Coronavirus and Contact Tracing Apps: The Italian Case

Contact-tracing apps and technologies are a hotly debated issue with legal, medical and technological implications.

The most common mistake in the public debate is to put the tracing carried out by a private tech company to sell a service on the same level as the tracing carried out by governments to better manage infection risk during a pandemic.

The experience with COVID-19 and contact-tracing apps has shown that when the government intrudes in our private lives, our deepest anxieties of being persecuted come to the surface. This feeling harks back to the 19th and 20th centuries, but it is still very much alive and kicking. It was this kind of feeling (specifically, a desire for freedom from government intrusion) that led to the birth of personal data protection, when Brandeis and Warren theorised about "the right to be let alone" (their paper, "The Right to Privacy", was published in the *Harvard Law Review* in 1890).

Thus, it is neither correct nor useful to compare Google's GPS tracing (to cite one example) with contact-tracing apps used to manage the COVID-19 emergency.

Nevertheless, any analysis of contact-tracing apps must focus on:

(a) the person responsible for the tracing (i.e., the data controller);
(b) the purpose for which a contact-tracing app is used; and
(c) the utility of contact-tracing apps and balancing that with people's privacy.

The EU's Role

EU institutions have taken stances to encourage politicians to coordinate technologies within an EU framework of pandemic risk management. The most important documents published in this regard are:

- the European Data Protection Board's (EDPB) first statement (19 March);
- the EDPB's Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (21 April);
- the European Data Protection Supervisor's (EDPS) Tech-Dispatch 1/2020: Contact Tracing with Mobile Applications (7 May); and
- the European Commission's Recommendation 2020/518 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis (8 April), and its subsequent guidance and informal statement.

All these documents highlight that data protection is an indispensable part of building trust and creating the conditions needed to make any contact-tracing solution socially acceptable and ensure its effectiveness.

The Italian Case

The Italian government and Data Protection Authority (DPA) have followed the European institutions' same prudent approach from the outset.

Thus, even though European guidelines did not take an explicit stance on it, the Italian authorities designed a management risk framework in which **solely public health authorities are in charge of verifying and managing the infection chain and, consequently**, any contact-tracing app. Specifically, Art. 6 of Law Decree 28/2020 stipulates that the government – namely, the Ministry of Health – is the data controller and is responsible for making the contact-tracing app 'Immuni' available to citizens, given that it is in the public interest to manage the pandemic in the best way possible.

Data processed through Immuni **can be used exclusively by the Ministry of Health to implement safeguards to prevent and contain COVID-19, but aggregated and anonymised data can be used for public health, preventive, statistical or scientific research purposes.**

The use of Immuni is voluntary, with only approximately 3.3 million people having downloaded it to date. The app uses Bluetooth Low Energy technology (no geolocation whatsoever) – this ensures **a proper balance between the public interest of reducing infection risk and people's privacy**. The app does not (and cannot) collect any data that would identify the user. Therefore, Immuni can determine that two users came into contact without knowing who those users are or where the contact occurred. When two phones with Immuni on them come into close proximity (under 1.5 metres), each phone sends the other random codes that cannot identify the users in any way. The phones store each other's code for 14 days; if one of the phones' owners is then diagnosed with Covid-19, the competent public health authority asks that person if he/she wants to alert other users he/she exchanged random codes with. In any case, alerts do not (and cannot) reveal users' identities.

No specific instructions are currently in place regarding the behaviour to adopt if you receive an alert.

In compliance with transparency duties – and as suggested by the EDPB – the government published Immuni's source code on the app's website.

Points of Discussion

One of the main sticking points concerns the voluntary basis of Immuni's use and the lack of specific instructions to follow when an alert is received. This discussion revolves around the abovementioned balance of interests and the frequent opposition in the management of the health emergency between measures that depend on citizen responsibility and those imposed by law.

With Immuni, the Italian government has chosen – as suggested by European institutions – to adopt the responsible citizenry approach. And it is probably the best option, given that fundamental rights and freedoms and potentially high-impact technologies are involved.

The situation is different when it comes to software that enables citizens to carry out voluntary self-screening (the results of which are automatically sent to the government). In this regard, the Italian DPA stated that differentiating between the various apps used to manage the pandemic is not a good strategy to ensure the efficiency and effectiveness of contact tracing, or the security of personal data. Several Italian regions have adopted this kind of software, but it has not met with much public success.

No specific provisions permit the use of contact-tracing technologies in the private sector. Nevertheless, the DPA clarified on 6 June that the only current provision on contact tracing is that concerning Immuni, which is managed by the government. The DPA also clarified that employers can use technologies that do not register any kind of data, such as social distancing wristbands.

Conclusion

The number of Immuni users is currently too low to ensure effectiveness, but public authorities are hopeful that downloads will increase this autumn – though that will require a new communication strategy.

In the meantime, private solutions such as wristbands will likely enjoy increasing success.

Vincenzo Salvatore

Vincenzo Salvatore is counsel and leader of the Healthcare and Life Sciences Focus Team at BonelliErede. Full Professor of European Union Law, he joined BonelliErede in 2015, bringing his specific regulatory and compliance skills in terms of clinical trials, marketing authorisation procedures, pharmacovigilance, personal data protection, promotion and marketing of medical devices, inspections and enforcement. Vincenzo has gained significant experience in complex litigation representing public and private entities before the European Court of Justice based in Luxembourg, in EU law disputes. In addition, he was Head of the Legal Service at the European Medicines Agency from 2004 to 2012.

Email: vincenzo.salvatore@belex.com

Giulia Tenaglia

Giulia Tenaglia joined BonelliErede in 2018 and specialises in privacy, data security and information technology law. She assists both Italian and multinational companies, most frequently on complex, innovative projects involving data management and the use of new technologies in regulated and non-regulated sectors, data reuse and anonymisation, profiling, the management of partnership data and technological JVs based on IoT and big data, direct marketing, data transfer abroad, and internal audits. She represents clients before the Italian Data Protection Authority and in court. Giulia also teaches a course on privacy and personal data protection at the University of Pavia's Almo Collegio Borromeo and is a founding board member of the DPO innovation association.

Email: giulia.tenaglia@belex.com