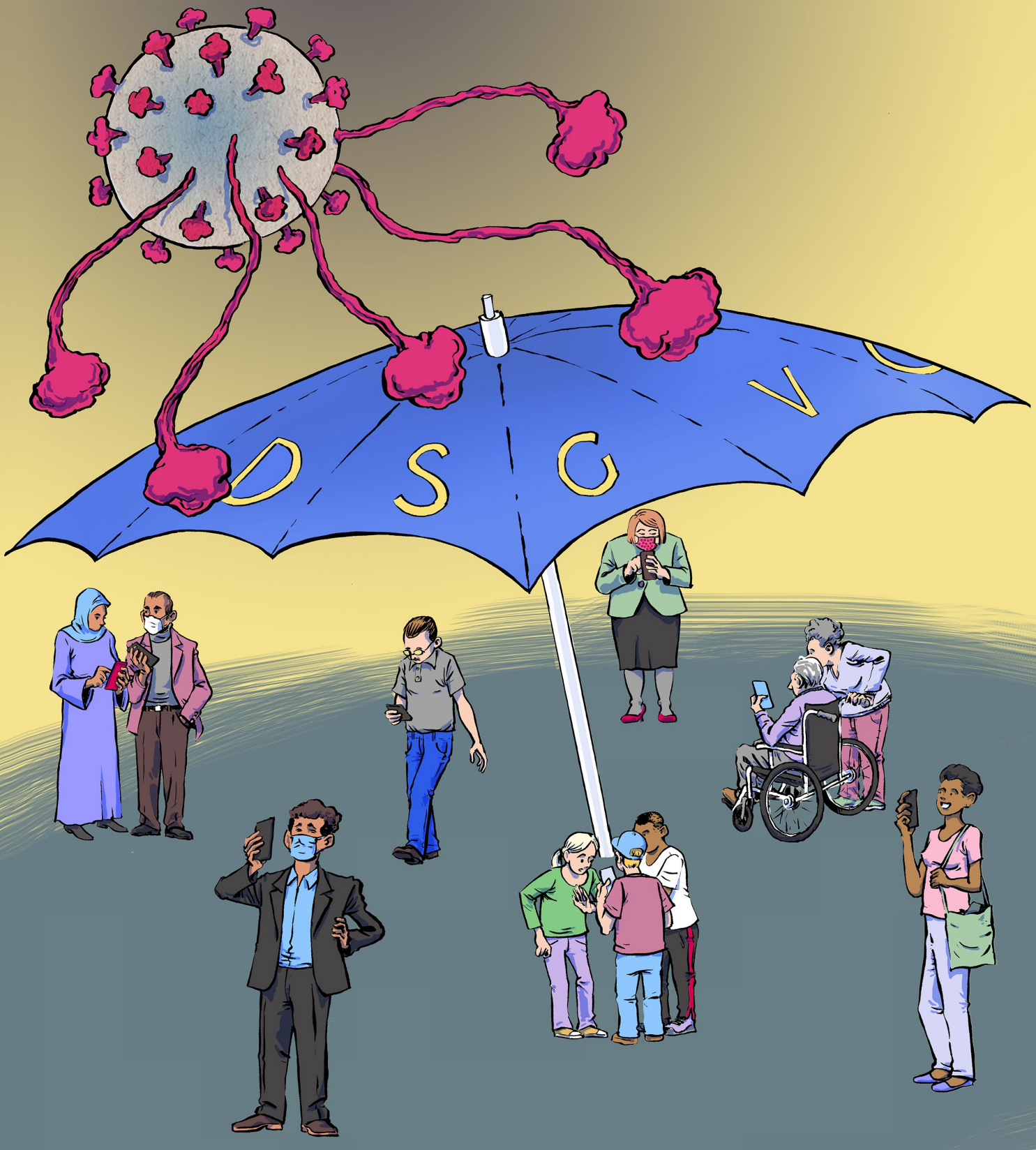
„Corona-Apps“ und Zivilgesellschaft: Risiken, Chancen und rechtliche Anforderungen



www.greenpeace.de

GREENPEACE

„Corona-Apps“ und Zivilgesellschaft:
Risiken, Chancen und rechtliche Anforderungen

Contact-Tracing-Apps auf Smartphones werden als ein wichtiger Baustein zur Eindämmung des Corona-Virus diskutiert. Mit ihnen soll es deutlich schneller und leichter möglich sein, Menschen zu identifizieren, die mit infizierten Personen Kontakt hatten. Im Gegenzug könnten die Kontaktbeschränkungen in absehbarer Zeit gelockert werden. Im besten Falle können Contact-Tracing-Apps also dazu beitragen, die weitere Übertragung des Virus einzudämmen und gleichzeitig einen Teil unserer in den letzten Wochen verlorenen Freiheiten zurückzugewinnen.

Empirische Untersuchungen zur Effektivität solcher Apps gibt es bislang nicht. Theoretische epidemiologische Studien kamen jedoch zu dem Ergebnis, dass ein effektives Contact-Tracing nur möglich ist, wenn circa 60 Prozent der Bevölkerung eine entsprechende App verwenden. Der Erfolg von Tracing-Apps wird somit maßgeblich von ihrer breiten gesellschaftlichen Akzeptanz abhängen. Diese Akzeptanz lässt sich jedoch nicht durch rechtlichen Zwang verordnen, sondern hängt unmittelbar davon ab, in welchem Maße die Nutzer*innen der App und den mit ihr verbundenen Akteur*innen vertrauen – Datenschutz und Sicherheit sind dabei zentral.

Bei allen Chancen, die Contact-Tracing-Apps bieten, bergen sie auch Risiken. Datensparsame Modelle sind genauso denkbar wie Apps, die „Social Graphing“ ermöglichen würden, also die umfassende Nachverfolgung sozialer Interaktionen von Individuen. Hiervor warnt beispielsweise das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V. in seiner Datenschutz-Folgenabschätzung. Apps mit umfassenden Nachverfolgungsmöglichkeiten können gerade für zivilgesellschaftliche Organisationen gefährlich werden. Denn in ihrer Arbeit ist es oft wesentlich, personenbezogene Daten geheim halten zu können. Zum Beispiel, wenn es um den Kontakt mit Whistleblower*innen geht oder um die medizinische Behandlung von Menschen ohne gültige Aufenthaltspapiere, die von der Abschiebung bedroht sind. Zivilgesellschaftliche Organisationen können gefährdete Personen in vielen Fällen nur ausreichend schützen, wenn sie ihre Anonymität gewährleisten können.

Dieser Beitrag des Monitoring-Projekts „Corona-Virus und Civic Space in Deutschland“ untersucht daher die möglichen Auswirkungen von Contact-Tracing-Apps auf die Zivilgesellschaft. Wir beleuchten die Risiken und Potenziale der Apps, und auch die wichtige Rolle, die zivilgesellschaftliche Akteure in der öffentlichen Diskussion über ihren Einsatz spielen.

Eine finale Bewertung ist indes noch nicht möglich, solange noch keine fertige App vorliegt. Denn die Details sind wesentlich, insbesondere die rechtlichen Grundlagen, die geplante Anwendung und der Quellcode. Im Sinne der Zivilgesellschaft ist es zwingend notwendig, dass vor einem flächendeckenden Einsatz der App ihr Quellcode veröffentlicht wird, denn nur so können unabhängige Datenschutz- und IT-Expert*innen sie kritisch untersuchen.

Doch auch unabhängig von der konkreten Ausgestaltung der Tracing-Apps gibt es klare rechtliche Anforderungen: Die bestehenden datenschutzrechtlichen Grenzen müssen eingehalten werden. Sie sind Schutzschild der Zivilgesellschaft. Darum sollten sie auch in der Debatte um die geplanten Apps eine zentrale Rolle spielen.

A. Contact Tracing-Apps & Datenspende-Apps: Wie funktionieren sie?

Wie funktionieren Contact Tracing-Apps und welches Modell wird von der Bundesregierung unterstützt?

Die Bundesregierung hat während der letzten Wochen verschiedene App-Modelle geprüft, die effektives „Contact Tracing“ und Datenschutz miteinander in Einklang bringen sollen. Insbesondere sollen keine Standortdaten erhoben werden, höchstmögliche IT-Sicherheitsstandards eingehalten und die Informationen über die App-Nutzer*innen datenschutzkonform erhoben werden. An der praktischen Umsetzung wird bereits mit Hochdruck gearbeitet.

Grundlage soll die „Bluetooth Low Energy“-Technologie sein. Denn die zuverlässige Reichweite des Bluetooth-Signals könnte sich in etwa mit dem decken, was Virolog*innen in Bezug auf die Corona-Infektionsgefahr als „Hochrisikokontakte“ bezeichnen – anderthalb bis zwei Meter physische Nähe über eine gewisse zeitliche Dauer. Zurzeit ist noch unklar, wie zuverlässig die Entfernungsbestimmung mittels „Bluetooth Low Energy“ wirklich funktioniert. Einige IT-Expert*innen sind skeptisch angesichts verschiedener Geräte und Betriebssysteme. Zudem muss ausgeschlossen werden, dass alltägliche Zufälligkeiten, etwa ob das Gerät in der Hosentasche transportiert oder in der Hand gehalten werden, die Messungen verfälschen. Dafür laufen derzeit Kalibrierungsversuche, auch mit Unterstützung der Bundeswehr.

Von allen Smartphones, die der entsprechend kalibrierte Bluetooth-Sensor erfassen konnte, soll die App eine ID-Liste anlegen. Diese IDs fungieren als Pseudonyme der Geräte-Nutzer*innen; sie sind temporär und werden auf ihrem Smartphone erzeugt. Mithilfe dieser Liste soll die App zeitnah alle „Hochrisikokontakte“ von Personen warnen können, die positiv auf Corona getestet wurden. Wenn Nutzer*innen der App positiv auf Corona getestet werden, können sie freiwillig und pseudonym über ihre Infektion informieren. Technisch unterscheiden sich die daran anschließenden Matching-Ansätze, das Ziel bleibt aber gleich: Hochrisikokontakte sollen schnellstmöglich darüber informiert werden, dass sie sich möglicherweise mit Corona angesteckt haben. Außerdem könnten die betroffenen Personen aufgefordert werden, sich testen zu lassen und/oder sich in Quarantäne zu begeben bzw. beim Gesundheitsamt zu melden. Es benötigt dafür entsprechende Kommunikations- und Begleitungskonzepte von der Bundesregierung, damit Betroffene die Situation gut bewältigen können.

Nachdem zunächst unterschiedliche Modelle für Contact-Tracing-Apps diskutiert wurden, hat sich die Bundesregierung am 26. April 2020 für den Einsatz einer

dezentralen Softwarearchitektur ausgesprochen. Damit wird der sogenannte PEPP-PT-Ansatz (Pan-European Privacy-Preserving Proximity Tracing) nicht weiterverfolgt, der einen zentralen Datenabgleich vorsieht und anfangs auch durch Bund, Länder und andere europäische Staaten unterstützt wurde. Diese Initiative wurde von 130 europäischen Wissenschaftler*innen, Firmen und Forschungseinrichtungen Anfang April ins Leben gerufen, federführend war dabei das Heinrich-Hertz-Institut (HHI) der Fraunhofer-Gesellschaft. Aufgrund innerer Konflikte ist das Bündnis dann jedoch immer weiter zerfallen.

Mit Blick auf den zentralen Ansatz hatten zuletzt der Chaos Computer Club (CCC), netzpolitische Vereine, Informatiker*innen und die Stiftung Datenschutz gewarnt, dass der „geringe Datenschutz eines zentralen Ansatzes und das Fehlen technischer Beschränkungen gegen Zweckentfremdung“ das Vertrauen in eine App untergraben würde. Zuvor mahnten über 300 Wissenschaftler*innen aus den Bereichen IT-Sicherheit und Datenschutz, dass mit einem solchem Werkzeug nicht im großen Stil sensible Daten der Bevölkerung erhoben werden dürften.

Der dezentrale DP-PPT-Ansatz (auch DP^3T-Initiative) wurde ebenfalls von einem internationalen Konsortium aus Expert*innen unterschiedlicher Fachrichtungen entwickelt. Der Bundesregierung schwebt derzeit auf Basis dieses Ansatzes eine App vor, die „die in Kürze zur Verfügung stehenden Programmierschnittstellen der wesentlichen Anbieter von mobilen Betriebssystem nutzt und gleichzeitig die epidemiologische Qualitätssicherung bestmöglich integriert“.

Eine ständig im Hintergrund aktive Contact-Tracing-App kann allerdings nur dann technisch effizient eingesetzt werden, wenn die entsprechenden Schnittstellen (sogenannte *Application programming interfaces,* oder *APIs*) der Smartphone-Betriebssysteme zur Verfügung stehen. Sprich: Ohne die großen Hersteller Apple und Google geht es nicht. Apple und Google haben bereits angekündigt, dass sie an einer API für Contact-Tracing-Apps arbeiten – allerdings nur für dezentrale App-Modelle. Damit erschweren die Hersteller es Gesetzgebern schon im Vorhinein, alternative Modelle zu etablieren, etwa eine zentrale und eine dezentrale Alternative mit Auswahlmöglichkeiten für individuelle Nutzer*innen anzubieten. Dies war Presseberichten zufolge auch der Grund, warum die Bundesregierung letztlich die Unterstützung für PEPP-PT beendete.

Was ist die Corona-Datenspenden-App und wie unterscheidet sie sich vom Contact-Tracing?

Während Tracing-Apps noch in der Entwicklung sind, ist bereits eine **Corona-Datenspende-App** verfügbar. Hierbei handelt es sich um ein völlig anderes und von den Tracing-Apps unabhängiges Konzept: Die Datenspende-App verfolgt keine Kontakte nach, sondern übermittelt die von Fitnesstrackern oder Smartwatches erhobenen gesundheitsbezogenen Daten. Die sogenannten Wearables messen Körperfunktionen wie z. B. Puls, Blutdruck, Temperatur oder Schlafphasen. Nutzer*innen solcher Technologien können diese Daten einverständlich über eine sogenannte Corona-Datenspende App an das Robert-Koch-Institut (RKI) „spenden“,

gemeinsam mit soziodemographischen Daten wie Alter, Geschlecht, Gewicht und Postleitzahl, damit das RKI weitere Erkenntnisse zu Ausbreitung und Verlauf der COVID-19-Erkrankungen gewinnen kann.

Die Corona-Datenspende App steht aus unterschiedlichen Gründen in der Kritik. Kritisiert werden sowohl das Entwicklungsverfahren als auch auf die konkrete Ausgestaltung der App, insbesondere unzureichender Datenschutz und IT-Sicherheit. So erhielt die zuständige Datenschutz-Aufsichtsbehörde nicht die endgültige Version der App für eine Vorab-Prüfung. Zudem konzipierte ein eHealth Start-Up die App mit einem proprietären Quellcode, der nicht Open Source und daher nicht für Dritte einseh- und überprüfbar ist. Darüber hinaus bestehen Bedenken hinsichtlich der Nutzung der Daten. Denn der Zweck der App ist mit der „verbesserten Steuerung von Eindämmungsmaßnahmen gegen die Corona-Pandemie“ sehr weit gefasst. Da er eben nicht auf ein bestimmtes Forschungsvorhaben begrenzt ist, könnte er nachträglich noch erweitert werden. Zudem ist fraglich, ob die angelegte Speicherdauer von zehn Jahren dem Grundsatz der Datensparsamkeit gerecht wird.

B. Risiken und Problemfelder

In der aktuellen Debatte um Contact-Tracing-Apps zeichnen sich insbesondere vier Problemkomplexe ab: Missbrauchsmöglichkeiten, Fehleranfälligkeit, rechtliche Konsequenzen für Nutzer*innen und die Freiwilligkeit der Nutzung. Hierzu haben sich bereits verschiedene zivilgesellschaftliche Akteur*innen geäußert, etwa der CCC, FifF und Reporter Ohne Grenzen.

1. Missbrauchsmöglichkeiten wegen des großen Datenumfangs

Die Contact-Tracing-App soll die Daten eines Großteils der Bevölkerung verarbeiten. Zwar werden diese Daten grundsätzlich mit kryptographischen Mitteln pseudonymisiert. Temporäre IDs dienen als Pseudonyme, die nach kurzer Zeit ausgetauscht werden, um eine Identifizierung einzelner Personen durch Unbefugte zu erschweren. Die Schwierigkeit ist aber, dass die erhobenen Daten durch die Zusammenführung mit anderen Daten de-pseudonymisiert und damit im Nachhinein ein Personen-Bezug hergestellt werden könnte.

Damit das System funktioniert, muss es im Falle einer bestätigten Infektion eine bestimmte ID als infiziert markieren und alle IDs, die mit ihr in Kontakt waren, benachrichtigen können. Sobald es bestimmten Akteuren möglich wird, diese IDs durch Hinzuziehung weiterer Daten Individuen zuzuordnen, sind sensible Gesundheitsdaten im Umlauf (vgl. Art. 9 DSGVO) – mit unterschiedlichen Risiken für die Nutzer*innen, je nachdem, wie die App konkret ausgestaltet wird.

2. **Wer hat Zugriff auf die Daten und inwieweit eröffnet dies Überwachungs-möglichkeiten?**

Eine wesentliche Frage bei der Umsetzung der App ist, wie genau die temporären IDs miteinander abgeglichen werden. Beide Umsetzungsmöglichkeiten, sowohl die zentrale als auch die dezentrale, bieten hierbei Angriffsflächen, anhand derer ein Personenbezug hergestellt und Überwachung ermöglicht werden könnte.

Werden die ID-Listen auf einem zentralen Server gespeichert, könnte der Betreiber die pseudonymisierten IDs theoretisch durch Verknüpfung mit anderen Daten – etwa mit den bei der Kommunikation mit dem Server verwendeten personenbezogenen IP-Adressen – re-personalisieren und so Nutzer*innen überwachen. Dies ist ausdrücklich nicht vorgesehen, dennoch könnten die gesammelten Daten Begehrlichkeiten wecken. Auch ein Zugriff mit kriminellen Absichten ist eine potenzielle Gefahr.

Bei der Implementierung ist also auch zu klären, **wer Anbieter der Tracing-App sein sollte und inwiefern sichergestellt wird, dass unabhängige Audits durchgeführt werden**.

Bei einem dezentralen Ansatz besteht hingegen eher das Risiko individueller Angriffe auf die Privatheit der Nutzer*innen: So könnten individuell publizierte Infektionsmeldungen leichter Individuen zugeordnet werden; etwa, wenn eine Kamera mit einem Bluetooth-Scanner kombiniert würde, der IDs von Kund*innen oder Arbeitnehmer*innen aufzeichnet. Käme dann über die App die Liste „infizierter“ IDs, wäre ein rascher Rückschluss auf das Aussehen und damit die Identität Infizierter möglich.

Zudem stellt sich die Frage, ob verhindert werden kann, dass die **Betriebssysteme für die App,** Apple iOS und Google Android, Zugriff auf die Daten erhalten. Die Konzerne verneinen, dass ein solcher Zugriff möglich sein wird. Die Daten sollen lediglich geräteintern in einer sogenannten „Secure Enclave“ gespeichert werden – also einer Art geheimem Daten-Tresor, auf den auch die Betriebssystem-Hersteller nicht zugreifen können sollen. Bis der Quelltext sowohl konkreter Apps als auch der entsprechenden Funktionen der Betriebssysteme vorliegt, kann dies nicht abschließend bewertet werden.

3. **Sind Tracing-Apps fehleranfällig?**

Eine weitere Gefahr sind sogenannte „False Positives“, dass also die Contact-Tracing-App fälschlicherweise davon ausgeht, eine Person sei in Kontakt mit einer infizierten Person gekommen. False Positives könnten z. B. entstehen, wenn Personen sich zwar räumlich nah gekommen sind, aber durch eine Glasscheibe getrennt waren und sich deswegen gar nicht anstecken konnten. False Positives könnten aber auch durch missbräuchliche Meldungen – sogenanntes „Trollen“ – ausgelöst werden, wenn sich also Personen bewusst als infiziert melden, obwohl sie keinerlei Hinweise auf eine Infektion haben, um andere in die Quarantäne zu zwingen. Dies muss unbedingt durch eine geeignete Gestaltung der Apps ausgeschlossen werden, beispielsweise indem eine Infektionsmeldung nur möglich ist, wenn zugleich eine TAN eingegeben wird, die

das Testlabor zusammen mit dem positiven Testergebnis mitteilen könnte. Dieser Aspekt sollte auch deshalb im Blick bleiben, weil Infizierte stigmatisiert und ausgegrenzt werden könnten.

Der umgekehrte Fall ist ein „False Negative“. Hierbei geht die App davon aus, eine Person habe keinen Kontakt mit einer infizierten Person gehabt, obwohl dies tatsächlich der Fall gewesen ist. Dies kann zum Beispiel geschehen, wenn das Bluetooth-Signal gestört wird und deshalb zu schwach ist. Dann könnten Hochrisiko-Personen unerkannt andere anstecken.

Bei der weiteren Umsetzung der Contact-Tracing-App sollte auch sichergestellt werden, dass False Positives oder False Negatives weitestgehend verhindert werden. Eine mögliche Lösung wäre die laufende Verbesserung und Korrektur des Bewertungs- und Meldesystems der App, indem dieses als lernendes System gestaltet wird. Die App könnte jeweils abgleichen, welche Initialmeldungen bei Kontaktpersonen zu Folgemeldungen geführt haben. Dadurch könnte sie immer bessere Parameter zur Erkennung und Bewertung möglicher Fehlmeldungen entwickeln. Bei einer zentralen Lösung ließe sich eine solche künstliche Intelligenz leicht im zentralen Server installieren. Bei einer dezentralen Lösung ist eine Fehlmeldung-Korrektur zwar auch denkbar (sog. „federated learning“), aber technisch deutlich schwieriger umsetzbar.

4. **Welche rechtlichen Konsequenzen hat die Contact-Tracing-App für die Nutzer*innen?**

Für die User der Contact-Tracing-App stellt sich die Frage, was es für Konsequenzen für sie hat, wenn die App ihnen meldet, dass sie mit einem*r Infizierten Kontakt hatten.

Unklar ist bisher, wie genau die Gesundheitsämter in die Abläufe integriert werden sollen und könnten. Eine Infizierung mit dem Corona-Virus ist nach dem Infektionsschutzgesetz meldepflichtig (§ 6 IfSG i.V.m der Verordnung über die Ausdehnung der Meldepflicht) und muss daher an das Gesundheitsamt weitergegeben werden. Fraglich ist, ob das Infektions-Meldungsverfahren ab Einführung der App parallel manuell weiterläuft oder nur noch elektronisch funktioniert. Eine elektronische Lösung würde in jedem Fall datenschutzrechtlichen Rechtfertigungsbedarf auslösen, zudem wäre nach Art. 9 Abs. 2 lit. h DSGVO eine Rechtsgrundlage erforderlich.

Weiterhin ist bisher offen, ob mit der App Quarantäneanordnungen digital überwacht werden können und wer diese Überwachung kontrollieren würde. Je nachdem könnte die Gefahr bestehen, dass das Gesundheitsamt anhand der Meldungen jegliche Kontakte nachvollziehen kann, also deutlich mehr als im derzeitigen analogen Verfahren. Hierdurch lassen sich soziale Netze nachvollziehen. Bei einem digitalen Contact-Tracing würde die App zudem auch unbemerkte und unbekannte Kontakte, etwa Sitznachbar*innen im Zug, registrieren und könnte diese melden. Dies würde einerseits deutlich die Effektivität, andererseits aber auch den datenschutzrechtlichen Rechtfertigungsbedarf erhöhen.

5. Die Bedingung: Freiwillige Nutzung

Eng mit den rechtlichen Konsequenzen hängt die Freiwilligkeit der App-Nutzung zusammen. Insbesondere wenn als Rechtsgrundlage eine datenschutzrechtliche Einwilligung dienen soll, ist eine freiwillige Nutzung Voraussetzung. Die Bundesregierung versichert aktuell, dass die Nutzung freiwillig sein soll.

Ein Problem könnte sich aber aus einem mittelbaren Nutzungszwang ergeben. Denn: Die App soll insbesondere dazu dienen, den „Lockdown“ abzumildern, der unsere Grundrechte aktuell stark einschränkt. Sollten Menschen ihre Grundrechte aber nur ausüben können, wenn sie die App nutzen, besteht keine Freiwilligkeit mehr, die ihren Namen verdient. Das wäre zum Beispiel der Fall, wenn Arbeitgeber*innen die Nutzung der Contact-Tracing-App durch ihre Beschäftigten kontrollieren oder wenn der Zugang zu Dienstleistungen und Orten – Flughäfen, Restaurants, Pflegeheime – davon abhängig gemacht wird, dass Personen „freiwillig“ ihre App-Inhalte offenbaren, z. B. „zehn Tage kein Kontakt zu positiv getesteten Personen“.

Wenn die Bundesregierung also beim Einsatz der App weiter auf Freiwilligkeit setzen will, was die grundrechtsfreundlichere Position wäre, so gilt es sicherzustellen, dass der Einsatz der App in der Lebensrealität auch wirklich freiwillig ist. So könnte es etwa explizit verboten oder an hohe Voraussetzungen geknüpft werden, dass der Zugang zu zentralen Infrastrukturen vom Einsatz der App abhängig gemacht wird, sei es seitens staatlicher oder privater Akteur*innen.

C. Tracing-Apps und Zivilgesellschaft: besondere Risiken und die starke Rolle der Zivilgesellschaft im Diskurs

Die dargestellten Probleme betreffen jede*n einzelne*n Nutzer*in, zivilgesellschaftliche Arbeit ist jedoch im besonderen Maße von einigen Risiken betroffen. Einige zivilgesellschaftliche Organisation können ihre Arbeit nur dann ausführen, wenn sie sichergehen können, dass sie und die Menschen, mit denen sie Kontakt haben, nicht von möglicher (staatlicher) Nachverfolgung, betroffen sind. Beispielsweise besteht bei Menschen ohne gültige Aufenthaltspapiere und jenen, die sich im laufenden Asylverfahren befinden, ein besonderes Interesse an staatlicher Verfolgung und Überwachung.

Ein praktisches Problem ist dabei auch, dass einige Organisationen, die unter prekären Bedingungen arbeiten, oft nicht über ausreichende Kapazitäten verfügen, um die Einhaltung ihrer Datenschutz-Rechte zu überprüfen. Vor diesem Hintergrund wird deutlich, wie wichtig es ist, dass Anwendungen von Beginn an datenschutzrechtliche Anforderungen erfüllen und über datenschutzfreundliche Voreinstellungen verfügen (sog. privacy by design). Beim Angebot von Datenspende-Apps muss vorgesorgt werden, dass gerade vulnerable Gruppen adäquat und verständlich über datenschutzrechtliche Risiken aufgeklärt werden, sodass deren Unkenntnis nicht missbraucht werden kann.

Auch bezüglich der Freiwilligkeit bedarf es hier besonderer Schutzmaßnahmen. Insbesondere Geflüchtete sind rechtsförmigen und faktischen Zugangsbeschränkungen zu öffentlichen Ressourcen oft schutzlos ausgeliefert. Es muss sichergestellt sein, dass sich ihr Verhalten zu allen denkbaren „Corona-Apps“ niemals negativ auf ihre Grundversorgung oder ihr Asylverfahren auswirken kann.

Positiv hervorzuheben ist die bisherige Rolle der Zivilgesellschaft im Diskurs um den Einsatz von Technologien in der Corona-Krise. Zivilgesellschaftliche Akteur*innen sind an der Diskussion zu den Corona-Apps aktiv beteiligt und nehmen starken Einfluss auf die Debatte zur konkreten Ausgestaltung der App. In einem Fall hat der Kurswechsel der Bundesregierung gezeigt, dass auch der Protest aus der Zivilgesellschaft gehört wird und Folgen hat. So wurde ein vom Gesundheitsministerium erarbeiteter Gesetzesentwurf, der den Gesundheitsbehörden ermöglichen sollte, „zum Zwecke der Nachverfolgung von Kontaktpersonen […] technische Mittel" einzusetzen und von den Anbietern von Telekommunikationsdiensten Verkehrs- und Standortdaten heraus zu verlangen, zurückgezogen, nachdem diverse zivilgesellschaftliche Akteur*innen zu Recht kritisierten, dass die Abfrage von Funkzellendaten ungeeignet und die Abfrage von GPS-Daten unangemessen wäre. Auch die Entwicklung verschiedener, auf der BLE-Technologie basierender Projekte, insbesondere der Verlauf des PEPP-PT-Projekts, wurde stets intensiv und kritisch begleitet.

D. Anforderungen und rechtliche Grenzen für den Einsatz von Tracing-Apps

Das Datenschutzrecht ist Schutzschild der Menschen und damit auch der Zivilgesellschaft gegen Nachverfolgung und Überwachung. Deshalb ist es wichtig, dass vor dem flächendeckenden Einsatz einer Contact-Tracing-App ihr Quellcode offengelegt wird. Nur so kann vor Beginn des Einsatzes sichergestellt werden, dass die App die datenschutzrechtlichen Vorgaben erfüllt und keine verborgenen Gefahren enthält. Im Anschluss muss der Einsatz der App laufend am Maßstab der Grundrechte überprüft werden. Dabei sind grundsätzlich die folgenden Punkte zu beachten:

1. Datenschutz ist Grundrechtsschutz

Das Grundrecht auf Datenschutz in der EU-Grundrechtecharta (Artikel 8 GRCh) und das Recht auf informationelle Selbstbestimmung des Grundgesetzes (Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG) stellen die verfassungsrechtliche Grenze für den Einsatz von Contact-Tracing-Apps dar. Die daraus abgeleiteten Schutzstandards für Betroffene können daher nicht einfach abgesenkt werden.

Vor diesem Hintergrund sind entsprechende Forderungen wie in der Leopoldina-Stellungnahme kritisch zu bewerten. Diese forderte, dass „angesichts der Erfahrung der derzeitigen Pandemie […] auf europäischer Ebene die Datenschutzregelungen für Ausnahmesituationen überprüft und ggfs. mittelfristig angepasst werden [sollten]. Dabei sollte die Nutzung von freiwillig bereit gestellten personalisierten Daten, wie beispielsweise Bewegungsprofile (GPS-Daten) in Kombination mit Contact-Tracing in der gegenwärtigen Krisensituation ermöglicht werden.“ Hierbei ist zu beachten, dass

Abweichungen von datenschutzrechtlichen Grundsätzen nach der ständigen Rechtsprechung des EuGH restriktiv auszulegen sind. Wenn Mitgliedstaaten von den Möglichkeiten für Abweichungen von den Betroffenenrechten Gebrauch machen (vgl. Art. 23 DSGVO oder Art. 15 ePrivacy-Richtlinie), müssen sie sicherstellen, dass die entsprechenden Gesetze den Wesensgehalt der Grundrechte achten und verhältnismäßig sind.

Eine Änderung der datenschutzrechtlichen Grundlagen ist zum Einsatz von Contact-Tracing-Apps aber auch gar nicht nötig: Das Datenschutzrecht steht dem Einsatz von Contact-Tracing-Apps nicht grundsätzlich entgegen. Vielmehr formuliert es Anforderungen an deren Ausgestaltung, die bezwecken, dass die Grundrechte der Menschen – und damit auch die Zivilgesellschaft – auch in Krisenzeiten nicht unverhältnismäßig eingeschränkt werden.

Dass datenschutzrechtliche Anforderungen in der Gestaltung von Contact-Tracing-Apps zu berücksichtigen sind, ist daher kein Bug, sondern ein Feature. Datenschutz und Contact-Tracing können miteinander vereinbart werden.

Im Datenschutzrecht konkretisieren sich wichtige verfassungsrechtliche Grundsätze. Darunter fallen etwa die Grundsätze der Rechtmäßigkeit (jede Datenverarbeitung muss durch eine Rechtsgrundlage gerechtfertigt sein), der Zweckbindung (die Datenverarbeitung darf nur für vorher und abschließend festgelegte Zwecke erfolgen) und der Datenminimierung (es dürfen nicht mehr Daten verarbeitet werden, als zur Erreichung des Zwecks erforderlich). Diese Anforderungen gelten für sämtliches staatliche Handeln.

2. Gesetzesgrundlage und präziser Zweck

Jede staatliche Maßnahme gegenüber Einzelnen, die mit einem Eingriff in Grundrechte verbunden ist, muss sich im Rechtsstaat auf eine hinreichend bestimmte gesetzliche Rechtsgrundlage stützen. Die Maßnahme muss zudem einem legitimen Zweck dienen und verhältnismäßig sein. Das bedeutet, sie muss geeignet sein, den angestrebten Zweck zu erfüllen, und von allen gleich geeigneten Mittel dasjenige sein, das am wenigsten intensiv in die Grundrechte der Betroffenen eingreift. Außerdem darf der Eingriff in die Grundrechte nicht außer Verhältnis zum angestrebten Ziel stehen.

Besonders wichtig ist bei einer Contact-Tracing-App, dass die Rechtsgrundlage den Zweck der Verarbeitung präzise festlegt. An diesem Zweck wird die gesamte Datenverarbeitung und ihre Erforderlichkeit gemessen. Je weiter der Zweck definiert ist, desto größer ist der Eingriff in die Grundrechte der betroffenen Personen; es ist daher wichtig, dass der Zweck möglichst eng gefasst wird. Außerdem muss die Speicherdauer für die Daten auf das absolut notwendige Maß begrenzt werden.

Bei der Zweckbindung ist auch wichtig, dass der Zweck der Datenerhebung nicht nachträglich stückweise ausgeweitet werden darf. Dies gilt insbesondere im Hinblick auf einen Daten-Zugriff durch Ordnungs- und Sicherheitsbehörden. Dies wird von der Zivilgesellschaft mit großer Aufmerksamkeit verfolgt werden und die Akzeptanz der App maßgeblich beeinflussen.

Der Staat sollte daher transparente Schutzmaßnahmen ergreifen, die einem solchen missbräuchlichen Umgang mit den Daten, etwa ihre Nutzung für andere Zwecke oder die Repersonalisierung, entgegenwirken.

3. Datenschutz-Maßnahmen über die gesamte Lebensdauer der App

Bei der Gestaltung und Implementierung von Contact-Tracing-Apps sind insbesondere zwei Anforderungen zu beachten: Datenschutz by Design bedeutet, Datenschutz von Beginn an in das Entwicklungs-Verfahren zu integrieren. Datenschutz by Default bedeutet, dass für einzelne Nutzer*innen schon bei der ersten Nutzung standardmäßig die datenschutzfreundlichsten Voreinstellungen ausgewählt sind. Dies sind keine „Möglichkeiten“ zur Gestaltung, sondern Normen, die für die Betreiber einer Contact-Tracing-App verpflichtend sind.

Die App-Betreiber müssen zudem gewährleisten, dass die Daten der Nutzer*innen ausreichend abgesichert werden, um etwa Missbrauch oder unberechtigten Zugang zu verhindern. Die bereits angesprochenen Risiken für die Rechte Einzelner erfordern daher geeignete Schutzmaßnahmen.

4. Vertrauen erfordert Transparenz

Eine Kontaktnachverfolgung kann potenziell zu einer umfassenden Dokumentation des Alltags führen. Aufgrund dieses Risikos und der Neuheit der Technologie muss bereits vor der Einführung einer Contact-Tracing-App eine transparente und umfassende Datenschutz-Folgenabschätzung durchgeführt werden.

Bei der Datenschutz-Folgenabschätzung muss die gesamte mit dem Contact-Tracing einhergehende Datenverarbeitung in ihrer konkreten praktischen Umsetzung analysiert werden. Hierbei wird geprüft, ob die datenschutzrechtlichen Vorgaben – zum Beispiel Datenschutz by Design – eingehalten werden. Diese Analyse muss aus der Perspektive der Betroffenen geschehen, um angemessene Maßnahmen zum Schutz ihrer Rechte zu identifizieren. Der Analyse-Bericht sollte veröffentlicht werden, nicht nur im Interesse der Akzeptanz der App; Transparenz trägt auch wesentlich dazu bei, dass die Zivilgesellschaft das staatliche Handeln kontrollieren kann.

Informationsfreiheits- oder Transparenzgesetze auf EU- und Bundes- und Landesebene verlangen, dass staatliche Stellen Informationen grundsätzlich veröffentlichen oder auf Anfrage herausgeben müssen. Über diese Regelungen bestehen weitere Möglichkeiten für zivilgesellschaftliche Gruppen und Organisationen, das Handeln von Regierung und Verwaltung zu kontrollieren. Diese Informationsfreiheit darf nicht pauschal unter Hinweis auf Geheimhaltungsinteressen oder Interessen der Exekutive verkürzt werden.

Es muss auch sichergestellt werden, dass die User ihre Rechte ausüben können. Dazu gehören umfangreiche Informations- und Auskunftsrechte, die dazu dienen, ihnen die Datenverarbeitung transparent und verständlich zu erklären. Die konkreten Verarbeitungsschritte einer Contact-Tracing-App sind dabei nicht für alle Nutzer*innen relevant. Die Information kann deshalb auf verschiedenen Ebenen und in abgestuften

Komplexitätsgraden erfolgen. Wichtig ist jedoch, dass jede*r Nutzer*in die Möglichkeit haben muss, die abstrakte Funktionsweise der App nachvollziehen zu können.

5. **Rechte der Betroffenen durchsetzen**

Nutzer*innen sind jedoch nicht nur passive Konsument*innen mit Informationsrechten. Betroffene können sich bei einer Datenschutzaufsichtsbehörde beschweren, wenn sie der Meinung sind, dass eine Datenverarbeitung nicht den gesetzlichen Vorgaben entspricht. Sie können auch gerichtlich gegen die für die Datenverarbeitung verantwortliche Stelle vorgehen. Diese Rechte der Betroffenen können auch zivilgesellschaftliche Gruppen, Organisationen oder Vereine ausüben.

6. **Effektivität der Contact-Tracing-App muss laufend überwacht werden**

Bisher gibt es, jedenfalls in Europa, noch keine praktischen Erfahrungen mit dem Einsatz vergleichbarer Apps auf Basis von BLE. Die Nützlichkeit von Contact-Tracing-Apps wird daher bisher aufgrund von Prognosen eingeschätzt. Deswegen muss ihr tatsächlicher Einsatz laufend empirisch evaluiert werden. Das bedeutet auch, dass die jetzt eingeführten Maßnahmen nach dem Ende der Pandemie, wenn sie also nicht mehr zum Infektionsschutz erforderlich sind, vollständig zurückgefahren werden müssen.

7. **Die Entwicklungen auf EU-Ebene und in anderen EU-Mitgliedsstaaten müssen in den Blick genommen werden**

Längerfristiges Ziel ist eine europaweite Nutzung von Contact-Tracing-Apps. Dies erfordert Verknüpfungen mit Contact-Tracing-Systemen aus anderen EU-Mitgliedstaaten. Daher müssen auch die Diskussionen auf EU-Ebene und die Entwicklungen in den EU-Mitgliedstaaten in den Blick genommen werden – und es müssen auch diesbezüglich die rechtlichen Grenzen klar sein.

Kritische Aspekte sind hier insbesondere eine mögliche Erweiterung des Zwecks sowie ein fragwürdiger Umgang mit Daten und digitaler Überwachung in anderen EU-Mitgliedstaaten.

So setzt sich die EU-Kommission für eine Verarbeitung von Gesundheitsdaten ein, die über das Contact-Tracing hinaus geht; ähnlich wie bei der Datenspende-App des RKI sollen Gesundheitsdaten zur epidemiologischen Forschung eingesetzt werden. Die EU-Kommission sieht eine EU-weite App auch als Chance, eine schon länger geplante EU-weite digitale Infrastruktur für die Speicherung und Verarbeitung von Gesundheitsdaten zu ermöglichen.

Hier wird es wichtig, sicherzustellen, dass die Contact-Tracing-App nicht zum Einfallstor für datenschutzrechtlich problematische Pläne mit weitreichenden Folgen für die Zukunft wird. Insbesondere die Zivilgesellschaft wird diese Entwicklungen intensiv beobachten und kritisch begleiten.

Besondere Schutzmechanismen und Exit-Strategien sind erforderlich, wenn eine Verknüpfung mit Staaten angestrebt wird, in denen die Kompetenzen zur Kontaktnachverfolgung nicht auf die Gesundheitsbehörden begrenzt ist und in denen

die datenschutzrechtliche Aufsicht nicht gewährleistet ist. Fraglich ist auch der Umgang mit EU-Staaten, in denen bereits die Ausgangsbeschränkungen mit Drohnen überwacht werden, wie z. B. in Belgien, oder in denen die Einhaltung von Quarantäne-Anordnungen bereits digital überwacht wird, wie beispielsweise in Polen.

Klar ist, dass Datenschutz-Grundrechte nicht an der Grenze Halt machen – auch in der Zusammenarbeit mit anderen Staaten müssen die Grundrechte gewahrt werden.

E. Zwischenfazit und Ausblick

Datenschutz und Infektionsschutz sinnvoll miteinander zu vereinen, ist eine große gesellschaftliche Aufgabe. Der dezentrale Ansatz, den die Bundesregierung gewählt hat, könnte grundsätzlich dazu geeignet sein, dieser Aufgabe gerecht zu werden.

Bis der Quellcode einer nutzbaren App veröffentlicht wird, verbleiben jedoch noch viele offene Fragen: Wie werden Nutzer*innen vor Angriffen auf ihre privaten Daten geschützt? Wie wird mit dem erhöhten Risiko an Falschmeldungen umgegangen? Was passiert mit Infektionsmeldungen? Welche Schutzmaßnahmen werden hierfür getroffen, und wie transparent wird die Technik sein? Und wie wird sichergestellt, dass der Schutz der Anonymität, der für viele zivilgesellschaftliche Akteure zentral ist, nicht durch das Contact-Tracing aufgehoben wird?

Eines steht jedoch fest: Bei der Bewältigung all dieser Herausforderungen wird die kritische Zivilgesellschaft eine zentrale Rolle spielen. Sie muss Antworten auf die offenen Fragen einfordern und Entwicklung und Einsatz der App kritisch begleiten. Sie muss sich aber auch aktiv in die Mitgestaltung und Bewältigung dieser Epidemie einbringen.

Die zivilgesellschaftliche Verantwortung endet auch nicht mit der Corona-Epidemie: Es gilt zu verhindern, dass die drastischen Maßnahmen nach der Krise zur Normalität werden. Daher ist es besonders wichtig, dass das Contact-Tracing nicht zum Einfallstor für eine umfassende Gesundheitsüberwachung wird. Der Staat ist deswegen bereits jetzt in die Pflicht zu nehmen, eine überzeugende Strategie für den Exit aus dem digitalen Contact-Tracing zu präsentieren.

„Corona-Apps“ und Zivilgesellschaft: Risiken, Chancen und rechtliche Anforderungen

Autoren:
Greenpeace und Gesellschaft für Freiheitsrechte

Eine juristische Kurzexpertise der Gesellschaft für Freiheitsrechte (GFF)
im Auftrag von Greenpeace

Hamburg, im Mai 2020

Impressum
Greenpeace e.V., Hongkongstraße 10, 20457 Hamburg, Tel. 040/3 06 18-0 **Pressestelle** Tel. 040/3 06 18-340, F 040/3 06 18-340, presse@greenpeace.de, www.greenpeace.de
Politische Vertretung Berlin Marienstraße 19–20, 10117 Berlin, Tel. 030/30 88 99-0 **V.i.S.d.P.** Anna von Gall **Ilustration** © Greenpeace **Gestaltung** Klasse 3b

S 0286 1 **Stand** 05/2020