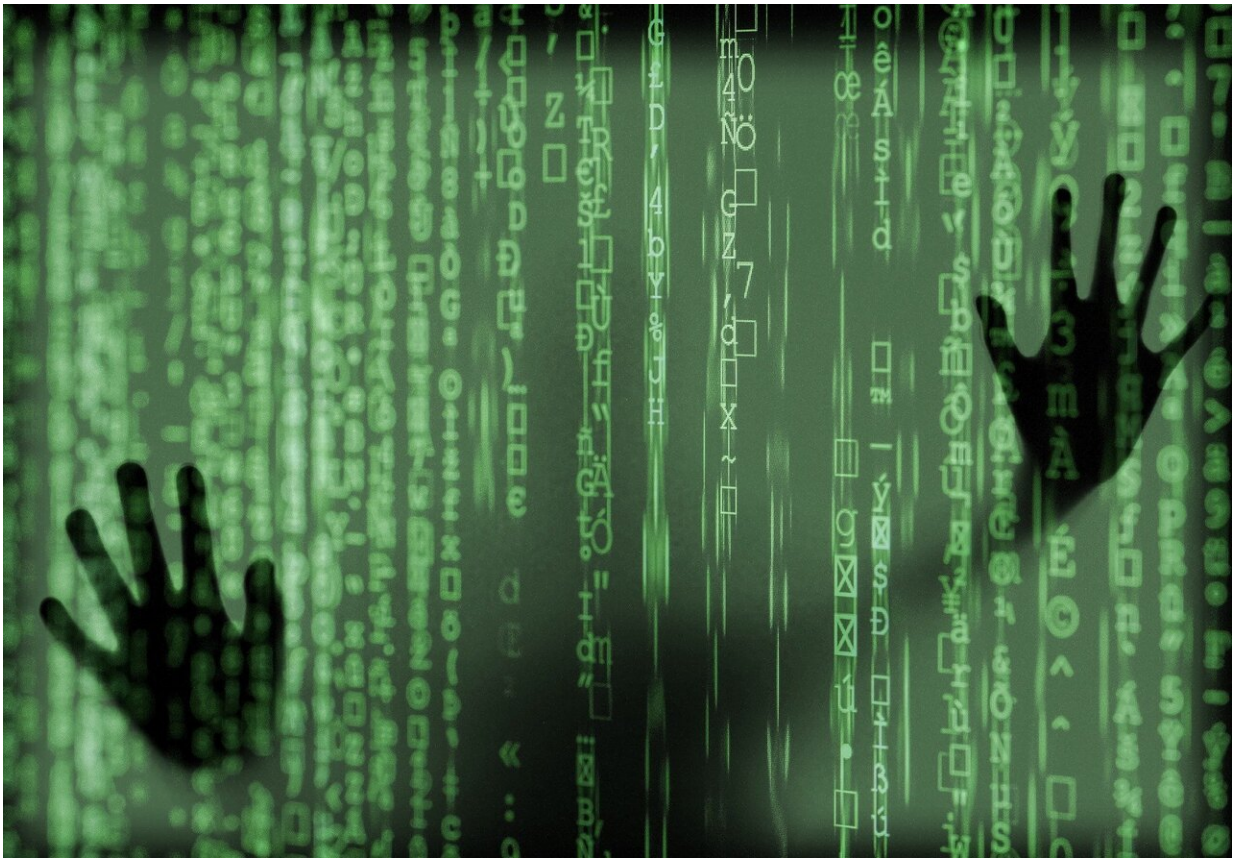
Digital privacy and COVID-19: between a paradox and a hard place

November 17 2020, by Florencio Travieso



Credit: CC0 Public Domain

The situation in which the world is currently living is extraordinary in every sense of the word: since the outbreak of the COVID-19 pandemic, there have been over 53 million confirmed cases and more than 1.3

million people have died. After a round of lockdowns in the spring and deconfinements in the summer, the much-feared "second wave" has emerged in many countries, plunging us again into the unknown.

From a legal perspective, it is understandable and justifiable that in such times, civil liberties might be temporarily restricted through legal instruments that embody the legality and proportionality of the measure (legal authorization, proper authority in charge and duration in time or scope of the decision, reasonability of means), the respect of constitutional rights (privacy of users) together with mechanisms to provide public safeguards (data controllers, independent authorities or watchdogs).

This article reflects on the measures that countries have taken to monitor their residents so as to effectively trace COVID-19 cases. The search for a balance between the expression of public policy and the respect of basic civil liberties is, traditionally, an essential question behind a complex legal situation.

The temptation to mishandle the restriction of rights

Certain nations have been sufficiently focused on contact tracing that methods have been used that would be highly criticised in Western countries. For example, in South Korea, authorities used location data from cell phones, credit-card transactions, and CCTV footage to identify potentially infected persons. As noted Jung Ki-suck, the former director of the Centers for Disease Control and Prevention (CDC), "people [in South Korea] are OK with their privacy being infringed for the wider public interest."

China is another much-cited example: the country's applications, which are mandatory, use facial recognition, biometric data, location tracking and other data to generate health-status colour codes. An analysis by *The*

New York Times of one of the apps indicated that it appeared to share information with police authorities. Even the basis on which the colour codes are assigned is unclear, and while the lack of transparency has been criticised, Chinese authorities are not known for their openness.

On May 4 the Hungarian government adopted a decree, 179/2020, in which data protection and access to information rights were restricted during the "state of danger." Exercise of essential rights under articles 15 to 22 of the European Union's General Data Protection Regulation (GDPR) – right of access, rectification, erasure, restriction of processing, etc. – were suspended. The decree also authorised the prime minister to rule on legislative matters without defining an end date. After pressure, the authorities finally lifted the restrictions on June 16, the same day a complementary law gave the executive the power to restrict freedom of movement or assembly for six months.

However, restrictions on data-protection rights should only be of legislative nature (issued by the parliaments), and not decided unilaterally by the executive branch (a decree). This legal nature of the restriction is protected by Article 52(1) of the Charter of Fundamental Rights of the European Union, article 8(2) of the European Convention of Human Rights, and, more recently, article 23 of the GDPR.

Restrictions of certain rights, from a legal perspective need to be:

- of an exceptional nature.
- imposed for a limited duration in time (temporary)
- not to be applied retroactively
- subject to clear and defined conditions (criteria of "foreseeability").

France developed an application, StopCovid, based on Bluetooth technology—and voluntary adoption—that aimed to be less intrusive. It

was first released on June 2 but was downloaded by less than 5% of the French population. By comparison, the equivalent UK application was downloaded by 20% of the population and the Irish application by 35%. The low adoption rate of StopCovid meant that not only that the application was inefficient, but it also revealed a certain apprehension from French users. Indeed, even before the application's launch, the then–Minister of Interior, Christophe Castaner, stated that digital tracing was "not in French culture."

On October 22, an updated version of the application was rolled out, now called TousAntiCovid (United Against COVID). It was downloaded more than 4.5 million times over last week of October, a better adoption rate than the first version. Part of the reason could be that it can be switched off, facilitates the creation of documents allowing travel and provides information on and access to medical and testing facilities. It is still too early to determine its efficiency.

Earlier epidemics

How much has humanity learned from past events? A few somewhat recent examples can be revisited: the Influenza H1N1 pandemic in 2009 and the Ebola outbreak in 2014.

During the Ebola outbreak, similar questions and issues were discussed, including contact tracing and community monitoring. (One of the lessons learned was that the measures had taken too long, something that's familiar to us all now.) A 2015 study by Yaneer Bar-Yam, Vincent Wong, and Daniel Cooney) showed that community monitoring—tracking a larger group of people and treating all of them as if they had been in contact with someone infected—was more effective than contact tracing.

In the first stages of the COVID-19 pandemic, testing was not easily

available, hence the nationwide lockdowns; subsequently, testing capacities have been developed and contact tracing and isolation emphasised.

Authors such as María Lucrecia Rovaletti have also analysed contact tracing on HIV cases and use and dissemination of information on patients on databases. The discussion revolved around the importance of determining the personal and sensitive character of information and to restrict access to statistics and medical research only.

Contact tracing apps are not a magical solution to the spread of COVID-19. Multiple issues are at stake, from privacy to technology options and politics and public health. Systems are divided between centralised and decentralised, and based on voluntary or mandatory use. As seen, countries like South Korea deployed both an active behavior of the state intervening in the supply chain for medical supplies, but also a technological strategy that actually invaded users' privacy.

European models, where citizen are more conscious of their privacy rights, have been based on the voluntary downloading of the apps and legal constraints from GDPR. On the technological side, Google and Apple developed a decentralized system that used servers to collect information on exposure alerts. But this system comes with a cost for privacy of users, as these companies hold the key to the data obtained. It is true that it is encrypted, anonymised, and limited by Bluetooth, but with current technology, reverse engineering the source data would not be a particularly difficult task.

Centralized systems such as France's TousAntiCovid keeps the information on users' phone. It uses temporary pseudo-identifiers (anonymous string of letters and numbers) to collect information, using a protocol called ROBERT (ROBust and privacy-presERving proximity Tracing protocol), developed by the technology research hubs Inria

(France) and Fraunhofer AISEC (Germany). Data will only be analysed by the government in case of a COVID-19 diagnosis, and only when analysed the user has given her or his explicit consent. A positive diagnosis of a possible contact will be shared with users without including any personal data. Data stored in the phone and server will be deleted after 14 days.

How long is "temporary"?

When tackling urgent public situations, states can sometimes decide to (temporarily) empower the executive branch to fast-track regulation. It involves placing the parliament (national congress) in a second frame, generally by delegating those powers to, again, the president or prime minister.

How long is "temporary" is the key question. The risk today is that urgency has become normality, in the same way that working from home, wearing face masks, and keeping physical distances have become the rule. They're the new normal. The reason for a state to start rolling back those temporary powers is both clear and vague. Clear because those restrictive measures will stop once the virus is no longer a menace for public health. And in this lies the vagueness of the concept. The virus could linger for years and thus "temporary" measures could remain in force for a long time.

Once we as a society have accepted such infringements in our privacy and civil liberties, when will they be lifted? Emergency measures, once considered temporary, can easily become the norm, part of the usual legal scenery in a country. Under certain regimes or countries, the temptation of utilizing these methods for reasons other than COVID-19 are enormous.

What can states do with the data collected?

The first (and the main) goal of collecting data from users is to track social contacts and stop contagion. This would allow states to enforce measures such as lockdowns and quarantines at the same time that the populations are being (for public health reasons) monitored. But by accessing these data, we can also extract information on people on different grounds—revenues, political opinions, even sexual orientations.

From a human-rights perspective, if a country decides to restrict citizens' rights during an emergency situation, the measures must be lawful, necessary and proportionate. A state of emergency based on public health must be limited in time, and no measure can have an indirect collateral effect on specific populations (minorities or marginalised groups, for example). The Americans Civil Liberties Union (ACLU) has stated that "if measures are time-limited and have a rational basis in science," they can be acceptable.

In countries such as Israel, Armenia, Russia and Ecuador, governments have access to the telecommunication companies or satellite information that allows them to identify infected people and monitor self-isolation or quarantines.

Digital contact tracing, privacy and civil liberties

The use of algorithms and artificial intelligence can enable the processing of enough data from users to predict the spread of the pandemic. This is in principle useful, as societies can monitor the situation almost in real time and take quick measures (health policies) to adapt and adjust.

A global pandemic could, in principle, convince people to accept a

certain level of restriction in their civil liberties that could imply a surveillance regime. A logical trade-off must take place, between civil liberties, security, public health, and risk avoidance, and these restrictions can take the shape of smartphone applications

Central to this discussion is the trade-off between individual privacy and the need to protect public health. Short-term restrictions of individual liberty are enacted to protect the long-term interests of communities. These restrictive measures include, in our opinion, the seed of a potential abuse.

A noteworthy example of mass-surveillance measures has been the EU directive 2006/24/EC (March 15, 2006) on the retention of data by electronic communications services and networks. Enacted after the Madrid (2004) and London (2005) bombings, it required member states to adopt measures to ensure potentially relevant data is retained. However, in 2014 the measure was annulled by the Court of Justice of European Union (CJEU). It stated that the directive entailed "a wide-ranging and particularly serious interference with the fundamental rights to the respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary."

The example of South Korea, which gathered—and presumably continues to gather—a nearly unlimited amount of data on its citizens, demands an enormous responsibility on the way it is processed and released—policies must guarantee privacy, regulate the way data is analysed, reduce risks of leaks and guarantee its destruction after the pandemic ends. China has gathered even more data, but given the nature of the country's government, its destruction seems unlikely.

Data access, processing power and a guardian

In this sense, a one-side solution cannot be imagined; it must be done in

coordination of multiple players. As stated by Georgios Petropoulos, a research fellow at MIT on Digital Economy, the telecommunication companies have access to individuals' data and the high-tech industry have the tools to process it, and the state must oversee how it is processed and respected.

As a safeguard, contract-tracing phone apps should be voluntary, guaranteeing users anonymity, data collected should only be needed for the tracing, data retention should be limited to the actual measures, and access to the privileged data should only be given to specific people. Strictness that we usually find in the respect of health data privacy of individual users.

As the crisis continues to unfold, topics such as civil liberties and privacy have been placed in the centre of the scene. In an April 2020 interview for *The New Yorker*, European commissioner Margrethe Vestager asserted that we've reached a point where we might be able to trust our privacy to the technology that we use in our daily lives. How society as a whole reacts to this question might take longer, however.

Provided by The Conversation