Die Spur von Corona Alle Tracing-Apps bergen Datenschutzrisiken

*Rainer Rehak**

Summary: The development and use of tracing apps to limit the spread of Covid-19 infections is associated with high hopes in the fight against the pandemic. It is also linked to the fear of massive infringements of fundamental rights. Conducting a data protection impact assessment, a structured risk analysis that identifies and evaluates possible consequences of data processing for fundamental rights in advance also considering measures to minimize these risks, fundamental rights infringements can be discussed in detail.

Kurz gefasst: Mit dem Einsatz von Apps für die Verfolgung von Covid-19-Infektionen werden einerseits große Hoffnungen bei der Pandemiebekämpfung verbunden, andererseits massive Grundrechtsgefährdungen befürchtet. Anhand einer Datenschutz-Folgenabschätzung – einer strukturierten Risikoanalyse, die mögliche grundrechtsrelevante Folgen der Datenverarbeitung im Voraus identifiziert und bewertet sowie Maßnahmen zur Minimierung dieser Risiken beschreibt – kann Letzteres differenziert diskutiert werden.

Viele Hoffnungen ruhen derzeit auf den sogenannten Corona-Tracing-Apps. Diese sollen automatisiert die epidemiologisch relevanten Kontaktereignisse von Nutzer*innen aufzeichnen, um im Infektionsfall zeitnah und rückwirkend die Kontaktpersonen der Infizierten zu warnen. Bislang wird diese Rückverfolgung der Kontakte von Mitarbeiter*innen der Gesundheitsämter telefonisch durchgeführt. Seit Mitte Juni ist nun auch in Deutschland eine solche App im Einsatz.

Auch wenn die Tauglichkeit einer solchen App für diesen Zweck sowohl epidemiologisch als auch technisch umstritten ist, soll es an dieser Stelle nicht um das Ob, sondern um das Wie einer solchen Anwendung gehen. Denn erst bei der Betrachtung der konkreten technischen Umsetzung lassen sich individuelle und gesellschaftliche Konsequenzen analysieren.

Ein geeignetes Mittel dafür ist eine Datenschutz-Folgenabschätzung, wie sie die Datenschutz-Grundverordnung (DSGVO) in Artikel 35 für bestimmte Fälle auch vorschreibt, wenn voraussichtlich hohe Risiken für die Grundrechte und -freiheiten von Personen entstehen. Datenschutz und seine Verankerung in der Gesetzgebung garantieren die Grundrechte und Grundfreiheiten im digitalen Zeitalter. Er bezieht sich nicht nur auf individuelle, sondern auch auf kollektive Rechte. Datenschutz hält die funktionelle Differenzierung moderner Gesellschaften aufrecht, indem er strukturelle Machtasymmetrien problematisiert und somit gesellschaftliche Grundfunktionen absichert. Im Unterschied zu Fragen der IT-Sicherheit geht es dem Datenschutz weniger um externe Angriffe auf Systeme und Daten, sondern um Grundrechtseinschränkungen durch die Datenverarbeitung selbst. Im Fokus steht deshalb nicht die „Privatheit" der einzelnen Person, sondern alle individuellen und strukturellen Auswirkungen einer Datenverarbeitung auf die Grundrechte. Eine Datenschutzanalyse geht somit prinzipiell von der verarbeitenden Organisation als der primären Risikoquelle aus, um den Blick von dort schließlich auch auf Plattformen, Dienstleister*innen, Nutzer*innen und externe Dritte zu richten.

Für das methodische Vorgehen im Rahmen einer Datenschutz-Folgenabschätzung (im folgenden DSFA) gibt es unterschiedliche Ansätze. In Deutschland wird dafür von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder das „Standard-Datenschutzmodell" empfohlen, an dem auch wir uns orientieren. Dieses verlangt zunächst eine Schwellwertanalyse, um zu klären, inwiefern eine DSFA für ein gegebenes Datenverarbeitungssystem nicht nur gesellschaftlich wünschenswert, sondern auch datenschutzrechtlich gefordert ist. Weil mit den Contact-Tracing-Apps sowohl eine neuartige Technologie sowie in großem Umfang personenbezogene und im Infektionsfall sogar medizinische Daten verarbeitet werden, ist dies hier ohne Zweifel der Fall. Trotzdem hat bis Ende Mai keine verantwortliche Stelle eine DSFA für eine der in Deutschland diskutierten Apps vorgelegt. Um die gebotene Aufmerksamkeit auf dieses Thema zu legen, haben wir, eine Gruppe von Wissenschaftler*innen und Datenschützer*innen, im April eine Muster-DSFA zur Corona-App erarbeitet und in die öffentliche Diskussion eingebracht. Sie wurde europaweit von diversen Datenschutz-Expert*innen, -Aufsichtsbehörden und der Zivilgesellschaft aufgenommen.

Aus Gründen der Minimierung des Grundrechtseingriffs und zur Vereinfachung der Analyse gehen wir in unserer DSFA von einem eng umrissenen Zweck für die Datenverarbeitung aus: die Warnung von Personen, die mit Infizierten Kon-

**in Zusammenarbeit mit Kirsten Bock, Christian Ricardo Kühne, Rainer Mühlhoff, Měto R. Ost und Jörg Pohle*

takt hatten. Die Grundfunktionalität einer solchen App wird im Idealfall umgesetzt, indem Smartphones mit der installierten App via Bluetooth regelmäßig pseudonyme Funksignale versenden und von anderen empfangen, sogenannte temporäre Kennungen. Diese Daten ermöglichen eine Kontaktnachverfolgung. Aus Dauer und Nähe der Kontakte soll ein Ansteckungsrisiko berechnet werden. Ortsinformationen, also zum Beispiel der GPS-Standort, werden durch dieses System nicht erhoben.

Dennoch gibt es verschiedene Ausgestaltungen des Systems. Ein wichtiger Diskussionspunkt war, ob die Berechnungen des individuellen Ansteckungsrisikos lokal auf den Mobiltelefonen der Nutzer*innen oder auf zentralen Servern stattfinden würden. Damit hängt auch die Frage zusammen, wie genau die relevanten Kontaktpersonen gewarnt werden. In der zentralen Architektur werden im Fall eines positiven Tests alle Kontaktereignisse von der App der infizierten Person auf einen Server hochgeladen. Dieser Server berechnet das Ansteckungsrisiko für alle Kontakte dieser Person und informiert diese dann aktiv. Der Server hat in dieser Variante Kenntnis der Infizierten, ihrer Kontakte und des Zusammenhangs zwischen den Kontakten, des sogenannten sozialen Grafen.

Die dezentrale Architektur dagegen sieht vor, dass bei einem positiven Test einer Nutzerin, eines Nutzers nur die von ihrer App in den vergangenen 14 Tagen ausgesendeten Funksignale als Datensatz auf den Server geladen werden, niemals aber die empfangenen. Die Apps aller anderen Nutzer*innen laden regelmäßig die Datensätze aller infizierten Nutzer*innen vom Server herunter und berechnen lokal auf den Smartphones, ob sie diese zuvor empfangen haben und somit ein Risiko der Ansteckung vorliegt. Der Server kennt in dieser Variante nur die temporären Funksignale der Infizierten, er kann weder ihre Kontakthistorie noch das Kontaktnetzwerk der Nutzer*innen nachvollziehen. Aus diesem Grunde ist die dezentrale Variante deutlich datenschutzfreundlicher.

Unsere DSFA betrachtet nur diesen dezentralen, grundrechtsschonenderen Ansatz, der inzwischen von Ländern wie etwa Österreich, Schweiz, Estland und seit Ende April auch von Deutschland verfolgt wird. Im ersten Schritt definieren wir den Zweck des Datenverarbeitungsverfahrens, in diesem Falle ausschließlich das Erkennen und Unterbrechen von Infektionsketten. Im zweiten Schritt gilt es, den Kontext der Verarbeitung deutlich zu machen. Dies umfasst neben dem allgemeinen gesellschaftlichen und politischen Hintergrund des App-Einsatzes sowie der technischen Umstände explizit auch die verschiedenen Akteure und ihre Interessen, um später eine fundierte Analyse von Risiken zu erstellen. Drittens müssen Annahmen und Anwendungsfälle für die Verarbeitung erarbeitet werden, um daran anschließend die Verarbeitungstätigkeit im Detail zu beschreiben. Dabei ist zu beachten, dass das Verfahren nicht nur die App, sondern auch die dazugehörigen Serversysteme sowie die verwendeten Smartphone-Funktionen von Apple und Google umfasst. Viertens wird dann auf dieser Basis die rechtliche Situation erarbeitet.

All diese Vorarbeiten kombinierend werden Schwachstellen, Gefahren und Risiken der Datenverarbeitung entwickelt. Damit sind Risiken bezüglich der Grundrechte der Betroffenen gemeint, und zwar aller Grundrechte. Auf die Risikoanalyse aufbauend werden dann Schutzmaßnahmen für die Rechte der Betroffenen bestimmt und zuletzt Empfehlungen für die Verantwortlichen gegeben. Risiken, für die keine Schutzmaßnahmen existieren, können ein Verarbeitungsverbot bedeuten.

Ausgewählte Erkenntnisse

(1) Die häufig beteuerte Freiwilligkeit der App-Nutzung könnte sich in der Praxis als Illusion herausstellen. Wie bereits politisch diskutiert wird, könnte die Nutzung als Bedingung für die individuelle Lockerung der Ausgangsbeschränkungen gelten. Das Vorzeigen der App könnte weiterhin als Zugangsbedingung für öffentliche oder private Gebäude, Räume oder Veranstaltungen dienen. Eine solche Verwendungsweise ist nicht durch den Zweck des Systems gedeckt, könnte aber durch Dritte (zum Beispiel Arbeitgeber oder private Veranstalter) dafür

Rainer Rehak ist Doktorand in der Forschungsgruppe Quantifizierung und gesellschaftliche Regulierung des Weizenbaum-Instituts für die vernetzte Gesellschaft und forscht zu systemischer IT-Sicherheit. Er studierte Informatik und Philosophie in Berlin und Hongkong. Seine Forschungsinteressen sind Datenschutz, IT-Sicherheit, staatliches Hacking, kritische Informatik sowie Technikzuschreibungen, etwa bei KI-Systemen. *[Foto: privat]*

rainer.rehak@wzb.eu

missbraucht werden. Dieses Szenario würde eine implizite Nötigung zur Nutzung der App bedeuten und zu einer erheblichen Ungleichbehandlung der Nicht-Nutzer*innen führen; die ohnehin vorhandene digitale Schere zwischen Smartphone-Besitzer*innen und -Nicht-Besitzer*innen würde sich auf weitere Lebensbereiche ausweiten. Zudem könnte der eigentliche Zweck der App unterlaufen werden, wenn Nutzer*innen aus Angst vor Nachteilen ihr Smartphone absichtlich nicht bei sich führen oder abwechselnd verschiedene Geräte nutzen. Nur durch eine flankierende Gesetzgebung, die diese und andere Zweckentfremdungen effektiv unterbindet, ist dieses Risiko abzumildern. Hierbei ist darauf hinzuweisen, dass die informierte Einwilligung kein geeigneter rechtlicher Rahmen für eine freiwillige App-Nutzung ist. Denn die informierte Einwilligung verlagert das Risiko der (Grundrechts-)Folgen sowie die Abwägung zwischen Nutzen und Folgen auf die Betroffenen. Dabei wäre es wichtig, gerade diese Abwägung zum Gegenstand demokratischer Aushandlung zu machen. Als Rechtsgrundlage wäre deshalb ein Gesetz erforderlich, in dem die (demokratisch legitimierte und kontrollierte) Gesetzgebung die Verarbeitung festlegt und auch deren Grenzen definiert.

(2) Ohne die Möglichkeit, die Daten und Ergebnisse anfechten zu können, ist der Grundrechtsschutz gefährdet: Es besteht ein hohes Risiko fälschlich registrierter Risikokontakte (Wände, Masken oder Laborfehler), die zu Unrecht auferlegte Selbst-Quarantäne zur Folge hätten. Um dem zu begegnen, bedarf es rechtlicher Möglichkeiten zur konkreten Einflussnahme, etwa das Zurückrufen falscher Infektionsmeldungen oder die Löschung falsch registrierter Kontaktereignisse.

(3) Alle bislang besprochenen Varianten eines Corona-App-Systems verarbeiten personenbezogene Gesundheitsdaten. Nur durch das Zusammenspiel organisatorischer, rechtlicher und technischer Maßnahmen kann der Personenbezug wirksam und irreversibel von den hochgeladenen Daten abgetrennt werden. Dieses Anonymisierungsverfahren kann diverse Formen annehmen, muss jedoch kontinuierlich datenschutzrechtlich durch die zuständigen Aufsichtsbehörden prüfbar sein. Organisatorisch müssen die Verantwortlichen in strategischer und die Betreiber in operativer Hinsicht eine Mischstruktur etablieren. Die Verantwortlichen – etwa das Robert Koch-Institut – könnten beispielsweise zwei unterschiedliche Betreiber auswählen: einer betreibt die Eingangsknoten im Netzwerk und trennt die Metadaten ab, darunter die IP-Adressen, der andere betreibt den eigentlichen Server. Auf der Ebene der Betreiber*innen muss etwa die informationelle Gewaltenteilung innerhalb der Organisation sichergestellt werden. Rechtlich müssen die Betreiber unabhängig sein, keine eigenen Interessen an den Daten haben und vor Pflichten zur Herausgabe von Daten geschützt sein, auch gegenüber staatlichen Sicherheitsorganen.

(4) Die Rolle der Plattformanbieter Apple (iOS) und Google (Android) ist kritisch zu begleiten. Eine Bluetooth-basierte Corona-Tracing-App ist aus technischen Gründen auf die Kooperation der Plattformanbieter angewiesen. Diese Machtposition haben die Plattformanbieter in den vergangenen Wochen genutzt, um gegen zahlreiche Regierungen eine dezentrale und somit datenschutzfreundlichere Architektur zu erzwingen. Damit ist das Datenschutzrisiko, das von den Plattformbetreibern selbst ausgeht, in der öffentlichen Diskussion weitestgehend aus dem Blick geraten. Die DSFA zeigt, dass es durchaus realistisch ist, dass Google und Apple an die Kontaktinformationen gelangen und daraus Informationen über Infektionsfälle und -risiken ableiten können.

Schließlich verlangt die nötige Transparenz bei der Umsetzung aller Datenschutz-Grundsätze eine quelloffene Entwicklung von Server und App nebst allen ihren Komponenten, beispielsweise als freie Software. Die Erkenntnisse unserer Risikoanalyse zeigen jedoch, dass eine Fokussierung auf die Technik die durchaus größeren gesellschaftlichen Implikationen des gesamten Verfahrens verschleiern kann. Nur Datenschutz-Folgenabschätzungen können Derartiges offenlegen. Sie sollten in diesem, aber auch in anderen, ähnlich folgenreichen Datenverarbeitungsprojekten veröffentlicht werden, damit sie nicht nur von Datenschutzbehörden eingesehen, sondern auch mit den Bürgerinnen und Bürgern breit diskutiert werden können.

Literatur

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: Das Standard–Datenschutzmodell – Eine Methode zur Datenschutzberatung und –prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 2.0b. 2020. Online: https://www.datenschutz–mv.de/datenschutz/datenschutzmodell/ (Stand 30.04.2020).

Podlech, Adalbert: „Die Trennung von politischer, technischer und fachlicher Verantwortung in EDV–unterstützten Informationssystemen". In: Wilhelm Steinmüller (Hg.): Informationsrecht und Informationspolitik. München: Oldenbourg Verlag 1976, S. 207–216.

Pohle, Jörg: Datenschutz und Technikgestaltung: Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung. Dissertation. Mathema–tisch–Naturwissenschaftliche Fakultät: Hum–boldt–Universität zu Berlin 2018. Online: https://edoc.hu–berlin.de/handle/18452/19886 (Stand 09.06.2020).

Rost, Martin: „Zur Soziologie des Datenschutzes". In: DuD – Datenschutz und Datensicherheit, 2013, 37. Jg., H. 2, S. 85–91. Online: https://www.maroki.de/pub/privacy/2013–02_DuD–SozDesDS.html (Stand 30.04.2020).