

DATA HUNTING, INCLUDING LOCATION DATA, IN A HEALTH CRISIS SITUATION: ADDRESSING THE ISSUE OF THE RIGHT OF INDIVIDUALS TO PRIVACY AND THE PROTECTION OF THEIR PERSONAL DATA

IT and Data Commercial and international agreements Competition and Distribution Law | 30/03/20 | Florence Chafiol Roxane Blanc-Dubois



The coronavirus crisis is the occasion to note the emergence of certain initiatives that are either legitimate and controlled or abusive and intrusive, and that come from both private entities and state authorities, involving the use, sometimes massive, of data, including personal data.

Abuses have been observed from private entities: some of them have taken advantage of the health crisis to unfairly collect personal data about individuals, by inviting them to fill out derogatory travel certificates online. The French data protection authority ("CNIL") has warned citizens against this practice, reminding them that only certificates that are available on the French government's website are valid.

On the state authorities' side, several of them have approached mobile phone operators, social media, search engines or other technology companies in order to obtain data about their users. In the age of new technologies and smartphones, it is indeed potentially easy to track movements of individuals. This information can be useful to identify individuals who have been in contact with infected people and/or to anticipate medical needs.

In some countries, including especially outside the European Union, certain authorities have gone so far as to massively track individuals, sometimes without their consent, by obtaining data from telecom operators and/or via mobile applications, and have publicly disclosed information enabling the identification of individuals infected with the virus.

Within the European Union, initiatives based on mass collection of location data are also underway or under consideration, including for the purpose of modelling the spread of the virus and/or preventing individuals from infecting each other. While these initiatives seem legitimate and useful in the context of the current health crisis, they cannot, however, be exempt from the rules laid down by the European Union and the Member States on the protection of individuals' privacy and personal data. Indeed, this type of initiative is governed, in particular, by the General Data Protection Regulation ("GDPR") and the ePrivacy Directive which includes provisions relating to location data resulting from electronic communications.

Electronic communications data such as mobile location data (which are of particular interest to authorities) may, in principle, only be processed if they are anonymised or with the consent of the data subject (Article 9 of the ePrivacy Directive). However, the ePrivacy Directive provides (by way of exception) that Member States may take specific legislative measures to derogate from the previous rule for the purpose of safeguarding public security (Article 15 of the ePrivacy Directive). However, such legislative measures, which would allow for the use of non-anonymised location data without the consent of individuals, must be necessary, appropriate and proportionate to the public security risk involved. Consequently, such measures may not be implemented without appropriate safeguards.

In this respect, the European Data Protection Board ("EDPB") recommended, via two press releases published on March 16 and 19, 2020, that Member States' authorities give first priority to the processing of anonymised data (for the record, the GDPR does not apply to such data). If the processing of such anonymised data does not make it possible to achieve the objective related to the fight against the spread of the virus, then legislative measures could allow for the processing of non-anonymised location data. In this case, the EDPB recommends that priority be given to the least intrusive measures possible for individuals. In addition, such processing operations must be limited in time (i.e. limited to the management of the health crisis, and data must be deleted as soon as the health crisis ends) and not be used for any other purposes.

It should be noted that concerns are emerging regarding the use of location data for the purpose of punishing individuals who do not comply with containment rules. For example, in Italy, Italian authorities were able to identify that around 40% of the population in the Lombardy region had not complied with the containment rules. However, this finding could not, in principle, result in penalties since the data used by Italian authorities are anonymised.

At European level, rumours are spreading about a European Commission's project relating to mass surveillance based upon aggregated and anonymised data provided by telecom operators (with a view to modelling the spread of the virus and anticipating medical needs).

On March 24, 2020, the French Government created a committee called the "CARE" ("Analysis, Research and Expertise Committee"), whose mission is to *"help authorities give thought to the opportunity of implementing a digital strategy for identifying people who have been in contact with infected persons"*. For the time being, no other more precise information has been provided. Such strategy could, for example, consist in collecting anonymised location data from telecom operators as recommended by the EDPB or, possibly, in inviting French people to download an application intended to combat the spread of the virus, provided that the downloading of such application and the provision of data are on a voluntary basis and that appropriate safeguards are in force. Just like certain neighbouring European countries that have undertaken similar initiatives, and for which the opinion of the local personal data protection authority has been requested, the CNIL could be officially consulted on the final project contemplated by the French State regarding the processing of location data in the context of this health crisis.

It should be noted that during the review of the French health emergency bill (the final version of which was adopted on March 23, 2020), an amendment, of imprecise scope, aimed at authorizing *"any measure allowing for the collection and processing of health and location data"* for six months from the publication of the said law, was rejected by the Senate.

Useful links:

EDPB press release of March 16, 2020

EDPB press release of March 19, 2020

Press release from the Elysee dated March 24, 2020 (in French)

