DEMOKRATIE IM AUSNAHMEZUSTAND

Verstoßen Tracing-Apps gegen den Datenschutz?

Alexander Roßnagel

Tracing-Apps dienen dem Zweck, Kontakte, durch die das Sars-Cov-2-Virus übertragen werden könnte, zu erkennen und dadurch Infektionsketten nachzuverfolgen sowie potenziell Infizierte zu warnen und zu veranlassen, Isolierungsmaßnamen zu ergreifen. Sie ergänzen dadurch die Handlungsmöglichkeiten der Gesundheitsämter. Diese werden erst tätig, wenn eine infizierte Person starke Symptome wie Husten oder Fieber bei sich erkannt, deswegen eine Arztpraxis aufgesucht und diese die Infektion dem Gesundheitsamt gemeldet hat. Dann kann das Gesundheitsamt versuchen, den Kontakten der infizierten Person nachzuspüren. Gegenüber dieser analogen Verfolgung der Infektionsketten hat die App drei entscheidende Vorteile: Sie ist schneller, sie vergisst nichts und sie erfasst auch die „Dunkelziffer".

„Eine App hat drei Vorteile: Sie ist schneller, sie vergisst nichts und sie erfasst auch die ‚Dunkelziffer`."

Das Tracing-App-System hält (mit Hilfe von Bluetooth-Kommunikation) fest, mit welchen Personen ein infizierter Mensch in den letzten Tagen Risikokontakte (15 Minuten im Umkreis von etwa 1,5 bis 2 Metern) hatte. Es kann diese Kontaktpersonen unmittelbar nach einem positiven Test der infizierten Person warnen, auch wenn die Kontaktpersonen noch keine Symptome haben, aber schon infektiös sind – oft Tage, bevor das Gesundheitsamt dies könnte.

Eine infizierte Person kann sich oft nicht erinnern, mit wem sie Risikokontakte hatte – insbesondere nach Situationen mit vielen anonymen Beteiligten, wie im Zug, in einer Versammlung oder einer Demonstration. Die Apps tauschen untereinander bei jedem Risikokontakt pseudonyme IDs aus, die eine Warnung aller Kontaktpersonen sicherstellen.

Hat eine Person etwa auf einer Versammlung zehn andere Personen angesteckt, die sie nicht kennt, wird das Gesundheitsamt nur von den Personen erfahren, die wegen Symptomen eine Arztpraxis aufsuchen. Alle anderen infizierten Personen sind aber auch ohne Symptome infektiös und verbreiten – unbewusst – das Virus „im Dunkeln". Dagegen warnt die App alle Risikokontaktpersonen und damit die gesamte „Dunkelziffer".

„Tracing-Apps sind datenschutzrelevant. Ob sie gegen das Datenschutzrecht verstoßen, hängt von der Gesamtgestaltung ab."

Aufgrund ihrer Vorteile hilft die App, die Pandemie zu bekämpfen. Verstößt sie dabei aber gegen den Datenschutz? Das ist grundsätzlich möglich. Die Informationen über eine tatsächliche oder mögliche Infektion sind personenbezogene Daten und als Daten über die Gesundheit sogar besonders schützenswert. Die Daten über Kontakte und Orte sind ebenfalls personenbezogen und

FRIEDRICH EBERT STIFTUNG
Forum Politik und Gesellschaft

ermöglichen, Bewegungs- und Verhaltensprofile einer Person zu erstellen. Tracing-Apps sind daher datenschutzrelevant. Ob sie gegen Grundsätze und Vorgaben des Datenschutzrechts verstoßen, hängt ab von der Gestaltung ihres Gesamtsystems. Die folgenden Überlegungen vergleichen die wesentlichen Anforderungen des Datenschutzes mit der Ausgestaltung der Corona-Warn-App des Robert Koch-Instituts (RKI).

Freiwilligkeit: Soweit die Nutzenden freiwillig die App herunterladen, sie nutzen und eine Infektion eingeben, verstößt dies nicht gegen die informationelle Selbstbestimmung. Trotz der Freiwilligkeit muss aber die Datenverarbeitung den Vorgaben des Datenschutzrechts entsprechen.

Zweckbindung: Die Daten dürfen nicht zu anderen, als den festgelegten Zwecken verwendet werden. Die Corona-Warn-App dient nur dem Zweck, Kontakte nachzuverfolgen und ihre Nutzenden zu warnen. Das RKI erklärt in seinen Nutzungsbedingungen, Apple und Google haben öffentlich zugesagt, die Daten nur für diesen Zweck zu verwenden.

Transparenz: Die betroffenen Personen müssen über die verarbeiteten Daten und die wesentlichen Funktionen der App informiert sein. Hier geht die Corona-Warn-App über das Geforderte hinaus. Ihr gesamter Sourcecode ist auf der Plattform Github offengelegt und kann von allen daraufhin geprüft werden, welche Funktionen der App programmiert sind und welche Daten sie verarbeitet.

Datenvermeidung: Das System darf nur so viele personenbezogene Daten verarbeiten, wie für den Zweck, Nutzende zu warnen, benötigt werden. Die Corona-Warn-Apps tauschen bei einem Risikokontakt untereinander alle 20 Minuten wechselnde IDs aus, die keine Identifizierung ermöglichen. Gespeichert wird außerdem nur der Tag des Kontakts, nicht aber Ort und Zeit.

Datensparsame Architektur: Für das System der Corona-Warn-App wurde diejenige Gestaltungsoption gewählt, die Datenschutz am besten gewährleistet. Die IDs werden nur in den Smartphones verarbeitet und gespeichert. Im zentralen Server beim RKI werden nur die IDs der Personen, die sich freiwillig als infiziert gemeldet haben, zum Abruf durch alle anderen Apps bereitgehalten. Missbrauch ist extrem erschwert, weil zentral nur wenige, für Angreifer anonyme Daten gespeichert und die Millionen Smartphones für Missbrauch kaum erreichbar sind.

„Die Corona-Warn-App zeigt, dass durch Technikgestaltung Gesundheits- und Datenschutz vereinbar sind.“

Das gesamte System der Corona-Warn-App ist nach Kriterien des Datenschutzes entworfen und umgesetzt worden. Für ein solch großes gesellschaftsweites IT-System ist dies einmalig und beispielgebend – für andere Tracing Apps, aber auch für andere IT-Systeme. Es zeigt, dass durch Technikgestaltung Gesundheits- und Datenschutz vereinbar sind.

Dies ist nicht bei allen Corona-Tracing-Apps der Fall. In Frankreich z.B. werden alle Daten der Risikokontakte auf einem zentralen Server gespeichert. Dies ermöglicht Missbrauch und erfüllt nicht die Forderungen nach einer datensparsamen Architektur und der Vermeidung nicht erforderlicher personenbezogener Daten. Auch die vom Bundesgesundheitsministerium zuvor vorgeschlagene Erfassung der Funkzellendaten oder der GPS-Daten der Smartphones hätte gegen die genannten Anforderungen verstoßen.

Auch wenn die Corona-Warn-App grundsätzlich datenschutzkonform ist, gibt es Schwachstellen, die beseitigt werden müssen. Zum einen müssen alle Corona-Teststellen so ausgerüstet werden, dass sie an der digitalen Kommunikation im Corona-Warn-App-System und damit an der anonymen Verarbeitung der Infiziertendaten teilnehmen können. Zum anderen müssen Lösungen für die Personen gefunden werden, die nicht an dem System teilnehmen können, weil sie nicht über neue Smartphone-Systeme verfügen. Schließlich bedarf es einer gesetzlichen Absicherung des Datenschutzes.

„Jetzt müssen der Datenschutz und die Folgen der App-Nutzung gesetzlich abgesichert werden.“

Denn die Freiwilligkeit der Nutzung ersetzt keine datenschutzrechtliche Einwilligung, schützt nicht vor Diskriminierung, sichert nicht die Zweckbindung, verhindert keine technischen Änderungen am Datenschutz und untersagt Apple und Google nicht den Zugriff auf die Daten. Gesetzliche Rahmenbedingen sind außerdem notwendig

FRIEDRICH EBERT STIFTUNG
Forum Politik und Gesellschaft

für die Folgen der App-Nutzung. So ist z.B. festzulegen, ob die App die Gewarnten dazu anhalten darf, sich testen zu lassen und sich in Quarantäne zu begeben, ob diese Warnung ausreicht, um sich wenigsten für drei Tage „krank“ melden zu können, und wie diese Meldung ansonsten zur Rechtfertigung genutzt werden kann, bestimmte private oder öffentliche Pflichten wegen der selbst auferlegten Quarantäne zu vernachlässigen. Nach der datenschutzgerechten Gestaltung der Corona-Warn-App ist auch eine technik- und nutzungsgerechte Gestaltung des rechtlichen Rahmens gefordert.

November 2020

Prof. Dr. Alexander Roßnagel ist Senior-Professor für öffentliches Recht mit dem Schwerpunkt Recht der Technik und des Umweltschutzes im Wissenschaftlichen Zentrum für Informationstechnikgestaltung (ITeG) der Universität Kassel und Sprecher des vom Bundesministerium für Bildung und Forschung geförderten „Forum Privatheit“.

DEMOKRATIE IM AUSNAHMEZUSTAND. WIE VERÄNDERT DIE CORONAKRISE RECHT, POLITIK UND GESELLSCHAFT?

Die Corona-Pandemie markiert die entscheidendste Krise der demokratischen Staaten und Gesellschaften seit dem Zweiten Weltkrieg. Von erheblichen Grundrechtseingriffen über die strapazierte Funktionsfähigkeit der politischen Institutionen bis hin zu immensen wirtschaftlichen und sozialen Folgeschäden stellt sie unser Gemeinwesen auf eine vorher nicht gekannte Probe. Gleichzeitig macht die Krise bestehende, längerfristige Herausforderungen des demokratischen Systems mit besonderer Deutlichkeit sichtbar. Daraus ergeben sich vielfältige demokratierelevante Fragen an die Wissenschaft, die wir in der neuen E-Paperreihe diskutieren wollen.

Alle bisher erschienen Beiträge sind **hier** abrufbar.

Kontakt: Alina Fuchs, Friedrich-Ebert-Stiftung, alina.fuchs@fes.de

FRIEDRICH EBERT STIFTUNG
Forum Politik und Gesellschaft