COVID-19 and privacy: a European dilemma

Andrea Renda

TRIGGER Director

8 April 2020

After a shocking beginning (to say the least), 2020 promises to remain a nightmare year through to the end. As many developed countries approach the peak of the (first wave of) the COVID-19 contagion, the world is faced with multiple challenges. On the one hand, there is a need to avoid that the outbreak massively reaches developing countries, where it could lead to even more catastrophic figures in terms of infections and deaths. On the other hand, policymakers in countries that saw the first epicentres of the virus are starting to analyse possible policy measures to allow a swift economic recovery, to avoid an even deeper recession, and hoping not to unlock a new wave of contagion.

Digital technology plays a major role on all these fronts. The experience in South-East Asian countries, and particularly in China, South Korea and Singapore has shown to many political leaders the power of digital technology in facing emergency situations of this sort. Governments in those countries have made massive use of cell phone data to map people movement, which helped in monitoring the outbreak. One country, Singapore, developed an app (*TraceTogether*) that stores a log of anonymous IDs on users' devices, representing users that have been within reach of the device's Bluetooth. If the user tests positive for SARS-COV-2, then he or she receives a code to input into the app; this triggers an automatic, privacy-preserving communication to all other anonymous IDs, which will then receive an alert about their possible contagion. The anonymous nature of these communications makes it, however, in principle impossible for authorities to mandate that informed users undergo testing, or respect restrictive measures.

Other countries have gone way beyond Singapore in their use of technology. For example, in South Korea, a country where the memory of epidemics like SARS and MERS is tragic, apps have been tested since 2015 to enable better monitoring of the contagion. Among the several applications made available in the country at the beginning of 2020, *Corona 100m* alerts users when they come within 100 meters of a location previously visited by a confirmed patient. The app quickly reached more than one million downloads. Other apps, such as *Corona Map* and *Corona Doctor*, provide similar services. The country's Ministry of Health and Welfare also asked travellers from virus epicentres to download a "self-diagnosis" app, to allow government to quickly react to travellers carrying the virus. The combined use of these and other technological means transformed South Korea, a democratic country with a tradition of resistance to authoritarian regimes, into an epicentre of mass surveillance, with extensive use of credit and debit card information, and digital tracking through CCTV cameras and cell phone data to keep the population under control.[1]

In China, the use of technology to contain the spread of the virus has been even more ubiquitous. In addition to the already-existing social credit scoring system, the government obliged citizens

[1] See Yung Wong Sonn, "Coronavirus: South Korea's success in controlling disease is due to its acceptance of surveillance", The Conversation, 19 March 2020.

to download apps, available through Alipay and WeChat, through which citizens report their symptoms. Both health conditions and travel history are used to develop a "colour code", which designates citizens as green, yellow or red. "Yellow" citizens should remain in home isolation, whereas "red" citizens are confirmed COVID-19 patients, who should therefore be quarantined.[2] The government has also coupled the use of apps with enhanced deployment of technology in public places, including facial and body recognition associated with temperature measurement.

All in all, it would be exaggerated to claim that these countries have been able to control the spread of the COVID-19 simply by deploying technology. Lessons learnt during past epidemics have led these countries to develop a much more resilient health system, something that cannot be stated for most European countries, as well as the United States. However, widespread penetration of wireless broadband and mobile payments, coupled with very loose privacy laws and a culture of mass citizen surveillance (in China), offered governments a very useful ally in the fight against the virus. Regretfully, fundamental rights like privacy and self-determination, as well as the freedom of movement and association, seem to have been further compressed in this time of emergency, and there is no clear timeframe for going "back to normal".

Technology and COVID-19: the European dilemma

Faced with the emergency, European countries have adopted a variety of policy measures to counter the spread of the virus. Initially, technology did not play a major role. Compared with what happens in China or South Korea, European citizens do not yet make the same massive use of mobile payments and are therefore less easily traceable through credit card data. Digital identity is still rather under-developed; and even if smartphones are ubiquitous among the population, strict privacy laws have kept government surveillance largely at bay. Accordingly, most European countries have initially faced the virus through testing, and Non-Pharmaceutical Interventions such as quarantine, isolation, and the lockdown of entire cities, regions, and often whole countries.

The reproduction factor of the COVID-19 has however remained very high, testifying of a serious difficulty in keeping the outbreak under control. Governments and EU institutions are thus turning towards technology as a lifeline in the fight against COVID-19. Similarly to what occurred in Asia, there are at least four different ways in which digital technology is being used to help in the fight against the virus. First, smartphone apps can be used to enable voluntary self-reporting of symptoms, which can help public authorities monitor the situation and issue isolation and quarantine orders: this is what new applications like *SymptomTracker* do.[3] Second, technology can help governments map the movement of the population on the territory, mostly through cell data tracking and modelling. Third, apps can help health authorities become more accurate and precise in choosing who should be tested, similarly to what *TraceTogether*, or the *PrivateKit* application developed at the MIT do. Fourth, technology can be used to track individual patients' movements, which in turn helps in the enforcement of policy measures such as restrictions of movement, and potentially goes as far as sending alerts to users, warning them that a user that recently tested positive for COVID-19 is within Bluetooth reach.

European governments are already experimenting with a variety of such solutions. In Germany, Austria and Italy governments have reached data-sharing agreements with telecommunications companies. In Spain to Romania, Slovakia, Poland, apps have been developed, whereas Italy is

[2] See Helen Davidson, "China's coronavirus health code apps raise concerns over privacy", The Guardian, 1 April 2020.
[3] See https://covid.joinzoe.com/

selecting among dozens of proposals to select the app that most suits its needs. At the EU level, the Commissioner for Internal Market and Growth Thierry Breton held talks with executives from large telecom operators, asking them to share "anonymised mobile metadata to help analysing the patterns of diffusion of the coronavirus."[4] Breton later noted that data would be used in anonymised form to anticipate the spread of the pandemic and plan the supply of medical equipment, and that data would be deleted as soon as the crisis comes to an end.

All these initiatives have been undertaken in an emergency situation, often not the most appropriate moment to strike accurate trade-offs between fundamental rights. Accordingly, concerns have emerged that both during and after the "lockdown phase", the widespread deployment of technological solutions may lead Europe into a new age of mass surveillance.[5] After all, some EU Member States (Hungary and Poland above all) are already witnessing attempts to use the pandemic as grounds, or excuse, for authoritarian power grabs.

Privacy and Public Health: friends or foes?

To be sure, this trade-off between privacy and public health is not new. Already in 52 BC, Cicero observed in his *De Legibus* that "*salus publica suprema lex esto*" (people's well-being shall be the supreme law). Since then, the idea that in extraordinary times, in which a nation is threatened at its core, some rights may be compressed to prioritise public health or safety has been at the centre of the debate. For example, when Louis Pasteur (1822–1895) and Robert Koch (1843–1910) started the bacteriological revolution in public healthcare, providing scientific backing for already-existing practices such as quarantine, sharp resistance emerged in many countries, based on the fear that the imposition of such measures would limit the freedom of movement of people and goods. The fights against tuberculosis and smallpox, and later HIV and Ebola, created tensions between the protection of public health and other fundamental rights, including personal privacy, over the course of more than a century. A similar compression of civil liberties is also seen in other fields, such as in the fight against terrorism.[6]

In 1966, the International Covenant on Civil and Political Rights provided that, in times of a public emergency threatening the life of a nation, the need to protect public health is a permissible ground for limiting certain rights, including the liberty of movement, freedom of expression and the right to freedom of association. In Europe, this possibility must be gauged against extremely high standards when it comes to privacy and data protection, with far-reaching provisions in EU Treaties, as well as in the European Convention on Human Rights, the EU Charter of Fundamental Rights and the General Data Protection Regulation, which firmly established privacy as a fundamental right, and data ownership as belonging to individuals, not States. The EU Charter of Fundamental Rights specifically mentions both the need to ensure protection of personal data (Articles 7-8) and "a high level of human health protection" (Article 35) in the definition and implementation of all Union policies and activities.[7] Article 15 of the

---

[4] See Samuel Stolton, "EU's Breton defends COVID-19 telecoms data acquisition plans", Euractiv, 26 March 2020.

[5] See Hans Kundnani, "Coronavirus and the Future of Democracy in Europe", Chatham House, at https://www.chathamhouse.org/expert/comment/coronavirus-and-future-democracy-europe

[6] See Eran Shor, Leonardo Baccini, Chi-Ting Tsai, Tai-Ho Lin & Titus C. Chen (2018), Counterterrorist Legislation and Respect for Civil Liberties: An Inevitable Collision?, Studies in Conflict & Terrorism, 41:5, 339-364, DOI: 10.1080/1057610X.2017.1314653

[7] The successful invocation of any of the legitimate purposes attaching to the second paragraphs of Articles 8 to 11 of the Charter is contingent upon compliance with two vital conditions: that the interference, or limitation, is prescribed by, or is in accordance with, law (the "rule of law test"); and that it is necessary in a democratic society in pursuit of one or more of the second paragraph objectives (the "democratic necessity test"). See i.a. Janneke Gerards, How to improve the necessity test of the European Court of Human Rights, International Journal of Constitutional Law, Volume 11, Issue 2, April 2013, Pages 466–490; and EDPS (2016), at https://edps.europa.eu/sites/edp/files/publication/16-06-16_necessity_paper_for_consultation_en.pdf.

European Convention on Human Rights allows for derogations, provided that they are temporary, proportionate and strictly required by the exigencies of the situation. And the European Data Protection Supervisor has already clarified that measures that weaken the protection of the right to privacy should comply with both a necessity and a proportionality test.[8]

But what is necessary, and what is proportionate in the face of such crisis? Governments are likely to struggle to answer these questions. Restrictions of privacy that do not prove essential to save lives, or allow the continuation of essential economic activity, are unlikely to be found necessary. And the availability of feasible privacy-preserving alternatives should rule out the possibility of implementing intrusive policies, even if temporarily, as these would fall short of meeting the proportionality test. The European Data Protection Supervisor has issued dedicated guidance on the two tests, but the need to act quickly in a pandemic may lead governments to rush the tests in their attempt to try all possible measures.[9]

The COVID-19 crisis is already creating trade-offs between the need to safeguard public health and the limitation of certain civil liberties. Estonia, Latvia, and Romania have already notified the application of Article 15 ECHR;[10] and a recent collection of guidance documents shows that countries like Ireland and Poland are implementing a rather permissive approach to data processing activities.[11] The list of national measures, ranging from cooperation between governments and mobile operators to developing tracking and alert applications, gets longer every day.[12] The concern is so strong that in a diplomatic statement adopted on 1 April 2020, thirteen Member States announced that they were "deeply concerned about the risk of violations of the principles of rule of law, democracy and fundamental rights arising from the adoption of certain emergency measures." The countries also observed that "emergency measures should be limited to what is strictly necessary, should be proportionate and temporary in nature, subject to regular scrutiny, and respect the aforementioned principles and international law obligations. They should not restrict the freedom of expression or the freedom of the press."[13] The concern becomes even stronger if one considers that EU institutions have proven to have rather weak tools to contrast violations of the rule of law in Member States.[14]

Europe after the lockdown: hyperconnected, or hypercontrolled?

Will this emergency period lead some countries, even in Europe, to establish a regime of mass citizen surveillance?[15] The risk is real, notwithstanding all the constitutional safeguards that exist in Europe, which stand in defence of our democratic societies. If anything, governments would be tempted by the fact that citizens in emergency situations tend to display through higher-than-average approval rates for their political leaders, and appear animated by a sort of "Stockholm syndrome", which makes them easily prey to would-be captors. For example, after the terrorist attacks towards Charlie Hebdo and in the Bataclan, French citizens reportedly became more willing to trade their privacy in exchange for enhanced security, in a clear manifestation of what behavioural scientist call "availability bias".[16]

---

[8] https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf
[9] https://edps.europa.eu/sites/edp/files/publication/20-01-28_edps_quickguide_en.pdf
[10] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005/declarations?p_auth=oC00wpDO
[11] https://www.hldataprotection.com/files/2020/03/Coronavirus-and-Data-Protection-Guidance-by-DPAs-Hogan-Lovells-1.pdf
[12] https://www.top10vpn.com/news/surveillance/covid-19-digital-rights-tracker/
[13] https://www.government.nl/documents/diplomatic-statements/2020/04/01/statement-by-belgium-denmark-finland-france-germany-greece-ireland-italy-luxembourg-the-netherlands-portugal-spain-sweden
[14] https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/642280/EPRS_BRI(2019)642280_EN.pdf
[15] https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75
[16] https://onlinelibrary.wiley.com/doi/10.1111/pops.12439

The temptation should however be firmly resisted. A widespread, intrusive use of technology is unlikely to pass the necessity and proportionality test specified by the EDPS, for several reasons outlined below.

First, the successful experience of countries like Hong Kong, South Korea and Singapore can be traced back to a mix of measures, including enhanced levels of preparedness (also due to the legacy of SARS in those countries), a well-developed health infrastructure, massive use of testing and very rigid enforcement practices. There is no evidence that deployment of technology, alone, can contain the virus, unless European countries manage to invest in more generalised testing. As a matter of fact, Taiwan appears to have achieved similar results through widespread testing, enhanced preparedness, and a less intrusive use of technology: all quarantined patients are being monitored through their mobile phones in what has been termed "electronic fence", but there is generalised surveillance of the population.[17]

Second, technology has important limits. Geolocational data via GPS are relatively inaccurate, especially outside densely populated areas, and can only be used to monitor the effectiveness of social distancing measures, rather than to sanction citizens directly.[18] Even in urban areas, phones are typically able to determine their position with an accuracy between 7 and 13 meters. And Bluetooth data vary in intensity depending on the location and the distance between the devices, in a way that is often hardly predictable. This, in turn, means that the intensity of the signal cannot be used as a proxy of the actual distance, which undermines the possibility of using Bluetooth to single out cases of possible contagion, especially in crowded public spaces.

Third, data collection and transfers can be hacked. For example, hackers can reidentify anonymous and ephemeral IDs from infected people by modifying an app and collecting extra information about identities through additional means, such as a surveillance camera to record and identify the individuals. Or, antennas can be deployed to eavesdrop on bluetooth connections to learn which connections correspond to infected people, and then estimate the percentage of infected people in a small radius of 50m. If in addition, the adversary has a camera, he can capture images and potentially re-identify those people.[19]

Fourth, the use of apps for self-diagnosis and reporting, similar to the "colour code" app deployed in China, might be easily gamed or boycotted by citizens outside countries that rely on surgical enforcement practices such as China or Singapore. The level of social acceptance in the event of such measures, especially if applied to a population already in lockdown, would be much lower in European countries compared to where they have been successfully applied, unless enforcement becomes rigid and intrusive: but this would not be possible with the privacy-preserving apps currently being developed in Europe.

Fourth, widespread use of technology is being presented as a temporary measure, but there is no guarantee that governments will roll back such a powerful set of instruments once the pandemic is gone. Even when the risk has faded away, assuming that this will be an uncontroversial truth, governments may use other risks, such as cyber-attacks or terrorism, as grounds for keeping the functionality in place. The head of the EDPS, Wojciech Wiewiórowski, recently stressed in a letter to the European Commission that "such developments usually do not contain the

[17] See Yimou Lee, "Taiwan's new 'electronic fence' for quarantines leads wave of virus monitoring", Reuters, 20 March 2020.
[18] The *PrivateKit* app developed at the MIT, however, was already used to alert the police of large gatherings occurring in public places.
[19] See Troncoso et al. (2020), "Decentralized Privacy-Preserving Proximity Tracing. Overview of Data Protection and Security", Version update at 3 April 2020, retrieved from Github.

possibility to step back when the emergency is gone", and that data sharing between telecommunications operators and governments should be recognised "as extraordinary".[20]

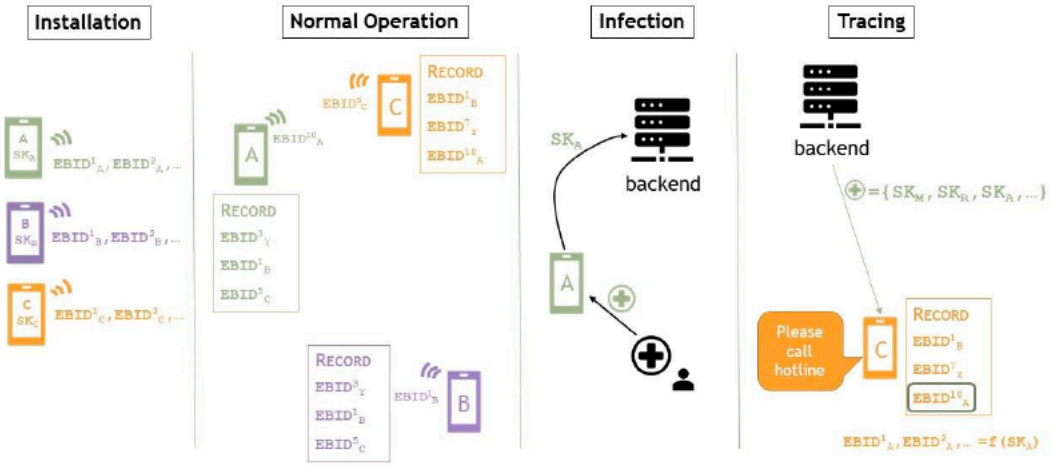
That said, there is no doubt that digital technology can, and will be a useful aid once patients have been diagnosed with COVID-19. In this case, restrictive measures such as isolation and quarantine can be usefully implemented with the help of tracking systems, without necessarily affecting the individual right to privacy. One such proposal is being developed in Europe, thanks to international collaboration.

The PEPP-PT proposal

Europe's technology community has responded to the virus in a more united and cooperative way than the Member States. One good example is the international effort of 130 between research institutions and corporations from eight EU Member States, aimed at developing a privacy-preserving app.[21] Researchers involved in the so-called PEPP-PT (Pan-European Privacy Preserving Proximity Tracing) observed that "some infrastructures that can enable proportionate proximity tracing may fail to protect data, or be misused or extended far beyond their initial purpose and beyond the lifetime of the crisis"; and that designs with centralized components, where a single actor, such as a server or a state, can learn a great deal about individuals and communities, need specific attention because if they are attacked, compromised or repurposed, they can create greater harm". Modern digital technology allows for completely decentralised design, which does not entail any centralized collection and processing of information on users.

In the PEPP-PT model, all smartphones obtain an ephemeral ID. When a patient is diagnosed with SARS-COV-2, and only with their consent and with authorization from a health authority, they use their phone to upload specific data to the backend server. From this data, the identity of the patient cannot be derived by the server or by the apps of other users, it is nearly anonymous. Before this point, no data other than the ephemeral ID leaves the phone.

Figure 1 - Phases in the decentralized proximity tracing system



Source: Troncoso et al. (2020)

[20] https://edps.europa.eu/sites/edp/files/publication/20-03-25_edps_comments_concerning_covid-19_monitoring_of_spread_en.pdf.
[21] See https://www.pepp-pt.org/

The system appears to be fully in line with the principles of data protection by design, data minimisation, purpose limitation, and security. In addition, end users participate voluntarily, and every data communication happens subject to their explicit consent. It also prevents function creep, for example for law enforcement or intelligence purposes, by strictly limiting how the system can be repurposed with cryptographic methods.

While the system has important advantages in terms of near-perfect privacy protection, one must be aware that its operation and impact depend on a variety of factors, which are more human than technological. First, the system requires widespread testing. There is not technological alternative to a massive investment in tests. And even if a high number of RNA-based tests is carried out, the technology-enhanced system would not enable the identification of the apparently high number of asymptomatic patients, who could be spreading the virus without knowing. In principle, both serological tests (allowing the detection of protected individuals who have been infected by the virus and have recovered) and tests based on an RNA diagnostic (which are only valid just before and during the infection) would be needed to fully increase the awareness of who, among smartphone users, is positive.[22]

Second, absent a widespread double-testing as described above (which is still difficult, as serological tests are still being developed and are currently unreliable), the system would require constant, repeated testing of random samples of the population. Especially in the post-lockdown phase, or in countries where NPIs are relatively permissive, individuals may test negative and later be infected. The Bluetooth-based system would not capture in real time new infections, so it still requires a massive amount of testing on the population.

Third, the system is voluntary. This presupposes that users download the app, and if they are later diagnosed with SARS-COV-2, follow the PEPP-PT procedure. If the whole procedure is anonymised, then any control measure on quarantined patients would not be possible. If anything, there would be a need to two parallel processes: an anonymised one, based on PEPP-PT, aimed at informing possible infected patients that they should take action; and a direct, personalised control aimed at ensuring that patients respect the quarantine. Measures such as random phone calls, location tracking, police enforcement would still be needed despite the operation of the PEPP-PT.

Fourth, the system essentially requires widespread, if not ubiquitous diffusion. Once a user tests positive, the spread of information to all the other ephemeral IDs collected requires all other involved users to have downloaded the app and opted into the data collection system. As a result, the success of the system requires that governments mandate that all citizens download the app.

Fifth, if the system if ubiquitous, then the PEPP-PT system may not be able to retrieve sufficiently actionable information whenever an individual has been visiting very crowded places such as a train station, subway, or a large marketplace. A user diagnosed with SARS-COV-2 would then trigger dozens of alerts to other users: if the contagion spreads quickly, users may receive several alerts a day: they may therefor start ignoring or downplaying the receipt of an alert message, which in turn would hamper the functioning of the system. Behavioural economics has long explored the propensity of individuals (especially if asymptomatic) to correctly gauge very low probabilities. The recommendation to take action, absent a legally enforced obligation, may not lead to a sufficient response on the side of alerted individuals. And in reality, if approaching health authorities to take the test is not made easier after a user has received the alert, the

[22] See Mathias Dewatripont, Michel Goldman, Eric Muraille, Jean-Philippe Platteau, "Rapidly identifying workers who are immune to COVID-19 and virus-free is a priority for restarting the economy", Voxeu.org, 23 March 2020.

difficulty of "taking action", let alone the lack of availability of testing equipment and material, may frustrate even the most proactive citizens.

Against this background, the work on PEPP-PT is unlikely to eliminate the temptation to use more intrusive (even if analogue) means to enforce restrictive measures. Health authorities may still need to identify the infected individuals, and public enforcers would need to ensure that the infected ones stay home. The expectation, therefore, is that many governments will want to go beyond PEPP-PT in devising ways to mitigate the impact of the pandemic, and this should keep the attention of privacy advocates as high as possible, compatibly with the emergency situation.

Surviving without surveillance

In the coming weeks, policy trade-offs between the protection of privacy and the need to safeguard healthcare will become almost inevitable. When the peak of contagion is passed and lockdown policies released to help the economy recover, will governments start implementing new systems, which warn citizens whenever they are interacting with infected individuals? Will these measures be purely anonymous, and thus potentially ineffective, or more intrusive, and thereby likely to impinge on user privacy? What if intrusive measures are presented as justifiable due to the need to balance privacy protection with the equally important fundamental right to free movement (of the non-infected)?

This is neither the first, nor the last time governments face the temptation of technology-enabled mass surveillance to secure society. In the future, especially with the rise of the Internet of Things and advances in Artificial Intelligence techniques such as body and facial recognition, the temptation to engage in surgical technological monitoring will become even stronger, and the potential benefits will skyrocket along with the associated risks. This is why establishing clear boundaries is essential to guide governments both in times of emergency, and when, hopefully soon, a less constrained course of life will again become possible.

Whatever measure will be adopted, some key principles will have to be respected. The measure must be temporary, even if obligatory. Citizens must be informed any time a data collection and retention system is used, be data locally or centrally stored. The measure should be necessary and proportionate, which implies that the measure be useful in the first place: at one extreme, untargeted, mass violation of citizen privacy would not be tolerable; but at the other extreme, systems that remain so private that they are unenforceable are equally preposterous. And whatever balance is struck between these two extremes, it will need to be temporary, and such temporary nature should be easy to verify by citizens. After all, as most authoritatively observed, it is important to remember that European law – the European Convention on Human Rights, the Charter of Fundamental Rights of the European Union, even the Lisbon Treaty – is the result of an attempt to exorcise the ghosts of totalitarian government in most of the continent in the 20th century.[23]

The fight against COVID-19 is likely to prove tough and will leave many victims behind. Technology can help save some lives, but does not replace traditional methods of public health protection, and should therefore approached not as a panacea, but as a useful help, to be handled with due care. This way, hose that will survive, will survive as free individuals.

[23] https://edps.europa.eu/sites/edp/files/publication/16-04-21_counterterrorism_data_privacy_en.pdf