The measures taken in Bulgaria and around the world to prevent the spread of the COVID-19 disease have posed the question of protecting personal data during a state of emergency in order to guarantee that quarantine measures are being observed. Undoubtedly, the opportunity to have easy access to personal data would allow governments to control the population and to limit the spread of the pandemic. The issue remains that this information can be used for a number of other purposes besides, and some of those purposes are incompatible with the requirements set out in international documents which guarantee the protection of the right to privacy.

So far, the Bulgarian State has shown moderation by providing the possibility in the Electronic Communications Act to access data from service providers about cells used on a mobile device for the purpose of compliance with quarantine measures. It has been announced that a special mobile application has been created to allow, on the one hand, easier control of quarantined persons and, on the other, quick communication between all persons and their GPs. At the moment this application is available, but there is limited information on the way it functions, so the analysis is based on the information provided by the Council of Ministers.

These measures have been criticized as they do not provide for reliable guarantees when the authorities access traffic data of individuals under quarantine. During the state of emergency, such data can only be accessed on request by the police, without the need for authorization from a court – and the service provider will be obliged to provide this data.

These criticisms are not entirely justified – mobile devices are proving to be a highly effective means of tracking the movement of their users, as is well known to various application and service providers. That is why devices usually transmit their location data – often this happens despite the user’s objection. It therefore seems proportionate and logical to ensure that this information is available to the authorities when necessary to take measures to protect public health. The experience of a number of countries, such as China and South Korea, shows that mobile device monitoring guarantees successful control of compliance with quarantine measures – and prevents the spread of infectious diseases.

However, this interference with privacy must be severely restricted in order not to become

CR legal DL 2018. Всички права запазени.

total State control over citizens. The processing of personal data in a state of emergency may be exempted from some restrictions, but the basic standards set out in, for example, the EU Charter of Fundamental Rights, the European Convention on Human Rights and the General Data Protection Regulation must be respected. The data should only be processed for quarantine purposes, and any exceptions to the data protection standards should apply only for the quarantine period.

In this respect, the amendments made to the Electronic Communications Act seem justified, insofar as the exception to judicial review is only for the duration of the state of emergency. The data collected in this way for possible non-compliance with the quarantine will, moreover, be grounds for liability of an individual only if the procedure for collecting such data is observed – i.e. courts will have subsequent control over the collection and processing. In this case, executive authorities have the responsibility to use this means of control only when absolutely necessary – and to prove that the trust placed in them during the state of emergency is justified. The legislature should not allow exemptions to be extended to cases not related to public health. Thus, a balance can be found between the right to protection of personal data in a state of emergency and the need for the authorities to be able to take swift and effective measures.

The problem of balancing between the right to privacy and the need for the authorities to have accurate data comes to the fore with the ViruSafe application announced by the Council of Ministers. The application is already available and currently allows you to enter symptom data – and can receive data about the connection of the mobile device to the networks, or its location. However, the information available to the public is scant and raises a number of questions.

First, can quarantined persons be required to use this application? At present, Bulgarian law does not provide a mechanism for such an obligation and it is debatable how effective it would be, if the user does not carry the mobile device with him. On the other hand, such an application may be effective in exercising control not only for quarantine purposes but also for the implementation of deterrence measures, for example.

Second, such an application can collect more data than just which cell the mobile device

CR legal DL 2018. Всички права запазени.

connects to. This data can be very useful – for example, allowing tracking of a person's symptoms, health status – but it is also considered sensitive and is subject to special protection. The processing of such data is subject to strict control requirements and should only occur when necessary.

The application will also allow non-quarantined people to submit data about their symptoms, but it is unclear to whom this data will be available, how and for what period it will be stored and for what purposes. This is where the flaws of the application become obvious, as it is not yet part of a comprehensive strategy on what to do with the data collected. This approach is completely at odds with privacy standards – as it means centralizing a huge array of sensitive data with no clarity what it will be used for. There is no dispute that an application for the data will be found – this data may serve to plan the National Health Card, to exercise control over the activities of health care facilities, etc. – but the goal-setting process must precede the decision to collect personal data. Especially when the collection has the potential to continue beyond the state of emergency.

When creating data sets, their security should also be ensured – since, after the leakage of personal data by the National Revenue Agency in 2019, the measures are essentially reduced to finding the person responsible for the disclosure of the data. However, the search for that person is not enough to guarantee the security of the other files of information stored by authorities, nor will it help to repair the damage. Information once shared on the Internet can hardly disappear – and damage once done can hardly be repaired. The authorities must therefore create trust that such security breaches will not occur – which necessitates measures such as decentralization of information, access control, pseudonymisation, etc.

Last but not least, creating an application to process this data implies that its developer will be committed to maintaining it and that the data will flow through mobile devices. Accordingly, we must ask ourselves, is it appropriate for everyone to have the opportunity to enter their health data without knowing who will have access to this data? It is a known fact that a number of applications are already collecting such information, but the authorities should be especially careful – because their recommendation to use a particular application can have very serious consequences. Therefore, the creation and use of such applications should comply with very strict standards – and the relationship between the State and their

CR legal DL 2018. Всички права запазени.

creator should be transparent so as to guarantee the rights of the citizens who enter their data.

In this regard, there is already a recommendation from the European Data Protection Supervisor that the EU should have a centralized application for processing this type of data. This approach may prevent some of the above issues – but it still leaves open questions as to what purposes this information will serve, or how its security will be guaranteed.

CR legal DL 2018. Всички права запазени.