Die "freiwillige" Corona-App

Die Bundesregierung setzt für eine schrittweise Rücknahme der Corona-Kontaktbeschränkungen auf eine breite Akzeptanz für die nach Ostern herunterladbare App zur nachträglichen Kontaktrekonstruktion Infizierter. Die (berechtigte) Angst vor dem Virus wird benutzt, um einem Großteil der Bevölkerung „freiwillig“ ein autoritär hochwirksames Werkzeug zu verabreichen.

Wir kritisieren in diesem Artikel die technische Konstruktion der App, aber auch ihre sozial-technokratischen Konsequenzen. Selbst wenn das Protokollieren von Kontakten vollständig pseudonym erfolgen würde, müssen wir dringend vor dieser App warnen. In dem Moment, wo (sogar anonyme) Verhaltensdaten flächendeckend anfallen, sind die prädiktiven Modelle, die damit trainiert werden, dazu in der Lage, ganze Populationen in Risikogruppen einzuteilen und algorithmisch zu verwalten. Hinzu kommt, dass ein simples Software-Update die App in ein wirksames Tool zur individuellen Zugangsbeschränkung verwandelt. Daher unser klares Nein zur Corona-App!

Ein internationales Team bestehend aus rund 130 Wissenschaftler*innen, IT-Entwickler*innen, Datenschutzerbeauftragten und Soldat*innen arbeiten derzeit in einem Projekt mit dem Namen Pan European Privacy-Protecting Proximity Tracing (PEPP-PT) an einer Software, welche die SARS-CoV-2-Virusverbreitung einschränken soll. Beteiligt sind aus Deutschland unter anderem das Robert-Koch-Institut (RKI), das Heinrich-Hertz-Institut (HHI) und das Bundesamt für Sicherheit in der Informationstechnik (BSI). Auch der Bundesdatenschutzbeauftragte begleitet die Entwicklung und Soldat*innen der Bundeswehr helfen bei den Tests. Bis auf RKI sind sie auf der Website des Projekts nicht gelistet. Das HHI ist unter Fraunhofer subsumiert. Bislang sind Forscher*innen und Institute aus acht Ländern an der Entwicklung beteiligt: Belgien, Dänemark, Deutschland, Frankreich, Italien, Österreich, Spanien und die Schweiz.

Um die Ausbreitung einzudämmen, sollen Kontaktpersonen von Infizierten frühzeitig gewarnt werden. Wenn Menschen Symptome zeigen, dann haben sie das Virus bereits weitergegeben. Deshalb sollen nach einer positiven Diagnose alle Handybesitzer benachrichtigt werden, deren Geräte in der Nähe des Erkrankten waren. Wenn es viele einzelne Ansätze und Software-Lösungen gibt, die jeweils nur ein kleiner Teil der Bevölkerung nutzt, kann das Konzept nicht aufgehen. Deshalb soll eine gemeinsame Grundlage entstehen, die möglichst schnell eine kritische Größe erreicht. Die Rede ist von einer gemeinsamen Plattform: einer Client/Server-Referenzimplementierung, aber auch von einem Softwaregerüst auf dem Smartphone-Apps aufsetzen können. Diese Smartphone-Apps, die Nutzer*innen auf ihrem Telefon installieren, bilden einen wesentlichen Teil des Systems. In Deutschland arbeiten RKI und HHI an einer solchen Anwendung. Um Infektionsketten wirksam zu unterbrechen, streben die Forscher*innen eine Nutzer*innenbasis von etwa 60 Prozent der Bevölkerung an. In Deutschland wären das 50 Millionen Menschen. Bislang gibt es in Deutschland keine App, die nicht auf Smartphones vorinstalliert ist und bewusst heruntergeladen werden muss, die so viele Nutzer*innen hat. Allerdings könnte auch ein geringerer Anteil helfen, die Ausbreitung zumindest zu verlangsamen. Laut Bitkom besitzen 81 Prozent aller Menschen in Deutschland über 14 Jahren ein Smartphone. Normale Handys und ältere Geräte unterstützen den nötigen Bluetooth-Standard noch nicht. Insbesondere Senior*innen, für die das Virus besonders gefährlich ist, können nur zum Teil gewarnt werden. Deshalb denken die Forscher darüber nach, künftig auch Bluetooth-Armbänder oder andere Wearables zu verteilen. Einer repräsentativen Umfrage (Stand 31.03.2020) zufolge, würden mehr als 70 Prozent der Befragten so eine App auf jeden Fall oder wahrscheinlich nutzen. Die Mehrheit gibt an, den Aufforderungen der App nachkommen zu wollen und sich in Quarantäne zu begeben, sollten sie mit einer infizierten Person in Kontakt gekommen sein. Umfragen zufolge wäre ein Großteil der Bevölkerung in Deutschland bereit, einen Teil ihrer Privatsphäre aufzugeben, um das Virus zu stoppen. Die PEPP-PT-Plattform soll am 7. April fertiggestellt werden. RKI und HHI wollen die App für deutsche Nutzer*innen etwa eine Woche später veröffentlichen.

Das System soll als Gegenentwurf zu den repressiven und invasiven Ansätzen anderer Länder verstanden werden. Anstatt massenhaft sensible Standortdaten zu sammeln, Nutzer*innen zu überwachen oder Infizierte an einen digitalen Corona-Pranger zu stellen, soll PEPP-PT komplett freiwillig und datenschutzfreundlich sein. Die Betreiber versprechen, die Privatsphäre von Nutzer*innen der Software zu schützen. Die Identität der Nutzer*innen bleibt zu jedem Zeitpunkt geschützt heißt es: weder Ärzt*innen noch die Betreiber der Plattform können Einzelpersonen identifizieren. Für gute PR sorgen Zeitungen, die sogar von einer anonymen Nutzung

schreiben, obwohl es sich um eine Pseudonymisierung handelt. Das PEPP-PT-Modell scheint auch nicht zu 100 Prozent Privacy-by-Design zu erfordern. Die Spezifikationen und den Quellcode gibt es laut der bisher sehr informationsarmen Webseite aktuell allerdings nur als Mitglied des Konsortiums.

> *Wir sagen: Code und alle Dokumente offenlegen, sonst glauben wir gar nichts. Und nicht nur irgendeine Client-Referenzimplementierung, sondern die ganze Spezifikation und den ganzen Server-Code.*

Kritik 1: Technische Details

> *Folgende technische Details beruhen auf den wenigen Informationen der PEPP-PT-Website und Berichten von Netzpolitik.org.*

Die Apps weisen jedem Gerät eine vorübergehend gültige, authentifizierte und zufällig generierte Identifikationsnummer (ID) zu. Die temporär, zufällig erzeugte ID funktioniert als Pseudonym, welches die Identität zuverlässig schützen sollen. Sie wird in regelmäßigen Abständen geändert (die Rede ist von 30 Minuten) und sollen nicht mit dem Telefon in Verbindung gebrach werden können. Des Weiteren soll niemand im Nachhinein herausfinden können, welche Person sich hinter einem solchen Pseudonym verbirgt. Jedes PEPP-PT-Telefon (gemeint ist ein Smartphone auf dem die App installiert ist) sendet über eine kurze Entfernung mit Bluetooth-Funktechnik (Bluetooth-Low-Energy) seine aktuelle ID und scannt gleichzeitig die Umgebung und erfasst, welche anderen Smartphones mit installierter PEPP-PT-Software sich in Reichweite befinden. Wenn sich zwei Geräte näher kommen, speichern die Apps die temporäre ID des jeweils anderen Smartphones. Die Annäherung von Telefonen anderer PEPP-PT-Benutzer wird durch die Messung von Funksignalen (Bluetooth usw.) realisiert. Die Daten bleiben zunächst verschlüsselt auf dem Smartphone, niemand kann darauf zugreifen, heißt es. Aufgrund der geringen Informationen ist offen, wie das konkret kryptographisch umgesetzt wurde. Nicht jede Annäherung wird gespeichert. Nur wenn sich PEPP-PT-Telefon A über einen epidemiologisch ausreichenden Zeitraum in der Nähe von PEPP-PT-Telefon B befindet (die Rede ist von 15 Minuten in 1,5 Metern Entfernung), dann wird die aktuelle temporäre ID von Telefon B, in der verschlüsselten, lokal auf dem Telefon gespeicherten Annäherungsgeschichte (Proximity-Historie) von A gespeichert (und umgekehrt). Offen bleibt, ob die Wahl von 15 Minuten eine sinnvolle Zeitdauer ist, denn Anhusten im Bus oder im Geschäft dauert nur wenige Sekunden, Kurzgespräche 1-2 Minuten. Das reicht auch schon für die Ansteckung. Offen bleibt auch was konkret gespeichert wird. Laut PEPP-PT-Website werden keine Geolokalisierung, keine persönlichen Informationen, einzigartige Gerätekennungen wie die IMEI-Nummer des Smartphones oder andere Daten protokolliert, die eine Identifizierung des Benutzers ermöglichen würden. Weiter heißt es: Die pseudonyme Annäherungsgeschichte kann von niemandem eingesehen werden, auch nicht vom Benutzer von Telefon A. Ältere Ereignisse in der Annäherungsgeschichte werden gelöscht, wenn sie epidemiologisch unbedeutend werden.
"Wir messen nur, wie lange und wie nahe sich zwei Personen begegnet sind", sagt Thomas Wiegand, der das HHI leitet. Wo das Treffen stattgefunden habe, sei dem Virus egal. "Das sind die einzigen Informationen, die epidemiologisch von Bedeutung sind." Nach 21 Tagen werden die Daten automatisch gelöscht. Statt auf Tracking setzt PEPP-PT auf Tracing – es sollen nicht die Bewegungen von Menschen verfolgt, sondern nur ihre Kontakte nachverfolgbar werden. Auf dem Smartphone entsteht eine Liste mit IDs mit Zeitstempeln, hinter denen sich Personen verbergen, die man selbst angesteckt haben könnte, oder von denen man Viren erhalten haben könnte.

Um Fehlalarme zu reduzieren, haben die Forscher*innen alle weit verbreiteten Smartphonemodelle untersucht und die Signalstärke der Funktechnik gemessen, da sie sich teils unterscheidet.
Soldat*innen der Bundeswehr haben geholfen, die Technik so zu kalibrieren, dass sie etwa erkennt, ob zwischen den beiden Kontaktpersonen eine Glasscheibe oder andere Hindernisse waren, die eine Übertragung des Virus verhindern. Eine zuverlässige Genauigkeit der Aussage, ob jemand innerhalb eines Radius von 1,5 Metern war oder nicht, mittels Bluetooth ist äußerst zweifelhaft.

Nutzung der Annäherungsgeschichte

In dem Fall, dass eine Benutzer*in nicht getestet wird oder negativ getestet wurde, bleibt die Annäherungsgeschichte auf dem Telefon des Benutzers verschlüsselt und kann von niemandem eingesehen oder übertragen werden. Wenn allerdings bestätigt wurde, dass die Benutzer*in von Telefon A SARS-CoV-2-positiv ist, (also in der Regel bereits an Covid-19 erkrankt ist), dann soll diese Person ihre aktuelle bis dato lokal gespeicherte ID-Liste in der Annäherungsgeschichte auf einen nationalen zentralen Server übermitteln. Das ist nicht ohne

weiteres möglich. Ärzt*innen, Labore und Gesundheitsbehörden müssen die Meldung bestätigen. Es braucht also zwingend eine positive Diagnose. Dann setzen sich die Gesundheitsbehörden mit Benutzer*in A in Verbindung und stellen ihr eine TAN zur Verfügung, die sicherstellt, dass potenzielle Malware keine falschen Infektionsinformationen in das PEPP-PT-System einschleusen können. Die Schnittstelle soll verschlüsselt und geheim funktionieren, sodass die Identität der Erkrankten geschützt bleibt. Die Benutzer*in verwendet diese TAN, um freiwillig Informationen an den Server des nationalen Dienstleisters zu übermitteln, in Deutschland beispielsweise beim Robert-Koch-Institut, die die Benachrichtigung von PEPP-PT-Anwendungen ermöglichen, die in der Annäherungsgeschichte aufgezeichnet und somit potenziell infiziert sind.

Noch ist die Rede davon, dass alles freiwillig passiert. Nur falls die Nutzer*in zustimmt, erfährt der zentrale Server, mit welchen anderen temporären IDs dieses Smartphone in Kontakt war. Der soziale Druck wird ausgeblendet.

Was passiert mit den Daten auf dem Server?

Das Konsortium schreibt, da die Annäherungsgeschichte pseudonyme Identifikatoren enthält, kann der Server aus diesen IDs nicht auflösen, welche Menschen sich dahinter verbergen, er kann aber alle betroffenen Kontaktpersonen über die App benachrichtigen und auffordern, sich testen zu lassen.

Diese Benachrichtigung kann dabei ganz ohne Ansehen der Personen verschickt werden, die die Smartphones nutzen. Denn um eine Nachricht auf dem Smartphone anzeigen zu können sind keinerlei personenbezogene Daten erforderlich. Es genügt vielmehr ein sogenanntes Push-Token, eine einzigartige App-Geräte-Kennung, um über Apples oder Googles Push-Notification-Gateways eine Push-Nachricht auf das Gerät zu schicken. Dieses Push-Token wird bei der Installation der App auf dem Handy generiert. Zugleich hinterlegt die App sowohl das Push-Token als auch die temporären IDs, die sie im Laufe der Zeit aussendet, auf einem zentralen Server. Auf diese Weise können die Smartphones allein anhand von temporären IDs und Push-Tokens adressiert werden, ohne dass die Identität der Personen feststellbar wäre, die diese Smartphones bei sich tragen. Dazu ist es aber notwendig, dass zu jedem Account Push-Token und alle generierten aktuellen tempörären IDs inklusive Zeitstempel, wann sie generiert wurden, auf dem Server liegen. Es muss dem Server vertrauen entgegen gebracht werden, dass er nach 21 Tagen epidemiologisch irrelevante Daten löscht – und nicht für Big-Data-Zwecke weiterhin speichert. Sobald man die das Push-Token mit Daten des Providers verknüpfen würde (Push-Token-Zuordnung zu Gräte-ID, IMEI, oder Rufnummer), wäre eine Zuordnung leicht.

Kritik 2: Auch anonym trainieren wir KI

Die PEPP-PT-App soll nicht auf personenbezogene Daten des einzelnen Individuums zugreifen. Doch die Gefahren entstehen nicht nur unmittelbar bei der digitalen Ausleuchtung Einzelner, sondern dadurch, dass die entstehende Datensammlung algorithmische Verfahren zur Bevölkerungsverwaltung ermöglicht. Pseudonymisierte Massendaten dienen zum Training künstlicher Intelligenzen (KI) z. B. im Kontext vorhersagender Analysen. In dem Moment, wo Verhaltensdaten fast flächendeckend anfallen und (sei es auch anonymisiert) erhoben werden, sind die prädiktiven Modelle, die damit trainiert werden, dazu in der Lage, ganze Populationen in Risikogruppen einzuteilen und algorithmisch zu verwalten. Datenbasierte Algorithmen können die Gesellschaft dann in unsichtbare soziale Klassen einteilen, zum Beispiel in Bezug darauf, wer aufgrund seiner Bewegungsmuster vermeintlich ein besonderes Sicherheits- oder Gesundheitsrisiko darstellt, weil das Bewegungsprofil erkennen lässt, dass jemand das Virus in besonderem Maße verbreitet hat oder wer prioritären Zugang zu knappen medizinischen Ressourcen wie Beatmungsplätzen verdient.

> *Algorithmische Scoring- und Entscheidungsverfahren beruhen auf einem anonymen Abgleich mit den Daten viele anderer Individuen.*

Daher kann mensch durch Weitergabe der eigenen (selbst anonymisierten oder pseudonymisierten) Daten potenziell anderen Individuen und Gruppen schaden und umgekehrt durch die Datenweitergabe anderer potenziell selbst betroffen sein. Diese Gefahr wird in der verkürzten Debatte um die PEPP-PT-App und auch schon bei der Weitergabe anonymisierter Telekom-Daten oder anonymisierter Google-Positionsdaten ausgeblendet. Sie ist auch nicht Gegenstand wirksamer datenschutzrechtlicher Bemühungen. So schützt auch die Datenschutzgrundverordnung DSGVO nicht vor der Verwendung anonymisierter Daten für prädiktive

algorithmische Entscheidungen, Risikoklassifizierung (Scoring) und verhaltensbasierte Ungleichbehandlung von Individuen oder Gruppen. In diesem Sinne trägt jeder, der die PEPP-PT-App nutzt, zu solch einer Ungleichbehandlung bei.

> *Hier ist die Unterscheidung von anonymen und personenbezogenen Daten überholt, weil irrelevant!*

Kritik 3: „Freiwilligkeit“

> *"Bitte haben Sie Verständnis dafür, dass wir zu ihrer eigenen Sicherheit und zur Sicherheit unserer Mitarbeiter*innen nur nachweislich nicht-infizierte Personen befördern können."*

So könnte die Erklärung der Deutschen Bahn an allen Automaten und Ticket-Schaltern lauten, die ihre Dienstleistung „bis zum Ende der Corona-Krise“ nur Fahrgästen mit einer modifizierten PEPP-PT-App anbietet. Die PEPP-PT-App 2.0 würde dazu (wiederum absolut freiwillig und erst bei Einwilligung durch die Nutzer*in) "auf Wunsch" **alle** Kontakt-Ereignisse direkt an den Server melden – quasi mit einer Frei-TAN. Weiterhin werden keine persönlichen Daten, also auch keine Ortsdaten aufgezeichnet. Nur wenn sich aus der Echtzeit-Auswertung aller Kontakt-Ereignisse der letzten 14 Tage *keine* Verbindung zu einer infizierten Person ergibt oder zu einer Person, die zuvor mit einer infizierten Person Kontakt hatte, leuchtet der QR-Code des elektronischen Bahntickets grün, also *"wahrscheinlich nicht infiziert"*. Das bedeutet grünes Licht wahlweise bei der Fahrkartenkontrolle oder beim Betreten des Bahnhofs.

Nach dem gleichen Prinzip könnten Einkaufszentren, Konzerthallen, Stadien, … den Zutritt oder die Bezahlung an der Kasse an die Bedingung knüpfen, ein Smartphone mit PEPP-PT-App-Status "Grün" vorzuzeigen. Das wäre eine massive Einschränkung der Bewegungsfreiheit – wer "frei" sein will, muss sich der App (und der dahinterstehenden Serverinfrastruktur) unterwerfen. Das ist vergleichbar mit einer elektronischen Fußfessel: Freigänger müssen sie tragen, oder zurück in den geschlossenen Vollzug.

Die "freiwillige" PEPP-PT-App wird damit zum Unterscheidungs-Werkzeug für individuelle soziale Teilhabe. Wer Bahn fahren will, bräuchte dann diese PEPP-PT-App 2.0. Der Staat "verordnet" diese erweiterte PEPP-PT-App nicht, er stellt sie lediglich zur Verfügung. Wirtschaftliche Akteure – in unserem Beispiel die Deutsche Bahn – würden ihre Dienstleistung nur denen anbieten, die in diese weiterführende Variante der PEPP-PT-App einwilligen. Regierung und Dienstleister würden dabei ganz im Sinne einer übergeordneten Verantwortung für das Gemeinwohl handeln. Wer will da noch meckern ...?

Auf dieser Form von "Freiwilligkeit" basieren viele der derzeit erprobten Social-Scoring-Modelle in China. Wer nicht mitmacht, oder die erforderliche Eigenschaft (gemäß App, nicht infiziert zu sein) nicht erfüllt, kann ohne Verbotsverfügung "freiwillig" vom öffentlichen Leben ausgeschlossen werden: Die PEPP-PT-App als Einübung individueller Einschluss- / Ausschluss-Mechanismen zukünftiger Soziale-Punkte-Systeme auch in Deutschland.

Ein letzter Aspekt ist, dass Daten von denen versprochen wird, dass sie vertraulich behandelt werden, immer wieder zur Strafverfolgung verwendet werden und die Diskussion wird erst aufhören, wenn die Nutzung freigegeben wurde. Wo ein Trog ist, kommen die Schweine. Beispiele (wie etwa die Kennzeichenerfassung der elektronischen Maut) gibt es viele. Dazu kommt die behördliche Weigerung bei Löschung einst erhobener Daten.

Aktuell müssen Personen aktiv die Daten in ihrer Annäherungsgeschichte freigeben. Aber mit einem Software-Update ist es leicht zu beheben, derart dass immer *alle* Kontakte hochgeladen werden. So entsteht zum Einen ein riesiger Heuhaufen, der für Big-Data-Zwecke nutzbar ist. Wenn immer alle Kontakt-IDs übermittelt werden (also nicht mehr nur freiwillig wenn eine Person infiziert ist), dann kann der Server auch Traces bilden und Verbindungen herstellen, wer wie oft wen trifft. In Zusammenarbeit mit den Telekommunikationsanbietern zur Auflösung von IP-Adressen könnten Strafverfolgungsbehörden, dann auflösen, wer sich hinter den IDs verbirgt.

capulcu, 5. April 2020
capulcu.blackblogs.org