May 2020

IN BRIEF

Wilfried Martens Centre for European Studies

Thinking Europe, our Common House

#StayHomeStayInformed

COVID-19 and Technology in the EU: Think Bigger than Apps

Dimitar Lilkov

One of the most pertinent questions posed during the ongoing COVID-19 outbreak is whether technology can be successfully utilised to mitigate the spread of the virus or otherwise limit its impact on everyday life. This In Brief takes stock of the technological measures taken in several Asian countries as a reaction to the outbreak and examines the recent response of European Union member states. The text also maps out workable solutions and important future considerations on the digital front for the EU.

Key Takeaways

Following the practice of separating the wheat from the chaff, European policymakers should sieve workable technological solutions from disproportionate mass surveillance measures, which produce questionable results. The *black or white* choice between safeguarding individual privacy and preserving human health is a false dilemma. There are ways to design digital tools that could help ease lockdown measures and also provide sufficient privacy safeguards. European member states must craft a coordinated digital response, which is not only a workable solution for their citizens but can also serve as a global template when it comes to efficiency, privacy, and proportionality.

Additionally, the debate should not be limited to privacy or individual contact tracing. Sensible technological tools offer several positive opportunities for improving everyday life or organising a better societal response, which is not limited to a digital icon on your phone.

If this health crisis persists longer, the countries that will succeed are the ones who will have managed to adapt public systems and optimise technology for beneficial societal purposes. The states which managed to contain the epidemic more successfully until now have relied on pre-existing infrastructure and governmental planning, along with a smart application of technological measures. Technology (not only limited to contact tracing or surveillance) should be seen as one of the useful tools against the pandemic, not as a master key in the current crisis.

The virus outbreak also has important implications on the European Union`s aspirations of technological sovereignty. Europe's addiction to third-country digital platforms will increase, and many big issues on the exploitation of user data, monopolistic practices, online manipulation, and skewed digital taxation policy will likely remain unresolved. With unrestrained private juggernauts to the West, and hostile state-backed data hoarders to the East, the EU`s case for its own technological model and digital muscle is becoming an ever more daunting task.

There is a certain fear that in the future, the US will provide the software, China will provide the hardware, and Europe, embarrassingly, will only provide the data. COVID-19 might reinforce such trends and make this equation axiomatic. In the coming months, European policymakers must think bigger than apps.

The Asian Response

Several countries in Asia have been praised by medical experts and international media for their response to COVID-19 in recent months. This section briefly summarises the most relevant steps when it comes to technology, followed by a discussion of the applicability of such solutions in Europe.

South Korea managed to grab the spotlight with the array of measures it took, especially after the infamous Patient 31 case, which led to the accelerated spread of the virus. After patients tested positive, officials began tracking their past social interactions using a variety of tools. Surveillance camera footage was used, in combination with smartphone location data and credit card purchase data in order to map out transport routes. The authorities began informing the public via phone alerts whenever positive cases were identified in certain cities, neighbourhoods, and even apartment blocks. People put in quarantine are monitored by a mobile application developed by the Ministry of Interior, which can be used to update symptoms and report the location of the person in lockdown via GPS location and random check prompts.

South Korean legislation provides for complete transparency during a pandemic, and apart from daily briefings and reports, the country has launched a comprehensive online map with precise information about identified cases and outbreak hot-spots. De-tailed input is provided about the routes of identified patients, as well as public buildings or specific locations which have hosted a concentration of cases. The 'travel log' of the infected patient also contains information about gender, age and professional occupation, making the person easily recognisable, which has led to cases of shaming and social stigma. As an additional measure, the government also publishes open data on the availability of masks and other protective equipment across the country which is easily accessible by citizens and businesses alike. The openness of the government to provide this data was a major factor in preventing unnecessary anxiety, or panic buying among the population.

A very similar approach was adopted in **Taiwan**, which also managed to avoid a public lockdown and has kept the number of infected citizens relatively low. Even though the country is not a member of the World Health Organisation, due to China`s diplomatic isolation policy, Taiwan successfully implemented a number of early mitigating measures on its own initiative.

When it comes to technology, the Asian republic conducted rigorous checks of the travel history of each person coming from abroad by relying on huge analytical datasets containing personal information. The country`s health insurance database is integrated with immigration and customs personal records, which gave the government the chance to do individual monitoring and anticipate potential carriers. This personal data was also provided to hospitals and clinics, and used to provide rapid risk assessment of patients and trace new cases.

Foreign travellers were provided with a digital health application on arrival, in order to ascertain their health status and record their contact information. People subject to obligatory home quarantine were given government phones, which receive official calls or notifications prompts to ascertain the location of the individual thanks to cellular data. The effective implementation of this 'digital fence' made sure that thousands of people travelling from risk countries would stay in their homes, or risk paying hefty fines.

Another key feature of the Taiwanese digital response was a combination of civil society initiatives and the willingness of the government to provide open data. Different digital platforms and applications were quickly developed by Taiwanese entrepreneurs in support of the government`s efforts, in an attempt to boost coordination, and democratise the overall digital response. Moreover, the authorities provided an online map listing the availability of masks and medical supplies throughout the country and have encouraged the private sector to make use of publicly available government data.

The response of **Singapore** was similar to the steps listed above, but with an extremely targeted effort on contact tracing among the population. The country relied heavily on designated 'detectives', who had to identify individuals who had been potentially exposed to the virus. Initially, this was done by teams of specialists who used face to face interviews, surveillance footage, and analytical mapping in order to trace the social interactions of patients that tested positive for COVID-19.

Additionally, Singapore rolled out a mobile application called *Trace Together*, as a supplementary tool for digital contact tracing. It relies on Bluetooth signalling, which detects other mobile devices in close proximity and stores encrypted record data in the person's device for up to three weeks.

Should a person become diagnosed with the virus, the application can be used to provide reliable information to the Ministry of Health about the identity of citizens who were most probably exposed to the infection in the past days or weeks.

The most drastic measure when it comes to restraining people in quarantine came from **Hong Kong**, which obliged all overseas arrivals to wear a special wristband that uses geofencing technology to ascertain if a person remains indoors in a fixed location.

Why Copy & Paste Might Fail

The countries studied above managed to contain the virus in March of this year and avoided many of the tougher lockdown measures which were implemented in many countries globally, including the European Union. Although appealing, would a simple copy and paste of such measures really be a guarantee for success in Europe?

First of all, these measures don`t work in a vacuum, and context is needed. They were deployed in societies which had already faced a number of contagious outbreaks in previous decades, such as SARS or MERS. Countries like Taiwan and South Korea have effective policy blueprints which were rolled out as soon as the first COVID-19 cases were confirmed. Citizens were also quick to individually respond to the threat, by heeding health advice; furthermore, they are already used to wearing masks in public. Most importantly, robust biotech firms managed to produce sufficient numbers of testing kits, which were deployed to pinpoint virus hotbeds among the population and provide an adequate estimate of the actual number of infected people.

Second, some of these measures have only been applied for a very limited amount of time and are already showing problematic effects. Using mobile phone data to trace the route of an infected person can tell us a lot about individual activity, but can it provide reliable information about contagion? This type of location data is imprecise and can provide only an approximate radius for movement – perhaps the person was not in a general store, but in a small cafeteria 10 metres across the street. The insights yielded by location data might prove redundant or produce extremely blurry predictions about the spread of the virus to other people.

For the time being, the Bluetooth-based app developed in Singapore shows the most promising results in terms of identification accuracy and safeguarding privacy, as it only records the proximity of contacts and not actual geolocation. Even though Singapore carried out one of the most effective contact tracing efforts globally, the country is facing a new surge in cases and introducing partial lockdowns. Interestingly, one of the main experts involved in the creation of the Trace Together app stated that digital contact tracing can only be used as a supplement to manual efforts, and can also produce a number of unreliable false positives and false negatives. These types of tracing tools are far from being fool proof. Even the most draconian measure applied by Hong Kong to monitor people via wristbands led to technical glitches and only a third of them being operational, with many people under supposed quarantine actually roaming free.

Lastly, copying and pasting digital measures would not prove successful unless there is at least a basic public debate, and corresponding research, about the applicability of such technological tools in Europe. Nobody would deny the need for better testing infrastructure, improved transparency in online reporting of the cases, or enhanced cooperation between the private and public sector via digital tools. But how about using surveillance footage or credit card transactions to map out individual movements? Or rolling out new facial recognition infrastructure to make sure individuals don`t break quarantine?

There is a fine line between adopting useful technological solutions in the fight against the virus, and effectively institutionalising disproportionate surveillance measures, with the risk of some of them becoming a permanent feature even after the health crisis. European governments should also overcome the urge to introduce digital tools that are likely to be unsuccessful but might give the general public the sensation that new solutions are being implemented.

All of this doesn`t mean that the EU should sit on the fence and tackle the pandemic with early XXth century tools. Technology has an important role in this, but European member states need to show that new digital measures are proportionate, useful, and secure before deploying them. Otherwise, they won't be picked up by the population, or simply prove ineffective.

The EU: 'Is there an app for that?'

The debate in Europe has so far centred on data, mobile apps and potential contact tracing. The European Commission was quick to recognise the importance of aggregated and anonymised mobile data, and has requested mobile data in bulk from major European telecom operators, in order to monitor movement among countries and cities. This approach is useful for monitoring large-scale patterns and visualising a movement 'heat map' but can only provide limited information about actual contagion or individual exposure. On the legal front, European data protection rules allow for certain exceptions when there are overriding reasons of public interest or public health. Both the GDPR and the ePrivacy Directive allow for public authorities to process personal or location data in such exceptional circumstances if it is a proportionate measure, allowing for judicial review and only if it concerns anonymised and aggregated data.

In parallel, many EU member states rushed ahead with the creation of national mobile applications as a response to COVID-19. The initial efforts were aimed mostly at designing self-diagnostic mobile applications that provide useful practical information or can be used as a tool to notify health authorities of potential symptoms. Such apps are mostly passive instruments, as they do not perform any form of geolocation or contact tracing of previous contacts. The only notable exception is Poland, which rolled out a phone application that is obligatory for anyone who is under quarantine. After receiving a randomly scheduled prompt from the app, users are obliged to upload personal photos and confirm their geolocation as proof that they are staying indoors.

Journalistic inquiries have reported that the tool has been rolled out extremely quickly, registering numerous technical problems that can make it impractical. Questions also abound about user privacy and the necessity of the government to retain the acquired data for up to six years. Even though the Polish quarantine app scenario is an exception (for now), we are yet again confronted not only with the question of user data, but whether technology is actually efficiently serving the purpose it was created for.

As of mid-April 2020, the focus in Europe has completely shifted to mobile contact tracing. At least a dozen[1] EU/EEA countries have launched, or plan to launch tools that involve digital contact tracing in their national jurisdictions. The growing interest in this tool was prompted by the aforementioned Trace Together app in Singapore and the Bluetooth-based technology to anonymously record close social interactions. The fact that this solution is 'blind' to actual geographic location and can register contacts that were in close proximity (1-2 metres) for a certain amount of time is an encouraging prospect.[2] Privacy experts have commented on potential drawbacks of this technology but consider that this is the least intrusive tracking method compared to alternatives such as GPS or Wi-Fi location data.

The next few months will be characterised by a heated debate about the design blueprint and privacy safeguards of these tools in Europe. Even if we assume that developers get it right on the privacy front, the actual impact of these contact tracing apps remains highly dubious. They need to be adopted by a large segment of society (estimates suggest at least 60 % of the population) and overcome numerous practical challenges when it comes to the elderly and overall digital connectivity. Even the most widespread entertainment or chat applications don't register such high adoption rates in many countries in Europe. The trail-blazing Singapore has registered only about 15 % of its population on the contact tracing application and has reported a large number of inaccurate reports. Even a privacy-friendly and technically fine-tuned app will still require human experts to verify submitted data in order to minimise false notifications. Furthermore, the flawlessness of the design won't be able to compensate for inherent problems – such as the fact that the virus spreads through physical surfaces, not only through humans, or that people might simply decide to disregard digital notifications that they might have been exposed to the virus.

All in all, digital proximity tracing should be seen as a useful complementary tool in the fight against COVID-19. Still, it won't be able to fully replace

1 Austria, Cyprus, Czechia, Denmark, France, Ireland, Italy, Iceland, the Netherlands, Norway, Poland and Portugal as listed by the eHealth Network from 15 April 2020. The UK is also considering its own application.

2 Lots of open questions remain about the set-up and effectiveness of these national contact tracing apps. To name a few: Is the data going to be stored on the individual device or shared on a cloud service? Is this application voluntary to use? How to minimise the number of errors?

manual contact tracing in Europe, nor be a substitute for comprehensive health measures during an outbreak. Given the intricacies involved with the design of these applications and the time needed for their roll-out/adoption, we can only assume that digital contact tracing could be applied in Europe during a second or third wave of COVID-19 later in 2020 or 2021. One can only hope that such tools, if designed and implemented successfully, can be part of the overall strategy aimed at relaxing the current confinement measures in Europe.

A final observation can be made about the EU`s joint effort. Would it be useful to have a cacophony of two dozen different contact tracing apps in Europe with potentially different designs or privacy standards? What would be the point if this data can`t be shared between European countries and used to limit cross-border contagion in the future? The European Commission and the e-Health network have rightfully developed detailed instructions for member states' authorities on how best to design these applications, in order to keep the same technical, encryption, and performance standards across the EU.

It is essential that the roll-out of national contact tracing apps takes place within a pan-European framework, which ensures their effectiveness, proportionality, and democratic legitimacy. Coordination and supranational oversight by the European Commission and the European Data Protection Supervisor would be essential. Most importantly, these digital tools should have expiration dates and be dismantled as soon as the crisis has ended. Such privacy-intrusive measures should always be recognised as exceptional and never allowed to become a permanent feature of policy or technology design.

The Bigger Picture

The debate about technology and COVID-19 in Europe has been limited to contact tracing and its potential design. Important as this debate is, it does feel odd that a lot of resources and political oxygen will be invested in a tool with limited impact on the handling of the crisis. Designing a mobile application certainly corresponds to the modern expectations that tech can improve our daily lives and can serve as tangible proof that governments are actually doing something. However, is this a crowning technological achievement or just a drop in the digital ocean?

The recent pandemic confirms a gloomy observation. We are far from harnessing the true potential of technology in our European societies, both in 'normal' times and during the current crisis. It might be easy to talk about early warnings and prevention in hindsight, but much more can be done. Many European airports, train stations, and ports lack the necessary thermal cameras that perform the basic screening function of people arriving from abroad. For all the talk about big data and Artificial Intelligence, it is embarrassing that many European citizens had no access to publicly accessible anonymised information about the real-time development of the outbreak in their cities and residential neighbourhoods. The inability of many citizens with different symptoms to tap into virtual healthcare or electronic prescriptions during lockdowns has exacerbated the health crisis, both for actual COVID-19 patients and people with other health problems.

European member states needn't become the global outlier Estonia, but they can provide better e-government tools and make better use of technological infrastructure. Improved early warning systems and algorithmic predictions can feed into upgraded public health administrations to trace the outbreak and minimise its impact. If this health crisis persists for a prolonged period of time, the countries that will thrive will be those who have managed to adapt public systems and use technology for beneficial societal purposes - not the ones who have managed to best supervise and profile their citizens.

If there is an actual lesson to be learned from countries like South Korea or Taiwan, it is about the value of open data and public incentives to include both the private sector and civil organisations in the common fight against the virus. A democratised response that manages to involve as many societal stakeholders as possible eases the pressure and improves vital coordination on the redistribution of essential supplies and medical equipment. By the time we have a vaccine or an effective drug, our European society must adjust to living and working in these new conditions.

Technology must be fully optimised, not only for consumer convenience and entertainment, but for better societal coordination, improved working conditions, and democratic participation.

The final point to be raised concerns the relationship with third-country digital companies. Experts and reporters expect the return of *Big Government* as a result of COVID-19, but let's not forget the role of *Big Tech*. Google and Apple have benevolently teamed up and are designing their own contact tracing feature, which is expected to become part of the operating systems of the majority of mobile devices globally. Millions of citizens are relying on Amazon`s services and its supply chains for deliveries across Europe during lockdown. Facebook and Twitter are spreading important news updates about COVID-19, but also serve as fertile ground for conspiracy theories, online manipulation, and damaging disinformation about the virus, which is part of China and Russia`s hybrid warfare manual. Because of their monopolistic features, all of these digital companies have become essential services, especially during the current crisis, which has led some to argue that they are becoming public utilities that need to be regulated and managed accordingly. Even if one disagrees with this notion, fundamental questions remain.

Third-country digital platforms are not only fortifying themselves as the backbone of the European digital economy, they are also developing a growing sway on public debate and even government policy. With an upcoming built-in contact tracing feature, both Google and Apple will turn into gatekeepers of vital information, which will be essential for health authorities in Europe in the fight against COVID-19. These same two companies can provide policy-makers with extremely detailed movement data of their citizens during lockdowns in countries across the globe. Facebook continues to be a global content moderator online and has the ultimate authority over political advertisements on its platform, even if they are spreading falsehoods during electoral campaigns. The current virus outbreak in Europe will further postpone vital decisions about Big Tech's misuse of consumer data, overall transparency, and democratic accountability, as well as the never-ending call for these companies to pay their fair share in taxes.

The coronavirus will likely embed these digital actors even deeper in Europe, while, in parallel, aggressive Chinese companies will continue their quest for growing market access and infrastructure roll-out in the Old Continent. European member states find themselves squeezed between the unrestrained data monopolies from Silicon Valley and the state-orchestrated digital authoritarianism of the Communist Party of China. In this constellation, European technological sovereignty and the improved muscle of the European digital single market are becoming an ever more difficult but urgent necessity.

Dimitar Lilkov *is a Research Officer at the Wilfried Martens Centre, where he is responsible for matters involving the digital economy, energy, and the environment. Dimitar is the host of the Martens Centre's 'Brussels Bytes' podcast series on technology and European policy.*

The Wilfried Martens Centre for European Studies is the political foundation and think tank of the European People's Party (EPP), dedicated to the promotion of Christian Democrat, conservative and likeminded political values.

This publication receives funding from the European Parliament.

Wilfried Martens Centre for European Studies Rue du Commerce 20
Brussels, BE – 1000
http://www.martenscentre.eu