with such authoritarian measures has been reduced" — so much so that it wasn't unusual to read headlines and comments like Fortune's "China's response to COVID showed the world how to make the most of AI" in both European and US-based media.

And yet, important differences remain. For example, the choice of only supporting decentralized, "privacy-preserving" apps by the EU prevented most Chinese-style location tracking efforts from happening in Europe. In addition, Europe's normative framework provided some leeway for national privacy authorities to act — or react whenever governments went too far in the quest for health surveillance.

So, yes, as noted by political scientist Sheena Chestnut Greitens, "to date, the pandemic has largely augmented existing trends, meaning that autocracies have been likely to respond in ways that infringe upon citizen rights, and weak democracies have exhibited some risk of democratic erosion and pandemic-associated autocratization." Yet at the same time, "a large number of consolidated democracies have employed surveillance, but have managed to navigate the initial stages of crisis without significantly compromising democratic standards."

This was not the case in autocracies and illiberal democracies, where we documented several instances in which privacy and fundamental rights were treated as an afterthought, if given a thought at all.

However, it is clear that Europe needs to show better leadership, both in terms of practices and norms, if it wants to truly separate itself from contexts in which rights do exist, but mostly just on paper. Mass surveillance must not become the new normal in democratic contexts — not even in response to a public health emergency. Our monitoring efforts recorded no sound proof that it is somewhat necessary to give

up privacy and other fundamental rights to obtain greater safety and more efficient protection of individuals from COVID-19. While often assumed by solutionists, we could not find any evidence supporting this claim — and this is a striking result of our investigation.

Defeating the solutionist view of ADM systems in public health emergencies — and in societal responses more broadly — is a crucial task for those who wish to maintain geopolitical stability. AI has emerged as the pretext for blunt, irresponsible assessments on the necessity of ramping up investments in a vaguely defined set of "smart" technologies in order to obtain an allegedly indispensable "AI leadership," including in autonomous weapons.

This could create lasting damage - not only to technological critique and policymaking during a public health emergency, but also to diplomatic relationships. AI is increasingly framed as a major driver of conflict on a global scale — given that the two major players in this new Cold War-style drama, the US and China, happen to be the world's biggest military and economic superpowers.

In other words, an evidence-based approach around the uses of AI and automated systems in health would not only inform much-needed additional research on their effectiveness and compatibility with democratic values, but also help avoid yet another war based on lies and solutionism.

BELGIUM

BY BRAM VISSER AND
ROSAMUNDE VAN BRAKEL

/ CONTEXT

The pandemic proved to be an excellent opportunity to accelerate the increase of surveillance in many countries and Belgium is no different. In the 2019 'Automating Society' report, Rosamunde Van Brakel mapped the policy developments, political debates, and societal players with regards to the implementation and use of algorithms and ADM systems in the Belgian public sector.

This set out the digital policy agenda at both the federal and federated entity level announcing investments in AI, the development of a think tank, and other activities related to the promotion and uptake of AI in the public sector, such as a stakeholder forum and the introduction of AI-focused university courses. At that time, active use of ADM systems included an algorithmic work activation system used by the public employment service in Flanders, and the localized use of predictive policing software by police.

In this report, we intend to provide an update on the current situation; how ADM systems have evolved and been implemented as a reaction to contain and manage the spread of COVID-19. We also provide an overview of the different surveillance tools that were put in place and we dive deeper into the efficacy, public reception, and possible incentives for the implementation of such tools. We conclude with a critical note on the implementation of these tools and their implications.

/ CASES

From informative to intrusive drones

During the first lockdown (March/April 2020), Brussels police tested the use of drones to inform people in public places about the dangers of not respecting the social distancing rules and encouraging them to stay home as much as possible. By the end of the year, with the accompanying festivities in prospect, plans emerged that certain police zones in Flanders (more specifically in Limburg and Western Flanders) would use drones (some of them equipped with thermal imaging cameras) to monitor adherence to social distancing measures. At that time, there were severe restrictions on the number of people that could gather in one room. However, Brussels police announced that it would not be using drones to monitor violations of social distancing measures as this would provide *"no added value"* and their "*current tools are sufficient to serve that end".*

The announcement of the plans for the intrusive use of drones elicited a lot of response from academia, NGOs, politicians, and the Belgian Supervisory Body for Police Information (hereafter: the Supervisory Body). Johan Vande Lanotte, a lawyer, former politician, and professor in constitutional law, warned that the indiscriminate surveillance of everyone at will is the definition of a police-state and that the use of drones should only be permitted in case of a clear and targeted suspicion.

Stijn Derammelaere, professor in Mechatronics at the University of Antwerp, pointed to technical limitations, accuracy issues, and the related elevated number of false positives. Matthias Dobbelaere-Welvaert, a privacy expert, denounced the lack of proportionality of the measure and warned of the risk of becoming a surveillance society through function creep, reminding us that ANPR (automatic number plate recognition) cameras—that were initially installed to act upon severe criminal offenses—were now being

used to monitor 'essential displacements' (one of the social distancing measures, whereby a person could only leave their house for essential reasons, e.g., for grocery shopping or to see a doctor).

In the federal parliament, both right-wing opposition parties Vlaams Belang and Nieuw-Vlaamse Alliantie (N-VA) and liberal coalition partner Open Vlaamse Liberalen en Democraten criticized the plans as undemocratic and treating citizens as suspects by default. Frank Schuermans, director of the Supervisory Body, was mainly concerned with whether these cameras could capture images in private places and whether these could then be used for police reports. The Supervisory Body's investigation in Limburg concluded that discrepancies between the permission request and reality prevented the body of elected representatives in the municipality from making an informed decision.

Furthermore, the Data Protection Impact Assessment (DPIA) was not validated by the chief of police, was incomplete, and contained a lot of errors. The Supervisory Body ordered the police zone to renew the requests for drone use to the municipal council accompanied by the newly, properly conducted DPIA's.

Cameras

Matthias Dobbelaere-Welvaert's warning about the risk of turning into a surveillance society took a stark turn in March 2021. The Supervisory Body saw no legal issues whatsoever regarding an expansion in the use of security cameras used by the police in Antwerp — that began after the 2014 terrorist attacks to fight serious crime and terrorism — to monitor compliance with social distancing measures. Academics saw this as a textbook example of function creep, while the Supervisory Body pointed to the wide use of cameras to assist the police in all their duties. In an opinion piece on the matter, Juraj Sajfert, a legal scholar, identified an erroneous transposition of the Law Enforcement Directive into domestic law as basic data protection principles of necessity, proportionality, and purpose limitation were not present, allowing for a legal basis that facilitated function creep.

Coronalert

To optimize the process of contact tracing, a privacy-friendly app that relied on Bluetooth technology to trace and notify whether someone had a high-risk of exposure to COVID-19 was launched country-wide on September 30, 2020. The application keeps track of codes corresponding to a device that has been in a 1.5-meter range for 15 minutes or longer. The application can identify a high-risk contact only if people using the application indicate - by way of a 'test code' – that they tested positive and have consented to link to the relevant information in a database. The database thus only contains a list of codes possibly linked to a positive or negative test result.

The application communicates with the database on a daily basis to check for high-risk exposure and notifies the users accordingly by way of a red screen. No names, phone numbers, or location details are communicated. Public adoption and the goodwill of links in the chain (patients, doctors) were important factors in determining the efficacy of the application in achieving the desired outcome. Evaluations of the application showed that 25% of the Belgian population downloaded the application (which does not mean that they also used it) and that only 3% of those infected used the application to notify their high-risk contacts.

To what extent the application has been effective in preventing infections is hard to measure due to the lack of relevant data collected. The privacy guarantees the application provided – that it does not track location data – seemed to be the biggest hindrance to the effectiveness of the application.

Dr. Wouter Arrazola de Oñate, epidemiologist and a tuberculosis contact tracing specialist, thinks that local, manual contract-tracing would have worked better than an application. He lamented the absence of basic contact tracing principles such as the presence of a case manager, who would be in an ideal position to identify links and follow-up cases thoroughly. Furthermore, the artificial nature and industrial scale of contact tracing call centers hindered the efficacy of the operation as the intimate link with the patient is lost.

For example, local communities might not be familiar with the doctor in charge of following up. Most importantly, confidential conversations with patients allow doctors to ask relevant questions that can help limit the spread of a virus, *"as epidemiologists have been doing for over 40 years,"* added Arrazola de Oñate, as opposed to an application that automatically collects this information.

Related to this, in an extensive working paper, entitled 'Necessity knows no law in contaminated times: the rule of law under pandemic police and pandemic legislation', Paul De Hert, a privacy expert, denounced the lack of adherence to important legal provisions that grant patients the right to be informed by a professional opinion to facilitate a judicious decision. The concrete example of vaccination centers is described whereby this option is skipped altogether. De Hert asserts that the process of de-professionalizing professions in which trust plays an important role undermines both that trust as well as important societal checks and balances.

CovidSafeBE

CovidSafeBE is the application that grants citizens the Covid Safe Ticket (CST) - the Belgian equivalent of the EU Digital Covid Certificate, the Green Pass. It contains a unique QR code that provides medical information in the form of a vaccination certificate, a test certificate, or a recovery certificate. It was originally intended as a measure for safe travel inside the EU. However, policymakers quickly realized its potential and formed a cooperation agreement between the federated entities and gradually broadened the use of the app to include an ever-increasing range of social activities.

This is a controversial issue that has attracted headwind, though still in vain as the Flemish and Walloon governments — following in the footsteps of Brussels — recently broadened the use of the CST. This app was originally intended for use at mass events of 3,000 people or more. However, since November 1, 2021, the app has been used to gain entrance to bars, hotels, restaurants, fitness centers, and events with over 200 indoor participants, or 400 for outdoor events.

The Belgian Data Protection Authority (BPDA) expressed its concerns and has warned of converging toward a *"controlling society"*, the occurrence of a normalization effect, e.g., that in the future, entrance to some places might be conditional upon proof of health status. The BPDA also criticized the lack of essential mechanisms for democratic transparency accompanying the legal text, such as evaluations of the necessity and proportionality of the measure.

Paul De Hert also described the ever-broadening scope of the CST as problematic because the much-needed proportionality test – especially when dealing with health data – is not considered with discriminatory practices on the basis of health as a consequence. Refusal to implement the measure from an ideological point of view has come mainly from a part of the cultural sector that *"refuses to divide society and stigmatize certain groups within the population",* stressing their societal role of bringing people together. In practice, bars in Brussels are not able to keep up with the increased workload the introduction of the CST implies and hope that police will be willing to help them, rather than fine them for non-compliance.

Some bars that can carry the financial burden have appointed a security guard to mitigate the increased chaos.

It is uncontested that the ever-increasing scope of the CST is a strategy to nudge people into vaccination. This is highly problematic as it is at odds with the freedom of choice principle that accompanies the country-wide vaccination policy, as decided in mid-November 2020 by the Interministerial Conference on Public Health. In a report about conditioning access to goods and services upon proof of vaccination, the Interfederal Centre for Equal Opportunities and Opposition to Racism (Unia) concluded that individual freedom must be respected and that measures constraining that freedom can only be implemented by law with respect for anti-discrimination principles.

While Paul De Hert acknowledges the legal possibility of mandatory vaccination (granted there is a demonstrated necessity), he contends that it is unlikely that western countries will do so as they prefer indirect nudging practices, subject to little scrutiny. Additionally, the Human Rights League pointed to the subversion of the freedom of choice principle, the risks to equality, direct and indirect discrimination, and issues of privacy and data protection.

CovidScan application

The CovidScan application makes it possible to read the CST digitally and check its validity. Where the Coronalert application paid the needed attention to privacy and data protection safeguards, it seems those considerations were lost in the creation of the CovidScan app. The application is available in Google Play and the App Store and has two scanning modes. One is to be used by the event sector, bars, and all other areas where the CST is used (apart from traveling), and the other is for use by police and border control (for travel purposes). The latter mode contains more information than is needed for the former, and there are no special authorizations required to switch between the two modes as time constraints for app development led to convenient decisions being made with privacy harms. Digitaal Vlaanderen, responsible for the development of the application, advises people to check whether the person who scans your CST is doing so in the correct mode.

/ ANALYSIS

As mentioned, at the beginning, and substantiated throughout this contribution, the COVID-19 pandemic has created an opportunity for an extensive broadening of the surveillance apparatus of the state beyond what was deemed acceptable before the pandemic. Ranging from the introduction of drones to pre-empt offenses, the use of cameras beyond their initial purpose, to the introduction of tracing applications, and the ever-broadening scope of COVID passports.

Luckily, not all doom scenarios unfolded, and, in most cases, common sense won the battle over police-state tendencies. Contrary to the stated plans, the police did not use drones to indiscriminately monitor the population, indicating that the public backlash had an effect. The voluntary and privacy-friendly nature of the contact tracing application hindered its effectiveness and taught us a valuable lesson in techno-solutionism. However, we wish to highlight a common thread that needs to be heeded and invite policymakers, lawmakers, and government authorities to think of creative solutions instead of lunging for the most readily available option.

When police officers first started using cameras — intended to monitor serious crime and terrorist threats — to monitor compliance with COVID-19 measures, no effort was made to think about less intrusive solutions that respect data protection principles of necessity and proportionality, opening the door for indiscriminate surveillance of whoever they see fit. As the DPA warned, the legal texts regulating

the use of the Covid Safe Ticket should clearly evaluate these principles to prevent exactly what has happened, namely that CST-use would be normalized, and society is consequently controlled, free from democratic checks and balances.

As recent academic research into the speculative issue of the normalization effects of surveillance, by Selinger and Rhee, has shown, *"seeing something as normal does mean becoming more favourably disposed to it".* An ever-increasing, widespread surveillance infrastructure (e.g., the city of Leuven recently decided to use smart cameras to monitor sporting behavior in a public park), little adherence to legal safeguards allowing for its expansion, coupled with a population favorably disposed to these evolutions is a recipe for an accident waiting to happen. To end, these are the words of Alistair Duff, information policy professor, *"There can be no doubt that the infrastructure for complete totalitarianism is now in place, should power fall into the wrong hands".*

CYPRUS AND GREECE

BY ELEFTHERIOS CHELIOUDAKIS

CYPRUS

/ CONTEXT

The Republic of Cyprus was the last EU Member State to report a case of coronavirus at the beginning of the pandemic, back in 2020. The response of the Cypriot authorities to COVID-19 involved the adoption of a contact tracing app, called COVTRACER, in spring 2020. This tool was replaced by a second app called CovTracer-Exposure Notification (CovTracer-EN) in spring 2021. Both apps were used on a voluntary basis.

/ CASES

COVTRACER

COVTRACER was developed by the Cypriot Deputy Ministry of Research, Innovation and Digital Policy (DMRID) in collaboration with the government-funded Centre of Excellence (CYENS) in spring 2020. The app created a timestamped log based on the user's GPS location, which was stored on each user's device. If users tested positive for COVID-19, they could voluntarily share their log files with the respective health authorities. In this way, the authorities knew the different places each infected user had visited and then notify other COVTRACER users who had been in the same areas and recommend them to get tested.

CovTracer-EN

CovTracer-EN was launched in spring 2021 to replace the COVTRACER app. It was developed under the coordination of the National Electronic Health Authority, and the advisory role of DMRID (the Digital Ministry of Research Innovation and Digital Policy) together with the Ministry of Health. Development of the application was entrusted to the KIOS center of the University of Cyprus along with the CYENS center. The app uses Bluetooth and Google-Apple Exposure Notification (GAEN) to trace the proximity of its users. If a user of CovTracer-EN tests positive for COVID-19, then he/she has the option of reporting this to the app, and the app instantly informs other app users if they have been in close proximity with the infected user.

/ ANALYSIS: LIMITED UPTAKE LEADS TO A NEW APPROACH?

At the beginning of the pandemic, Cyprus decided to adopt the COVTRACER app which was based on GPS technology. According to a group of researchers who reported on COVTRACER, it is hard to assess whether its deployment was successful since limited related data is available. Nevertheless, based on their findings the app was downloaded approximately 8,000 times, which represents roughly 1% of smartphone users in Cyprus.

The new app, called CovTracer-EN followed a different approach using Bluetooth technology and the GAEN system. The Cyprus Commissioner for Personal Data Protection, Ms. Irene Loizidou Nikolaidou, made a public statement about the new app, informing the people of Cyprus that the technology used was in accordance with the related guidelines from the European Data Protection Board, and complied with GDPR principles, while her office was consulted by the Cypriot authorities on this matter.

Again, limited research is available regarding the adoption and effectiveness of the CovTracer-EN app. Although no definitive conclusion can be drawn, there is an indication that the CovTracer-EN app was not

widely adopted. According to the download data of the Google Play Store, until November 2021 the app had been downloaded to more than 10,000 Android devices. However, this data cannot be seen as representing the actual number of app downloads, since data for the Apple store and iOS devices that have been used to download the CovTracer-EN app are not publicly available to non-developers.

GREECE

/ CONTEXT

In Greece, different technological tools and initiatives were adopted in an attempt to control the pandemic at the national level and limit the spread of COVID-19. Contrary to many EU Member States, the Hellenic authorities did not launch a mobile contract tracing app, even though such a tool was under development. Nevertheless, other tech instruments, from simple SMS services to advanced data analytics tools and machine learning (ML) algorithms, were included in the country's arsenal to tackle the COVID-19 pandemic.

/ CASES

SMS to 13033

During the two lockdown periods in 2020 and 2021, people in Greece were only authorized to leave their homes for specific reasons and after notifying authorities by sending an SMS to 13033, a service run by the Hellenic Ministry of Citizen Protection. Even though people could choose to provide a handwritten or printed permit to leave their homes, the SMS service was commonly used - more than 885 million SMSs were sent during the two lockdown periods. Nevertheless, political parties and journalists raised concerns regarding data protection issues. In February 2021, the civil society organization Homo Digitalis filed a complaint to the Hellenic Data Protection Authority (DPA) against the Hellenic Ministry of Citizen Protection, representing five data subjects. The data subjects claimed that the privacy policy of the SMS service was not in compliance with the GDPR, since it only provided limited information on how their personal data was processed, while the Ministry failed to respond to their data access requests. The Hellenic DPA is investigating the case, and a hearing of both parties took place in summer 2021.

The Eva algorithm

As mentioned in the 'Automated Decision-Making Systems in the COVID-19 Pandemic' report, in July 2020 the Hellenic Government launched the "Passenger Locator Form (PLF)". This was a questionnaire that all incoming travelers had to complete before entering Greece, covering biographical information (name, age, gender, contact details), as well as information about the travelers' permanent country of residence and previously visited countries. The purpose of collecting this data was to screen incoming travelers so that the Greek authorities could assess whether they should be tested for COVID-19 upon arrival. This assessment was provided by a ML algorithm, nicknamed Eva. Eva was offered pro bono to the Hellenic Government by a group of scientists who wanted to assist the Greek authorities. According to the researchers who developed the algorithm, *"Eva represents a successful example of the potential of reinforcement learning and real-time data for safeguarding public health."* Nevertheless, the Hellenic Union of Computer Scientists expressed their concerns about the Eva algorithm, emphasizing that even though it was provided pro bono, its adoption was not a result of an open public procurement procedure. In addition, Eva was accepted for use in screening incoming travelers without prior evaluation and no guarantee that it would be effective at an operational level.

Partnerships on big data analytics

Since March 2020, Palantir has worked pro-bono with the Greek government to enable data-driven decision-making in response to the pandemic. This collaboration was announced by Palantir itself nine months after its initiation, while the Hellenic Government did not made any statement about it. Political parties, journalists, and civil society organizations criticized the lack of transparency regarding this partnership. Moreover, following requests from members of the Greek Parliament, the Hellenic Government published their agreement with the company, announcing that they had decided not to renew it. Even though the partnership was terminated in December 2020, during the same month the Hellenic DPA started a related investigation to assess the compliance of this partnership with the GDPR. The investigation is still ongoing, while a related hearing of the parties took place in July 2021.

In January 2021, the Hellenic Government announced that in December 2020 it had signed a €73,000 contract for a partnership with PwC Greece. The company offered consultancy services to the Hellenic Government on matters related to big data analytics within the context of the pandemic. According to the Hellenic Government, the goal of this contract is the development and deployment of a tool that will enable the Greek authorities in the field of public health and the protection of citizens to extract useful findings from data collected from the PLFs.

/ ANALYSIS: OPENNESS, TRANSPARENCY, AND PUBLIC TRUST IN CHALLENGING TIMES.

Undoubtedly, the pandemic is an unprecedented crisis that has touched every aspect of our lives. On a global scale, millions of people have been victims of this deadly virus, while countries have been confronted with the challenge of delivering a rapid response. However, when taking measures to address a major health emergency, it is crucial to continue delivering good democratic governance.

Openness and transparency about partnerships, measures, and tools to fight COVID-19 are necessary to ensure public trust and the broad acceptance of governmental decisions. The Greek case serves as a good example of how a lack of transparency and open procedures could lead to public mistrust, political criticism, and investigations from independent authorities.

To begin with, the Eva algorithm is considered a "success story" by its developers. According to the scientific data that was recently published, this ML algorithm could identify "1.25×–1.45× more infections" - in comparison to policies that screen incoming travelers and decide who to test based on the probabilistic risk assessment models that are proportional to cases per capita, deaths per capita, or positivity rates for the passenger's country of origin.

However, this data was not available when the government decided to adopt the Eva algorithm back in summer 2020. More precisely, according to the Hellenic Union of Computer Scientists, the research team behind Eva had not published the algorithm as part of a scientific paper back then. This made it *"impossible to evaluate its expected effectiveness",* while there was, *"no guarantee that at the operational level any effectiveness of the Eva algorithm has been confirmed by sufficient real epidemiological data from Greece".* Based on the above, one could argue that the government did not have enough data in its hands to evaluate and understand the effectiveness of this algorithm when it was first adopted. Thus, when the Greek authorities were first presented with Eva, it was crucial to open a consultation and to call the related stakeholders from the scientific community — such as the Hellenic Union of Computer Scientists — to present their views and openly debate the adoption of this tool. Such a consultation would have enhanced trust in the adoption

of the tool or led to necessary steps/procedures that would increase the acceptance of this governmental decision, such as, for example, a pilot period to test Eva prior to its official adoption.

Finally, it is useful to mention that there is an ongoing scientific debate about whether ML algorithms could have a predictive advantage over regression analysis procedures, which over recent decades have dominated the actuarial determination of risk. So, even though, ex-post, this ML algorithm appears to be superior to probabilistic risk assessment tools, this was not proven when it was adopted. Since governmental decisions regarding the pandemic should be based on scientific evidence, it is clear why the adoption of Eva attracted criticism from expert bodies in Greece.

ESTONIA

BY MARIS MÄNNISTE

/ CONTEXT

Estonia is well-known around the world for good digital governance. So much so, that it has also become a branding tool for the country (see, for example, e-estonia.ee webpage or Hammersley, 2017). As described in the Automating Society 2020 report, the future of digital governance in Estonia increasingly concerns the implementation of different AI solutions and automation in public and private sector institutions (see Eesti Digiühiskond 2030 strategy, 2021). The strategy for Estonian Digital Society 2030 stresses that — although 80 AI projects have already been implemented — to continue to develop AI there needs to be a clearer understanding of what AI is. In addition, current legislation poses obstacles for the use of data.

Although automation is seen as an opportunity for more efficient governance, Estonia also aims — through Data Tracker (mentioned in the Automating Society report 2020) and Consent service (currently under development (Eesti Digiühiskond 2030, 2021)) — to run human-centered digital governance. This is emphasized in the Estonian Digital Society 2030 strategy, *"every individual and entrepreneurs have power over their data and they can share their data. They have clear overview who has their data and with whom this data is shared."*

Estonia uses a nationwide electronic health record system (e-health record) which integrates data from different healthcare providers to create a record every patient can access online. Health data is kept completely secure and is only accessible to authorized individuals (e.g., family physicians, emergency services). Through this system, patients can access their health information and that of their children. Therefore, in an emergency, just by using a patient's ID code, doctors can see the time-critical information they need. This data is also used as the basis of national health statistics.

During the COVID-19 crisis, Estonia's e-health system proved essential for accessing COVID-19 test results, downloading EU COVID-19 digital certificates, and booking vaccination appointments.

In the special report on ADM systems used in Estonia during the COVID-19 pandemic, I highlighted some of the solutions Estonia aimed to develop to tackle the health crisis. These were either never fully realized or have been realized (COVID-19 Travel app, Immunity Passport) by other systems today (e.g., EU COVID-19 certificate).

/ CASES

COVID-19 certificates and apps

Testi.me

After the first wave of the pandemic in 2020, people started traveling again and they needed a certificate to prove their COVID-19 test was negative, or they had previously had the virus. To do this, they could use a webpage or app called testi.me – which was developed by Synlab in partnership with the Estonian Health Board. Citizens could download a certificate through this service free of charge. Whereas, requesting a certificate manually cost about €10-13. This app can still be used to give a quick overview of all the COVID-19 tests citizens have taken during the pandemic. The results of the tests are also accessible via the Estonian e-health system for patients (digilugu.ee). In addition, patients can forward the testi.me certificate to anyone they choose.

In the beginning, these certificates did not contain QR-codes like the EU COVID-19 certificate. This

opened up the opportunity for people to make and use fake certificates when traveling. People either printed these by themselves (and changed the data on the document someone shared with them) or they even bought similar-looking certificates from someone. Surprisingly, this information was shared publicly on Facebook.

The EU COVID-19 certificate

Estonia was one of the first countries to start using the EU COVID-19 certificate. In the beginning, these certificates were mostly used to travel. However, since the end of August 2021, they have increasingly been used for other domestic reasons. To verify if the EU COVID-19 certificate is valid in Estonia, institutions can use a solution on the kontroll.digilugu.ee website. Until recently, many places did not verify the certificates nor ask to see any accompanying identification. However, as the pandemic progressed and infection rates increased in the autumn of 2021, controls and certificate checks got stricter. Places like bars, restaurants, cinemas, gyms, and spas can be fined for not checking the certificates of people. If they continue to flout the rules, their work can be temporarily terminated by Estonian Health Board. From mid-October 2021, certificates that prove someone has tested negative for COVID-19 could not be used to enter restaurants, cafeterias, spas, etc. So far, there have been 33 cases where the police have fined people for using fake EU COVID-19 certificates.

Citizens can access their EU COVID certificate through the Estonian e-health portal. The certificate is supposed to be valid for one year for people who have been vaccinated. However, in October, it was revealed that the Health and Welfare Information Systems Centre (TEHIK), which is responsible for the system, had put a limit of 180 days on the certificate. Therefore, those who had completed their vaccinations before July 2021 had to renew their digital certificates.

It also came to light that it can be very difficult for older people to receive the digital EU COVID-19 certificate as they are not used to using different digital identification systems and may not remember their PIN codes. Proof of vaccination can also be made by using the yellow vaccination passport, however, this is not always available for older people as family doctors are no longer required to issue them. TEHIK will provide yellow passports, but citizens must visit Tallinn in person to do this.

SUVE chatbot

SUVE is an automated chatbot that was created for people in Estonia to answer questions they might have about the COVID-19 situation. SUVE was developed during the Hack the Crisis hackathon, which was organized by the Estonian start-up community, Garage48, and Accelerate Estonia. In spring 2020, SUVE was integrated into several public websites including, Government of the Republic, the Health Board, the Ministry of Social Affairs, Work in Estonia, the International House, the Foreign Investment Center, and TV3, to provide accurate and trustworthy information in English, Estonian and Russian. SUVE continues to work albeit with limited functionality. However, this limited functionality means there is a possibility that SUVE might give incorrect information about vaccinations or travel restrictions. For example, in October 2021, on the webpage Work in Estonia, SUVE answered a question in Estonian about COVID-19 vaccination by saying there is no vaccine against COVID-19. This suggests that SUVE may use data that is not up to date and, as a result, it may give incorrect answers.

SIXFOLD – Vaccine distribution

Estonian logistics start-up, Sixfold, together with a team of volunteers, developed an app for use by family physicians and the Estonian Health Insurance Fund. The app aims to distribute vaccines efficiently by

using data on the number of vaccines arriving in the country, which is matched with COVID-19 risk groups, to propose how best to automatically distribute the vaccines to more than 700 family doctors throughout the country. Doctors then have the opportunity to order what they need and confirm their order through the Health Board. The app also gives an overview of the preliminary information of pending deliveries.

Estonian Emergency Response Center Assistant for Risk Assessment – Under development

By transcribing and prototyping the sound files of emergency calls, this project aims to find out how AI can help rescue organizers in assessing hazards. The problem is that the emergency notification procedure is complex and very expensive and may lead to errors in risk assessment or it might take too much time for the rescue organizers. The hope is that, in the future, this solution will provide rescue organizers with a typical case scenario of the most likely outcomes by transcribing an incoming call and crosschecking it with previous activities. This solution is being developed by Mindtitan and financed through the European Structural and Investment Fund with €65,680.

HOIA – COVID-19 contact tracing and warning app

HOIA is a contact tracing and warning app developed by a consortium of Estonian IT developers. The app uses Bluetooth technology in phones to detect the signal of other phones that have been in close proximity for a certain amount of time. If a person confirms a positive COVID-19 infection using the app, an anonymous code is uploaded from their phone to a central server for all users to download. It is not possible to identify a person based on an anonymous code. The user's phone checks to see whether the patient's anonymous code matches a code previously-stored on his or her phone. If it does, the user is considered a close contact and is notified with instructions of what to do. HOIA has been used for contact tracing since 19 August, 2020.

/ ANALYSIS

After the first wave of COVID-19, Estonia was often portrayed as an example of how digital governance solutions can help tackle the health crisis. Sudden events like the pandemic require immediate action, however, in the Estonian context, this has been difficult to achieve because many of the solutions may end up being stuck in long, costly, and challenging procurement processes. In e-health and e-schooling — which were the two most important governance systems during the crisis — Estonia relied heavily on outsourcing and private sector companies to develop services. Usually, this process is used to support digitalization. However, during the pandemic, this reliance on procurement increased the number of regulations and decreased the speed at which the government was able to respond to the constantly changing situation (McBride, 2021).

During the crisis, private companies, and volunteers offered their knowledge and workforce to develop solutions to help tackle the virus and offer vital information and services for decision-makers and citizens (i.e., HOIA, SIXFOLD, koroonakaart.ee). However, in the case of the contact tracing application, critics have argued that this has led to a situation where the app does not belong to anyone. Therefore, the latest regulations related to COVID-19 may not be implemented in the application (i.e., the most accurate information about isolation requirements). A similar fate happened to the SUVE chatbot, which was developed during the first wave of the pandemic, but has not been further developed. However, SUVE is still used on several Estonian websites and can, on some occasions, give false information. Given that Estonia is struggling with vaccinations, this is problematic.

THE NETHERLANDS

BY JILL TOH, NAOMI APPELMAN
AND RONAN Ó FATHAIGH

/ CONTEXT

The purpose of this chapter is to provide a brief overview of the ADM systems deployed during the COVID-19 pandemic in the Netherlands. The chapter builds upon the work in an earlier AlgorithmWatch special issue on *Automated Decision-Making Systems in the COVID-19 Pandemic* — a time when new ADM systems were at an early stage of being rolled out in the Netherlands. The chapter also builds upon the 2020 edition of AlgorithmWatch's Automating Society Report, which detailed the increased prevalence of ADM systems in the Netherlands, and documented the considerable criticism of such systems, including the infamous SyRI system for welfare-fraud detection. In this latest chapter, we first provide an updated overview of the ADM systems being used in the Netherlands during the pandemic; then contribute some critical reflections on the systems and related policies; and finally, we conclude with some lessons to be learned.

/ CASES

In our August 2020 report on pandemic-related ADM systems in the Netherlands, we outlined the winding road the Dutch government took in developing its contact tracing app *CoronaMelder.* After staging an elaborate public contest ('hackathon') to develop the app (live-streamed on YouTube), the government ended up building a decentralized, Bluetooth-based system. Since the previous report, extensive research has been published on the uptake and effectiveness of the contract tracing app discussed below. Other important ADM systems employed during the pandemic — highlighted in the previous report — are online proctoring systems used in Dutch universities. Despite vehement protests and legal action from students, several universities persisted in obliging students to use the systems. Indeed, in that same report, we wrote about the litigation launched by a student union over the online proctoring system — the students eventually lost their case in the District Court of Amsterdam. Since then, the student union launched an appeal, which they lost at the Amsterdam Court of Appeal.

During the past year, there have been several developments in the deployment of pandemic-related ADM systems in the Netherlands, although the flurry of ADM-related initiatives seen at the start of the pandemic seems to have calmed down significantly. One of the few newly developed systems is part of a large project under the name 'COVID-RED'. In this project, the Utrecht University Medical Centre is researching whether a wearable (bracelet) medical device could be a useful addition to contract tracing apps to detect early COVID-19 symptoms. Another noticeable development is the 'CoLab blood score' for COVID-19. Researchers from the Eindhoven University of Technology developed an algorithmic tool to quickly analyze incoming ER patients to detect the presence of COVID-19 in their blood.

Importantly, in March 2021, the Dutch government began trialing its *CoronaCheck* app. This allows people to show they have been vaccinated, tested negative for COVID-19, or have recently recovered from COVID-19 and could be used to access certain locations. Then, in May 2021, the Dutch Parliament passed legislation *(Tijdelijke wet coronatoegangsbewijzen)* allowing the use of the *CoronaCheck* app for entry to restaurants, cultural institutions, events, and sports competitions. Additionally, from July 2021, the CoronaCheck app also functioned as a Digital Corona Certificate for traveling within the EU. Notably, there were considerable issues with the CoronaCheck app, with certificates not being generated, and instances of increased COVID-19 cases despite the use of the app. Most recently in the autumn of 2021, with rising cases despite an adult vaccination rate of around

85%, a new issue with the *CoronaCheck* app came to light. It transpired that the QR code of a vaccinated person cannot be revoked once issued, even when they test positive for COVID-19. This is due to the decentralized and privacy-sensitive design of the app.

As already mentioned, over the past year the government has given the most attention to managing ADM systems that were implemented at the start of the pandemic. In particular, in June 2021, the Dutch public health institute, the RIVM, published a major study on the *CoronaMelder* contact tracing app. It concluded that the app only made a 'small contribution to the fight against the coronavirus'. Between December 2020 and March 2021, 7,514 people tested positive after receiving a message from the *CoronaMelder* app, and this 'prevented an estimated 15,000 infections', out of around 1.8 million infections in the same period. The app was downloaded 4.6 million times, but only used by 16% of the population.

Further, both the *CoronaCheck* app and the local health authorities responsible for testing and vaccinating *(Gemeentelijke Gezondheidsdienst)* (GGD) have been plagued by expansive data leaks and privacy breaches. In July 2021, it came to light that a company involved in issuing test certificates and connected to the *CoronaCheck* app had leaked private data of more than 60,000 people. As a result, it was possible to manipulate the *CoronaCheck* app in such a way that everyone could get fake test results. Following the revelation, the Dutch Ministry of Public Health, Welfare and Sport discontinued its connection with the company. Similarly, at the start of the year, Dutch media reported that employees at the GGD had been selling private data such as addresses, phone numbers, and social security numbers from people who had taken a test for COVID-19. All 26,000 employees of the GGD had access to all of the data, making it open for abuse. Several employees searched for the data of celebrities and even sold a large amount of personal data. So far, two employees have been convicted of data theft.

Despite the (in)effectiveness and (lack of) uptake of the *CoronaMelder* app, the justification for the development and use of data-driven technologies is crucial to note, particularly in the context of pervasive techno-solutionism. In the Netherlands (and other European countries), consent tends to be relied upon as legitimate grounds to introduce new technological solutions to cope with public issues. While such informed consent is legitimate, and enshrined in data protection law, an empirical study by the University of Amsterdam (published in September 2021) on the *CoronaMelder* app, cautions that (individual) consent is insufficient when introducing data-driven technologies to support government action and decision-making. The survey findings of a representative sample of the Dutch population highlighted that those who installed the app were not highly cognitively engaged with the consent they were asked for, particularly related to the technical aspects of the app, data sharing with the municipalities, and the overall app infrastructure. The varying trade-offs, including the significant economic and social costs that come with them, underscores that individual consent to the use of certain technologies cannot be used as a proxy for societal or democratic decision-making related to the utilization of those technologies as part of a nationwide response to a crisis.

Finally, throughout the past year, it seems that Dutch NGOs have remained relatively silent on the management of these existing systems, and the implementation of the *CoronaCheck* app. Strikingly, this is in contrast to the broad public discussion on the development of the initial *CoronaMelder* app. However, several dedicated campaign groups have been established as vehicles to fight the COVID-19 measures, which they see as government overreach. These groups reflect various perspectives, including those opposed to lockdown measures, vaccinations, and mask rules.

/ ANALYSIS

Several patterns can be discerned, based on this brief overview of pandemic-related ADM systems in the Netherlands. Perhaps unsurprisingly, the use of ADM systems by the government reveals the pervasive techno-solutionist assumptions underlying the Dutch government's management of the pandemic. Secondly, the legislative context of the ADM systems involved is interesting as it diverts from the usual understanding of technology as a mere tool and executive matter. Finally, the overview clearly shows the narrow focus of the government on privacy and data protection, disregarding other relevant considerations.

To start, the past year of measures to manage the pandemic in the Netherlands was not so much aimed at the development of new ADM systems, but rather on managing the systems introduced in the first few months of the pandemic. The slew of scandals plaguing the Dutch track-and-trace app, *CoronaMelder,* and the track-and-trace systems of local health authorities, did not seem to dampen the government's persistence and reliance on technological measures. Similarly, even though some university courses renounced the use of invasive online proctoring software, many universities continued to use these systems.

Connected to this is a more muted public discussion on these systems. Whereas at the start of the pandemic, there was a lively public debate on the implementation of and requirements for these systems, this debate seems to have dwindled. While there are still regular protests against COVID-19 measures in general, and the *CoronaCheck* app in particular, these have become part of the rhythm of daily life and do not seem to form a real challenge to the government's use of ADM systems.

The exception to this general pattern is the *CoronaCheck* app that was developed in the past year but has only been widely used since July 2021. The app makers learned from the controversies surrounding the *CoronaMelder* app and, from the beginning, its development was based on a decentralized and privacy-friendly design. Although similar to the other systems in use, public debate regarding the implementation of the *CoronaCheck* app was muted. This may have been because the app was created to allow vaccinated people to travel. Only months later, did the QR code become mandatory for visiting indoor spaces within the Netherlands. Although definitely not without its problems, as indicated in the previous section, the app seems to work largely as intended.

When the use of these ADM systems, the issues plaguing them, and the (lack) of public debate on them, are placed in the wider context of the government's strategy for managing the pandemic, the reliance on technology becomes clear. Throughout the pandemic, the government put great emphasis on the potential of technology to solve or help manage the crisis. At the start of the crisis, the development of a contact tracing app was a high priority, which raised the question: why was the same effort not put into strengthening the existing track-and-trace infrastructure? Similarly, great importance is currently given to the CoronaCheck app. This focus on technological ways out of the pandemic falls within a wider trend of techno-solutionism where structural issues are eclipsed by spotlighting technology.

Another pattern has been the specific enactment of legislation providing a legal basis for the use of COVID-19-related technologies, in particular the use of the *CoronaCheck* app. In a positive sense, the provision in law to use such ADM systems strengthens the rule of law and reduces the scope the government has to implement arbitrary measures. Indeed, the legislation passed in May 2021 regulating the use of COVID-19 passes and the app *(Tijdelijke wet coronatoegangsbewijzen)* specifically provides that the app must only make personal data 'visible for a number of seconds' to those checking the COVID-19 pass.

The app must 'delete the personal data immediately afterwards', while there is an overall requirement to use 'as little personal data as possible'.

However, the legislation is framed nearly exclusively in terms of data protection, and the focus on technology in this way is, perhaps, too narrow an approach. There is, arguably, a lack of consideration for a broader perspective in the legislation, particularly the exclusionary effects COVID-19 entry requirements have and the impact upon human rights. Indeed, human rights groups have argued that app-based solutions can create 'a two-tiered response' to COVID-19 by 'leav[ing] the poorest and most vulnerable people behind', and 'tech-driven responses' can 'reinforce systemic inequalities facing those hardest hit by the virus'. Notably, the Secretary-General of the Council of Europe has explicitly recognized not only the risk of discrimination in relation to COVID-19 passes and apps, but also the risk of 'stigmatization' and 'arbitrariness', and that they have consequences for human rights, and access to employment, housing, or education. However, there has been litigation over the COVID-19 pass and app, and the District Court of The Hague found that the legislation was not discriminatory.

Finally, and building upon the previous point, in the earlier examples of the *CoronaMelder* app — and the use of online proctoring in the education context — the Dutch (legal and public) discourse has often narrowly framed and utilized data protection law by focusing mainly on privacy concerns. As with the *CoronaMelder* app, there is a tendency in the Netherlands and, more widely, in other European countries, to view the over-reliance on consent as legitimate grounds for introducing data-driven technologies.

In a strategic litigation case brought forward by some Dutch university students related to the use of online proctoring, the arguments revolved around whether the University of Amsterdam should have consulted the Student Council for permission to roll out the proctoring software and assess compliance with privacy legislation. However, the use of online proctoring technologies is proven to have racist, discriminatory, and exclusionary effects, which go beyond the scope of privacy issues. These instances often correspond with the adoption of these technologies to matters solely associated with data protection, even if data protection is neither only about privacy nor consent. While important, this approach tends to obscure or disregard other related (and potentially pressing) legal considerations (i.e., non-discrimination), when deciding to utilize digital technologies in the context of the public interest.

We can also take heed from the SyRI case, in which a digital welfare fraud detection system that the Dutch government used was ruled unlawful by the Dutch Court in the Hague because it did not comply with the right to privacy under the European Convention of Human Rights. While it was a landmark judgment, the focus on privacy, particularly in the context of fraud detection, loses sight of other more harmful effects, such as discrimination targeted disproportionately at lower-income groups. Does this mean that digital fraud detection systems should still be implemented if they respect the right to privacy and data protection principles? Further, big tech companies are also pivoting to being privacy-friendly (or 'privacy washing', and the effects of tech-driven harms related to discrimination, exclusion, and inequality have been increasingly documented. It is critical to ensure that privacy rights do not become the main (or only) basis upon which to assess the rollout of digital technologies for public interest use by governments.

/ CONCLUSION

In conclusion, two main points can be made. Firstly, in the previous edition of Automating Society — published just as the COVID-19 pandemic was beginning to emerge — the large increase in Dutch government policy documents on ADM systems was noted, in

particular the supposed regulatory frameworks for ADM systems. However, it may be asked whether the frameworks for protecting human rights and public values were adequately applied during the pandemic? Especially given the criticism leveled at the rollout of the contract tracing apps, and other pandemic-related systems. Indeed, a recent Council of Europe report on the Netherlands — and another scandal involving an ADM system used to identify child benefit fraud — needed to include a whole series of reforms relating to parliamentary, executive, and judicial scrutiny of such systems.

Finally, in the debates around the use of technology, the focus and prioritization of certain rights have often been more prominent than others, as evident in some examples shown in the Dutch context. At the European level, civil and political rights, such as fundamental rights related to individual privacy, data protection, freedom of expression, and information, tend to dominate the framing of issues related to tech policy. On the other hand, socio-economic rights — related to the redistribution of wealth and income, equality, social protection, and welfare — have often been side-lined. While there are reasons for this, the consequence means setting priorities on how issues and harms are understood. This will determine the parameters for solutions and responses — including the type of actors who can be involved — and the kinds of technologies that should or should not be developed and used in public forums.

NORDIC COUNTRIES

BY CLAUDIA WLADDIMIRO QUEVEDO AND ANNE KAUN

/ CONTEXT

There are clear similarities between the COVID-19 ADM systems in the Nordic countries of Norway, Finland, and Denmark. However, Sweden is an outlier here — both in terms of ADM systems — and the general approach to tackling the pandemic.

There have been some legal developments relating to the use of ADM in public administration. Sweden, for example, published an extensive governmental inquiry into ADM in March 2021 (Regeringsutredning om en väl fungerande ordning för val och beslutsfattande i kommuner och regioner). The report suggests the legal framework needs to be adjusted to allow for fully automated decisions at the municipal level. At the national level, the legal framework was adjusted in 2018 to allow governmental agencies (Förvaltningslagen) to make fully automated decisions.

Since people started meeting in workplaces again, on public transportation, and have started socializing again, tracing apps have come into play. The data gathered by these apps are useful for the "Digital Green Certificate". This is a European Commission initiative to facilitate safe and free movement within the EU during the pandemic. The certificate is seen as a temporary measure and will be suspended once the World Health Organization declares the pandemic over.

The Digital Green Certificate can be used across all EU Member States, as well as in Iceland, Liechtenstein, Norway, and Switzerland. It acts as proof that a person has been vaccinated against COVID-19, has received a negative test result, or has recovered from COVID-19. It is available free of charge in digital or paper format, with a QR code to ensure security and the authenticity of the certificate. To prevent discrimination against individuals who are not vaccinated, the Commission proposed an interoperable vaccination certificate and a COVID-19 test certificate for people who have recovered from COVID-19. The personal data: name, date of birth, date of issue, information related to the vaccine/test/recovery, and a unique certificate identifier, can only be checked to confirm and verify the authenticity and validity of certificates.

The first versions of the apps used GPS and satellites, but now they use GAEN API that relies only on Bluetooth for tracing (as happened with two versions of the Smitte|stop app in Norway).

/ CASES

Denmark

In June 2020, the Danish government launched the COVID-19 infection tracing app Smitte|stop. This is the most downloaded app in the history of Denmark. However, just a few months after it was launched, the app was criticized for the lack of clear wording in the notifications related to the number of "potential exposures". This happened because the Apple and Android operating systems did not follow the criteria of the Danish health authorities for close contact, which, for users of the app, is a proximity of 1 meter from an infected person for 15 minutes or more.

The most recent Danish project used by the authorities is the Coronapas. It allows citizens to access certain non-essential businesses, including hairdressers, beauty salons, and driving schools.

In addition, the COVIDmeter platform is also available in Denmark. This initiative was developed in

collaboration with the IT service provider Netcompany and it allows users to input and monitor COVID-19 symptoms. The platform is linked to the Danish Ministry for Health in charge of infectious diseases. Citizens volunteer to answer a weekly questionnaire about their health status, including whether they have been tested for the virus or have been exposed to it, as far as they can tell. The log-in procedure has security protections similar to online banking, and any identifying information is anonymized to prevent possible misuse.

Norway

The Norwegian Institute of Public Health ("Folkehelsesinstituttet, FHI") has been working on the Smitte|stop app that can be used by everyone over 16 years old. However, the first version of the app was shut down. Norway's DPA raised concerns that the software posed a disproportionate threat to user privacy, including the continuous uploading of the user's location. The new app, Smitte|stop v2, is based on the GAEN API and only uses Bluetooth for tracing.

Finland

In August 2020, Finland launched Koronavilkku, a contact tracing app that uses Bluetooth technology, produced by the Finnish Institute for Health and Welfare (THL). If someone tests positive for COVID-19, they can use the app to anonymously share this information with those who have been in close contact with them. In English, the name of the app translates as "Corona Blinker" and it was developed by the private Finnish software company Solita after it won a public procurement process in June 2020.

Sweden

In Sweden, there have been no major changes in the approach since the last report in Automating Society 2020. At least three applications have been developed to document and map symptoms among the Swedish population. One of these apps, smittspridningsapp, was developed by a non-profit group to map the development and spread of COVID-19 based on self-reported symptoms, and now it is connected to the Swedish Health authorities. A second app, called COVID Symptom Study and first developed in the UK, is now used by a research group at Lund University to 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. At the beginning of January 2021, the study had just over 202,000 participants in Sweden. The last initiative came out of 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). Together with industry partners, they worked on a digital tool to map experiences of symptoms among the population. However, the Swedish authorities later confirmed that it would pause the initiative as it was potentially doing more harm than good by worrying and confusing Swedes with the information collected. In addition to the applications already discussed, the Public Health Agency has repeatedly relied on mobile phone data provided by Telia, the largest service provider in Sweden, to track the movement of Swedes during bank holidays, for example.

/ ANALYSIS: THE OVERALL CONTRIBUTION OF ADM AGAINST COVID-19 IN THE NORDIC COUNTRIES

In the Nordic countries, fast and reliable communication between citizens and the health authorities has been the goal for the tracing apps. Periodically, civic organizations and academia provide updated information about ADM projects relating to contagion tracking and the online availability of personal data and certificates. However, issues, such as the invasion of privacy, are a major concern.

In terms of ADM systems used to contain the pandemic, Sweden is clearly an outlier. It has not further pursued a centrally commissioned contact-tracing app and currently offers no digital infrastructure for a vaccine pass (confirmations that include a QR code can be downloaded as a PDF). As a result, Sweden stands out from the other Nordic countries.

POLAND

BY KRZYSZTOF IZDEBSKI

/ CONTEXT

Although Poland was not as dramatically affected as many other countries by the pandemic, it was hit hard. As the infection rate increased with each wave, the authorities decided on further lockdowns. For a long time, pupils did not attend school, where possible employees worked remotely, and shops were closed or operated on a limited basis. From the start of the pandemic (March 2020) until now (October 2021), 2,982,143 people have contracted COVID-19 in Poland of which 76,540 have died.

In an attempt to control the pandemic, many people were obliged to quarantine. These included people returning from abroad or those who had contact with people who had tested positive for COVID-19. At its peak, as many as 500,000 Poles were in quarantine, mainly at home. Despite the much-declared resistance to "house arrest", the vast majority of people accepted the obligation to stay confined.

Poland currently ranks below the EU average in terms of people who have received two vaccine doses (23 out of 27). As of 26 October 2021, only 52.3% of Poles had been fully vaccinated. In some regions, vaccination rates are very low. For example, in Podkarpackie Province, in the southeastern part of the country, 38% of the population is fully vaccinated. These low figures are not related to problems with the availability of vaccines - shots are available for anyone who wants one. Furthermore, the authorities have taken several measures to facilitate vaccination, such as mobile vaccination points, intensive promotion, and even a lottery for those who have been vaccinated.

According to polls, some people believe the vaccines were developed too quickly. This causes fear of possible side effects and uncertainty about whether the vaccine is safe or not. These are the three main reasons behind the reluctance of those who do not want to be vaccinated. However, what draws attention is the fourth most popular reason. 40% of respondents refuse to get the vaccination because of a lack of trust in the pharmaceutical companies for whom "money is more important than health care".

Accompanying the relatively low number of vaccinations, there has been resistance to the introduction of the so-called 'covid passports'. These allow vaccinated people to enter bars, shops, and some workplaces. A September 2021 survey found that 24.8% of respondents believe that giving privileges to fully vaccinated people and restricting the movement of those who are not vaccinated is a violation of civil liberties. On the other hand, 46.6% of respondents are in favor of the need to show a vaccination certificate when going to the cinema or theater. So far, the Polish authorities have not decided to make covid passports mandatory for access to certain places. They are used mostly for foreign travel, and so that those who have been vaccinated are not counted when it comes to limiting the number of people who can attend mass events.

/ CASES

One of the first responses to the challenges of the pandemic was the use of technology. Work on this has mainly focused on applications to improve control in a variety of situations. The government financed the development of contact tracing solutions, applications to monitor people staying in quarantine, and an algorithm to control entrepreneurs who received government support because their ability to work was restricted during the pandemic. Another example is the city of Gdynia, which implemented a city monitoring system that included rapid identification of large concentrations of people. The code was placed on GitHub. However, after a test phase, this function was abandoned.

STOP COVID - ProteGO Safe app

STOP COVID - ProteGO Safe is an application that uses an API developed by Apple and Google, Bluetooth technology and non-exposure notifications. The app monitors the user's environment for other devices on which the app is also installed. It "remembers" any encounter that lasted more than 15 minutes and took place within 2 meters. If one of the users falls ill - the other people with whom he or she has been in contact with over the last 14 days receive a notification. Despite the increase in infections recorded in recent weeks, data on the use of the app shows that it is not commonly used.

As of October 17, the STOP COVID application had been downloaded 2,189,266 times. As of the same date — according to the install/uninstall information available in both the Google and Apple shops — the estimated number of active installations was 650,663.

Within the app, users can voluntarily submit 'keys' indicating potential contact with an infected person. These keys relate to the risk of contact with a person infected with COVID-19 and do not include any other information about the user's health status. To prevent false alarms, a PIN must be obtained from a contact center operated by the Chief Sanitary Inspector to send keys indicating the risk of infection. As of 17 October 2021, the contact center had issued 9,435 PINs. So far, the cost of running the STOP COVID app is over €140 million.

As can be seen, despite an extensive promotional campaign, the government failed to convince Poles to use the STOP COVID application. It seems that citizens did not see the direct benefits of using the application. In addition, there was no obligation to use it, nor was installing the app a pre-condition for using selected services, as is the case in some other EU countries.

Home Quarantine app

Home Quarantine is another application developed on behalf of the Ministry of Digital Affairs. This app is an adaptation of the "Kantar GO" application developed by the TakeTask company – part of a project management tool, the functions of which include taking photographs in strictly defined places. As a result, it was quick and easy to convert this functionality to monitor people in quarantine.

The app aims to make it easier and more efficient to carry out mandatory quarantine at home. The app allows the user to confirm the location of the place where they will quarantine. It also facilitates contact with a social worker or psychologist. Installation and use of the app are a legal obligation for those who have to undergo quarantine due to a suspected infection. The visually impaired — and those who do not subscribe to or use a telecommunications network or do not have a mobile device — are exempt from the obligation to use the app. Such a statement is made under pain of criminal liability for making a false statement.

The obligation to install the app was primarily introduced to relieve police officers who had to carry out checks on people quarantining at home. Already, a year ago, the chief of one of the police stations in the north of Poland said that, "Every day police officers in the Pomeranian province have to supervise the course of quarantine of more than 24,000 people, which is a really demanding and time-consuming challenge."

According to user reviews, which can be found in the Google Play store among other places, the application does not work well. It has a one-star rating. Among the reviews of the app, the following sentiment prevails,

"Quarantine taken off in the morning, after a negative test result. After 8 hours a text message arrives

– you are in quarantine, you are required to install software!"

"I take a picture and it disappears. So, I take another one and it disappears too, so I take it again for the 3rd time until finally it says I can send it and finish the task. Hopeless."

"Doesn't save photos, shows my quarantine locations incorrectly, comes a notification that I'm not doing tasks that don't save as I do anyway!"

In another - ironic - comment, someone claims that,

"Today is the last day of isolation and the app only asked to send a photo the first time right after downloading, since then I have peace of mind as the app has never asked for anything again. Perfect for me."

Although there are thousands of similar opinions in the reviews, the authorities do not seem to care much about them. There are only occasional replies from officials to selected commenters asking people to forward their comments to an official email address. Although the app was last updated on September 22, subsequent comments after that date show that the app is not working any better. Almost identical comments can be also found in the App Store.

Algorithmic control of government subsidies

An algorithm to control entrepreneurs received government subsidies. A special algorithm was developed to verify the tax residence of entrepreneurs and any decrease in revenue they experienced because of the pandemic. A decrease in revenue is one of the criteria used when applying for aid. In addition, the main beneficiary must be a tax resident in Poland or declare a transfer of residence within nine months. The algorithm was developed by the Central Anti-Corruption Bureau and the National Tax Administration.

The authorities decided not to disclose the full details of how the algorithm works. The limited information that was disclosed related to the verification of statements made by entrepreneurs who had applied for subsidies against documents held in public registers (e.g., income declarations). When asked by the Moje Państwo Foundation about the cost of developing this algorithm and who created it, the Central Anticorruption Bureau — which commissioned the algorithm — said that this was classified information. The Foundation has submitted a complaint to the Regional Administrative Court in Warsaw and awaits a hearing.

/ ANALYSIS

Although the authorities were quite quick to implement technological solutions to combat COVID-19, these solutions seem to have run alongside more analog activities. Except for the Home Quarantine app, the solutions that restricted civil liberties in any way were not mandatory. Their use, therefore, did not generate much resistance, or at most — as in the case of STOP COVID — very low interest. Or, as in the case of the Covid passport, a rational attitude that it was simply easier to travel with it. Due to the secrecy of the algorithm that controls entrepreneurs who received government support, it is difficult to assess at present not only its effectiveness, but the scale of its use.

As the development of applications was accompanied, from the beginning, by a very heated discussion about potential privacy risks, it was possible to ensure that these risks were not hidden in the code. The seven pillars of trust – a list of principles proposed by a group of experts for creating technology based on trust — remain valid. From the Polish experience, we can see that modern users do not "throw themselves" at technical innovations and have high expectations from these types of applications. Both in terms of their usefulness and in terms of safety when using them.

PORTUGAL AND SPAIN

BY JOSE MIGUEL CALATAYUD

COVID-19 tracing technology in Spain: a missed opportunity and normalization of surveillance

/ CONTEXT

Before the COVID-19 pandemic, the situation in Spain concerning the use of ADM systems in the public administration could be summarized as providing a generally good legal framework but lacking in transparency and accountability. Spain is also characterized by a high level of administrative decentralization, as the 17 autonomous regions have much leeway to test and implement their own ADM procedures.

The developments brought about by the pandemic indicate an increasing public awareness, both about the need for legal clarity and the risks associated with ADM technologies. This could be seen when, on the days following the declaration of a state of alarm on 14 March 2020, 62 experts on data and AI sent a letter to the Spanish government calling for the "legal, ethical and transparent management of personal data" collected on any future apps related to the pandemic. Then, on 27 March 2020, the government passed an order entrusting the Secretary of State for Digitalisation and AI with "the development of different actions to manage the public health crisis caused by COVID-19". Days later, the Hay Derecho Foundation, which is made up of public administrators and legal experts, analyzed the order and found it in line with the current Spanish and European protection laws.

/ CASES

Analysis of mobility data

On 28 March 2020, the central government announced that the National Statistics Institute (INE) would launch a mobility study by aggregating anonymized mobile connection data from telecommunications companies to monitor the movement of people during the lockdown.

After accusations from the extreme right and by some news media of wanting to geolocate individuals, the government issued a clarification that the data would only serve to quantify the number of phones in a given area at a given time, and that there was no way to identify the phones or the people carrying them. In fact, getting those data was nothing new: the government had already carried out a similar study during 2019, and, by that time, telecommunications companies were already selling similar data to advertisers.

After the initial controversy, the National Statistics Institute (INE) carried out the study. It has been publishing weekly reports about mobility data, and these have become something normal. The news media have been using them in their coverage of the pandemic.

Self-diagnosis apps

The other main point of contention was the different self-diagnosis apps launched by both the central and some regional governments. As reported by AlgorithmWatch in September 2020, the Madrid region was the first to launch such an app. The original app required users to enter sensitive data (including GPS location, national ID number, full name, birth date, full residential address, and email address). The app's privacy policy stated that this 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. After criticism in the media and by social media users, a subsequent version of the app had a stricter privacy policy, which did not let companies use the data for their own means. In addition, the app no longer asked users for their email address and allowed them to keep their location private, in which case the app would use the user's residential address for geolocation purposes.

In the end, eight of the 17 autonomous regions (Andalusia, Aragon, Castille-Leon, Catalonia, Navarra, Valencia, Madrid, and the Basque Country) released their own distinct self-assessment apps. While, the central government released its own version servicing six other regions (Canary Islands, Cantabria, Castille-La Mancha, Extremadura, Balearic Islands, and Murcia). The remaining regions (Galicia, Asturias, La Rioja, and the autonomous cities of Ceuta and Melilla) are not listed as having an official self-assessment app.

Radar COVID exposure notification app

Between June and July 2020, the Spanish government ran a pilot of what would become of its official contact tracing app, released as Radar COVID. The published results of the pilot were promising, as the app detected 6.4 contacts at risk for each case of COVID-19 logged into the app, well above the 3.5 contacts detected by human tracers for each case.

On 30 July 2020, the Spanish government made Radar COVID available to the regional governments, which are the ones in charge of healthcare. The app used the GAEN protocol, which only accepted one functioning app per country to prevent the launch of non-official versions. That meant that regional authorities in Spain had to link their own version of the app to a single central system, and that process took a long time. Radar COVID was first used in four regions on 19 August 2020. The app was not available in Madrid and Catalonia — the two regions with the highest infection rates — until 1 September and 27 October 2020, respectively.

From October 2020 to January 2021, almost 7 million people downloaded the app, which by 17 October 2021 had been downloaded a total of 7.9 million times (of which the number of individual active users is not known), out of a total population of 47.4 million people. By 17 October 2021, the ratio of cases confirmed on the app — per codes provided by the regional health authorities — was 31.7%. However, the ratio of cases confirmed on the app — per number of total cases in the country — was only 1.7%.

Given those figures, many have questioned the usefulness of Radar COVID. It cost €3.5 million of public money to develop, almost half of which, €1.5 million, was earmarked for PR and advertising. In addition, the procurement process lacked transparency because of the emergency measures in place. The government was also criticized for not releasing the code of the app until 9 September 2020 — three weeks after the app was released — and for taking several months before starting to publish all the relevant statistics about how the app was being used.

Fighting COVID-19 with "AI" in the Valencian region

The autonomous status of the regions in Spain when it comes to policymaking, allowed the Valencian region to take an AI-based approach. This was led by Nuria Oliver, a prominent data scientist, co-founder, and vice-president of the European Laboratory for Learning and Intelligent Systems, who comes from the region.

Mr. Oliver's team was given access to the mobility data being compiled by the INE at the beginning of the lockdown in spring 2020. They supplemented this with other sources, including a series of online surveys — originally aimed at people in Spain, now open

to other countries too — about how people perceived the crisis and what their behavior was.

Based on those different kinds of data, the team developed predictive models through machine learning that aimed, for instance, to forecast what the number of general and ICU hospitalizations overall, and for COVID-19, would be. The team also developed an ADM system that advised the Valencian authorities about which particular interventions to implement to get supposedly "optimal" results in the trade-off between restrictions and the number of COVID-19 cases.

/ ANALYSIS

The story of Radar COVID summarizes the situation in Spain regarding tracing and other ADM technologies during the pandemic: high hopes placed by the government, early controversy about privacy and transparency surrounding the apps, lack of coordination between the autonomous regions and the central government, and then normalization of the technologies even though there are doubts about their usefulness and efficacity. This was also the case with the use of drones to watch, count, and even talk to people during the pandemic, as reported by AlgorithmWatch in September 2021.

Lastly, regarding the obligation to show a COVID-19 health pass to gain access to bars and other indoor entertainment venues, the Spanish authorities have, again, taken what appear to be inconsistent steps. As the state of emergency was lifted on 9 May 2021, several regional governments tried to impose the obligation to show a health pass. However, the high courts in the respective regions annulled these regulations, generally arguing that they violated the rights of citizens without a clear public health benefit. Curiously, the Spanish Supreme Court confirmed such a ruling by the Andalusian top court on 18 August 2021, which prevented the Andalusian government from enforcing the health pass. While, weeks later, on 14 September 2021, the Spanish Supreme Court decided against a similar ruling by the Galician high court, which in this case meant that the Galician government could go on and enforce the health pass.

In one sense, the pandemic has been a missed opportunity. Despite the urgency of having to deal with the public health crisis, the authorities could have been more transparent and promoted an informed public debate about the possibilities and challenges posed by tracing technology and by ADM systems in general, and about how to test, implement, and monitor the use of such technologies throughout a decentralized state like Spain. Instead, apps were rushed into use without much public debate. Furthermore, the lack of coordination between the state and the autonomous regions made for a chaotic deployment of tracing and ADM technologies connected to the pandemic.

/ COVID-19 TRACING TECHNOLOGY IN PORTUGAL: WHEN THE GOVERNMENT WANTS TO FORCE CITIZENS TO INSTALL A TRACING APP

"I hate to be authoritarian, but we have to get this pandemic under control," said the Portuguese Prime Minister, Antonio Costa, on 15 October 2020. The day before that, Mr. Costa announced that he was asking parliament to pass an urgent law to make it compulsory for people in Portugal to install the official contact tracing app, called Stayaway COVID.

By then, 1.7 million people had downloaded the app — out of a total population of 10.3 million people — however, the government thought this was not enough. The Portuguese DPA spoke out against making the app compulsory. The guidelines issued by the European Commission and the European Data Protection Board said that countries should make the use of contact tracing apps voluntary. Reportedly, the

expert legal opinion in Portugal was divided. Some lawyers said such a law would be unconstitutional, while others said it might be acceptable because it was aimed at protecting lives.

Soon after, the lack of public consensus forced Mr. Costa's government to withdraw the proposal, and the app was never made mandatory.

Automating COVID responses.
The impact of automated decision-making on the COVID-19 pandemic
Tracing The Tracers 2021 report

December 2021

Available online at https://algorithmwatch.org/en/tracing-the-tracers/

Publisher:
AW AlgorithmWatch gGmbH
Linienstr. 13
10178 Berlin
Germany

Contact: info@algorithmwatch.org

Project lead and editor:
Fabio Chiusi

Authors:
Naomi Appelman, Rosamunde van Brakel, Jose Miguel Calatayud,
Eleftherios Chelioudakis, Fabio Chiusi, Krzysztof Izdebski, Anne Kaun, Maris Männiste,
Ronan Ó Fathaigh, Jill Toh, Bram Visser, Clauddia Wladdimiro Quevedo

Copy editing:
Graham Holliday

Layout:
Beate Autering
https://www.beworx.de/

The project Tracing The Tracers is funded by