

DATA PROTECTION AND THE HEALTH CRISIS

BACKGROUND

1 - In light of the Corona health crisis, the European Institutions are wondering which measures to implement and how, in order to limit the spread of viruses and the conditions under which personal data, particularly health data, can be used.

2 - In pandemic situations, the possibility of collecting data, apart from when we are under medical care (in order to determine whether a person presents symptoms of a virus, or data relating to movements and events) cannot be considered without guaranteeing the full application of fundamental freedom rights which protects the privacy of each citizen.

CURRENT SITUATION

3 – There have already been several thoughts on the use of personal and location data when decisions on this matter have not yet been endorsed, with in certain cases in a drastic manner.

4 - Thus, in Israel, since 16 March of this year, the internal intelligence service, Shin Bet, which usually focuses on « anti-terrorist activities » can now, without prior authorization from the courts, track the location data of a citizen's mobile phone. In practice, Shin Bet can obtain the location of infected individuals over a period of 14 days prior to their diagnosis and identify the routes and people with whom they came into contact. The aim is to notify those having been in contact with sick people, by text message, and to ask them to place themselves in quarantine. The left-liberal delay « Ha'Aretz » did not hesitate to denounce the « *most draconian measures in Israeli history to track down the movements of law-abiding citizens on a large scale* » Israel's case is similar to those of China and South Korea, two countries in which quarantined people are being traced via an application on their mobile phones.

As for The United States, they are preparing to launch a plan to share anonymized data with the main tech giants (Apple, Google, Facebook...) in order to develop a tracking system using location data and facial recognition technology.

5 – Fortunately, in Europe, the situation is somewhat different. In Lombardy (Italy), the region which is most affected by the epidemic, telephone operators have provided the

authorities with data concerning the transfer of a mobile phone from one telephone terminal to another. This data is anonymous and makes it possible to know what percentage of the population respects the lockdown. According to the information collected by regional authorities, only 60 per cent of its population is said to be staying at home. In Belgium, once the Ministry of Health gives its green light, operators provide the Dalberg Data Insights platform with anonymous « mobility maps » based on geographic aggregates, such as the postal code, which is crossed with epidemiological data from the authorities, it then enables them to predict the spread of the outbreak.

In Germany, the Government is about to launch a mobile application, inspired by Singapore, to facilitate the individual tracking of cases and the identification of coronavirus chains as part of the containment phase-out strategy. This tracking uses Bluetooth technology. As for France, it has asked a scientific committee to study the possibility of setting up a population tracking system.

6 - However, and regrettably, the European Data Protection Committee (EDPS) has just reminded us of the rules which are applicable for the European Union. Though, and at the same time, the European Commission is asking for data from telephone operators in order to assess the effect of the containment measures.

This paradox is difficult to understand, especially for citizens who are increasingly disoriented by the procrastination of certain member state governments. Mainly, and not surprisingly, the use of facial recognition, a technology which has been developing rapidly throughout the world, is being considered more and more, even though it can lead to numerous disadvantages. Facial recognition is not fail-proof and always requires, in the event of potential sanctions, a human intervention of, namely, a judge.

THE EUROPEAN UNION AND DATA PROCESSING

7 - As a reminder, two legal texts are applicable in the current situation, even if the second is often forgotten or ignored:

- the General Data Protection Regulation (GDPR) provides mechanisms for the collection and processing of personal data by public health authorities usable in the case of outbreaks, without the need to obtain the consent of the person in question;
- the processing of location data collected by electronic communication operators is regulated by the e-privacy guideline; the revision of this guideline is unfortunately pending.

8 - DATA PROCESSING IN THE EUROPEAN UNION IS THEREFORE BASED, INTER ALIA, ON THE PRINCIPLES OF NECESSITY, PROPORTIONALITY, TRANSPARENCY AND CONFIDENTIALITY.

9 - The Commission's request to telephone operators in several countries « *to provide aggregated data on their mobile subscribers in order to understand and anticipate the evolution of the pandemic better*» can therefore be interpreted as an instinctive facilitative reaction to a reality that is hits the entire world very hard.

At the same time, the Commission clearly explains through the spokesperson, the Commissioner, that it wishes to « *give European researchers at the joint Research Center, which will be the recipient of the data, the means to help local authorities to correctly size the care supply by checking, thanks to mobile data, whether the containment instructions are being applied* ».

The position seems problematic to us even though the preservation of fundamental freedom rights could be ensured by using less intrusive tools that are equally compatible with the objective of effectively combating the pandemic.

POSITION OF THE INSTITUTE FOR DIGITAL FUNDAMENTAL RIGHTS (iDFrights)

10 - iDFrights calls for vigilance in terms of privacy protection and insists on the fact that a mobile application for tracking movements could facilitate the collection of personal information and, consequently, should be extremely closely supervised. Considering this point of view, we would all be geolocated and identified within the authority of our States once the data has been collected.

Implementing measures appropriate to the situation such as limiting travel and meetings does not mean taking measures that could infringe the privacy of the individuals concerned by the collection of health data, if they were to go beyond the management of the crisis of this virus.

iDFrights considers that not all means of geolocation are equal. Tracking population flows via the anonymized data of a telecom operator raises fewer questions than tracking a citizen, even with his consent, via his personal smartphone, during the incubation period of a disease. And it goes without saying that the obligation for a person to activate such an application to get out of confinement would be totally unacceptable and contrary to the European texts of the GDPR and the e-privacy guideline.

iDFrights calls for continuous vigilance and a periodic evaluation of protection devices. It is essential to keep « the human being » at the center of all decisions. The Institute particularly insists on the preservation of human intervention at every stage of the data analysis process allowing an informed citizen consent.

Generally speaking, the unprecedented seriousness of this health crisis may legitimize the use and aggregation of data, or even geolocation, demarcation, obfuscation or any other similar means, provided that there is constant vigilance carried out by an authority which has permanent control, created or mandated for this purpose. In such cases, it is essential to require the destruction of information thus collected, as soon as the health crisis is over.

11 - As it concerns the sovereignty of a continent as a whole, iDFrights insists on the need to entrust European associations and companies the means to give priority to their research and to promote their actions, in order to create, between the American and the Asian model, a third way: the European way has already been endorsed by a series of texts including the RGPD of 2018. Their experience must be valued because they are perfectly capable of proposing axes of reflection to unite saving human lives with the achievements of the Union. As the Treaties currently stand, health policies are the exclusive responsibility of Member States, European companies are therefore very good at integrating into their projects the societal elements that are the hallmark of the Member States and work together.

12 - iDFrights is concerned that the RGDP only applies to Europe. Indeed, as the generated and gathered data are collected on platforms that are not based in Europe, managing the processing will automatically be beyond the control of the European authorities. That is why, we therefore recommend:

- to give European platforms the means to emerge and thrive, - to ensure that technologies and the Internet provide a framework for the use of massive data, - and to open a new reflection on the ethical challenges raised by « big data ».

13 - iDFrights worries about potential errors in facial recognition that may outweigh the security benefits. Indeed, several studies have shown that facial recognition software can be racially or ethnically biased. The Institute is therefore not in favor of the widespread use of this technology which raises problems in terms of protection of fundamental freedom rights. This is all the more serious since, in combination with other

data, the gathered data may be used to draw conclusions about the identity of the individuals in question.

14 - iDFrights will sustain all European options that are based on a system that ensures strict compliance with the RGPD and in particular the initiative on which the European Commission, France and Germany are working, and which, moreover, are cooperating and seem to favor a so-called « contact-tracing » system. This technology would use Bluetooth type waves. Their transmission, from a smartphone, would make it possible to identify the possible contacts of an infected person (who will voluntarily come forward by accessing the application thanks to a code he will receive) with an uninfected person, the latter receiving the information by alert, which will enable him to be tested immediately, and thus limit the chain of propagation of the virus.

The development of this application that the French call « stop Covid 19 » does not require identification. No need to centralize data either they assured us.

However, this application (which is not yet technologically mature) will have to be phased out as soon as the outbreak is over, and the appropriate authorities will have to ensure that this is done.

CONCLUSION

15 - The peculiarity of great crises is that they require the preparation of a new future, not the restoration of the past. The one imposed on us by COVID 19 has been unprecedented since 1945 - at least - for the northern hemisphere. Its consequences are already of a health and economic nature. But there is no doubt that they will also impact the political order of nations, sometimes pushing them towards dangerous authoritarian responses. During the Second World War, the camp of the free countries worked on the « aftermath » long before arms were put down. That is why, as of now, we need to seize the digital tools to help fight the spread of the pandemic that may return year after year. But we also, as of now, need to set up authorities to control the massive use of personal data and give them real power. On a member state level, these powers must be brought together and strengthened.

As far as the European Institutions are concerned, a supervisory authority must be raised at an almost constitutional level knowing what is at stake: a council for digital rights and freedom, bringing together and consolidating small existing structures, such as the « data controller » for this immense, permanent task. This Council will

complement national structures. Individual member countries of the Union are too weak to supervise and regulate the use of these new digital tools on their own. The capitalist industries that exploit them sometimes transgress - this has already been the case for at least a decade - the rules, laws, and sometimes even the sovereignty of certain states.

History will surely show us whether we will have been able to cope with the powerful abuse so often perceived as the opposite of individual and, in the future, collective freedom. And if the pandemic has courageously brought people but also States together it might also succeed in infecting everything.