KNOW-HOW

Gleiss Lutz

06.04.2020

DATA PROTECTION

MANDATORY TRACKING - A LEGAL NO-NO?

The longer the restrictions on private and public life imposed by the state governments to flatten the COVID-19 infection curve go on, and the more burdensome the economic consequences of these measures become, the more urgent the need to discuss additional or alternative measures to contain the pandemic. Front and centre in the discussions are the meanwhile ubiquitous smartphone and its ability to collect and share information about its owner's location and surroundings. Tracking citizens on the basis of their mobile phone data would make it possible to trace and interrupt chains of infection. Reports from Asia (appear to) show that these technical means play an effective role in controlling the COVID-19 outbreak.

It comes as little surprise that ideas of this kind meet with serious misgivings in Europe, not only from data protection hardliners. The very idea that ones own mobile phone could serve as a tool for monitoring all the places you visit and the contacts you meet fills many people with dread. Statements by politicians and data protection officers to the effect that, if at all, the use of location and other data as a means of disease control is only permissible if it meets data protection standards in all respects and – what is especially important – is carried out voluntarily, are likely to meet with broad approval.

It remains to be seen, however, whether this broad consensus will still stand if the situation fails to ease at the hoped-for rate and the governments at national and regional level find themselves after Easter in the position of having to extend the lockdown, heralding an economic crisis with possibly incalculable consequences. There are already voices in the business sector calling for certain movement data (e.g. from credit card usage) to be used, even without consent, in the fight against the spread of the infection.

Following a cursory look at the various options available to control the spread of the pandemic using mobile phone data that are currently under discussion or – especially abroad – already in use, this article deals – from the legal perspective – with the question of whether measures of this kind really can only be implemented with the consent of the persons concerned.

What are other countries doing?

Proponents and opponents alike of the use of smartphones and mobile communications technology in the battle against COVID-19 base their arguments on the experience of, primarily, the countries of eastern Asia:

- South Korea has evidently had considerable success in using a GPS app to help contain the epidemic. The app sets off an 'alarm' if the owner leaves the area they are allowed to move within. There have been reports, however, of infected persons being publicly exposed because the app allowed them to be identified. That could have deterred infected persons from reporting the disease.
- In Taiwan a GPS-based app is being used to monitor compliance with the lockdown. The app alerts the competent authorities if the smartphone leaves the area within which the owner is allowed to move about. It also alerts the authorities if the smartphone is switched off. There are reports of a number of cases in which flat smartphone batteries have resulted in citizens receiving a visit from the police.
- The 'TraceTogether' app in use in Singapore is regarded as a data protection-friendly solution. The app does not use location data, but, with the help of Bluetooth signals, registers the presence of other smartphones in the vicinity and generates temporary IDs that are only stored on the devices concerned. If an app user becomes infected with COVID-19, they can call up their movement profile so that the IDs with which they had

- relevant contact during the previous 21 days can be sent a push notification.

Which measures are being implemented/discussed in Germany?

- In Germany, as in the other EU Member States, the mobile communications providers already made it known early on that they would be prepared to provide the competent authorities or bodies (in Germany the Robert Koch Institute) with anonymised location data from cell site analysis. This data can be used to trace movement flows in areas in lockdown, for example, so as to analyse how efficient the measures are. The data protection authorities have given their approval for this measure.
- A draft bill drawn up by the Federal Ministry of Health seeking to compel mobile communications providers to supply the Robert Koch Institute, under certain circumstances, with location data of individual mobile phone users was quashed, however. Alongside fundamental reservations as regards the constitutionality of intrusion of this kind into the privacy of telecommunications and the fundamental right to determine what one's personal data is used for, one objection of many of the critics of this proposal was that cell site data is far too imprecise and therefore unsuitable as a way of identifying contacts of infected persons.
- The approach adopted by a European research initiative that has developed a basic app technology by the name of PEPP-PT is currently attracting the largest amount of interest and support. Like TraceTogether in Singapore, PEPP-PT uses Bluetooth technology, the advantage of which is that it is designed for use over short distances and can collect precise data within its range. All contacts with other devices that have the app installed on them and Bluetooth activated can actually be traced precisely, to the metre. The contacts recorded in this way are encrypted under a pseudonym ID on the respective end device only. Where an app user is found to be infected with COVID-19, they can 'unlock' the contacts saved on their device over the last 14 days and those people will then receive a push notification via a special server informing them that they have had contact with an infected person. Neither the identity of the infected person, nor the place and time of the contact will be disclosed. This solution is generally seen as GDPR compliant and also has the support of the German Federal Data Protection Commissioner, albeit with the caveat that use has to remain voluntary at all times.

Can tracking really only be on a voluntary basis?

Even the best technical solution is ineffective unless it is actually put into use. Estimates assume that approximately 30-60 % of the population would have to be using a PEPP-PT-based app if it is to be able to identify a sufficiently large number of contacts with infected persons. If not enough smartphone users install the app and if the infection rates remain at a level that would only allow an easing of the lockdown at the expense of overwhelming the healthcare systems, the question of whether the state could also force its citizens to use the app is almost unavoidable.

What does EU law say?

EU law does not forbid the state a priori from issuing an order of this nature to its citizens. Article 9 General Data Protection Regulation explicitly allows the Member States to create the legal basis for the processing of sensitive (health-related) data if there is a vital public interest that justifies doing so.

And the German Basic Law?

That puts the ball in the court of national (constitutional) legislation. A duty to use a technology that stores and analyses location data and contacts represents a far-reaching incursion into citizens' fundamental right to determine for themselves what happens with their personal data. Incursions of this kind are not per se improper – fundamental rights have boundaries, and the protection of other fundamental rights and constitutional freedoms can justify substantial restrictions. But what is needed in any case is a parliamentary basis that sets out, with sufficient precision, the material conditions for the incursion into fundamental rights, especially the prerequisites and the limits. The existing legislation, e.g. the Infection Protection Act or the Telecommunications Act, would presumably not be sufficient for this purpose and would first have to be amended.

A law ordering or enabling mandatory tracking has to satisfy the proportionality test, which means that it must be appropriate and necessary to achieve the public interests it seeks to achieve, namely to protect public health and maintain public order. In addition to that, it may not place an unreasonably heavy burden on the holders of fundamental rights.

When carrying out the test of the appropriateness and necessity of measures that restrict fundamental rights, the

legislator has some discretion when it comes to making forecasts and judgements, and this is of special importance in the current situation, with all its inherent uncertainties. Nevertheless, the idea of compulsorily collecting and processing individual location data from mobile phone use is likely to fall at the first hurdle, namely the test of appropriateness, unless proponents can show how the relatively imprecise cell site data could be used effectively to interrupt chains of infection.

The necessity criterion carries special weight when it comes to deciding whether to make the use of tracking technology compulsory. The legislator must look carefully to see whether there are not other, less invasive means available to contain the spread of the COVID-19 epidemic with a similar success rate. As long as voluntary measures and initiatives promise sufficient success, compulsory measures are not necessary and therefore unlawful. If, however, a prognosis suggests that a sufficient number of users for a tracking app cannot be reached or cannot be reached sufficiently quickly on a voluntary basis, and the only choice is between extending (or tightening) the lockdown and compelling people to use tracking technologies, then the outcome might be different. The fundamental right to decide for oneself what one's personal data is used for will not in any case be given any general precedence over other fundamental rights such as the freedom of movement and the freedom of economic activity. Where the legislator finds itself in a situation where granting one fundamental right is possible only at the expense of another fundamental right, it must find a careful balance. Instead of ordering all citizens to install and use tracking apps, for example, it may be conceivable to limit their use to those citizens who want to seek an exemption from the general lockdown that otherwise continues to apply. In that way, citizens would have the option of whether to remain in 'voluntary' isolation or accept incursions into their right to decide for themselves what their personal data is used for.

Lastly, the reasonableness of (compulsory) measures ordered by the state must always be guaranteed. The use of smartphones as 'electronic tags', as practised in some Asian countries, is likely to only be an option, if at all, under narrowly defined conditions, namely if people in respect of whom there is good reason to suspect that they are infected give reason to fear that they will not comply with the quarantine measures ordered by the authorities. The policing laws of some states stipulate prior monitoring by the courts in similar scenarios.

On the other hand, even if made compulsory by the state, a clearly data protection-friendly technology like PEPP-PT could possibly satisfy the proportionality test. However, before taking any such decision, there would be many matters of detail that the legislator would still have to look at closely, which we cannot discuss in detail here. For instance, there is the question of what to do about citizens who do not (want to) have a smartphone. Whether the proposal discussed in this context, namely to provide wristbands with a Bluetooth-capable chip and pre-installed PEPP-PT technology, would be practicable and implementable on a large scale, is uncertain.

Conclusion

For the time being, we all just have to hope that the measures aimed at containing the coronavirus pandemic are successful and that no further restrictions on personal and economic freedoms are needed. Should this hope be dashed, however, there would be nothing, legally, to stop the legislator of making incursions into the fundamental right to decide for oneself how one's personal data is used in order to protect other important fundamental rights and public interests. Within the limits laid down by the constitution in terms of proportionality, it is up to the politicians to decide whether compulsory tracking is an appropriate tool and, if so, how to implement it.

EXPERTISE

Corona Pandemic
Data Protection
Digital Future
Public Law

EXPERTS

Dr. Christian Hamann

Simon Clemens Wegmann

Dr. Manuel Klar