TRACKING-APPS UND DATENSCHUTZ IM ZUSAMMENHANG MIT DER COVID-19-PANDEMIE

EMPFEHLUNGEN FÜR DEN EINSATZ VON COVID-19-TRACKING UND TRACING APPS AUS DATENSCHUTZRECHTLICHER SICHT

FRANZISKA BOEHM, DIANA DIMITROVA, FRANCESCA PICHIERRI UND DARA HALLINAN[1]

April 2020

Seit dem Ausbruch der COVID-19-Pandemie werden weltweit zahlreiche Apps entwickelt, die unterschiedliche Daten erheben und sammeln. Die Spanne reicht von anonymisierten Standortdaten bis zu sensiblen Gesundheitsdaten. Mediziner halten den Einsatz solcher Apps für sinnvoll, ja notwendig, um die Pandemie langfristig einzudämmen. Politiker diskutieren, ob sie den Bürgerinnen und Bürger die freiwillige Nutzung empfehlen sollen. Möglicherweise stehen wir also demnächst vor der schwierigen Wahl, ob wir solche Apps installieren wollen und wenn ja, welche.

Denn: je nach Ziel und Einsatzzweck sind sie unterschiedlich gestaltet, und sie greifen auch unterschiedlich tief in die Rechte derjenigen ein, die die App nutzen. Einige Apps dienen der Benachrichtigung von Personen, die Kontakt mit COVID-19-Infizierten hatten, andere unterstützen Forschungszwecke oder sollen die Einhaltung einer Ausgangssperre kontrollieren.

Unbenommen ist: Alle Apps haben, mehr oder weniger stark ausgeprägt, den Schutz der Gesundheit der Bevölkerung als oberstes Ziel. Dennoch bergen alle Anwendungen auch insbesondere Risiken für den Schutz personenbezogener Daten in sich, und ihre Auswirkungen auf dieses Recht müssen aufmerksam abgewogen werden. Das heißt, alle, die eine App nutzen wollen, können nur dann eine informierte Entscheidung über das Für und Wider treffen, wenn sie sich der Vorteile, aber auch der Risiken der Anwendung bewusst sind.

Es wird die Aufgabe der Politik sein, hier für Transparenz zu sorgen und eine App zu empfehlen, die am wenigsten in die Rechte all derjenigen eingreift, die sie anwenden – im Interesse des eigenen ebenso wie des allgemeinen Gesundheitsschutzes. Andernfalls könnte ein schwerwiegender Vertrauensverlust entstehen, dadurch bedingt, dass Nutzen und Rechtseingriff in keinem ausgewogenen Verhältnis stehen. Damit sind vor allem App-Entwicklerinnen und -Entwickler sowie die Datenschutzverantwortlichen aufgefordert, die Apps so zu gestalten, dass diese die Verhältnismäßigkeit wahren.

Zur ersten Orientierung hat ein Forscherteam um Professorin Franziska Boehm bei FIZ Karlsruhe **folgende Datenschutzempfehlungen** erarbeitet. Sie basieren auf einer Analyse der EU-rechtlich notwendigen Voraussetzungen, denen die COVID-19-Tracking und Tracing Apps genügen müssen. Begleitend wurden durch das Forscherteam in dieser Analyse sieben kürzlich entstandene Apps aus unterschiedlichen EU-Mitgliedsstaaten hinsichtlich ihrer Datenschutz-Konformität untersucht. Die vorläufigen Ergebnisse sind in zwei vergleichenden Übersichten festgehalten, die zukünftig an die jeweiligen (Weiter-)Entwicklungen dieser Apps und die später verfügbaren Informationen angepasst werden sollen.

1 Prof. Dr. Franziska Boehm ist Leiterin des Bereichs Immaterialgüterrechte bei FIZ Karlsruhe – Leibniz-Institut für Informationsinfrastruktur und Inhaberin der gleichnamigen Professur am Karlsruher Institut für Technologie (KIT). Dem Bereich Immaterialgüterrechte gehören als wissenschaftliche Mitarbeitende u. a. an: Diana Dimitrova, Dr. Dara Hallinan und Francesca Pichierri.

DATENSCHUTZEMPFEHLUNGEN FÜR COVID-19-TRACKING UND TRACING APPS

Voreinstellungen	**Datenschutzfreundliche und IT-sicherheitsfreundliche Voreinstellungen** müssen bereits bei der Entwicklung von COVID-19-Apps mitgedacht werden. Datensicherheit, Datenvertraulichkeit und geeignete technische und organisatorische Maßnahmen müssen garantiert sein.[2]
Speicherung	Daten sollen möglichst **dezentral**, z. B. auf dem Gerät der Nutzerin und des Nutzers, und nicht zentral, d. h. in großen Datenbanken, gespeichert werden.[3]
Zugriff auf Daten	Der **Zugriff** auf Daten, insbesondere auf sensible Gesundheitsdaten, muss auf diejenigen beschränkt werden, die die Daten zu rechtmäßigen Zwecken benötigen, z. B. zur Behandlung, zur Forschung oder zur Krisenbekämpfung.
Übermittlung	Daten müssen **sicher**, z. B. durch **Verschlüsselung, gespeichert und übermittelt** werden.
Automatische Lösch-funktion	Die Daten auf den Apps sollten nach der Pandemie **automatisch gelöscht werden** (oder eine Löschfunktion/-taste vorsehen) u. a., um zu verhindern, dass die implementierten Überwachungsmaßnahmen länger als notwendig genutzt werden und um zu gewährleisten, dass die Nutzerin und der Nutzer jederzeit der Datenweitergabe widersprechen kann.
Zweckerfüllung	Nachdem die Zwecke der Datenverarbeitung durch die Apps erfüllt sind, müssen die Daten entweder **gelöscht oder anonymisiert** werden. Apps, die beispielsweise dazu dienen, die Einhaltung von der Quarantäne zu sichern, sollten die Daten nach 14 Tagen bzw. der angeordneten Dauer der COVID-19-Quarantäne löschen oder anonymisieren.
Anonyme Erhebung	Wenn eine App die intendierten Zwecke auch ohne die Verarbeitung von personenbezogenen Daten erfüllen kann, sollte eine anonyme Erhebung von Daten bevorzugt werden.
Re-identifizierung	Bei der Erhebung von pseudonymen oder anonymen Daten muss das **Risiko der Re-identifizierung**, vor allem auch durch Dritte, bedacht werden.
Transparenz	Der Datenfluss zwischen privaten und öffentlichen Stellen, die ggf. gemeinsam Daten verarbeiten, muss **transparent** sein. Das gilt auch für die **Datenverarbeitung, die Speicherdauer, die Zwecke der Verarbeitung, die Rechte der Betroffenen und für potenzielle Übermittlungen** der Daten an Dritte.
Information	Nutzerinnen und Nutzern müssen **leicht zugängliche und verständliche Informationen** über die Anwendbarkeit der Betroffenenrechte zur Verfügung gestellt werden. Die einfache Ausübung dieser Rechte sollte sich schon im **Design und der Gestaltung** der App wiederfinden.
Zusammenarbeit mit Aufsichtsbehörden	Eine **Zusammenarbeit mit den zuständigen Aufsichtsbehörden** und Datenschutz-expertinnen und -experten wird dringend empfohlen.
Sekundärzwecke, z.B. Forschung	Sekundärzwecke und die **Weiterverarbeitung der Daten zu anderen als dem ursprünglichen Zweck** muss beschränkt sein. Die Weiterverarbeitung zu Forschungszwecken muss z. B. die Voraussetzungen des Artikels 89 DSGVO erfüllen, wonach z. B. Daten, wenn möglich, anonymisiert werden sollten, wenn sie zu Forschungs- oder Statistikzwecken weiterverarbeitet werden (Prinzip der Speicherbegrenzung).
Datenschutzfolgen-abschätzung	Es sollte eine **Datenschutz-Folgeabschätzung**[4] durchgeführt werden, insbesondere wenn sensible Gesundheitsdatendaten verarbeitet werden oder Personen und deren Bewegungen durch die Apps kontinuierlich überwacht werden. Die Folgeabschätzung sollte veröffentlicht werden, auffindbar sein und regelmäßig aktualisiert werden
Berichtigung von Daten	Eingabedaten müssen richtig wiedergegeben werden. Nutzerinnen und Nutzer müssen zu jeder Zeit die Möglichkeit haben, die von ihnen erhobenen **Daten zu berichtigen**.
Beschränkungen und Wesensgehalt der Grundrechte	Alle **Beschränkungen von Datenschutzprinzipien** müssen die Voraussetzungen der Art. 23 und 89 DSGVO und Art. 15 e-Privacy Richtlinie erfüllen, insbesondere müssen sie den Wesensgehalt der Grundrechte wahren und verhältnismäßig sein.

2 Artikel 25 und 32 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), OJ L 119, 4.5.2016 (DSGVO).
3 Siehe zur Dezentralität solcher Apps, White Paper, Decentralized Privacy-Preserving Proximity Tracing, p. 2, verfügbar unter: https://github.com/DP-3T/documents.
4 Art. 35 DSGVO.