12. Mai 2020

## Datenverarbeitung als Mittel zur Pandemiebekämpfung

# Fragen und Antworten zur Verwendung von Daten

Die Bekämpfung der Verbreitung des Corona-Virus stellt für die Gesellschaft eine grosse Herausforderung dar. Eine der Schwierigkeiten ist, dass mit dem Virus infizierte Personen andere Leute bereits anstecken können, bevor die infizierte Person überhaupt merkt, dass sie infiziert ist. Der momentan vom Bundesrat verfügte Lock-Down ist nicht zuletzt darauf zurückzuführen, dass jeder ein potentieller Verbreiter des Virus und gleichzeitig ein potentielles Opfer einer Ansteckung ist. Das Ziel der Massnahmen ist daher bislang, dass sich durch Befolgung der Regeln zu Social Distancing die Infektionswege durch mehr Abstand zwischen den Menschen minimiert werden können.

**Wie können Daten eingesetzt werden, um die Pandemie zu bekämpfen?**

Zur Eindämmung der Verbreitung des Virus wäre es von grossem Nutzen, die persönlichen Kontakte eines Erkrankten gezielt zurückverfolgen zu können. So könnten die Kontakte eines (symptomlosen) Erkrankten gewarnt werden und sie könnten ihr Verhalten entsprechend anpassen. Auch lassen sich Visualisierungen darüber erstellen, ob die Regeln des Social Distancing eingehalten werden und theoretisch auch über den ungefähren Aufenthaltsort eines Erkrankten. Auf der ganzen Welt stellen Staaten und Unternehmen Überlegungen an, wie die Daten von Mobilfunkanbietern oder durch Apps auf den Smartphones generierte Daten der Nutzer hierbei genutzt werden können. Dabei gibt es unterschiedliche Ansätze, mit und ohne Personenbezug, abhängig vom Datenschutz, resp. persönlichkeitsrechtlichen Verständnis eines Landes.

Zun unterscheiden ist A) zwischen Daten, welche Nutzer des Mobilfunknetzes generieren und dem Bund zur Verfügung stellen und B) speziellen Apps, welche auf den Endgeräten der Nutzer installiert sind und eine Einschätzung der persönlichen Betroffenheit ermöglichen. Letztlich gibt es unter C) Anwendungsformen, welche in einzelnen asiatischen Ländern bereits genutzt werden, welche weitgehende und massive Eingriffe in das Persönlichkeitsrecht bedeuten und in der Schweiz oder in Europa gar nicht zur Diskussion stehen.

## A) Verwendung bestehender, nutzergenerierter Mobilfunkdaten

— **Zu welchem Zweck hat das Bundesamt für Gesundheit (BAG) unlängst Zugang zu visualisierten Daten der Swisscom erhalten?**

Die Swisscom stellt dem BAG auf dessen Anordnung Analysen zur Mobilität und zu Menschenansammlungen im öffentlichen Raum zur Verfügung. Die den Analysen und Visualisierungen zugrunde liegenden Daten sind anonymisiert und aggregiert. Rückschlüsse auf Einzelpersonen sind nicht möglich. Die Analysen ermöglichen es dem BAG zu überprüfen, ob das Verbot von Ansammlungen Personen auf öffentlichen Plätzen, Spazierwegen und in Parkanlagen, eingehalten wird. Zudem sollen dadurch Hinweise geliefert werden, ob die ergriffenen Massnahmen generell einen Einfluss auf die Mobilität der Menschen haben. So konnte festgestellt werden, ob es einer Anpassung der Massnahmen bedurfte.

— **Wie funktioniert die Mobility Insights Plattform (MIP) von Swisscom?**

Bei der Mobility Insights Plattform handelt es sich um ein bereits etabliertes Produkt von Swisscom. Geschäftskunden können mittels anonymisierter Gruppenstatistiken beispielsweise Erkenntnisse über Verkehrsflüsse zu bestimmten Tageszeiten gewinnen. Die hierfür verwendeten Daten werden direkt nach Entstehung im Mobilfunknetz in Einklang mit dem Datenschutzgesetz anonymisiert und für die Analyse in aggregierter Form aufbereitet. Auf diese Weise lassen sich «Heat Maps» erstellen, welche das Aufkommen von SIM-Karten an einem öffentlichen Ort aufzeigen (Basiseinheit: 100 x 100 m Quadranten, Messung beginnt bei über 20 SIM-Karten). Im Zuge der Verwendung der Mobility Insights Plattform durch das BAG hat Swisscom ein ausführliches FAQ-Dokument veröffentlicht, das die Funktionsweise und die Grundlagen im Detail beschreibt.

— **Wie ist die Verwendung der Standortdaten aus dem Mobilfunknetz durch das BAG datenschutzrechtlich einzuordnen?**

Das BAG erhält keine Standortdaten von Swisscom. Swisscom hat dem BAG ausschliesslich Zugang zu Analysen gewährt, die auf aggregierten, anonymisierten und zeitversetzten Daten beruhen. Diese wurden dem BAG in zum vorgesehenen Zweck aufbereiteter, visualisierter Form vorgelegt. Seitens BAG wurde lediglich einer einzigen Person Einsicht gewährt. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) hat den Vorgang unlängst als datenschutzrechtlich erlaubt eingestuft. Swisscom hat der Öffentlichkeit in der Zwischenzeit in der Form eines FAQ detaillierte Informationen zum Datenverarbeitungsvorgang zur Verfügung gestellt. Zudem ist es für den Inhaber einer SIM-Karte möglich, diese beim Anbieter online oder telefonisch für die Auswertung der Standort- oder Mobilitätsdaten zu sperren (Opt-out).

## B) Datenerhebung mittels spezifischer Apps

— **Können Datensammlungen internationaler Technologiekonzerne zwecks Pandemiebekämpfung eingesetzt werden?**

Die Besucherauslastung eines Ortes ist beispielsweise auf der App von Googlemaps ersichtlich. Auch Apple hat umfassenden Zugriff auf Positionsdaten von Smartphones. Obwohl die Herausgabeanordnung solcher Daten durch den Bund aufgrund der besonderen Lage möglich sein dürfte, schätzen Experten die Aussagekraft von Datenbeständen dieser Art nicht als hinreichend zuverlässig ein. Unter anderem ist unklar, welche Werte als Vergleichsbasis beigezogen werden. Im vorliegenden Kontext der Pandemie-Bekämpfung dürfte ein solches Vorgehen ausserdem nicht die beste zur Verfügung stehende Option sein. Das Ziel eines effizienten «Contact Tracing», der gezielten Identifikation und Information von Verdachtsfällen und deren Kontaktpersonen, ist mit anderen technischen Mitteln besser zu erreichen.

— **Wie können Smartphones zur Pandemiebekämpfung eingesetzt werden?**

Zurzeit sind diverse Anwendungen für Smartphones in Entwicklung. Im asiatischen Raum sind solche Anwendungen bereits im Einsatz. Sog. «Contact-Tracing-Apps» sollen es ermöglichen, Kontakte nachzuverfolgen und Verdachtsfälle zu isolieren. In den unterschiedlichen Ländern geht man dabei von einem unterschiedlichen Datenschutzverständnis aus.

— **Worum handelt es sich beim Software Projekt PEPP-PT?**

PEPP-PT steht für «Pan-European Privacy-Preserving Proximity Tracing", was zugleich der Name der unlängst gegründeten, europäischen Non-Profit-Organisation ist. Hinter dem Projekt steht ein Team von rund 130 Mitarbeitern aus 17 Instituten, Organisationen und Firmen in Europa. Federführend beteiligt war auch die Eidgenössisch-Technische Hochschule EPFL in Lausanne, die sich jedoch unlängst aufgrund einer unterschiedlichen Auffassung zur Zentralität bzw. Dezentralität der Speichermethode zurückgezogen hat. Nun gilt es die Interoperabilität zwischen den unterschiedlichen Ansätzen im In- und Ausland sicherzustellen. Das Projekt wird von renommierten Experten und Forschungseinrichtungen im Ausland getragen, was die Akzeptanz internationaler Behörden erhöhen dürfte, obwohl auch im Ausland vermehrt Stimmen nach einem dezentralen Speicheransatz aufkommen. Die Initiative hat zum Ziel, den gesamten technologischen Unterbau sowie eine Basisversion einer Contact-Tracing App zur Verfügung zu stellen. Darauf basierend können Länder

oder privatwirtschaftliche Unternehmen eigene Apps entwickeln.

— **Wie funktioniert eine PEPP-PT Applikation?**

Eine PEPP-PT Applikation basiert auf der Übertragungstechnologie Bluetooth Low Energy (LE). Hat eine Person die App installiert (dies ist freiwillig) und Bluetooth auf dem Smartphone aktiviert, sendet das Telefon regelmässig ein anonymes Signal und scannt nach identischen Signalen anderer Smartphones. Befinden sich zwei Personen in gegenseitiger Reichweite, werden die Signale ausgetauscht und verschlüsselt auf beiden Smartphones abgespeichert. Ein Algorithmus prüft anschliessend, ob die Dauer und Länge des Kontakts für eine Infektion ausreichen. Erkrankt eine Person am Coronavirus, so kann er dies über seine App freiwillig erfassen und diese leitet die Information über sein Smartphone an alle Kontakte während der Inkubationszeit weiter. Dies erfolgt anonymisiert, d.h. es ist für den Empfänger der Info nicht erkennbar, wer von seinen Kontakten infiziert war. Das System warnt auf dieser Grundlage potenziell gefährdete Personen und rät zur präventiven Selbstquarantäne sowie zum Test.

Die beschrieben Funktionsweise führt faktisch zu einer rückwirkenden Information über Kontakte während der kritischen, noch nicht wahrnehmbaren Inkubationszeit. Dies ist für die effiziente Pandemie-Bekämpfung sehr hilfreich. Weder sind dazu persönliche Nutzerdaten dazu erforderlich, noch eine geografische Nachverfolgung. Smartphones funktionieren dabei ähnlich wie ein Leuchtturm an einer vernebelten Küste: Ein Signal macht den Turm sichtbar. Nähert sich ein Schiff an, wird dieses Signal aufgenommen und erwidert, ohne dass eine genaue Kenntnis des Gegenübers besteht.

— **Wie ist PEPP-PT unter dem Datenschutzaspekt zu beurteilen?**

Europäische und Schweizer Datenschutzexperten sind sich einig, dass kein genereller Konflikt zwischen Datenschutz und der oben beschriebenen Nutzung von Daten zwecks Pandemiebekämpfung besteht. Vorausgesetzt ist dabei aber, dass die datenschutzrechtlichen Grundsätze ordnungsgemäss umgesetzt werden. Der Eidgenössische Datenschutzbeauftragte (EDÖB) begrüsst verschiedene Massnahmen des Projekts: Freiwilligkeit der Teilnahme, Verzicht auf Geolokalisierungsdaten und die Verwendung von temporären Identifikatoren. Diese Massnahmen zeigen gemäss EDÖB auf, dass wichtige Anliegen des Datenschutzes berücksichtigt wurden. Für eine abschliessende, datenschutzrechtliche Würdigung behält der EDÖB sich die definitive Ausgestaltung der Anwendung vor, die sich bezüglich der voraussichtlich bald einsetzbaren Schweizer Lösung herauskristallisiert.

— **Welche technischen Schwierigkeiten können sich bei der Anwendung von Contact-Tracing-Apps ergeben?**

Eine Herausforderung wird es sein, Fehlalarme zu vermeiden. So kann es beispielsweise sein, dass eine Person sich selbst versehentlich (oder absichtlich) als Infizierter deklariert, was zur Verunsicherung der weiteren App-Anwender führen kann. Eine mögliche Lösung ist, dass Meldungen verifiziert werden müssen, also beispielsweise nur im Auftrag eines Arztes erfolgen können. Dies ist aber letztlich kein technisches Problem, sondern eine Frage des Prozesses und der Bereitschaft der Anwender, die App bestimmungsgemäss zu verwenden. Zusätzlich wird eine kritische Anzahl von Anwendern notwendig sein, damit das System effizient funktionieren kann.

— **Welche Contact-Tracing-Applikationen werden in der Schweiz zurzeit entwickelt?**

In der Schweiz sind mehrere Lösungen in Entwicklung, welche den PEPP-PT-Ansatz verfolgen und damit die Privatsphäre der Bürger hinreichend zu schützen vermögen. Contact-Tracing-Apps können Begegnungen automatisch protokollieren, ohne sie zusammen mit heiklen Personendaten zentral zu speichern. Nennenswert ist «NextStep» von Ubique (zugleich Entwickler der SBB-App): Für Android Smartphones ist bereits eine Testversion verfügbar, für IPhones noch nicht. Ubique beteiligt sich zugleich am Projekt PEPP-PT. Die Funktionsweise der App wird von den Entwicklern in diesem Video anschaulich beschrieben. Unlängst hat unter der Schirmherrschaft des Eidgenössischen Departements des Innern sowie des Wirtschaftsdepartements ein Programmierwettbewerb, ein sog. Hackathon stattgefunden wobei mehrere datenschutzkonforme Lösungen gefunden wurden (Link), die nun in konkrete, marktfähige Produkte münden sollen. Generelle Beispiele für App-Entwicklungen sind «Virus Tracker», «We Trace», «geoHealthApp» oder weitere.

— **Wie soll die Schweizer Lösung technisch funktionieren?**

Die sich abzeichnende Ausgestaltung für eine Schweizer Tracing-Applikation basiert im Wesentlichen auf den Grundsätzen, die auch das Projekt PEPP-PT ursprünglich festgelegt hatte:

- Smartphones senden per Bluetooth zufällig generierte, temporäre Signale aus. Kommt es zu einem Kontakt, der während mindestens 15 Minuten und näher als zwei Meter stattfindet, werden diese Signale ausgetauscht und anonym auf beiden Smartphones abgespeichert.
- Sollte eine Person positiv auf COVID-19 getestet werden, kann sie oder er einen Benachrichtigungsdienst aktivieren. Sämtliche «Begegnungen», die seit dem Auftreten der ersten Symptome stattgefunden haben, werden dann benachrichtigt und aufgefordert, sich zum Test und in Selbstquarantäne zu begeben. Die Identitäten der infizierten Personen sind weiterhin nur den behandelnden Ärzten und den bereits heute bestehenden kantonalen Contact-Tracing-Stellen bekannt.
- Es werden keine Geodaten erfasst, eine Lokalisation oder geografische Rückverfolgung ist also technisch ausgeschlossen.
- Die Teilnahme ist freiwillig.

— **Wie weit ist der Bund mit der Ausarbeitung von Contact-Tracing-Apps?**

Das BAG hat sich dahingehend geäussert, dass am 11. Mai 2020 eine Contact-Tracing-App in der Schweiz einsatzbereit sein soll. Dafür arbeitet der Bund mit der ETH Lausanne und der ETH Zürich zusammen. An der Erarbeitung beteiligt sind noch weitere wissenschaftliche Institutionen auf internationalem Niveau sowie auch Schweizer Softwareentwickler (z.B. Ubique und PocketCampus).

— **Wie ist die Lösung des Bundes technisch aufgebaut?**

Die App basiert auf dem Konzept «DP-3T». Die Informationen hierzu (z.B. Architektur) sind offen im Netz einsehbar. Die technische Funktionsweise basiert auf anonymen Bluetooth-Kontakten zwischen Smartphones und verwendet keine Geolokalisation (kein GPS, keine Triangulation). Die genaue Funktionsweise ist hier in einem kurzen Cartoon veranschaulicht.

— **Wie ist die Lösung des Bundes datenschutzrechtlich einzuordnen?**

Es ist vorgesehen, dass die Nutzung der App auf Freiwilligkeit basiert. Das heisst, dass die Nutzung der App nie Bedingung sein wird, um ein Restaurant oder ein Fitnessstudio zu besuchen. Gemäss der Schweizer Lösung sollen die anonymisierten Daten über ein dezentralisiertes System laufen. Dies im Unterschied zu anderen Ländern wie Deutschland, Frankreich, Grossbritannien und Italien, wo man die Daten einem zentralen Server anvertrauen will. Der EDÖB, das Nationale Zentrum für Cybersicherheit und die Nationale Ethikkommission (NEK) sehen in der Schweizer Lösung den besten Schutz für die Privatsphäre. Auch Google und Apple befürworten in ihren Entwicklungen den dezentralen Ansatz. Der EDÖB prüft zudem zurzeit die sich aktuell herauskristallisierende Schweizer Lösung «Proximity Tracing-Application (PTAPP). Er kommt zum Schluss, dass die dort stattfindenden Datenbearbeitungen verhältnismässig sind. Er prüft zurzeit noch den Entwurf einer bundesrätlichen Verordnung über die PTAPP und die ihr zugrundeliegenden gesetzlichen Grundlagen.

— **Mit welchen Schwierigkeiten könnte die Schweizer Lösung behaftet sein?**

Offen ist zurzeit die Frage, ob die Schweizer Lösung international kompatibel sein wird, was einen wichtigen Bestandteil darstellt. Die Schweizer sowie die internationalen Entwickler arbeiten an diesem Aspekt. Die dezentrale Lösung hat den Vorteil, dass sie an weniger hohe technische Hürden gebunden ist und deshalb schneller zum Einsatz kommen kann. Es bleibt zudem die Frage offen, wie die Schweizer Bevölkerung auf die Freiwilligkeit reagiert. Damit die App funktioniert müssten gemäss Forschern 60 % der Bevölkerung, in der Schweiz somit ca. 5 Mio. Einwohner, partizipieren.

— **Was fordern die Kommissionsmotionen 20.3168 (SPK-SR) und 20.3144 (SPK-NR) mit «Gesetzliche Grundlagen zur Einführung der Corona-Warn-App (Corona-Proximity-Tracing-App)»?**

Die SPK-SR hat am 30. April 2020, die SPK-NR am 22. April 2020, die genannten Motionen eingereicht (20.3168 und 20.3144). Beide Motionen fordern vom Bundesrat, die notwendige gesetzliche Grundlage zur Einführung von Corona-Warn-Apps dem Parlament vorzulegen. Es sollen technische Lösungen verwendet werden, welche keine personenbezogenen Daten zentral speichern und die Anwendung der App soll freiwillig sein. Der Bundesrat hat beide Motionen am 01. Mai 2020 beantwortet: Solche Applikationen sind als Hilfsmittel zur Eindämmung der Virusausbreitung geeignet. Ein Kernpunkt der Entwicklung ist dabei die Freiwilligkeit und die Dezentralität und Anonymität, die im Schweizer Projekt bereits berücksichtigt sind. Zudem bestehen die erforderlichen gesetzlichen Grundlagen nach Epidemiegesetz bereits und eine Notverordnung ist nicht notwendig. Da die Anliegen der Motionen erfüllt werden, beantragt der Bundesrat die Ablehnung. Das Parlament hat den Motionen jedoch zugestimmt. economiesuisse hofft, dass dies die zeitnahe Einführung der Applikation nicht verhindert.

## C) Weitere - in der Schweiz aber undenkbare - Methoden zur Datenerhebung

— **Wie verwenden gewisse ostasiatische Staaten die neuen Technologien zwecks Pandemiebekämpfung?**

Einzelne ostasiatische Staaten setzen Applikationen zwecks Unterbrechung der Infektionsketten bereits ein. Dabei gehen sie bislang von einem anderen datenschutzrechtlichen Verständnis als europäische Staaten aus. So ist die Verwendung der Applikationen teilweise Pflicht. Aus China ist bekannt, dass aus diesen Systemen nicht nur der Gesundheitszustand, sondern Informationen bis hin zur Nummer des Personalausweises ersichtlich sind. Bevölkerungsgruppen werden mit einem Ampelsystem (Grün - Gelb - Rot) erfasst und entsprechend zur Wiedereingliederung in den Arbeitsprozess gesteuert. Auch besteht über Geolokalisation und entsprechende Online-Plattformen vollständige Transparenz von geografischen «Infektionsherden». Anders, als dies im europäischen Kontext bisher diskutiert wurde, dienen solche Systeme nicht nur der Nachverfolgung von Infektionsketten und der Warnung der Individuen vor einer potentiellen Ansteckung, sondern auch dem Aufbau einer sozialen Kontrolle und dem Erzeugen einer Verhaltensänderung. Was unter dem Zweck der Pandemiebekämpfung dienlich sein kann, ist unter europäischem und schweizerischem Datenschutzverständnis ausgeschlossen. Solch weitgehende Eingriffe in die Persönlichkeitsrechte zu Gunsten einer staatlichen Kontrolle stellen auch ganz grundsätzlich die Vereinbarkeit mit dem liberalen Staatsverständnis in Frage.

— **Wie sind diese Applikationen technologisch ausgestaltet?**

Der wesentliche Unterschied im Vergleich zu den in Europa diskutierten Ansätzen ist, dass sich der Staat sehr weitgehende Zugriffsrechte auf bestehende Systeme und Daten zugesteht. Das bedeutet beispielsweise, dass ohne spezielles Einverständnis Daten aus verschiedenen Alltags-Anwendungen aggregiert werden. In diesem Sinne kann auch nicht von einem Contact Tracing-App gesprochen werden, sondern von einem weit verzweigten System der totalen Überwachung.

In China erfolgt das «Contact Tracing» vornehmlich über ein System, das in die dort sehr beliebten und verbreiteten Apps WeChat und AliPay integriert ist: Über ein Formular geben die Nutzenden ihre Kontaktdaten an und ob sie Symptome wie Fieber oder Husten aufweisen. Die Informationen werden ausgewertet und die betroffene Person erhält einen «health code» (grün, gelb oder rot), der angibt, ob man gesund ist, mit infizierten Personen in Kontakt stand oder selbst infiziert ist. Der «health code» fungiert anschliessend als eine Art Pass im öffentlichen Raum. Nur «grüne» Personen dürfen sich weitgehend frei bewegen. Ergänzend kommt in China die ohnehin sehr starke Überwachung des öffentlichen Raums auch bei der Pandemie-Bekämpfung zum Tragen.

Diese Massnahmen sind sehr invasiv und lassen sich nicht auf eine Demokratie übertagen. Aber selbst in demokratischen Staaten wie Südkorea werden Daten von Sicherheitskameras, Kreditkarten, Mobiltelefonen oder Navigationssystemen in Autos fürs Contact Tracing verwendet.

— **Wie sind die ostasiatischen Abläufe aus datenschutzrechtlicher Sicht zu beurteilen?**

Unter dem europäischen und Schweizer Rechtsverständnis sind obligatorische und verpflichtende Applikation, bei denen zudem höchst sensitive und umfassende Daten erfasst werden, problematisch. Sie können zu Fehlanreizen führen (Leute lassen ihr Handy bewusst zu Hause und eröffnen Sicherheitsrisiken - so wird bereits von Schwarzmärkten berichtet, welche genaue Bewegungsabläufe von Menschen (auch in Echtzeit) offenlegen und damit weitgehende Eingriffe in die Privatsphäre ermöglichen. Die Bedenken gegenüber den sehr invasiven Ansätzen, die in China oder Südkorea verfolgt werden, sind aber nicht nur datenschutzrechtlicher sondern auch staatsrechtlicher Natur. In der Schweiz stehen solche Instrumente nicht zur Diskussion.

— **Welche weniger invasiven Methoden werden in Asien verfolgt?**

In weiteren asiatischen Staaten werden andersartige Massnahmen implementiert, die auf Transparenz setzen. Mittels Smartphone-Applikation sind Infizierte mit den Behörden direkt in Verbindung. Zugleich ist mittels GPS über Mobiltelefone die Ortung dieser Infizierten möglich. Die Behörden setzen generell auf umfassende Information der Bürger über verschiedene Kanäle. Dabei werden auch detaillierte Informationen über die Infizierten veröffentlicht, inklusive Orte, an denen sie sich in den vergangenen Tagen aufgehalten haben. Zugleich informieren die Applikationen bei einer Annäherung an einen Infizierten oder seinen vergangenen Aufenthaltsort. Obwohl es sich um weniger invasive Methoden als in Ostasien handelt, geben auch diese Art von Applikationen einen grossen Teil von persönlichen Daten preis.