System Security Lab

Sinn und Unsinn der Corona-Warn-App

Executive Summary

Die Corona-Warn-App auf dem Prüfstein: Was lässt sich nach mehr als 100 Tagen sagen?

Die Coronavirus-Pandemie hat seit Monaten die Welt fest im Griff. Die Infektionszahlen steigen. Die zweite Welle, sie rollt. Umso wichtiger ist eine sichere und schnelle Nachverfolgung der Kontakte und der damit verbundene Schutz aller Menschen. In vielen Ländern wurden deshalb bereits digitale Tracing-Apps eingeführt, um eine weitere Ausbreitung der Pandemie zu verhindern. Je nachdem wie hoch die Priorität der Datenschutzaspekte in den einzelnen Ländern ist, kommen dabei unterschiedliche Ansätze zum Tragen: ein zentrales oder dezentrales Kontaktnachverfolgungssystem.

In Deutschland gab es eine lebhafte Debatte über die Einhaltung des Datenschutzes und letztendlich fiel die Wahl auf eine dezentrale Lösung. Die Mitte Juni veröffentlichte Corona-Warn-App ist in Deutschland gut angenommen worden. Inzwischen mehren sich jedoch die Zweifel an ihrem Nutzen – besonders im Hinblick auf die Kosten. Es ist nicht klar, wie viele Menschen sie tatsächlich nutzen und welchen Mehrwert sie für die Eindämmung der Corona-Pandemie hat.

Um zu beurteilen, ob und inwiefern die Corona-Warn-App bei der Eindämmung der Corona-Pandemie nützlich ist, liefert der folgende Bericht einen Überblick. Dazu sind neben Ergebnissen eigener Untersuchungen, internationale Studien sowie die aktuelle Berichterstattung eingeflossen.

Unser Ziel ist es, eine kritische Auseinandersetzung zu initiieren, die die Kosten-Nutzen-Relation und noch wichtiger die technologische Souveränität erörtert. Außerdem geht es darum, die wissenschaftliche Forschung voranzutreiben. Dafür wurden folgende Aspekte näher betrachtet:

- Datenübertragung via Bluetooth-Technologie und deren Tücken
- Angriffe auf die Corona-Warn-App – wie sicher sind die Daten?
- Wie viele Menschen nutzen die Corona-Warn-App?
- Dezentrale App ohne datenschützende digitale Infrastruktur
- Souveränität statt Dominanz von Google und Apple

Unsere kritische Betrachtung fokussiert sich vor allem auf die Schwächen der gewählten Tracing-Lösung. Dennoch hat die Entwicklung der App in vielen Bereichen zu Kooperationen und Erkenntnissen geführt, die es unter anderen Umständen nicht gegeben hätte. Sichere Kontaktverfolgungssysteme liefern einen Teilbeitrag: Sie unterstützen die manuelle Nachverfolgung und helfen dabei Infektionsketten zu identifizieren. Trotz dieser Vorteile sind aus unserer Sicht Tracing-Apps nur ein Teil der Lösung für die COVID-19-Pandemie.

Zunächst brauchen wir eine digitale Infrastruktur und exakte Informationen, die es uns erlauben, die Effektivität der Corona-Warn-App evaluieren zu können. Dazu ist ein Kommunikations- und Informationsmanagementsystem erforderlich, um zum Beispiel Ärzten eine sichere und datenschützende Möglichkeit zu geben, zusätzliche Informationen zu kommunizieren. Außerdem ist es wichtig, die technologische Hoheit nicht in die Hände der beiden Datenriesen Google und Apple zu legen, sondern auf die in Deutschland vorhandene innovative Kraft zu setzen und eigene Lösungen voranzutreiben. Gerade für diesen Prozess brauchen wir weitere fundierte Studien und eine offene Diskussion. Nur so können die Tracing-Apps zu einer effizienten, effektiven und unabhängigen Lösung weiterentwickelt werden.

Zeit für eine Bilanz

Die ersten 100 Tage der offiziellen Corona-Warn-App sind vorbei. Schon vor ihrer Einführung im Mai wurde die Corona-Warn-App seitens der Bundesregierung mit flächendeckenden Werbeaktionen beworben und ihre Nutzung von Spitzenpolitikern wie der Bundeskanzlerin persönlich empfohlen. Das von der Bundesregierung in Auftrag gegebene Projekt schneidet zudem im internationalen Vergleich gut ab. Bereits im Juni haben Experten für IT-Sicherheit von Amnesty International[1] verschiedene Corona-Tracing Apps analysiert. Die deutsche Lösung ist besonders wegen der dezentralen Datenspeicherung, der Freiwilligkeit und der Transparenz gegenüber den anderen untersuchten Ansätzen positiv aufgefallen. Dadurch genießt die Corona-Warn-App das notwendige Vertrauen und erfährt eine breite Akzeptanz in der Bevölkerung. Das Robert-Koch-Institut (RKI) verzeichnete Ende September 18,4 Millionen Downloads der App[2].

Auch wenn die Corona-Warn-App als europäischer Musterschüler gegenüber anderer[3] sowohl dezentraler als auch zentraler Tracing-Apps[4] positiv verkauft wird, ist es an der Zeit eine Bilanz aufzustellen und uns einige kritische Fragen zu stellen.

Die aktuelle Situation kennzeichnen sehr viele heterogene Faktoren. Auf der einen Seite steigen die Infektionszahlen wieder an, was in einigen Regionen bereits wieder zu strengeren Maßnahmen geführt und Forderungen nach einheitlichen Regelungen nach sich gezogen hat. Auf der anderen Seite wächst neben der Verunsicherung vor den wirtschaftlichen Folgen der Pandemie auch der Widerstand gegen die Einschränkungen und gesetzlichen Regelungen. Gerade in dieser schwierigen Gemengelage ist es wichtig einen kühlen Kopf zu bewahren und sich neutral der Fakten zu widmen.

Das erklärte Ziel[5] der Corona-Warn-App ist es, Infektionsketten schnell zu erkennen und zu unterbrechen. Dabei sollen alle Nutzer*innen zuverlässig und zeitnah über Begegnungen mit auf Corona positiv getesteten Personen informiert werden. So wird die sehr zeitintensive und häufig unpräzise manuelle Kontaktverfolgung der Gesundheitsämter technisch unterstützt. Nachdem betroffene Personen über einen Kontakt informiert werden, können sie sich schnell in eine freiwillige Quarantäne begeben und einen Corona-Test durchführen. Damit können sie sich und ihr Umfeld aktiv schützen und zur Eindämmung der Corona-Pandemie beitragen.

Die Gretchenfrage: Sinnvoll oder nicht?

Mittlerweile sind Schutzmaßnahmen wie die sogenannten AHA-Regeln: Abstand halten – Hygiene beachten – Alltagsmaske (Mund-Nasen-Bedeckung) tragen, selbstverständlich. Nach wie vor ist Vorsicht geboten, da die Fallzahlen in mehreren Bundesländern wieder deutlich steigen[6]. Hilft die Corona-Warn-App dabei, die Ausbreitung von COVID-19 zu bremsen? Und wie wirksam ist die App tatsächlich?

---

[1] https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/

[2] https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Kennzahlen.pdf?__blob=publicationFile

[3] Eine Übersicht zu den verschiedenen Tracing-Apps finden Sie hier: https://tracecorona.net/de/ein-vergleich-von-kontakt-nachverfolgungsansatzen/ubersicht-uber-tracing-losungen-in-verschiedenen-landern/

[4] Einen Vergleich der technologischen Ansätze finden Sie hier: https://tracecorona.net/wp-content/uploads/2020/06/Pandemic-tracing-comparison-v.1.1.pdf

[5] https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-faq-1758392

[6] https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Situationsberichte/Okt_2020/2020-10-11-de.pdf?__blob=publicationFile

Alles beginnt mit der Datenübertragung

Werfen wir einen Blick auf die bei der Corona-Warn-App angewendete Technik: Bluetooth Low Energy. Die Corona-Warn-App nutzt die vorhandene Bluetooth-Technologie der Endgeräte. Dabei verwendet die App die Exposure Notification API von Apple und Google, die sogenannte GAEN[7]. Hier handelt es sich um eine Schnittstelle, die beide Hersteller inzwischen in die neuesten Versionen ihrer Smartphone-Betriebssysteme integriert haben. Aus der Softwareentwicklungsperspektive gehört diese von Google und Apple kommende API zu den Kerntechnologien, sie ist quasi eine Betriebssystemkomponente.

Mit Hilfe von Bluetooth Low Energy sollen zwischen Geräten automatisch zufällig generierte Identifikationsnummern (pseudonyme Bluetooth-IDs) ausgetauscht werden um Begegnungen zwischen Geräten und deren Dauer zu erfassen. Das RKI spricht erst bei mehr als 10 Minuten langen Kontakten von einer Risiko-Begegnung. Neben der Dauer einer Begegnung spielt jedoch auch der Abstand zur getroffenen Person sowie die Umgebung, in der die Begegnung stattfindet eine Rolle.

Was kann Bluetooth und was nicht

Die Bluetooth Low Energy Technologie ist nicht in der Lage, den genauen Abstand zwischen den Geräten zu messen. Ob man sich in nächster Nähe oder weit voneinander entfernt begegnet, lässt sich nur ansatzweise abschätzen. In einem Laborversuch hat sich gezeigt, dass es bereits durch Drehen und Kippen eines Smartphones zu Abweichungen der Signalstärke, welche als Grundlage für die Abstandsmessung benutzt wird, kommen kann[8]. Und das obwohl es keine Reflexionen durch Gegenstände gab und das Smartphone nicht in einer Tasche war.

Dies bestätigt auch die irische Studie von Douglas J. Leith und Stephen Farrell vom Trinity College in Dublin[9]. Dieser Untersuchung zufolge kann die Stärke des Bluetooth-Signals variieren je nachdem, wo sich das Gerät befindet. Es kommt demnach darauf an, ob das Smartphone in der Hand ist oder in der Handtasche.

Das irische Forscherteam um Douglas J. Leith hat außerdem herausgefunden, dass darüber hinaus äußere Faktoren die Signalstärke beeinflussen können[10]. Laut dieser Studie reflektiert das in Zügen verbaute Metall die Bluetooth-Signale. Als Lösung des Problems der Störungen durch Metall würden in der Corona-Warn-App Korrekturwerte in der Ermittlung des Risikostatus eingerechnet oder verworfen, wie eine Pressesprecherin des RKIs erläutert hat[11]. Die Corona-Warn-App erkennt nicht, wie und wo der Kontakt zustande kommt. Menschen bewegen und begegnen sich eben nicht unter Laborbedingungen, sondern in Räumen, im öffentlichen Nahverkehr oder im Freien.

Alt, älter, ohne Corona-Warn-App

Obwohl die Corona-Warn-App barrierefrei gestaltet ist, damit möglichst viele Personen die App nutzen können, ist sie nicht allen Menschen in Deutschland zugänglich. Die App läuft zwar auf der Mehrheit der gängigen Endgeräte, die ein Android oder iOS-Betriebssystem haben. Gleichzeitig muss jedoch die aktuellste Version dieser Betriebssysteme installiert sein. Damit scheiden eine Vielzahl älterer Endgeräte aus. Obwohl iPhone-Besitzer ihr Smartphone oftmals deutlich länger nutzen, bietet

[7] https://covid19.apple.com/contacttracing und https://developers.google.com/android/exposure-notifications/exposure-notifications-api
[8] https://www.researchgate.net/publication/302199860_Is_bluetooth_low_energy_an_alternative_to_near_field_communication
[9] https://arxiv.org/pdf/2006.06822.pdf
[10] https://arxiv.org/pdf/2006.08543.pdf
[11] https://netzpolitik.org/2020/contact-tracing-gesundheitsministerium-verteidigt-corona-warn-app/

Apple keine Unterstützung mehr für Geräte an, die älter als vier oder fünf Jahre sind. Daran können auch die Entwickler der Corona-Warn-App nichts ändern[12].

Neben der neuesten Version des Betriebssystems haben in der Vergangenheit einzelne Energiespar- und Akkueinstellungen sowie die Hintergrundaktualisierung per WLAN oder mobile Daten die Funktionalität der Corona-Warn-App beeinträchtigt[13]. Darüber hinaus gibt es trotz voranschreitender Digitalisierung unseres Alltages noch immer Menschen, die grundsätzlich auf ein Smartphone und damit auch auf den Nutzen der Tracing-App verzichten.

Unterwegs in Europa

Auch im Ausland können Nutzer*innen den Nutzen der Corona-Warn-App noch nicht vollständig ausschöpfen. Obwohl es in vielen europäischen Ländern mittlerweile nationale Contact-Tracing-Apps gibt, endet die Funktionalität bislang an der Grenze. Die verschiedenen nationalen Warn-Apps können bisher untereinander keine digitalen Schlüssel austauschen. Zwar hatte die EU-Kommission eine Lösung für die Sommermonate angekündigt, doch erst jetzt soll eine gemeinsame Schnittstelle die Lücke schließen und die sogenannte Interoperabilität der Apps gewährleisten[14].

Wie bereits die Corona-Warn-App wurde die europäische Schnittstelle vom deutschen Softwarekonzern SAP und der Deutschen Telekom entwickelt. Nach dem Ende des Probebetriebes sollen über das sogenannte Gateway ab Oktober die Daten aus sechs europäischen Ländern getauscht und ausgewertet werden. Allerdings funktioniert der Gateway-Server nur mit dezentralen Lösungen. Damit profitieren zunächst nur Deutschland, Italien, Dänemark, Tschechien, Lettland und Irland[15] von der europäischen Schnittstelle.

Das heißt, wer im Herbst an der dänischen Nordseeküste spazieren geht, sollte von der deutschen App im Falle einer Risiko-Begegnung gewarnt werden. In Frankreich hingegen werden die Daten zentral erfasst und deshalb nicht zusammengeführt. Wer also den Eiffelturm besteigt, wird nicht über eine Begegnung mit einer infizierten Person informiert[16]. Für die mangelnde Interoperabilität von zentralen und dezentralen Kontaktverfolgungs-Apps gibt es bislang noch keine Lösung. Denn dabei spielt vor allem der Datenschutz eine zentrale Rolle.

Sichere Daten oder der gläserne Patient?

Der Datenschutz ist mehr als zentral: Aus dem potenziellen Missbrauch der von den Contact-Tracing-Apps gesammelten Daten ergeben sich die größten Risiken. Verglichen mit vielen anderen Anwendungen sammelt die Corona-Warn-App vertrauliche und detaillierte Informationen während der Kontakte zwischen einzelnen Nutzer*innen. Es lässt sich darüber spekulieren, dass aktuell wohl kein anderes von den Behörden benutzte System das Potenzial hat, so viele Informationen zu den Kontakten von Personen zu sammeln wie die Corona-Warn-App.

Obwohl das System die wahre Identität einzelner Nutzer*innen nicht explizit erfasst oder aufzeichnet, können gleichzeitig die Bewegungsprofile zur Identifikation einzelner beitragen. Das betrifft bei der Corona-Warn-App vor allem Personen, die infiziert sind und ihre sogenannten

[12] https://www.coronawarn.app/de/faq/

[13] https://www.faz.net/aktuell/wirtschaft/digitec/was-die-probleme-der-corona-warn-app-sind-und-was-nicht-16880282-p2.html
[14] https://netzpolitik.org/2020/europaweite-loesung-laesst-auf-sich-warten/

[15] https://www.zeit.de/digital/2020-09/kontaktverfolgung-corona-warn-app-ausland-eu?print#comments
[16] https://www.handelsblatt.com/technik/medizin/pandemiebekaempfung-eu-startet-gemeinsame-schnittstelle-fuer-corona-

Tagesschlüssel (Temporary Exposure Keys) auf den Corona-Warn-App-Server hochgeladen haben. Sämtliche Bewegungsprofile sind einzigartig und unterscheiden sich von Person zu Person. Anhand des nächtlichen Aufenthaltsortes können Rückschlüsse auf den Wohnort gezogen werden. Schaut man sich das Bewegungsprofil über den Tag an, kann man durchaus den Arbeitsplatz einer Person eindeutig identifizieren[17].

Wir wissen, wo Du wohnst

Gemeinsam mit Forscher*innen der Universität Marburg und der Universität Würzburg ist es uns gelungen, die bis dahin nur theoretisch beschriebenen Datenschutz- und Sicherheitsrisiken des Google und Apple-Ansatzes (Exposure Notification API) auch praktisch nachzuweisen[18]. Ausgangspunkt für die Experimente waren zuvor veröffentlichte Berichte über mögliche Datenschutz- und Sicherheitsrisiken im Zusammenhang mit den Entwicklungen des sogenannten „Google Apple Protokoll“ (GAP). Wir haben getestet, ob die konzeptionell beschriebenen Angriffe in der Praxis ausgeführt werden können.

Die Experimente haben gezeigt, dass das Google Apple Protokoll (GAP) in vielerlei Hinsicht anfällig ist. Zum einen lassen sich Bewegungsprofile erstellen, die prinzipiell eine Identifikation von infizierten Personen ermöglichen können. An dieser Stelle weisen wir daraufhin, dass Google und Apple sowohl über die notwendigen Tools als auch die entsprechende Infrastruktur verfügen, um etwa soziale Beziehungen über sogenannte „Social Graphs“ fein-granularer abbilden zu können. Zum anderen sind sogenannte Relay- oder Wurmloch-Angriffe möglich, wodurch der Angreifer falsche Kontaktereignisse generieren und damit die Zuverlässigkeit des gesamten Systems manipulieren kann.

Für die bei dem Versuch realisierten Angriffe wurden handelsübliche und preiswerte Werkzeuge, wie Bluetooth-Sniffer (als App auf dem Smartphone oder Raspberry Pis anwendbar) eingesetzt, um die notwendige räumliche Nähe zu gewährleisten. Mithilfe dieser strategisch platzierten Sensoren konnten die Bewegungen und Aufenthaltsorte infizierter Personen rekonstruiert werden. Bei den sogenannten Relay- oder Wurmloch-Attacken ist es gelungen, die pseudonymen Bluetooth-IDs zu sammeln und unbemerkt an andere – auch weiter entfernte Orte weiterzuleiten. Der Angreifer kann Informationen zum Aufenthaltsort duplizieren und dadurch fehlerhafte Risiko-Begegnungen injizieren. Somit kann das Kontaktnachverfolgungssystem als Ganzes beeinträchtigt werden[19].

Kleingedrucktes und die Tücken

Darüber hinaus haben zwei kanadische Forscher im Rahmen ihrer kritischen Analyse der Risikobewertung der Schweizer Contact-Tracing-App einen weiteren einfachen Angriff dargestellt[20]. Im Gegensatz zu den beiden bisher beschriebenen Angriffen ist diese Attacke Smartphone-basiert. Bei diesem Angriff wird ein schadhaftes Software Development Kit (SDK) in eine vermeintlich sichere Anwendung eingebunden.

Sehr viele Apps sammeln im Rahmen ihrer Anwendung Daten, ohne dass den Nutzer*innen klar ist, welche Informationen das sein können. Wirft man einen Blick in die Datenschutzrichtlinien und

[17] https://tracecorona.net/de/2020/05/08/risiken-von-tracing-apps-mit-unzureichenden-datenschutzlosungen/
[18] https://tracecorona.net/de/2020/06/12/corona-tracing-ansatz-von-google-und-apple-hat-defizite-bei-datenschutz-und-sicherheit/

[19] https://arxiv.org/pdf/2006.05914.pdf

[20] https://arxiv.org/pdf/2006.10719.pdf

Nutzungsbedingungen, findet man die entsprechenden Informationen. Gesammelt werden: Mobile Werbe-IDs, genaue Standortinformationen (z.B. GPS-Koordinaten des Geräts), relative Standortinformationen (z.B. von WiFi-Signalen oder Bluetooth Low Energy-Geräten in der Nähe), gerätebasierte Werbekennungen, Informationen über das Endgerät wie Gerätetyp, Betriebssystem-Version und -Typ sowie Geräteeinstellungen, Zeitzone, Netzbetreiber und IP-Adresse.

In vielen Datenschutzrichtlinien steht ausdrücklich, dass solche Informationen gesammelt und an „vertrauenswürdige Partner“ weitergegeben werden. Jedoch fällt dabei häufig unter den Tisch, dass diese Daten gesammelt werden, sobald die App läuft bzw. das Gerät gestartet wird. Nehmen die Benutzer*innen die App in Betrieb und stimmen sie den Datenschutzrichtlinien zu, ist laut den beiden kanadischen Forschern die „Relais-Station“ für einen Angriff implementiert.

Der Aufwand für das im Angriff erläuterte Scannen und Broadcasting von Bluetooth-Signalen ist durch die Exposure Notification APIs von Apple und Google sehr gering. Beide Betriebssysteme sind auf diese Funktion bereits schon ausgelegt. Ohne es zu wissen, sind es die Anwender*innen selbst, die die Integrität des Kontaktverfolgungssystems beeinträchtigen und an einem Angriff teilnehmen.

Neben den hier geschilderten Angriffen wären aus unserer Sicht auch groß skalierte Relay-Angriffe durch feindliche Staaten denkbar. Solche Angriffe könnten durchaus das Potenzial haben, die nationale Sicherheit zu gefährden. Eine Pandemie wie wir sie derzeit erleben, kann das politische Geschehen und das gesellschaftliche Leben stark beeinträchtigen.

Klickrate zum Träumen und trotzdem nicht genug

An dieser Stelle zeigt sich, dass vor allem Datenschutz und Sicherheitsfragen immer noch eine große Schwäche der Contact-Tracing-Apps darstellen. Gleichzeitig können sie helfen, die vollkommen überlasteten Gesundheitsämter zu unterstützen. Nach wie vor brauchen wir für die erfolgreiche Bekämpfung der COVID-19-Pandemie eine wirksame Nachverfolgung. Die manuelle Rückverfolgung stößt derzeit an ihre Grenzen. Besonders zufällige Begegnungen, an die sich die Menschen oft nicht erinnern, können mithilfe von Tracing-Apps deutlich besser nachvollzogen werden.

Derzeit haben wir kaum Informationen darüber, wie viele Menschen die Corona-Warn-App tatsächlich nutzen und ob sie wirksam ist. Laut einer Studie der Universität Oxford beginnen Tracing-Apps zu wirken, sobald 15 Prozent der Bevölkerung mitmachen[21]. Weiteren wissenschaftlichen Schätzungen zufolge müssten sogar mindestens 60 Prozent der Bevölkerung an der digitalen Kontaktverfolgung teilnehmen, damit die Corona-Warn-App effektiv sein kann[22].

Schauen wir dazu auf die Daten, die uns vorliegen: Die Corona-Warn-App wurde bisher 18,4 Millionen Mal runtergeladen. Gleichzeitig bedeutet dies jedoch nicht, dass die App von 18,4 Millionen Menschen aktiv genutzt wird. Denn ein Download entspricht nicht einem Nutzer oder einer Nutzerin.

Die Anzahl der Downloads kann von Land zu Land unterschiedlich ausfallen. Aus unserer Sicht hängt die Akzeptanz und die damit verbundenen Downloads der Tracing-Apps auch von gesellschaftlichen Faktoren ab. Dazu gehört beispielsweise auch inwieweit die Menschen der Regierung und den

[21] https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown

[22] https://netzpolitik.org/2020/faq-corona-apps-die-wichtigsten-fragen-und-antworten-zur-digitalen-kontaktverfolgung-contact-tracing-covid19-pepppt-dp3t

Spitzenpolitiker*innen vertrauen, wenn es um die öffentliche Gesundheit geht. Wenn wie in Deutschland die Politik eine App mit einer großen Werbeaktion promotet, ist zu erwarten, dass viele Menschen diese herunterladen – sei es aus Neugier oder aus dem Glauben heraus, dass die Corona-Warn-App ihnen hilft.

Wenig Ergebnisse

Auch wenn die Corona-Warn-App im europäischen Vergleich eine große Verbreitung hat, wären 18,4 Millionen „echte“ Nutzer*innen nur etwas mehr als 22 Prozent der deutschen Bevölkerung. Damit wirkt die App. Von deutlich effektiven Folgen können wir gleichzeitig noch nicht ausgehen. Gemessen an der Bevölkerungszahl haben andere Länder die Nase vorn: In Irland und Finnland etwa liegt die Abdeckung bei rund 37 Prozent. Daten zufolge, die die Deutsche Telekom erhoben hat, sollen es 15 Millionen tatsächliche Nutzer*innen sein[23]. Einige haben die Corona-Warn-App auf mehreren Geräten laufen, andere haben sie in der Zwischenzeit gelöscht oder nicht vollständig in Betrieb genommen.

Neben den tatsächlichen Downloads veröffentlicht das RKI die Anzahl aller über die Hotline ausgegebenen Tele-TANs zur Verifizierung eines positiven Testergebnisses. Aktuell[24] wurden 4.373 Tele-TANs vergeben, obwohl seit dem Start der Corona-Warn-App Mitte Juni mehr als 87.000 Neuinfektionen registriert wurden. Diese Diskrepanz kann damit zusammenhängen, dass die Testergebnisse inzwischen auch per QR-Code hochgeladen werden können.

Um einen Missbrauch der App zu verhindern, muss eine in der App gemeldete Infektion offiziell bestätigt werden. Das geschieht mittels der Tele-TAN oder des QR-Codes, die vom Testlabor ausgegeben werden. Allerdings sind von den rund 180 Testlaboren nur 125 digital an den Verifikationsserver der Corona-Warn-App angebunden[25]. Das erschwert die Infektionsnachverfolgung[26].

Dezentrale App, aber keine datenschützende digitale Infrastruktur

Anhand eines auf github.com publizierten Algorithmus[27] haben wir versucht die öffentlich zugänglichen Nutzerdaten auszuwerten. Dafür haben wir im August für drei Tage die Anzahl der insgesamt täglich hochgeladenen Tagesschlüssel ins Verhältnis zur Anzahl der sogenannten Diagnoseschlüssel, d.h. der Positivkennung von infizierten Nutzer*innen gesetzt. Dieser groben Schätzung zufolge[28] nutzen lediglich 5% der infizierten Anwender*innen die Corona-Warn-App, um ihr Testergebnis zu teilen. Und das obwohl die Zahl derjenigen, die ihr ein positives Testergebnis in der App eingegeben haben laut den Berechnungen von *tagesschau.de*[29] von rund 20 Personen pro Tag im Juli auf mehr als 70 pro Tag im August zugenommen haben. Um eine präzise Aussage zur Effektivität der Corona-Warn-App treffen zu können, müssen definitiv viel mehr Daten vorliegen.

Die Corona-Warn-App soll aus Datenschutzgründen und Aspekten der Privatheit keine zentrale Datenbank nutzen und daher lässt sich die genaue Zahl der App-Nutzer*innen nicht exakt

[23] https://www.br.de/nachrichten/netzwelt/so-koennte-es-mit-der-corona-warn-app-weitergehen,S9W9yzW
[24] RKI-Zahlen vom 22. September 2020
[25] https://www.nzz.ch/technologie/die-beste-corona-app-ist-auf-dem-boden-der-realitaet-angekommen-ld.1574541
[26] https://www.sicher-im-netz.de/corona-warn-app-der-dsin-news-blog-f%C3%BCr-verbraucherinnen

[27] https://github.com/mh-
[28] Die genaue Anzahl der hochgeladenen Daily Keys kann nicht exakt ermittelt werden, da der Server auf dem die Daten liegen, bei einer geringen Gesamtmenge zusätzlich zufällige Schlüssel generiert, um die „echten“ Schlüssel zu verschleiern.
[29] https://www.tagesschau.de/inland/corona-warn-app-risikoermittlung-101.html

bestimmen. Darüber hinaus ist nicht nachvollziehbar, wie viele Personen durch die Corona-Warn-App gewarnt werden. Die Entscheidung, ob Nutzer*innen ein positives Testergebnis teilen, ist freiwillig. Laut aktuellen Veröffentlichungen auf github.io haben dies bisher mehr als 9.500 Nutzer*innen getan[30].

Es fehlt hier eine digitale Infrastruktur, die eine datenschützende und vollkommen anonyme Verarbeitung der Informationen von involvierten Parteien wie Nutzer*innen, Gesundheitsexperten sowie Behörden erlauben würde. Auch das RKI würde gerne die Funktionalität der Corona-Warn-App erweitern und verschiedene bereits existierende Anwendungen in einer einzigen „Universal-App" zusammenführen[31]. Nur mit Hilfe exakter Informationen über die Nutzerdaten könnte die Effektivität der App entsprechend umfänglich evaluiert werden.

Risikogebiet Europa?

Allerdings ist auch ein zentraler Server, wie er in Frankreich genutzt wird, kein Garant auf Erfolg. Seit ihrer Einführung wurde die französische StopCovid-App 2,3 Millionen Mal runtergeladen. Laut Medienberichten hat nur ein Bruchteil der Anwender*innen Warnungen erhalten, so dass in Folge dessen mehr als 460.000 Menschen die App wieder deinstalliert haben[32].

Ein ähnliches Bild zeigt sich in Italien. Dort wurde die Warn-App Immuni von etwa 4,2 Millionen Italienern heruntergeladen. Das sind nur rund zwölf Prozent der Bevölkerung. Damit liegen die Downloadzahlen deutlich unter dem Ziel der Regierung. Die italienischen Behörden gehen davon aus, dass die Downloads anziehen könnten, sobald die COVID-19-Fallzahlen erneut stark steigen[33].

Dass diese Ereignisse nicht zwangsläufig kausal miteinander verknüpft sind, kann man derzeit in Spanien beobachten. Das südeuropäische Land ist aktuell am stärksten von einer zweiten Welle betroffen. Einer der Gründe für das hohe Infektionsgeschehen scheint die Überlastung des Gesundheitssystems zu sein. Die spanischen Behörden konnten nicht im notwendigen Umfang Kontakte nachverfolgen. Trotz dieser Tatsache liegen die Downloadzahlen der im August veröffentlichten Radar Covid-App bei nur rund vier Millionen[34]. Dazu kommt, dass erst Mitte September die Warn-App in ganz Spanien funktionieren sollte[35].

Hohe Kosten – wenig Wirkung

Am Londoner University College hat sich ein britisches Forscherteam um Dr. Isobel Braithwaite mit der Frage der Effektivität der Corona-Warn-Apps beschäftigt. Die Forscher*innen haben in einer Übersichtsstudie 15 Untersuchungen zu automatisierten und teilautomatisierten Kontaktverfolgungslösungen ausgewertet. Dabei wurden *„keine empirischen Belege für die Wirksamkeit der automatisierten Ermittlung von Kontaktpersonen (in Bezug auf die ermittelten Kontakte oder die Reduzierung der Übertragung) gefunden"*[36]. Abschließend konstatiert die Forschungsgruppe, dass die automatisierte Kontaktverfolgung bei der Eindämmung von COVID-19

[30] https://micb25.github.io/dka/
[31] https://www.heise.de/news/Corona-Pandemie-Robert-Koch-Institut-will-eine-App-fuer-alles-4915824.html
[32] https://www.theguardian.com/world/live/2020/jun/23/coronavirus-live-news-update-saudi-arabia-closes-borders-hajj-global-covid-19-cases-pass-9m-latest-updates?page=with:block-5ef228fe8f087111a86b7175
[33] https://www.bbc.com/news/technology-53485569; https://www.suedtirolnews.it/italien/coronavirus-keine-nachfrage-fuer-die-immuni-app-in-italien
[34] https://www.mallorcamagazin.com/nachrichten/lokales/2020/09/15/83757/immer-mehr-menschen-laden-spanische-corona-warn-app-herunter.html
[35] https://www.ovb-online.de/weltspiegel/spanien-corona-warn-app-bluetooth-nutzer-covid-19-sars-cov-2-zr-90022661.html
[36] https://www.thelancet.com/action/showPdf?pii=S2589-7500%2820%2930184-9

helfen könne, wenn genügend Menschen eine solche App nutzen. Um eine Wirksamkeit nachweisen zu können, müsse es zudem jedoch weitere prospektive Studien geben.

Neben der Bewertung ihrer Wirksamkeit ist es aus unserer Sicht ebenso wichtig die Kosten der Corona-Warn-App ins Verhältnis zu ihrer Nutzung zu setzen. Laut Vertrag[37] zwischen der Deutschen Telekom und der Bundesregierung belaufen sich die Kosten bis Ende 2021 auf 68 Millionen Euro. Allein die Entwicklung der Corona-Warn-App durch die Deutsche Telekom und SAP hat bereits 20 Millionen Euro gekostet. Die monatlichen Kosten für den laufenden Betrieb der App werden auf mehr als drei Millionen geschätzt[38].

Diese Kosten sind enorm. Im Vergleich dazu hat die Entwicklung der Schweizer StopCovid-App weniger als 5 Millionen Euro gekostet. Mehr Budget stand laut Aussage der ETH Lausanne für die Entwicklung des Prototyps nicht zur Verfügung[39]. Neben der Entwicklung stellen die beteiligten Firmen der Bundesregierung enorme Summen in Rechnung. Eine Übersetzung der App ins Kurdische zum Beispiel soll rund 250.000 Euro kosten[40]. Aufgrund dieser hohen Ausgaben mehren sich die kritischen Stimmen, die eine objektive Bewertung fordern. Denn im Grunde setzt die Corona-Warn-App lediglich auf eine Funktion auf, die im iOS- und Android-Betriebssystem vorhanden ist.

Wer hat es erfunden?

Dazu erklärte der Sprecher des Chaos Computer Club, Linus Neumann in der WirtschaftsWoche: Apple und Google haben die technischen Rahmenbedingungen für den Datenaustausch definiert und letztendlich damit die Entscheidung für das dezentrale Modell getroffen[41]. Auch Wissenschaftler der TU Darmstadt haben im Frühjahr bereits vermutet, dass die Funktion der Kontaktverfolgung ins Android- und iOS-Betriebssystem integriert wird[42]. Damit ist die Nachverfolgung direkt über das Betriebssystem möglich. Im Zuge der neuen iOS-Version 13.7 und Android 6 kann diese Funktion in den Einstellungen der Smartphones aktiviert werden. Bisher waren nationale Warn-Apps zusätzlich notwendig, um eine Infektion zu melden. In Zukunft könnten Länder und Behörden jedoch gänzlich auf die integrierte Technologie von Apple und Google setzen.

Rein technisch verändert sich wenig: die während des Kontakts erzeugten Zufallsschlüssel werden statt über die offizielle Corona-Warn-App direkt aus dem Betriebssystem an die Backend-Server übertragen. Was auf den ersten Blick wie eine Vereinfachung aussieht, offenbart auf den zweiten Blick deutliche Schwächen.

Souveränität statt Dominanz von Google und Apple

Zunächst der Mangel an Transparenz. Aus der vielfach diskutierten datenschutzrechtlichen Diskrepanz ergibt sich zudem eine Frage des Vertrauens: Sind Apple und Google eine vertrauenswürdige Instanz?

Während der Quellcode der offiziellen Corona-Warn-App öffentlich zugänglich ist, sind die Quellcodes der Betriebssysteme von Apple und Google – auch von Experten – schwieriger zu

[37] https://fragdenstaat.de/anfrage/vertragsdokumente-zur-corona-app-mit-der-telekom-und-sap/513354/anhang/Vertrag%20Telekom.pdf
[38] https://www.golem.de/sonstiges/zustimmung/auswahl.html?from=https%3A%2F%2Fwww.golem.de%2Fnews%2Fbundesregierung-entwicklung-von-corona-app-kostet-20-millionen-euro-2006-149033.html
[39] https://www.nzz.ch/technologie/die-beste-corona-app-ist-auf-dem-boden-der-realitaet-angekommen-ld.1574541
[40] https://twitter.com/cem_oezdemir/status/1304064631217020930?s=09
[41] https://www.wiwo.de/technologie/digitale-welt/corona-app-jetzt-noch-die-juristische-keule-auszupacken-waere-kontraproduktiv/25756524-all.html
[42] https://tracecorona.net/de/2020/06/12/corona-tracing-ansatz-von-google-und-apple-hat-defizite-bei-datenschutz-und-sicherheit/

überprüfen. Auch wenn nur wenige den Quellcode der offiziellen Corona-Warn-App einsehen, schafft allein die Möglichkeit es tun zu können, mehr Vertrauen und Akzeptanz als die Datenschutzrichtlinien dieser beiden Unternehmen.

Nicht nur in fehlender Transparenz zeigen sich Schwachstellen. Die ohnehin schon enorme Datenmacht dieser beiden Konzerne wächst weiter. Das wirft die Frage nach der technologischen Souveränität auf. Wem obliegt die Aufgabe, die Gesundheit der Bevölkerung zu schützen? Amerikanischen Datenriesen oder der Regierung? Damit die Menschen auf die Tracing-Funktion vertrauen, sind der Schutz persönlicher Daten und die Gewährleistung der Anonymität der Nutzer und Nutzerinnen unverzichtbar.

Entscheidend ist, wer die Kontrolle über die Daten hat. Neben dem möglichen Verlust der technologischen Souveränität und der damit verbundenen steigenden Abhängigkeit von Apple und Google steht noch eine weitere Frage im Raum: Was passiert, wenn der technische Support für die bisher entwickelten Tracing-Apps eingestellt wird?

Bisher ist unser Gesundheitssystem ein Bereich, der nur wenig von der Dominanz und der Datensammlung dieser beiden Datenriesen betroffen war. Wollen wir diesen Bereich aufgeben? Apple und Google haben Zugriff auf Unmengen an Nutzerdaten. Wer garantiert, dass die bereits gesammelten Daten nicht mit den Contact-Tracing-Daten verbunden und in Beziehung zueinander gesetzt werden? Wie bereits erwähnt leidet die Contact-Tracing-Schnittstelle von Google und Apple immer noch unter Datenschutzmängeln wie etwa der Möglichkeit Bewegungsprofile von infizierten Nutzer*innen zu erstellen. Und wer garantiert, dass sich andere Staaten nicht einmischen und die Contact-Tracing-Ergebnisse etwa durch Relay-Angriffe manipuliert werden?

Dranbleiben, um effektive Lösungen zu fördern

Unser Überblick hat verschiedene Aspekte zum Sinn und Unsinn der Corona-Warn-App aufgezeigt. Neben den hier aufgeworfenen Fragen sind viele weitere noch offen: Entspricht die Corona-Warn-App den Erwartungen oder entpuppt sie sich nach einer kritischen Überprüfung als Fehlinvestition? Können wir den tatsächlichen Mehrwert in einer Wirksamkeitsstudie ermitteln? Auf welcher Datenbasis lässt sich die Wirksamkeit bewerten? Welche datenschutzrechtlichen Herausforderungen sind weiterhin zu bewältigen? Und bleibt die Anwendung freiwillig? Welche Langzeitfolgen hat diese Technologie, die jetzt bereits in fast allen Smartphones integriert ist und es damit den Datenriesen Apple und Google ermöglicht, noch mehr Daten über uns zu sammeln? Warum sollten sich die europäischen Länder Google und Apple unterwerfen?

Dieser Fragenkatalog ließe sich beliebig erweitern. Daher bedarf es aus unserer Perspektive dringend weiterer wissenschaftlicher Diskussionen und fundierter Studien. Dabei sollte man nicht aus Angst vor einem negativen Ergebnis die Auseinandersetzung scheuen, sondern im Sinne aller eine ehrliche Diskussion und eine kritische Bewertung vorantreiben.

Autoren:
Prof. Dr.-Ing. Alexandra Dmitrienko; Universität Würzburg
Lisa Fröhlich; Technische Universität Darmstadt
Dr.-Ing. Markus Miettinen; Technische Universität Darmstadt
Thien Duc Nguyen, Technische Universität Darmstadt
Prof. Dr.-Ing. Ahmad-Reza Sadeghi; Technische Universität Darmstadt