Datenschutz-Folgenabschätzung für die Corona-App

Kirsten Bock
kirsten.bock@fiff.de

Christian Ricardo Kühne
demian@fiff.de

Rainer Mühlhoff
rainer.muehlhoff@fiff.de

Měto R. Ost
meto.ost@fiff.de

Jörg Pohle
joerg.pohle@fiff.de

Rainer Rehak
rainer.rehak@fiff.de

Version 1.1 – 14. April 2020

Forum InformatikerInnen für Frieden und
gesellschaftliche Verantwortung (FIfF) e. V.

Kontakt: dsfa-corona@fiff.de

https://www.fiff.de/dsfa-corona

Inhaltsverzeichnis

Zusammenfassung und Ergebnisse

Seit der Ausbreitung des SARS-CoV-2-Virus auch in Europa Anfang 2020 lässt eine technische Vision unsere öffentlichen und politischen Debatten nicht mehr los: Die Pandemie könnte möglicherweise durch den Einsatz von Tracing-Apps für Smartphones eingedämmt werden. Dieses System würde automatisiert die zwischenmenschlichen Kontakte aller Nutzerïnnen aufzeichnen und es so erlauben, die Infektionsketten des Virus schnell und effizient nachzuvollziehen, um möglicherweise exponierte Personen frühzeitig isolieren zu können.

Staaten wie Singapur, Südkorea und Israel haben für diese Vorgehensweise teils radikale Vorbilder geliefert, die aus Sicht europäischer Rechtssysteme mit unverhältnismäßigen Grundrechtseingriffen verbunden sind. In Reaktion darauf haben sich europäische Initiativen gebildet, insbesondere das *Pan-European Privacy Preserving Proximity Tracing* (PEPP-PT)-Konsortium, die das Konzept einer Corona-Tracing-App aufgreifen und bereits im Namen mit einer Verpflichtung auf Datenschutz – oder zumindest auf »privacy«, was nicht dasselbe ist, – verbinden. So werden aktuell Tracing-Systeme konzipiert, die im Verhältnis zu den Maßnahmen bestimmter außereuropäischer Länder *vergleichsweise* datenschutzfreundlicher sind. Ein begleitender Mediendiskurs vermittelt seit Wochen konsequent das Bild: Corona-Apps *made in Europe* versprechen, die »Privatsphäre« aller Nutzerïnnen zu wahren und mit der EU-Datenschutzgrundverordnung (DSGVO) konform zu sein.

Datenschutzfreundlichkeit jedoch ist keine Ja/Nein-Frage, sondern eine komplexe Erwägung, die einer präzisen und detaillierten Diskussion bedarf. Die DSGVO selbst verpflichtet die Betreiberïnnen umfangreicher Datenverarbeitungssysteme (zu denen auch ein Corona-Tracing-System zählen würde, siehe Abschnitt 6) zur Anfertigung einer **Datenschutz-Folgenabschätzung (DSFA)** im Falle eines hohen Risikos für die Grund- und Freiheitsrechte. Hierbei handelt es sich um eine strukturierte Risikoanalyse, die mögliche grundrechtsrelevante Folgen einer Datenverarbeitung im Vorfeld identifiziert und bewertet.

Wir haben es angesichts der geplanten Corona-Tracing-Systeme mit einem gesellschaftlichen Großexperiment zur digitalen Verhaltenserfassung unter staatlicher Aufsicht in Europa zu tun. Wirksamkeit und Folgen entsprechender Apps sind noch nicht absehbar und es ist davon auszugehen, dass innerhalb der EU verschiedene Varianten erprobt und evaluiert werden. Die datenschutz- und somit grundrechtsrelevanten Folgen dieses Unterfangens betreffen potenziell nicht nur Einzelpersonen, sondern die Gesellschaft als Ganze. Aus diesem Grunde ist nicht nur die Anfertigung einer DSFA angezeigt, sondern insbesondere auch ihre Veröffentlichung – und eine öffentliche Diskussion. Da bisher keine der beteiligten Stellen eine allgemein zugängliche DSFA präsentiert hat und selbst die vorgelegten *privacy impact assessments* unvollständig sind, legen wir – eine Gruppe Wissenschaftlerïnnen und Datenschützerïnnen im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V. – mit diesem Dokument eigeninitiativ eine solche Datenschutz-Folgenabschätzung als konstruktiven Beitrag vor.

Überblick über das Verfahren

Wir beziehen uns in dieser DSFA auf die primär diskutierten Frameworks und Konzeptentwürfe für eine europäische Corona-Tracing-App, die auf Nahfeldsensortechnik mittels Bluetooth Low Energy (BTLE) beruhen. Dazu zählen insbesondere PEPP-PT, DP-3T, sowie ein allgemeines, vom CCC-Mitglied Linus Neumann vorgelegtes Konzept (siehe Neumann 2020). Unter diesen Projekten stellt PEPP-PT ein Rahmenkonzept dar, also keine konkrete App, sondern eine Spezifikation für ein solches Datenverarbeitungssystem. Innerhalb dieses Rahmens sind verschiedene Implementierungen, also konkrete Systeme/Apps, die das Framework umsetzen, denkbar; das DP-3T-Projekt ist dafür ein konkreter Vorschlag unter mehreren. Das PEPP-PT-Framework lässt prinzipiell zu, dass jede europäische Nation ihre eigene Implementierung entwickelt. Das Framework bietet also Gestaltungsspielraum, während es zugleich eine grenzüberschreitende Interoperabilität gewährleisten möchte.

In dieser Situation ist es ein zentrales Ergebnis unserer Untersuchung, dass alle betrachteten Frameworks – und insbesondere gilt dies für PEPP-PT – **wichtige technische Merkmale und Verfahrenseigenschaften offen lassen, die mit wesentlichen datenschutzrelevanten Folgen verbunden sind.** Es lassen sich grob mindestens drei Systemarchitekturen unterscheiden, die alle mit dem PEPP-PT-Framework kompatibel wären (vgl. Kapitel 1):

a) Eine **zentralisierte Architektur**: Anonymität der Nutzerïnnen und Geheimhaltung der Kontaktereignisse wird hier nur nach außen, also gegenüber anderen Nutzerïnnen und externen Akteurïnnen, angestrebt; die Betreiberïnnen und beteiligten Behörden können alle Nutzerïnnen identifizieren und mit den aufgezeichneten Kontakthistorien in Zusammenhang bringen.

b) Eine **teilweise dezentralisierte Architektur**, die zugleich **epidemiologische Forschung** erlaubt (DP-3T): Nutzerïnnen und Kontaktereignisse bleiben nur gegenüber anderen Nutzerïnnen und Dritten geheim, während der Server infizierte Nutzerïnnen de-anonymisieren kann. Das System verfügt über eine Datenspendefunktion, durch die Nutzerïnnen ihre Kontakthistorien für epidemiologische Untersuchungen zugänglich machen können – in diesen Fällen werden Kontaktereignisse infizierter Nutzerïnnen auch für Betreiberïnnen und Behörden nachvollziehbar.

c) Ein **gänzlich dezentralisierte Architektur** (vgl. Neumann 2020): Gegenüber anderen Nutzerïnnen und Dritten bleiben Nutzerïnnen anonym und Kontaktereignisse geheim. Betreiberïnnen und Behörden können infizierte Nutzerïnnen deanonymisieren, nicht jedoch ihre Kontakthistorien. Epidemiologische Untersuchungen werden nicht unterstützt.

Betreiberïnnen und Behörden können ...	Variante a	Variante b	Variante c
... alle Nutzerïnnen de-anonymisieren	ja	nein	nein
... infizierte Nutzerïnnen de-anonymisieren	ja	ja	ja
... alle Kontakte nachvollziehen	ja	teilweise	nein

Unsere **DSFA bezieht sich schwerpunktmäßig auf die datenschutzfreundlichste Variante c,** teilweise gehen wir auf technische Details von Variante b ein.

Im Ergebnis zeigt sich erstens, dass **selbst die dezentrale Implementierung zahlreiche gravierende Schwachstellen** (siehe Kapitel 7) **und Risiken** birgt, denen begegnet werden muss. Zweitens zeigt ein Vergleich der zentralen und dezentralen Varianten, den wir an relevanten Stellen ziehen, dass **wesentliche Datenschutz-Konsequenzen mit der Entscheidung zwischen Zentralität und Dezentralität verbunden sind.** Eine beliebige PEPP-PT-Implementierung als datenschutzfreundlich zu bezeichnen, ist deshalb pauschal nicht zutreffend.

Die wichtigsten Erkenntnisse, Risiken und Lösungsansätze

Wir führen hier vorab eine Auswahl der wichtigsten Erkenntnisse, Risiken und Lösungsansätze an:

1. Die in den Diskussionen vielfach betonte **Freiwilligkeit der App-Nutzung ist eine Illusion.** Es ist vorstellbar und wird auch bereits diskutiert, dass die Nutzung der App als Voraussetzung für die individuelle Lockerung der Ausgangsbeschränkungen gelten könnte. Das Vorzeigen der App könnte als Zugangsbarriere zu öffentlichen oder privaten Gebäuden, Räumen oder Veranstaltungen dienen. Denkbar ist, dass Arbeitgeberïnnen solche Praktiken schnell adaptieren, weil sie mittels freiwillig umgesetzter Schutzmaßnahmen schneller ihre Betriebe wieder öffnen dürfen. Dieses Szenario bedeutet eine *implizite Nötigung zur Nutzung der App* und führt zu einer erheblichen Ungleichbehandlung der Nicht-Nutzerïnnen. Weil nicht jede Person ein Smartphone besitzt, wäre hiermit auch eine Diskriminierung ohnehin schon benachteiligter Gruppen verbunden.

2. **Ohne Intervenierbarkeit und enge Zweckbindung ist der Grundrechtsschutz gefährdet.** So besteht ein hohes Risiko fälschlich registrierter Expositionsereignisse (falsch positiv), die zu unrecht auferlegte Selbst-Isolation oder Quarantäne zur Folge haben (zum Beispiel Kontaktmessung durch die Wand zwischen zwei Wohnungen). Um dem zu begegnen, bedarf es rechtlicher und faktischer Möglichkeiten zur effektiven Einflussnahme, etwa das Zurückrufen falscher Infektionsmeldungen, die Löschung falsch registrierter Kontaktereignisse zu einer infizierten Person und das Anfechten von infolge der Datenverarbeitung auferlegter Beschränkungen. Eine solche Möglichkeit sieht bisher keines der vorgeschlagenen Systeme vor.

3. **Alle bislang erwähnten Verfahren verarbeiten personenbezogene Gesundheitsdaten.** Das Verfahren besteht aus der Verarbeitung von Kontaktdaten auf den Smartphones, der Übermittlung dieser Daten auf einen Server nach der Diagnose einer Infektion und letztendlich deren Verteilung an alle anderen Smartphones zur Prüfung auf einen möglichen Kontakt mit Infizierten. Alle Daten auf einem Smartphone sind personenbezogen, nämlich bezogen auf die Nutzerïn des Gerätes. Weil nur diejenigen Personen Daten übertragen, die als infiziert diagnostiziert wurden, sind die übertragenen Daten zugleich Gesundheitsdaten. Somit unterliegen diese dem Schutz der DSGVO.

4. **Anonymität der Nutzerïnnen muss in einem Zusammenspiel rechtlicher, technischer und organisatorischer Maßnahmen erzwungen werden.** Nur durch einen mehrdimensionalen Ansatz kann der Personenbezug wirk-

> sam und irreversibel von den verarbeiteten Daten abgetrennt werden, so dass danach von anonymen Daten gesprochen werden kann. Allen derzeit vorliegenden Vorschlägen fehlt es an einem solchen expliziten Trennungsvorgang. Wir haben in dieser DSFA rechtliche, technische und organisatorische Anforderungen formuliert, deren Umsetzung in der Praxis eine wirksame und irreversible Trennung sicherstellen kann – nur unter diesen Voraussetzungen dürften die infektionsanzeigenden Daten ohne Personenbezug (iDoP) an alle Apps verbreitet werden.

Für eine umfassende Darstellung der Risiken und Schwachstellen verweisen wir auf Kapitel 7, für die notwendigen Schutzmaßnahmen auf Kapitel 8.

Die Perspektive des Datenschutzes geht grundsätzlich davon aus, dass **die wesentlichen Risiken der Datenverarbeitung von den Betreiberïnnen eines Datenverarbeitungssystems ausgehen.** In solchen Fällen ist es dringend erforderlich, dass die Barriere zur einer missbräuchlichen Verarbeitung, die den Datenverarbeitungszweck übersteigt, in einer wirksamen Kombination von rechtlichen, technischen und organisatorischen Maßnahmen besteht – und nicht bloß in öffentlich geäußerten Versprechungen der Betreiberïnnen, den Datenschutz zu beachten. Ergriffene Maßnahmen müssen aktiv prüfbar gemacht und sauber dokumentiert werden.

Die quelloffene Entwicklung von Server und Apps nebst allen ihren Komponenten – beispielsweise als freie Software – ist eine wesentliche Voraussetzung, damit es **Transparenz bezüglich der Umsetzung der Datenschutz-Grundsätze** nicht nur für Datenschutzaufsichtsbehörden, sondern gerade auch für die Betroffenen und die (Zivil-)Gesellschaft insgesamt gibt. Nur so kann es gelingen, Vertrauen auch bei jenen zu erzeugen, die nicht alle informationstechnischen Details verstehen.

Auch von Dritten können Risiken für Grundrechte ausgehen. Dabei ist nicht in erster Linie an Hackerïnnen, sondern an **kommerzielle Akteurïnnen,** etwa große Plattformbetreiberïnnen, und staatliche Stellen zu denken. Diese profitieren gegebenenfalls von einem erhöhten Aufkommen an Tracking-Daten, die sie selbst auswerten können, weil Bluetooth für die Corona-App immer eingeschaltet sein muss, oder durch umfassende Zugriffmöglichkeiten auf Daten, die bei privaten Akteurïnnen gespeichert sind.

Datenschutzanalysen betrachten die gesamte Verarbeitung von Daten, nicht nur die dabei eingesetzten Apps.

In der öffentlichen Diskussion und in den betrachteten App-Projekten wird Datenschutz nach wie vor auf den Schutz der Privatsphäre, also Geheimhaltung gegenüber Betreiberïnnen und Dritten, und auf Aspekte der IT-Sicherheit wie Verschlüsselung reduziert. Mit dieser Verengung der Sichtweise kommen die erheblichen, gesellschaftlich wie politisch fundamentalen Risiken, die wir in dieser Folgeabschätzung aufzeigen, nicht nur nicht in den Blick – sie werden zum Teil sogar verschleiert.