kurzum
Nr. 83 / November 2020

KONRAD ADENAUER STIFTUNG

Data protection "by design": An interim assessment of the German Corona Warning App

Pavel Usvatov

With the help of the corona app, Covid-19 infection pathways are to be made traceable. Countries around the world have introduced these apps. We look to South-Eastern Europe, Asia, Latin America, the Middle East, North Africa and Sub-Saharan Africa. What is the legal framework on the ground? What about practical implementation? What problems have arisen?

The development and introduction of the Corona-Warn-App in Germany was accompanied by a lively technical and political discussion, which was also conducted in a similar way in many other European countries and partly also outside the EU. Particularly controversial was the discussion of the requirements for the functioning of the warning programme, which must be fulfilled in order for the app to be compatible with the basic constitutional rights of users and data protection. In contrast to the governments of many other countries, the German Federal Government decided in favour of the so-called Tracing[1] App and against a tracking solution that would enable the monitoring of users. The German solution, with its decentralised approach to data storage, a waiver of data transmission and tracking, open source architecture and voluntary use, is a tailor-made technical solution that takes into account the concerns of users who want to decide for themselves whether to release their data ("data protection by design"[2]).

International comparison

In the current KAS publication series "Corona Perspectives", several authors examine how fundamentally different the German approach of "data protection by design" is from surveillance apps that really deserve this name, for example in Asia (especially in China, but also in India), the Middle East or Latin America.[3] Many corona apps in the countries and regions mentioned store and transmit not only the user's name, telephone number, age and gender, but often also the GPS location data when registering and in the course of subsequent use. The Corona tracking app in Bahrain, for example, performs a near-live positioning of the user's location and uploads the GPS coordinates to a central server. The BeAware Bahrain app was even linked to a nationwide live TV show called "Are You at Home?", where prizes were awarded to people who stayed home during Ramadan. In South Korea, special infection control regulations allow access to detailed personal data, including credit card transactions at banks or mobile phone location data at telecommunications operators. And in Singapore, the SafeEntry app works like a national digital check-in system that must be used at all workplaces.

Justified criticism from IT experts

Despite the data protection-friendly approach of the German warning app, IT experts have also criticised this solution and complained "that external attackers can create detailed movement profiles [...] and [...] identify persons".[4] There are also weaknesses in the Data Protection Impact Assessment (Art. 35 GDPR).[5] Such criticism, however, is fundamentally different from the criticism of tracking apps in other regions of the world: the

concerns expressed in Germany are not directed against the state, but apply to the possible misuse of data by private companies.[6]

Basic rights protection "by design" in Germany

Concerns that user data could be used by companies for improper purposes might be justified. Many providers generally have difficulties in bringing their services into conformity with the GDPR.[7] However, this concern differs fundamentally from the ideas of a part of the population that corona measures serve to introduce permanent state surveillance and establish a "dictatorship".[8] State monitoring using the current German “Corona-Warn-App” is ruled out - "by design".

With the approach of disclosing the source code, the Federal Government has also ensured maximum possible transparency. GPS data is neither recorded nor transmitted. In view of all other apps that are (pre-)installed on smartphones and collect extensive data around the clock and transmit them to the providers, the Corona-Warn-App should give the least cause for concern about basic rights.

1 Tracing involves the collection of information about whether and when contact has been made with an infected person; unlike tracking, there is no geolocation or recording of the location of users.

2 www.datenschutz-praxis.de/fachartikel/die-deutsche-corona-warn-app.

3 *Jason Chumtong*, Handytracking gegen COVID-19, A&A Nr. 386, April 2020; *Pavel Usvatov et al.*, With the smartphone against viruses, in: Coronaperspektiven, September 2020.

4 TU Darmstadt, Universities of Marburg and Würzburg, www.faz.net/aktuell/rhein-main/forscher-entdecken-sicherheitsluecke-bei-corona-apps-16812694.html.

5 FIfF e.V., Analyse und konstruktive Kritik der offiziellen Datenschutzfolgenabschätzung der Corona-Warn-App, Version 1.0 – June 29, 2020, p. 3, 5 et seq., www.fiff.de/presse/dsfa-corona-cwa.

6 In particular, the Google Apple protocol, GAP, is said to be vulnerable to motion profiling, and these companies can design IT interfaces in a one-sided way, www.faz.net/aktuell/rhein-main/forscher-entdecken-sicherheitsluecke-bei-corona-apps-16812694.html.

7 www.haufe.de/compliance/management-praxis/defizite-bei-umsetzung-der-dsgvo-in-deutschen-unternehmen_230130_500666.html

Konrad-Adenauer-Stiftung e. V.
Dr. Pavel Usvatov
Legal and policy advisor Rule of Law Dialogue
Politics and consulting
pavel.usvatov@kas.de