Das grosse sozial-digitale Experiment

Contact-Tracing-Apps sollen im Kampf gegen das Coronavirus eine wichtige Rolle spielen. Schweizer Anbieter haben bereits Lösungen entwickelt – nun preschen Google und Apple vor. Hält die digitale Epidemiebekämpfung, was sie verspricht?

Von Adrienne Fichter, 16.04.2020

Eine App solls richten: Contact-Tracing-Technologie gilt als wichtiges Mittel gegen die Corona-Epidemie. Oliver Ruether/laif

Die bisherigen Massnahmen gegen das Coronavirus waren mehrheitlich archaisch: die Hände waschen, zu Hause bleiben, Begegnungen vermeiden. Nur punktuell wurde in der westlichen Welt versucht, Infektionsketten manuell nachzuzeichnen und so die Weiterverbreitung zu unterbinden.

Bald soll sich dies ändern. Je näher das Ende der Lockdown-Massnahmen rückt, desto intensiver wird an digitalen *Contact-Tracing*-Lösungen getüftelt. Im Fokus steht das Smartphone: Es soll die Kontakte der Besitzer registrieren und bei Infektionsgefahr Alarm schlagen können. Zahlreiche Initiativen und Apps dazu sind in den letzten Wochen aus Hackathons hervorgegangen.

Die gute Nachricht: Anders als oft kolportiert müssen Gesundheit und Privatsphäre dabei kein Gegensatz sein. Es geht um ein anderes Thema: verantwortungsvolle versus nicht verantwortungsvolle Technologie. So formuliert es die Privacy-Expertin Frederike Kaltheuner, und so schreibt es auch der Republik-Entwickler Patrick Recher, der eine ausführliche Erklärung verfasst hat: «So funktioniert eine Corona-Tracing-App, die Ihre Privatsphäre schützt».

Wie eine verantwortungsvolle *Tracing*-Technologie im Detail aussieht, ist Gegenstand von gesundheits- und netzpolitischen Debatten. Dabei geht es:

- um das geeignetste technische Design und die Einbindung der Gesundheitsbehörden;
- um die konkrete praktische Anwendung und den Nutzen.

Die westlichen Länder, darunter auch die Schweiz, müssen sich überlegen, wie sie mit diesen Fragen umgehen – um schliesslich eine Technologie auszurollen, die nicht nur sämtlichen datenschützerischen Anforderungen gerecht wird, sondern auch tatsächlich ihren Zweck erfüllt.

Was bisher geschah

Damit nicht jedes europäische Land sein eigenes App-Süppchen kocht und die verschiedenen Lösungen miteinander kompatibel sind – sodass man über die Landesgrenze verreisen kann –, haben sich Wissenschaftlerinnen, Datenschutzexperten und Entwicklerinnen im März zusammengetan. Die meisten sind auf dieselbe Lösung gekommen: Die Nähe zwischen zwei Personen soll nicht anhand der Messdaten einer Handyantenne, sondern mit den Mobiltelefonen selbst gemessen werden.

Dies wäre ein Novum. Bisher wurden in der Schweiz einzig die Standortdaten des Mobilfunkdienstleisters Swisscom verwendet, um die Einhaltung der *Social-Distancing*-Massnahmen durch die Bevölkerung zu überprüfen. Dies war jedoch mit rechtlichen und technischen Problemen verbunden.

Probleme mit Mobilfunkdaten

Der Bundesrat erliess im März eine Verfügung zur Herausgabe der Standortdaten des Telecomkonzerns Swisscom. Dabei wurden die Aufenthaltsorte von Swisscom-Kunden (die Swisscom auch kommerziellen Kunden zur Verfügung stellt) mit einem Hash-Wert (einer Prüfsumme) pseudonymisiert und grafisch aufbereitet. Die Regierung erhielt dadurch einen Einblick, um die Einhaltung der *Social-Distancing*-Massnahmen durch die Bevölkerung zu überprüfen.

Obwohl die Aufbereitung einen grossen Grad an Anonymität gewährleistet, ist das Vorgehen dennoch fragwürdig.

1. Aufgrund der mangelnden Transparenz. Erst nachdem die Digitale Gesellschaft sowie eine Reihe von Journalisten (darunter auch solche der Republik) via Öffentlichkeitsgesetz die bundesrätliche Verfügung integral verlangt hatten, entschied sich das BAG am Freitagabend, 3. April, die Verfügung im Netz zu veröffentlichen. Dieser Schritt war überfällig.
2. Wegen der fehlenden Einwilligung der Swisscom-Kunden. Zwar berufen sich Bundesrat und Swisscom auf die Covid-19-Verordnung 2, auf das Epidemiengesetz (Artikel 7) und auf das Fernmeldegesetz (Artikel 45b), und die Swisscom verweist zusätzlich auf die Datenschutzerklärung, die jede Swisscom-Kundin beim Vertragsabschluss mitunterzeichnet. Der Verweis auf eine Einwilligung via pauschale Nutzungsbedingungen ist in Datenschutzfachkreisen aber sehr umstritten.
3. Wegen der mangelnden Genauigkeit. Die Mobilfunkdaten sind nur für grobe Analysen geeignet. Standortdaten, die via Antennenstandorte und Funkzellen gewonnen werden, versagen nicht nur in urbanen Räumen oder in der Umgebung von Hochhäusern. Sie können auch in ländlichen Gebieten sehr ungenau sein und taugen daher nicht zur Analyse der genauen Aufenthaltsorte von Personen.

Effizienter, transparenter und auch bürgerfreundlicher ist die direkte Kontaktnachverfolgung durch das Smartphone. Diese wird nicht *top-down,* sondern *bottom-up* umgesetzt und beruht auf der freiwilligen Mitwirkung der Nutzer. Ohne dass diese eine App herunterladen, das Bluetooth-Signal einschalten und dem *Tracing* aktiv zustimmen, geschieht bei dieser Variante – gar nichts. Die Bluetooth-Übertragungstechnik eignet sich mit ihrem beschränkten Aktionsradius besonders gut für das sogenannte *Proximity Tracing*.

Angestrebt wird eine Technologie, die vier Grundsätzen Rechnung trägt: Sie ist datensparsam, setzt auf *Privacy by Design,* beruht auf Freiwilligkeit und verfügt über einen öffentlich einsehbaren und überprüfbaren Quellcode.

Erfreulich ist: Die Schweiz ist bei der Entwicklung solcher dezentraler, datenschutzkonformer *Tracing*-Modelle vorne dabei. Kryptologinnen, Sicherheitsforscher und Epidemiologinnen der EPFL und der ETH Zürich sind führend bei der Entwicklung des in der europäischen Netzgemeinschaft beliebten offenen Protokolls DP3T.

Bis zum 10. April schien es sich beim Tüfteln an *Contact-Tracing*-Applikationen vor allem um eine europäische Angelegenheit zu handeln. Doch dann kündigten Google und Apple eine fast schon historische Partnerschaft an. Die Techkonzerne wollen im Mai eine gemeinsame Schnittstelle ausrollen, die *Contact-Tracing*-Applikationen einen einfacheren Zugang auf alle Android- und Apple-Handys ermöglichen soll. Gelingt den Konzernen dieser Schritt, wäre dies eine nahezu hundertprozentige Abdeckung: Fast jeder Schweizer Smartphone-Nutzer wäre *Contract-Tracing*-fähig, sofern er das möchte.

Damit erhalten die anstehenden Technologieentscheide zusätzliche Brisanz.

Die technischen Fragen

1. Zentrales versus dezentrales Modell?

Hier geht es um eine grundsätzliche Designfrage: Sollen Begegnungen an einem zentralen Ort aufgezeichnet werden oder verteilt bei den einzelnen Nutzern?

Bei einem zentralen Modell geschieht Folgendes:

- Zwei Nutzer, A und B, haben beide die *Contact-Tracing*-App installiert und begegnen sich. Ihre Apps speichern bei der Begegnung einen Zeitstempel (das aktuelle Datum) und Begegnungspaare (die zufällig generierten IDs ihrer Smartphones) unverschlüsselt auf den Endgeräten ab.
- Nun findet A heraus, dass sie mit dem Coronavirus infiziert ist, und möchte alle Leute benachrichtigen, denen sie in den vergangenen zwei Wochen begegnet ist. Sie sendet alle lokal gespeicherten Begegnungspaare (die verschiedenen IDs) samt Zeitstempel an einen zentralen Server.

Das Problem dabei: Die Begegnungspaare werden nicht verschlüsselt, da die wichtigsten Prozesse (Upload, Abgleich und Benachrichtigung) über den zentralen Server stattfinden. Damit werden Personen relativ leicht re-identifizierbar, insbesondere wenn Zeitstempel und Identitätenverbindungen unverschlüsselt auf dem zentralen Server liegen. Die Anonymität der App-Nutzerinnen wäre damit kaum mehr gewährleistet. Gesundheitsbehörden und App-Betreiber hätten direkten Zugriff auf sensible Daten und könnten Begegnungen rekonstruieren. Weiteres Missbrauchspotenzial besteht darin, dass Nutzer aus Spass Identitäten mit ihrer App generieren und diese an den Server senden könnten.

Simpler und bürgerfreundlicher wären die dezentrale Lösung des Schweizer IT-Unternehmens Ubique sowie das Protokoll der Autorengruppe DP3T rund um den Epidemiologen Marcel Salathé und IT-Expertin Carmela Troncoso. Google und Apple bieten eine sehr ähnliche vollständige Integration der Technologie auf Betriebsebene an. Allerdings wird diese erst ab einem unbekannten Datum Mitte Mai verfügbar sein und ist zurzeit nicht Open Source einsehbar.

Wie ein solches dezentrales Modell funktioniert, lesen Sie in dem bereits erwähnten Erklärtext: «So funktioniert eine Corona-Tracing-App, die Ihre Privatsphäre schützt». Die wichtigsten Eckpunkte:

- A und B tauschen ähnlich wie beim zentralen Modell einen Zeitstempel aus. Hinzu kommt ein kryptografisch generierter Code, eine Art «Schloss».
- Infiziert sich A mit dem Virus, so schickt es über einen Server nichts weiter als eine einzige Information: einen kryptografischen Schlüssel.
- Passt dieser Schlüssel auf ein lokal gespeichertes Begegnungs-Schloss, so erfährt B damit von der möglichen Infektionsgefahr.

Das Bestechende am dezentralen Modell ist: Die heiklen, personenbezogenen Daten verlassen zu keinem Zeitpunkt das lokale Gerät, also das Smartphone. A und B tauschen lediglich den privaten, anonymen Schlüssel ihrer hinterlegten Begegnungspaar-Einträge über einen zentralen Server aus. Dieser Server (und damit auch der App-Betreiber) kennt nur die Anzahl der Infizierten, kann aber nicht rekonstruieren, um wen es sich handelt.

Gruppierungen wie das Schweizer Netzwerk Digitale Selbstbestimmung oder der deutsche Chaos Computer Club sehen dieses Kernmerkmal –

die dezentrale Speicherung und Verarbeitung von Daten – als wichtigen, vertrauensstiftenden Grundsatz an. Das Netzwerk Digitale Selbstbestimmung merkt in einer Fussnote an: «Speicherung in zentrale Datenräume soll es nur geben, wenn hierfür ein wichtiges epidemiologisches Bedürfnis besteht.»

Ubique entwickelt nun zurzeit in Zusammenarbeit mit der Hochschule EPFL einen Prototypen des dezentralen DP3T-Protokolls zuhanden des Bundesamts für Gesundheit weiter und hat sich dem PEPP-PT-Konsortium angeschlossen, einer paneuropäischen Initiative unter Federführung des deutschen Heinrich-Hertz-Instituts. Dem Konsortium gehören rund 130-Wissenschaftler an, darunter viele der beiden ETH.

Da die Forscherinnen verschiedene Varianten entwickelt haben, bezog das Konsortium noch keine Stellung zur Frage, welches Modell das Bessere sei: zentrales oder dezentrales *Tracing*.

Doch Google und Apple haben die Entscheidung für die Regierungen gewissermassen gefällt: Möglich werde auf ihren Betriebssystemen ohnehin nur ein dezentraler Standard sein, behauptet zumindest der Jurist Michael Vaele, der an dem DP3T-Protokoll mitgearbeitet hat.

2. Staatlich oder nicht staatlich?

Eine weitere Gretchenfrage lautet: Soll der Staat die App bereitstellen oder nicht?

Die Lösung von Ubique (die bei einem Hackathon entwickelte App «Next Step») kann beispielsweise vollständig von privaten Anbietern betrieben werden. Dies wäre dann die maximal mögliche digitale Selbstbestimmung.

Infizierte würden dabei selbstständig ihr Umfeld und alle Begegnungen benachrichtigen. Voraussetzung dafür wären sehr gewissenhafte Bürgerinnen und Bürger. Das Problem wären wiederum schwarze Schafe, die das System aus Spass «trollen» und sich fälschlicherweise als infiziert ausweisen.

Die meisten Experten sind sich daher einig, dass der Staat an einer *Tracing*-App beteiligt sein muss. Denn ohne Autorisierung einer medizinischen Fachperson ist Missbrauch garantiert. Ausserdem würde keine Arbeitgeberin nur wegen einer «simplen» App-Benachrichtigung 14 Tage Urlaub gewähren. Dafür braucht es mindestens eine medizinische oder eine amtliche Bescheinigung.

Dass nur berechtigte Fachpersonen einen Alarm auslösen sollten, schreibt auch das Netzwerk Digitale Selbstbestimmung in seinem Grundsatzpapier.

Ein rein privates Modell ist auch aus epidemiologischer Sicht nicht sinnvoll, weil Gesundheitsämter wie das BAG damit keine Trends errechnen und den klinischen Verlauf der Infektionen nicht dokumentieren können.

Doch wie lässt sich verhindern, dass Ärzte oder Labors bei einem positiven Covid-19-Befund direkten Zugriff auf Smartphones und Mobile-IDs erlangen können und das BAG so Zugriff auf personenbezogene Daten erhält?

Ubique-CEO Mathias Wellig sagt, das sei durchaus lösbar: «Ein Arzt oder Testzentrum müsste zusammen mit dem positiven Test einen anonymen Code aushändigen. Der Nutzer gibt diesen Code zusammen mit der Meldung in der App ein. Nur Meldungen mit validem Code würden vom System akzeptiert.» Dieses Vorgehen entspricht dem üblichen 2-Faktor-Authentifizierungs-Prinzip, das man auch beim Onlinebanking kennt.

3. Silicon Valley oder Europa?

Die dritte Frage ist die nach der Zusammenarbeit. Dabei geht es etwa um Folgendes: Inwiefern werden epidemiologische Forscherinnen in die *Contact-Tracing*-Systeme des Silicon Valley und der Europäer eingebunden?

Eine Forderung dazu hat der deutsche Chaos Computer Club formuliert. Er verlangt unabhängig vom Anbieter einer App, dass Nutzer der Datenweitergabe zustimmen sollen: «Für freiwillige, über den eigentlichen Zweck des *Contact Tracing* hinausgehende Datenerhebungen zum Zweck der epidemiologischen Forschung muss in der Oberfläche der App eine klare, separate Einwilligung explizit eingeholt und jederzeit widerrufen werden können. Diese Einwilligung darf nicht Voraussetzung für die Nutzung sein.»

Diese Möglichkeit ist etwa beim dezentralen PEPP-PT-Protokoll DP3T vorgesehen. Jede App-Nutzerin könnte etwa freiwillig ihre lokal abgespeicherten Einträge für weitere epidemiologische Erhebungen und Statistiken auf den Server hochladen. Google und Apple bieten eine solche Option noch nicht, Wissenschaftler und Behörden müssten also beim Silicon Valley anklopfen, wenn sie Daten für die Forschung benötigen. Das spricht eher für die Lösungen der EPFL und der ETH. Denn die Tech-Giganten werden kaum Sonderwünsche jedes Staats technisch berücksichtigen wollen.

Doch Apple und Google haben aufgrund ihrer Marktmacht einen entscheidenden Vorteil: Ihre Technologie wäre im Betriebssystem für alle Apps integrierbar. Dies wiederum heisst: Jeder und jede mit einem Smartphone ist mit einem einsekündigen Opt-in beim nächsten Software-Update sofort kontaktfähig und braucht keine spezifische App mehr zu installieren.

Eine Analyse des Kryptologen Serge Vaudenay zeigt ein paar Schwächen des DP3T-Protokolls auf. Beispielsweise könnte ein krimineller Hacker eine eigene Variante des (öffentlich verfügbaren) DP3T-Protokolls implementieren. Läuft der Hacker frei herum, werden diese Begegnungen mit der offiziellen *Contact-Tracing*-App (basierend auf DP3T) protokolliert, ebenso der jeweilige Standort des Kontakts und vielleicht auch weitere Daten. Sollte sich eine Kontaktperson einer solchen Begegnung anschliessend als infiziert melden, kann der Hacker die Anonymität unter günstigen Umständen aufheben. Solche Angriffe wären theoretisch auch mit der Lösung von Google und Apple möglich, wären aber einiges aufwendiger.

Müssen sich also nun europäische Regierungen entscheiden zwischen einer europäischen App des PEPP-PT-Konsortiums und dem «All inclusive»-Paket des Silicon Valley?

Nein, nicht unbedingt.

Die Schweizer Forschungsgruppe rund um das DP3T-Verfahren hatte angekündigt, dass sie ihre Implementierung technisch an die Lösung der Tech-Konzerne angleichen werde. Das würde bedeuten: Die Schweiz kann theoretisch das digitale *Contact Tracing* baldmöglichst mit einer DP3T-basierten App starten und später auf den Standard von Google und Apple umschwenken, sobald dieser verfügbar ist.

4. Bluetooth oder nicht?

Die meisten netzpolitischen Gruppierungen befürworten den Einsatz von Bluetooth. Ein paar wenige Organisationen lehnen Bluetooth aber ab.

Etwa die deutsche Datenschutzorganisation Digitalcourage. Sie bezeichnet Bluetooth als «chronisch unsicher» und weist richtigerweise darauf hin,

dass bei Android mit eingeschaltetem Bluetooth die Aktivierung der Ortungsdienste einhergeht. Daraus kann eine Reihe von ernst zu nehmenden Kollateralschäden entstehen. Denn wenn eine App auf Bluetooth zugreifen kann, erhält diese gratis die Standortdaten ihres Nutzers (was diese vielleicht vorher verweigert hatten) dazu, und die App-Firma kann sie zu Marketingzwecken auswerten und verkaufen. Ausserdem hatten bisher rein auf Bluetooth basierende Apps kaum über längere Zeit hinweg funktioniert. Sie saugen den Akku des Smartphones leer und benötigen zu viel Rechenleistung. Deswegen werden sie von Google und Apple immer wieder gestoppt und deren Bluetooth-Verbindungen gekappt.

Hier verfügen die amerikanischen Tech-Konzerne über einen weiteren Machtvorteil gegenüber den europäischen Initiativen. Denn sie sind mit ihren Betriebssystemen Android und IOS «Gastgeber» und können die Spielregeln selbst festlegen.

Nehmen wir zum Beispiel an, die Netzwerk-App Instagram ermittelt dank ständig aktiviertem Bluetooth Informationen darüber, dass sich zwei Nutzer seit Minuten in unmittelbarer Nähe zueinander aufhalten. Instagram könnte ihnen dann während eines kurzen Zeitraums personalisierte Angebote (etwa Coupons für den Glacestand nebenan) ausspielen. Solche kommerziellen Überwachungstaktiken würden viele Nutzerinnen verärgern. Apple und Google können dieses Dilemma einfach lösen, indem sie den Zugriff auf Bluetooth im Gerät separat autorisieren und App-Nutzerinnen die Berechtigungen selber steuern lassen.

Doch auch wenn alle technischen und rechtlichen Finessen gelöst und alle Protokolle miteinander kompatibel sind, bleiben noch viele Fragen.

Die praktischen Fragen

1. Was passiert genau bei einer Meldung?

Entscheidend für die Privatsphäre ist letztlich, was eine Nutzerin (B) unternimmt, wenn bei ihr der App-Alarm losgeht. Spätestens hier wird eine Kontaktaufnahme mit Gesundheitsbehörden unumgänglich. Denn je nachdem kommen unterschiedliche Verhaltensprotokolle zum Einsatz:

- Ist die Nutzerin B eine Risikopatientin? Sofort testen lassen.
- Hat die Nutzerin B die Person A erst vor ein paar Stunden getroffen? Dann ist kein Test angezeigt, sondern eine Isolierung.

Das BAG kann den «Fall» von Nutzerin B nun mit personenbezogenen Massnahmen begleiten. Spätestens dann fällt aber die Anonymität im ganzen System ohnehin weg.

Epidemiologe Marcel Salathé findet das vertretbar: «Mit dem dezentralen *Proximity-Tracing*-Modell kann niemand rekonstruieren, wer wem zu welchem Zeitpunkt begegnet ist», sagt er. «Und allein das zählt.» Eine wachsende Zahl von Epidemiologen ist wie Salathé überzeugt, dass ein sozialverträgliches digitales *Contact Tracing* positive Effekte auf die Entwicklung der Corona-Epidemie haben könnte.

2. Wie gehen wir sozialpsychologisch mit *Contact Tracing* um?

Die Bereitschaft für die App-Installation scheint zwar hoch zu sein. Die Initianten des PEPP-PT-Konsortiums gehen von einer Mitmachrate von 60- Prozent der Bevölkerung aus. Der eidgenössische Datenschutzbeauftragte Adrian Lobsiger sowie die Nationale Ethikkommission gaben grünes Signal für *Contact Tracing,* betonten aber vor allem den *Consent*-Aspekt: Jeder

Schritt müsse freiwillig und ohne Zwang erfolgen, auch nach der Installation.

Doch gerade am Argument der Freiwilligkeit zweifeln einzelne Experten – wie etwa der baden-württembergische Landesdatenschutzbeauftragte Stefan Brink und seine Referentin Clarissa Henning auf «Netzpolitik.org». Denn der Nutzen einer App zeigt sich erst bei Masseninstallationen. Oder aber wenn die *Contact-Tracing*-Systeme der EPFL oder von Google und Co. in bestehende populäre Schweizer Apps integriert werden würden, etwa jene der SBB.

Was passiert, wenn sozialer Druck entsteht, wenn immer mehr Politiker die obligatorische Installation der *Tracing*-App fordern oder wie SPD-Vizekanzler Olaf Scholz von einer 100-prozentigen Installationsquote ausgehen, und wenn Krankenkassen ein Opt-in bei der Google-Apple-Lösung verlangen, bevor sie die Bezahlung eines Covid-19-Tests übernehmen? Solche Szenarien nennt die WOZ den Aufbau eines «Bioüberwachungsstaats».

Ein weiteres Problem wäre der Abnutzungseffekt: Gerade bei exponierten Arbeitnehmenden könnte es zu einer Benachrichtigungsflut kommen: Kassiererinnen und Krankenpfleger, die nahen Kundenkontakt haben, würden bei Bluetooth nonstop «on» sein und müssten in Quarantäne. Wie wären solche Ausfälle wirtschaftlich geregelt, wenn es keine Ersatzeinsatzkräfte gibt?

Es ist nicht unwahrscheinlich, dass die Bluetooth-Benachrichtigungen viel Datenmüll produzieren, also sogenannte *false positives*. Dies wäre zum Beispiel der Fall, wenn zwei Nachbarinnen auf ihren Sofas ein Buch läsen (ihre Smartphones daneben), aber durch eine Wand voneinander getrennt wären. Wird das Smartphone die Qualität einer solchen Nichtbegegnung richtig berechnen können? Führen die digitalen Benachrichtigungen nicht früher oder später zu einem Abstumpfen der Nutzer? So, dass sie sich nach der hundertsten Benachrichtigung irgendwann gar nicht mehr testen lassen?

Wie Menschen mit permanenten Virusbenachrichtigungen psychologisch umgehen, ist nicht erforscht. Kommt es zur Schockstarre? Werden die Benachrichtigten aus Neugier auf eigene Faust ihren vergangenen Begegnungen hinterherforschen? Können Nutzer die Anonymität einer App-Benachrichtigung wirklich akzeptieren?

Wie es jetzt weitergeht

Der epidemiologische Mehrwert von digitalem *Contact Tracing* ist bisher wissenschaftlich kaum erforscht. Somit gibt es weder einen bemessbaren Nutzen noch einen nachgewiesenen Schaden solcher Systeme.

Zwar wurde dieselbe *Proximity*-Technologie in den vergangenen Monaten in Asien angewandt. Doch existiert ein wichtiger Unterschied: Südkorea und Singapur haben mit ihren *Contact-Tracing*-Apps die Smartphone-Nummern von Infizierten und Standortdaten erhoben, ihre Quarantäneorte wurden sogar anonymisiert im Netz publiziert. Unvorstellbar für das datenschutzbewusste Europa, das deshalb die Entwicklung eigener Apps vorangetrieben hat.

Ob die Ankündigung der amerikanischen Tech-Konzerne die bisherigen App-Fahrpläne der europäischen Regierungen nun durcheinanderbringt, ist noch nicht klar. Es wäre für die meisten Staaten auf jeden Fall bequemer, zuzuwarten und eine offizielle *Contact-Tracing*-App rund um den fertigen technischen Baukasten von Apple und Google zu bauen.

Doch bis zu diesem Termin (Mitte Mai) würde kostbare Zeit verloren gehen. Viele Länder möchten baldmöglichst mit dem Ausstieg aus dem Lockdown beginnen.

Die deutsche Bundesregierung plant, ihre App heute (am 16. April) zu präsentieren. Österreich hat seine «Stopp Corona»-Applikation des Roten Kreuzes bereits lanciert, sie wurde 200'000-mal heruntergeladen. Das BAG arbeitet mit der Schweizer DP3T-Autorengruppe zusammen, wie Patrick Mathys an der Pressekonferenz vom 14. April bestätigte, und entwickelt bereits einen Prototypen.

Ob die digitale Epidemiebekämpfung erfolgreich sein wird, hängt letztlich stark von der Akzeptanz der neuen Technologie ab. Sowohl das PEPP-PT-Konsortium wie auch die Tech-Konzerne Apple und Google präsentieren datenschutzkonforme, nutzerfreundliche Modelle, die sogar miteinander kompatibel sind. Beide Varianten haben Vor- und Nachteile.

Unabhängig davon ist jedoch klar: Digitale Kontaktnachverfolgung wird für sich allein nicht den Durchbruch bringen in der Eindämmung des Virus. Entscheidend wird deren Einbettung in den gesamten Massnahmenmix sein und ebenso, wie der Austausch zwischen Infizierten, Gesundheitsbehörden und Ärztinnen ausgestaltet wird. Ob die App wirklich einen epidemiologischen Mehrwert bietet, wird sich erst im Nachhinein schlüssig beantworten lassen.

Vorerst bleibt das digitale *Contact Tracing* ein grosses, sozial-digitales Experiment – mit ungewissem Ausgang.

In einer früheren Version haben wir geschrieben, dass GLP-Nationalrat Martin Bäumle eine obligatorische Installation der *Tracing*-App fordert. Dies stimmt nicht. Für den Fehler entschuldigen wir uns.

Zum Update

Vor wenigen Tagen kam es im PEPP-PT-Konsortium zum Eklat um die Architektur, die der Tracing-App zugrunde liegen soll. In der Folge verliessen zahlreiche EPFL- und ETH-Mitglieder das Konsortium: Die europäische Forschungsgemeinschaft für Contact Tracing droht komplett auseinanderzubrechen.