Hogan Lovells

# The digital war to COVID-19: possible solutions at the crossroads of competition and regulatory checkpoints

8 April 2020

**A worldwide race.** Researchers and technologists in these days are scrambling to build apps that alert users when they have come into contact with people infected by coronavirus, as governments weigh up how to safely transition out of national lockdowns in the months ahead. Numerous mobile apps are being developed to enable the so-called contact tracing, namely, in a nutshell, the possibility for people to take preventive action and immediately exchange proximity and location data, in order to notify someone who has recently been near to an infected individual, by means of smartphones' "virtual handshaking".

Digital tools providing for mobility information services are already a market reality with an extensive user-base. The popularity of such tools will be further strengthened in the aftermath of the current emergency. In addition to the facilitation of social distancing during and after lock-downs (having succeeded in flattening the curve of the pandemic wave), they may be used in the long-run as platforms to run supplementary functions and achieve additional goals, such as, for instance, providing users with a tool to constantly self-asses their own health conditions, mapping the spread of viruses for the purposes of promptly halting any future hotbeds, setting up large scale of immunity tests and monitoring the progressive growth of herd immunity within communities.

Governments as well as public and private organizations around the globe are thus involved in a frantic race. The common goal, in this phase, is to come up as soon as possible with the most effective technological response to the emergency with the aim of temporarily embanking the virus spread pending the availability of a vaccine and medical treatments. Technologies developed in this phase may then become an important part of citizens' lives even after the end of the current emergency.

The successful development and diffusion of these tools is a hopeful and much-awaited step in the battle against COVID-19 but triggers a conundrum of various legal issues including data protection, regulation, and competition.

**Systems in place and projects in the pipeline.** The worldwide acknowledged paradigm of the winning technological response to Coronavirus, thus far, is South Korea. In general, effective

contact tracing so far has been one of the major ingredients of the successful response to the COVID-19 outbreak put in place by this nation, along with early detection and fast intervention methods, including massive, repeated and decentralized testing of patients, selective isolation of infected individuals (as opposed to total indiscriminate lock-down of communities) and pro-active cooperation between public authorities and citizens. The South Korean government has for weeks been using data collected from cellular networks, GPS systems, credit card transactions and video surveillance cameras to track the population's movements. The information collected is then shown anonymously on a dedicated website and, if necessary, sent via SMS to those who may have come across an infected person. By following the same model, other Asian countries have shifted to developing IT tools with the aim of slowing down the spread of the virus.

China, for obvious reasons, is among such countries and a front runner in the race. The Chinese government, in cooperation with a number of bodies, has developed and launched across the whole country since February 2020 the "Close contact detector", an app that allows people to check whether they have been at risk of catching the coronavirus, tells users if they have been near a person who has been confirmed or suspected of having the virus. People identified as being at risk are advised to stay at home and inform local health authorities.

In following the same path, Singapore, Hong Kong and Taiwan have all developed contact tracing smartphone apps that record symptoms and track users' movements, in some cases triggering an alarm if the device leaves a quarantine area. India, another very densely populated eastern country, is also rapidly developing its technological response to COVID-19. The government has announced the launch of the "Aarogya Setu", app - meaning "bridge of health" - which uses Bluetooth and location services to track if a user came into contact with a person "who may have tested COVID-19 positive". If a user of this app tests positive, the government will contact all other registered users that the infected person came in contact with over the last 30 days.

Also, on the western frontier of the technological fight to COVID-19, work is very intense. In the US, several groups (Covid Watch, CoEpi and NextTrace) using similar technology have made their projects public in recent weeks.

Italy, one of the countries after China most affected by the pandemic, is acting in parallel on two fronts, namely at the national and regional level. With regards to the former, it is getting to the heart of the matter, the "Innova per l'Italia" (a joint initiative of the Ministers for Technological Innovation and Digitization of Economic Development and of University and Research) call for action is addressed to companies, universities, public and private research centers, associations, cooperatives, consortia, foundations and institutes that, through their technologies, are able contribute in the digital sector for the prevention, diagnosis and monitoring for the containment and prevention of the spread of COVID-19. On the regional front, the twenty Italian regions, thus far, acted in rather a scattered manner in their choice of digital tools, apps and data analysis in their efforts to countermove the spread of the epidemic. Lombardy, the region most affected by the coronavirus epidemic, was also the first to launch the app service to map the population and screen COVID-19 transmission. Similar initiatives have been taken by the Regions of Lazio, Sicily and Sardinia, which have launched new apps (respectively called "Lazio Doctor Covid"; "Sicilia si cura "; "Covid 19 Regione Sardegna") to monitor movement of citizens and to provide any useful information on contacts with other people, the place where they are in isolation, thus creating a continuous flow of information essential for the emergency management system. Conversely, a private company - Webtek – has invented the app "STOPcovid19" that was introduced in Umbria. The app allows through the GPS localization of the smartphone to reconstruct a person's chain of contact, by connecting the other devices to which they have been close.

Moreover, in Europe, while the Pan-European Privacy Preserving Proximity Tracing (PEPP-PT) is bringing together 130 researchers from eight countries to develop applications that can support contact tracing efforts within countries and across borders, states are also bringing forward systems, projects and researches on autonomous trajectories. To our knowledge this is the case, at least, in Austria, Belgium, Bulgaria, Czech Republic, Denmark, Greece, Finland, Germany, Iceland, Ireland, Israel, Norway, Poland, Spain, Slovak, Switzerland and the UK.

**Different tools, common legal issues.** Overall, two technological trajectories seem to be under consideration: (a) geo-tracking via GPS, where the system tries to identify if the paths of two people crossed and (b) peer-to-peer connections (Bluetooth and ultrasound) between two phones to identify each other.

The website GDPR Hub provides a fairly complete and updated framework of projects and countries committed in the development of tools to combat the pandemic which entails the collection and processing of large amounts of citizens' data. Based on the specific function which is being pursued by the tool and the voluntary or mandatory nature of the participation/subscription by the individual to the project in question, GDPR hub purports a possible classification of these projects along the following lines:

1. Decentralized contact tracing apps or frameworks (Austria; Finland; Germany; Iceland; Ireland; Israel; Italy; Norway; Singapore; Switzerland; United Kingdom; United States)
2. Centralized contact tracing systems (Czechia; Slovakia; South Korea; Israel)
3. Enforcement of lock-down (Bulgaria; Greece)
4. Enforcement of individual quarantine (Poland)
5. Self-assessment apps (Spain)
6. Location mapping projects/mobility information services (South Korea).

All such tools first raise the same set of basic questions: what data is being gathered, how it is being used or could be used in the future, who collects this data, and for which use it is entitled to do? It is worth noting that these questions certainly reflect the issues highlighted in the Italian Sector Inquiry on Big data jointly conducted and recently concluded by the Italian Antitrust Authority, the Italian Communications Authority, and the Authority for the protection of personal data aimed at a better understanding the implications that developments in the digital economy have for regulation, antitrust, privacy and consumer protection issues. The processing of enormous quantities of data (personal and non-personal) for social and public health purposes is crucial for the implementation of the abovementioned IT solutions. Data and information are extrapolated, processed and aggregated to obtain reliable information (and in some cases predictive information) that can be now used for combatting the pandemic. But what emerges from the Italian joint sector inquiry is that it is not possible to "isolate" the regulatory approach to Big Data separately in data protection, protection of pluralism of information, or in the dynamics of market competition (or relating to consumer protection). Nonetheless, in order to try to nail down the issues originating in each of these legal domains, the following can be observed.

**Privacy.** Contact tracing, geo-localisation, mobility information services are by definition actions which implicate the collection and processing of extremely sensitive personal data, location and

personal health information to begin with. Having said that, notwithstanding the unavoidable differences in the approaches which will be ultimately endorsed by data protection authorities around the globe, flexibility is likely to be the key word in light of the public interest at stake. As far as the situation at the EU level is concerned, General Data Protection Regulation ("GDPR") already permits competent public health authorities and employers to process personal data when necessary for reasons of substantial public interest in the area of public health, as is the case during an epidemic, provided that any emergency measures are permissible only for the duration of the emergency and are subject to suitable safeguards. Whereas Article 112 of GDPR sets forth the general principle pursuant to which "derogations in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases".

Moreover, the European Data Protection Board, which is working closely with the European Data Protection Supervisor, has recently clarified, in the "Statement on the processing of personal data in the context of the COVID-19 outbreak" of 19 March that the rules and rights recognized by the GDPR, as a result of Article 23, would be susceptible to compression in the presence of certain extreme situations, such as the current serious health emergency. Likewise, Article 9(2)(i) of the GDPR legitimises the processing of special categories of data where the purpose of the processing is to pursue grounds of public interest in the field of public health, such as protection against serious cross-border threats to health, on the basis of European Union or Member State law, provided that appropriate and specific measures are implemented in order to protect the rights and freedoms of the data subject.

**Competition and TLC regulation**. The race to develop digital tools and technologies to fight COVID-19 pandemic may encourage various debate also in the antitrust and regulatory areas to the extent that such race will involve a number of undertakings either acting on their own, by manufacturing and commercializing their own digital tools and technologies or through significantly supporting national governments or other public bodies. Key issues may include the following.

The relatively new enforcement area relating to the relationship between the possible abusive nature of certain unilateral conducts by firms enjoying market power and data protection rules. Recent experience shows how competition agencies are always ready to reassess and reconsider the legal tools at their disposal in order to enhance the effectiveness in the prevention of antitrust violations, and when it comes to privacy issues the above seems to apply even outside the typical scenario of information and digital technology markets. Therefore, although the general principle maintained, at least at the EU level, is that issues concerning the processing of personal data are not as such a matter for competition law (European Court of Justice, Asnef-Equifax, para. 63), as a matter that personal data is becoming more and more a real asset and as a result privacy protection has become a central point of concern on the agenda of EU and competition agencies.

Moreover, interoperability between emerging/competing technologies and the role of network effects may be a source of concerns. As innovators crowd into the space, there is a growing risk that the various technologies which have been developed will render each other useless by dividing up the tracked population into ever smaller chunks and causing an issue of interoperability. In this perspective, standard essential patents (SEP), as well as, more in general, any possible unwarranted "use in courts" of IP rights, may be an issue. Standardization may be a

source of concern from an additional standpoint, namely, the natural tendency of the digital tools in question to tip the balance at a certain point in favour of a single product attracting a large user-base. Competition authorities and regulators may thus be wary of avoiding any possible abuse within the context of such "winner-take-all" races affected by strong network effects, whereby, ultimately, competition is "for the market" rather than "on the market".

Finally, access to any possibly relevant IT infrastructures, deemed essential for the diffusion of the digital tools, will likely be under the spotlight of antitrust agencies and regulators. A crucial role may be played by firms possibly enjoying a strong position through the control of physical or virtual infrastructure, as well as, in general, on vertically integrated firms which combine key inputs and resources indispensable to operate upstream and downstream on different levels of the value chain.

## Contacts

**Sabrina Borocci**
ACER
Partner, Milan and Brussels
**T** +39 02 720 2521
sabrina.borocci@hoganlovells.com

**Luigi Nascimbene**
ACER
Senior Associate, Milan
**T** +39 02 720 2521
luigi.nascimbene@hoganlovells.com

**Eugenia Gambarara**
ACER
Senior Associate, Milan
**T** +39 02 720 2521
eugenia.gambarara@hoganlovells.com

**Aurora Museli**
ACER
Senior Associate, Milan
**T** +39 02 720 2521
aurora.museli@hoganlovells.com