Tracing-Apps als Hilfe für die Gesundheitsbehörden

Proximity Tracing-Apps zur Erkennung von COVID-19 infizierten Personen

Olivier Heuberger, Dr. iur., Rechtsanwalt

Résumé: Les applis de traçage ont été élaborées pour améliorer la lutte contre la propagation du coronavirus en avertissant rapidement les personnes qui pourraient avoir été en contact avec lui. Elles soutiennent ainsi les efforts des autorités de santé publique des cantons. Pour cela, il faut que les données nécessaires soient échangées entre les usagers, les autorités locales et différentes entreprises, dans le respect de la protection des données. L'analyse qui suit explique le fonctionnement général des applis de *proximity tracing* et esquisse leurs particularités en matière de protection des données.

Zusammenfassung: Bei der Bekämpfung und Bewältigung des Coronavirus sollen Personen, die potenziell dem Virus ausgesetzt waren, rasch benachrichtigt werden können. Proximity Tracing-Apps helfen den lokalen Gesundheitsbehörden bei dieser Aufgabe. Dazu müssen notwendige Daten zwischen den Usern, den lokalen Behörden sowie verschiedensten Unternehmen unter Wahrung des Datenschutzes ausgetauscht werden können. Der vorliegende Aufsatz erklärt, wie Proximity Tracing-Apps in allgemeiner Weise technisch funktionieren und skizziert, welche datenschutzrechtlichen Besonderheiten sich daraus ergeben

INHALTSVERZEICHNIS

I. Die Ermittlung von potenziell COVID-19 erkrankten Personen

1. „Catch Me If You Can“

1

Weltweit versuchen Gesundheitsbehörden die COVID-19-Pandemie durch die Unterbrechung der Infektionskette zu bekämpfen und zu bewältigen. Dazu sollen potenziell infizierte Personen rasch identifiziert und informiert werden. Unterstützt werden diese Bestrebungen durch auf den Smartphones von Usern installierte Proximity Tracing Apps (PT-Apps). Diese messen die zeitliche und physische Nähe von Personen zu anderen potenziell oder bereits bestätigten COVID-19 positiven Personen.[1] Eine potenzielle Ansteckung durch COVID-19 liegt nach der aktuellen Einschätzung dem Bundesamt für Gesundheit (BAG) vor, falls der Abstand zwischen den betreffenden Personen während einer Dauer von 15 Minuten weniger als zwei Meter betrug.[2]

2

Die Einsatzmöglichkeiten von PT-Apps gehen erheblich über die technologischen Möglichkeiten des im Titel genannten Filmes aus dem Jahre 2002 hinaus, wenn es auch einige Gemeinsamkeiten gibt.[3] So repräsentiert Carl Hanratty (Tom Hanks) den Staat als *Verantwortlichen* der Verfolgung auf den sich nicht fangen lassen *wollenden* Frank Abagnale (Leonardo di Caprio) mit dem *Zweck*, die *weitere Verbreitung* von gefälschten Checks zu verhindern. Hingegen waren die *Technologien*, die den Behörden zur Verfügung standen, in den 60er Jahren durchgehend analoger Natur. Bluetooth, Smartphones, Orts- und Bewegungs-

Tracing in Echtzeit oder die dezentrale Datenbearbeitung waren der Science-Fiction-Literatur vorbehalten.

3

Behörden weltweit setzen PT-Apps sehr unterschiedlich um und auch deren Zweck ist teilweise verschieden.[4] Die Rechtsgrundlage für eine solche Datenbearbeitung beruht teilweise auf einer Einwilligung, einem überwiegenden Interesse oder einer gesetzlichen Grundlage. In der Schweiz ist die Installation der PT-App freiwillig und wird zudem auf einer gesetzlichen Grundlage basieren.[5]

2. Der Zweck der Datenbearbeitung bei PT-Apps

4

Der Zweck von PT-Apps besteht darin, die Kontakte einer COVID-19 positiven Person rasch darüber zu informieren, dass sie durch eine mögliche unmittelbare physische Nähe (eng.: proximity) zu einer an COVID-19 erkrankten Person exponiert wurde.[6]

A. PT-App als Tracking- und Monitoringinstrument im Allgemeinen

5

Wie der Name Proximity Tracing nahelegt, können PT-Apps dazu verwendet werden, die Mobilität und andere Verhaltensweisen von Person zu verfolgen und zu monitoren. Vorstellbar ist die Verwendung von PT-Apps zur Kontrolle durch die Behörden, ob sich die lokale Bevölkerung an die verordneten Massnahmen hält (z.B. Abstandsregeln oder Ausgangssperren). Eine PT-App kann auch dazu eingesetzt werden, um potenziell an COVID-19 erkrankte Personen proaktiv zu verfolgen und zu benachrichtigen und direkt in der App individuell-abstrakt Anordnungen zu verfügen. Diese könnten etwa darin bestehen, umgehend eine Gesundheitseinrichtung aufzusuchen, ein bestimmtes Areal nicht mehr zu verlassen bzw. sich nur noch in einem bestimmten Bereich aufzuhalten.

B. Schweizer PT-App als Warninstrument einer möglichen COVID-19 Erkrankung

6

Die skizzierten Massnahmen wären bei der aktuellen Situation der COVID-19 Pandemie in der Schweiz jedoch aus datenschutzrechtlicher Sicht kaum verhältnismässig und entsprechend nicht zulässig. Die Unterstützung der

Verhinderung oder Verlangsamung der COVID-19 Pandemie durch PT-Apps steht jedoch nicht im Widerspruch zum Datenschutzrecht. Es ist keineswegs zwischen der Nutzung von PT-Apps oder dem Schutz der Persönlichkeit vor missbräuchlicher Datenbearbeitung nach Art. 13 Abs. 2 BV i.V.m. Art. 1 Abs. 1 DSG zu wählen. Vielmehr kann eine entsprechende Datenbearbeitung in Einklang mit den datenschutzrechtlichen Prinzipien gebracht werden. Eine solche Zielsetzung verfolgt das BAG mit der eingeführten PT-App für die Schweiz.[7]

7

Eine PT-App wie sie in der Schweiz umgesetzt ist, unterstützt die Ermittlung einer relevanten physischen Nähe einer Person zu einer COVID-19-positiven Person, ohne der empfangenden Person deren Identität, Ort oder Zeit des Kontakts preiszugeben.[8] Erst sobald die PT-App die User informiert, dass ein Kontakt mit einer COVID-19-positiven Person stattgefunden hat, können die User eine Gesundheitsstelle kontaktieren, Instruktionen einholen (z.B. einen COVID-19-Test zu machen) und die PT-Daten in anonymisierter Form zu Forschungszwecken zur Verfügung stellen.[9] PT-Apps unterstützen damit die frühzeitige Erkennung von potenziell an COVID19 infizierten Personen.

8

Die Idee zur Ermittlung von potenziell an COVID-19 erkrankten Personen ist die möglichst rasche Befragung von Personen und aller ihrer kürzlichen möglichen Kontakte während der Ansteckungszeit. Als Warnmeldung sensibilisiert die PT-App die User, damit diese sich bei typischen Symptomen testen lassen und den Kontakt zu anderen Personen möglichst vermeiden, da man selbst schon ansteckend sein könnte.[10]

9

Im bekannten sozialen Umfeld – beispielsweise in der Familie – ist ohne Weiteres nachzuvollziehen, ob eine Person an COVID-19 erkrankte. PT-Apps helfen Personen zu benachrichtigen, die sich nicht kennen. Verstärkt werden die Herausforderungen der COVID-19-Pandemie, dass Personen auch dann ansteckend sind, wenn sie selbst noch keine Krankheitssymptome aufweisen.[11] Dies basiert auf dem derzeitigen wissenschaftlichen Verständnis der Epidemiologen, dass darauf hinweist, dass präsymptomatische Träger von COVID-19 zwischen ein bis drei Tagen vor dem Auftreten von Symptomen ansteckend sein können und COVID-19 eine Latenzzeit von zwei bis drei Tagen aufweist.[12]

II. Die Installation der PT-App

10

In einem ersten Schritt speichern User die PT-App von Apple‘s App Store oder von Google‘s Play Store auf dem Smartphone. Um Kontaktdaten zwischen den beiden mobilen Betriebssystem iOS-iOS, Android-Android und iOS-Android-Geräten zu erkennen und auszutauschen, entwickelten Google und Apple gemeinsam eine Anwendungsschnittstelle, eine Application Programming Interface (API), unter Verwendung desselben Algorithmus.[13]

11

Die Installation erfordert die Aktivierung von Bluetooth und die Zustimmung zum Empfang von push-Benachrichtigungen. Auf dem Betriebssystem von Android erfolgt dies durch Firebase Cloud Messaging und bei iOS durch den Apple Push Notification Service.[14] Damit die PT-App über Neuansteckungen von Personen erfährt, muss die App (das ist der ‚Frontend‘) diese Daten regelmässig von einem zentralen Datenbank-Server (dem ‚Backend‘) herunterladen. Der Backend übernimmt die Funktion der Koordination zwischen den Usern. Die Berechnung der Wahrscheinlichkeit einer unmittelbaren physischen Nähe zu einer bestätigten COVID-19 erkrankten Person (dem Risk Score) erfolgt einzig auf dem eigenen Smartphone der User.[15] Die PT-App läuft damit stets ‚im Hintergrund‘ eines Smartphones und fragt den Backend regelmässig nach Updates.

III. Die Generierung und Übertragung von EphIDs via Bluetooth Low Energy Beacon

1. Erzeugen einer pseudozufälligen Identifikationsnummer

12

Mit der Installation der PT-App generiert das App einen zufälligen, einmaligen digitalen Schlüssel, einen Secret Key (SK), der auf dem Smartphone der User gespeichert wird. Der SK ist eine zufällige Zeichenkette aus einer bestimmten Anzahl Bytes, beispielsweise ‚44c6dfb4cbdbea397122d47f9e0bfe397-aafcad3a38db91a13d617ec4a3cfa19‘.[16] Der SK wird regelmäßig neu generiert, beispielsweise jeden Tag, jede Woche, alle 14 Tage, usw. Die Funktion des SK besteht darin, für den definierten Zeitraum (täglich, wöchentlich, alle 14 Tage) eine Liste von temporären und zufälligen Identifikationsnummern (‚EphID‘ für

ephemeral, pseudo-random ID) zu erstellen. [17] Der auf dem Smartphone generierte SK wird für eine maximale Dauer von 21 Tagen gespeichert.[18] Die zugleich generierte EphID leitet sich von dem bei der Installation der PT-App generierten und für einen bestimmten Zeitraum gültigen, SK ab.[19] Damit ist die EphID stets einer bestimmten Person indirekt zuordenbar. Ob eine Person aus datenschutzrechtlicher Sicht auch bestimmbar ist, hängt davon ab, ob sie von anderen Personen eindeutig identifiziert, d.h. unterscheidbar ist. Darauf wird noch zurückzukommen sein.[20]

2. Übertragen und Empfangen der EphID via Bluetooth

13

Via Bluetooth Low Energy (BLE) sendet das Smartphone die EphID (basierend auf dem SK) kontinuierlich nach aussen. Die User anderer PT-Apps erkennen das Signal und speichern es auf dem eigenen Smartphone. Um das Tracken des Standorts des Absenders der EphID zu erschweren und kein über die Zeit ersichtliches Bewegungsprofil zu ermöglichen, wird die EphID regelmässig (beispielsweise jede Minute) geändert. Das Smartphone des Absenders sendet somit jede Minute eine neue EphID, basierend auf dem für diesen Zeitpunkt gültigen geheimen Schlüssel (den SK), via BLE an die anderen User der PT-App. Die Information der EphID wird in 16-byte Abschnitten (‚chunk') aufgeteilt. Jeder Eintrag einer EphID benötigt ungefähr 32 Bytes. Eher konservativ geschätzte Berechnungen gehen davon aus, dass während eines Tages die EphID von rund 100 anderen Usern gespeichert wird. Bei einem Zeitraum von 14 Tagen ergibt das rund 140'000 Einträge auf dem eigenen Smartphone. Entsprechend ergibt das eine Datenmenge von rund 6.1 Megabyte.[21] Das sind keine grossen Datenmengen, die bearbeitet werden, zudem noch in strukturiertem Format.[22] Folglich genügt ein relationales Datenbanksystem, d.h. die Sammlung von zentral strukturierten und dauerhaft in tabellarischer Form gespeicherten Daten, für diese Art der Datenbearbeitung mit einem SQL-Datenbankmanagementsystem. Es besteht keine offensichtliche Notwendigkeit, die Datenbearbeitung auf verteilten, nicht-relationalen Datenbanken zu bearbeiten.[23]

3. Lokale Speicherung von erhaltenen EphIDs

14

Die empfangenden User speichern fortlaufend die gesendeten EphIDs lokal auf dem eigenen Smartphone. Diese werden durch die auf dem eigenen Smartphone generierte Entfernungsangabe zum Absender sowie einen Zeitstempel ergänzt.[24] Der Zeitstempel hält das Datum, die genaue (z.B. 13:58 UTC) oder ungefähre

Zeitangabe (z.B. morgens / nachmittags / nachts) und die Dauer des Kontakts mit einem anderen PT-App User fest.[25]

IV. Die zentrale und dezentrale Speicherung von Proximity Tracing Daten

15

Sobald ein User von einer medizinischen Fachkraft positiv auf COVID-19 diagnostiziert wurde, kann diese selbst ihre EphID auf einen Server hochladen. Damit nur jene User ihre Daten auf den Backend hochladen können, die tatsächlich an COVID-19 erkrankt sind, verteilt ein Autorisierungsserver entsprechende Zugangscodes. Diese Zugangscodes können nur vom ärztlichen Personal oder einer Behörde an die Nutzer der PT-App weitergeleitet werden.[26]

1. Die Verantwortlichen des Backend und des Autorisierungsservers

16

Wer den Backend und die PT-App kontrolliert, bestimmt Zweck und Mittel der Datenbearbeitung. Sie sind die Verantwortlichen der Datenbearbeitung nach Art. 3 lit. i DSG. Die Durchführung des Autorisierungsprozesses (z.B. mittels eines QR-Codes oder anderweitig) und der Backend, sind länderspezifisch. Die Verantwortlichkeit der Datenbearbeitung für die PT-App und den Backen liegt in der Schweiz beim Bundesamt für Gesundheit. Die Verantwortung für den Autorisierungsprozess obliegt ebenfalls dem BAG. Sie sind verantwortlich, dem ärztlichen Personal Zugang zu den Autorisierungscodes zu geben, welche diese bei einem positiven COVID-19 Befund an die User weiterleiten können (z.B. durch Scan eines QR Codes). Verifiziert der Backend den Autorisierungscode, übermitteln die User die generierten EphIDs für den Zeitraum des ansteckenden Zeitraums an den Backend. Das Hosting und die Wartung des Backends sowie des Autorisierungsservers wird an das Bundesamt für Informatik delegiert.[27] Es bearbeitet in dieser Funktion Daten als Auftragsdatenbearbeiter.[28]

17

Falls die Behörden Sub-Auftragsdatenbearbeiter beiziehen, sind diese verpflichtet, die Daten entsprechend den schweizerischen Datenschutzbestimmungen zu bearbeiten.

2. Zentrales Privacy-Preserving Proximity Tracing

18

Beim Modell der zentralen Bearbeitung von PT-Daten, welches in der Schweiz nicht angewendet wird, ermittelt und benachrichtigt ein zentraler Server potenziell gefährdete Personen. Damit der Zentralserver die Nutzer benachrichtigen kann, muss ein solches System über einen permanente Identifikationsnummer (eine permanente EphID) verfügen.

19

Die Nutzer übermitteln die EphIDs an die anderen User und empfangen umgekehrt deren EphIDs. Die erhaltenen EphIDs werden zusammen mit der Angabe des physischen Abstandes, dem Datum und der Zeit sowie dem Zeitraum des Kontakts auf den Smartphones der User gespeichert. Im Falle einer bestätigten Infektion mit COVID-19 autorisiert eine lokale Gesundheitsbehörde die Übermittlung der EphID sowie den Zeitstempel an den Backend. Der Backend ermittelt die EphID einer potenziell erkrankten Person von den erhaltenen EphIDs, ermittelt die Identität der potenziell erkrankten Person, berechnet den Risikowert der Erkrankung und benachrichtigt die lokalen Gesundheitsbehörden. Damit die lokale Gesundheitsbehörde die betroffene Person kontaktieren kann, erhält sie auch Kenntnis von deren Identität.[29]

20

Auf dem Backend werden die personenbezogenen Daten pseudonymisiert und anderen User der PT-App übermittelt. Ein solcher Server unterliegt der Kontrolle einer Behörde, etwa einer lokalen Gesundheitsbehörde oder einer anderen vertrauenswürdigen Organisation (z.B. dem Roten Kreuz). Die auf einem solchen Server vorhandenen Daten können ohne Weiteres einer bestimmten Person zugeordnet werden. Die Identifikation einer Person geschieht damit auf dem Server selbst. Diejenigen Personen die Zugriff auf diesen Server haben, können entsprechend eine Person identifizieren.

21

Das zentralisierte Servermodel basiert auf der Annahme, dass der Verantwortliche der Datenbearbeitung die Datensicherheit garantiert und die Daten nicht zweckentfremdet.[30] Daten sollen beispielsweise nicht über die Zwecke der Bewältigung der COVID-19-Pandemie hinaus bearbeitet werden, beispielsweise für Strafverfolgungs-, Grenzkontroll- oder Geheimdienstzwecke.

3. Dezentrales Privacy-Preserving Proximity Tracing

22

Beim dezentralen Modell wie es in der Schweiz angewendet wird, ist der Datenfluss so aufgebaut, dass möglichst sämtliche für den Zweck der PT-App erforderlichen personenbezogenen Datenbearbeitungen auf den Smartphones der Nutzer selbst verbleiben und nicht auf dem Backend bearbeitet werden. [31] Ein solches dezentrales System verfügt zwar ebenfalls über ein Datenbanksystem auf einem zentralen Server. Der Zweck des Backends besteht jedoch einzig darin, die EphIDs, den SK und den Autorisierungscode (sog. Benachrichtigungsidentifier) zwischen den Usern der PT-App zu verteilen, damit diese via der PT-App von COVID-19 positiven Personen benachrichtigt werden können.[32] Der Backend speichert keine weitere Daten, weder personenbezogene (z.B. Gesundheitsdaten) noch nicht-personenbezogene (z.B. die Abstandsmessung oder den Risk Score).[33]

23

Die auf einem solchen Server gespeicherten Daten sollen es nicht erlauben, die User der EphID zu bestimmen oder bestimmbar zu machen. [34] Der Backend muss entsprechend so programmiert sein, dass es nicht möglich ist, die EphIDs zu ändern, also konsistent zu halten.[35]

V. Die Identifikation einer potenziell erkrankten COVID-19 Person

24

Eine PT-App verwendet nur jene Datenattribute, die notwendig sind, um eine Person zu ermitteln, mit denen ein User in relevanter Nähe war. Die Identifikation eines Users ist dazu nicht erforderlich, es müssen also auf dem Backend keine personenbezogenen Daten bearbeitet werden. Allein die Tatsache, dass ein User die EphID auf den Backend hochlädt, lässt aber den offensichtlichen Rückschluss zu, dass dieser User potenziell an COVID-19 erkrankt ist. Denn nur Personen, die vom ärztlichen Personal den Autorisierungscode erhalten haben, können ihre Daten auf den Backend hochladen.[36] Dass eine Person aufgrund dieser vermeintlich nicht-personenbezogenen Daten auf dem Backend nicht re-identifiziert werden kann, ist nicht gänzlich auszuschliessen.[37] Entscheidend ist, wie wahrscheinlich eine solche Re-Identifikation ist.

25

Allgemein und ausserhalb möglicher Anwendungsbereiche von PT-Apps im Zusammenhang der aktuellen COVID-19 Pandemie, besteht der Zweck von Proximity Tracing darin, die Standorte zwischen zwei Personen festzustellen, nach bestimmten Parametern zu messen und eine Folgerung zu definieren. Personen in kleineren Gemeinschaften – etwa in einer Familie, dem Arbeitsort, einer Jassgruppe – können durch die PT-App eine Benachrichtigung erhalten, in welcher ihnen mitgeteilt wird – sei es nun richtig oder falsch –, dass jemand anderer aus der Gruppe an COVID-19 erkrankt ist. Diese Information erhalten sie nicht durch die PT-App, sondern erschliesst sich ihnen durch Kontext-Informationen. Das datenschutzrechtliche Risiko, das sich hier verwirklichen kann, besteht darin, dass Angaben über die eigene Gesundheit Personen offengelegt werden, ohne dass diese Person das will.

26

Die Offenlegung von Gesundheitsdaten gegenüber nicht autorisierten Personen kann in einem manuellen Prozess erfolgen, beispielsweise durch Mitarbeitende einer lokalen Gesundheitsbehörde. Sie kann auch automatisiert durch die PT-App erfolgen. Das Risiko einer Offenlegung einer einzelnen Person könnte dadurch ausgeschlossen werden, falls diese Person keine sozialen Kontakte mit anderen Personen hätte. Eine solche Einschränkung wäre in unserem heutigen Rechtssystem nicht durchsetzbar und auf freiwilliger Basis (ohne jegliche staatliche Massnahmen) von eher theoretischer Natur. Die Familienmitglieder, der Arbeitgeber und die Mitspieler der Jassgruppe würden offensichtlich nachfragen wollen, weshalb eine Person über einen längeren Zeitraum nicht mehr persönlich erscheinen mag. In der Konsequenz bedeutet dies, dass soziale Kontakte zwischen Menschen immer das Risiko bergen, den eigenen Gesundheitsstatus offen zu legen.[38]

1. Personendaten im Verwendungszusammenhang mit PT-Apps

27

Die schweizerische PT-App ist so konzipiert, dass sämtliche an den Backend übermittelte Daten eine Person weder bestimmen noch bestimmbar machen. Eine Identifikation oder Re-Identifikation soll damit nicht möglich sein.[39] Nach der Definition des DSG sind Personendaten sämtliche Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 3 lit. a DSG). Entscheidend für die Qualifikation von Personendaten ist, ob diese Bestimmbarkeit vorliegt, also ein Bezug zwischen einer Information und einer Person besteht. Fehlt es an einem

solchen Personenbezug, liegen Sachdaten vor, die nicht in den Anwendungsbereich des DSG fallen.[40]

2. Die Re-Identifikation von Usern bei PT-Apps

28

Der Backend soll nach der technischen Konzeption keine personenbezogenen Daten speichern. Falls der Backend keine personenbezogenen Daten bearbeitet, ist das DSG nicht anwendbar, wohl aber noch das FMG.[41] Das DSG geht von der Vermutung aus, dass die Persönlichkeit einer Person geschützt ist, wenn keine personenbezogenen Daten bearbeitet werden. Die Re-Identifikation ist somit ein technischer Prozess den es aus datenschutzrechtlicher Sicht nicht geben sollte, untergräbt sie doch die Annahme, dass eine Person bei einer anonymisierten oder pseudonymisierten Datenbearbeitung nicht in ihrer Persönlichkeit verletzt werden kann.[42]

29

Die an den Backend gesendeten Daten besteht aus einer Abfolge von Zahlen und Buchstaben. Allein aufgrund dieser Angabe scheint eine Person nicht von anderen Personen unterscheidbar zu sein. Entscheidend ist, dass die auf dem Backend vorhandenen Daten nicht durch Dritte (etwa Sub-Auftragsdatenbearbeiter) für eigene Zwecke bearbeitet werden und in Korrelation mit anderen Daten ein User Re-Identifiziert wird. Sodann speichern alle User die EphID der anderen User lokal auf dem eigenen Smartphone. Diese EphIDs werden für eine zeitlich beschränkte Dauer von 21 Tagen gespeichert und anschliessend automatisch gelöscht. Gleiches gilt für die auf dem Backend gespeicherten Daten.[43]

VI. Die Übertragung von Proximity Daten an den Backend

30

Die PT-App selbst stellt nicht fest, ob eine Person an COVID-19 erkrankt ist oder infiziert wurde. Eine solche medizinische Untersuchung und der daraus hervorgehende Befund erfolgen ausschliesslich durch das ärztliche Personal. Ein medizinischer Befund einer Erkrankung stellt nach Art. 3 lit. c Ziff. 2 DSG[44] ein besonders schützenswertes Personendatum über die Gesundheit einer betroffenen Person dar. Art. 3 lit. c Ziff. 2 DSG verlangt jedoch nicht eine medizinische Diagnose, etwa die Klassifikation einer Krankheit. Es genügt eine körperliche, psychische, labor- oder gerätemedizinische Untersuchung.[45] Das Ergebnis der

medizinischen Untersuchung stellt eine Information über die Gesundheit einer Person dar, die direkt oder indirekt Rückschlüsse über deren früheren, gegenwärtigen oder zukünftigen körperlichen oder geistigen Gesundheitszustand zulassen.[46] Bei der medizinischen Feststellung einer potenziellen Erkrankung an COVID-19 handelt es sich demnach um ein solches besonders schützenswertes Datum. Es ist nicht der Zweck der PT-App, diesen medizinischen Befund festzustellen, sondern andere User über eine mögliche COVID-19 Infizierung zu informieren, damit diese sich wiederum medizinisch untersuchen lassen können. Es liegt damit auch in der Verantwortung des ärztlichen Personals zu bestimmen, ab wann eine Person ansteckend war und potenziell andere mit COVID-19 anstecken konnte

1. Der Input einer potenziellen COVID-19 Erkrankung in die PT-App

31

Der Input für die PT-App über eine potenzielle COVID-19 Erkranken kommt daher stets von ausserhalb der PT-App. Der Output, die Information an andere User über eine potenzielle COVID-19 Erkranken, erfolgt hingegen durch die PT-App. Das Zusammenwirken einer medizinischen Untersuchung, die Speicherung der Benachrichtigungsidentifier an den Backend und die Übertragung dieser Information via Bluetooth an andere User, erfordert folgende Prozessschritte:

a) Ein User erlangt Verdacht auf eine mögliche COVID-19 Erkrankung und benachrichtigt eine Gesundheitseinrichtung, z.B. die Hausärztin. Die Ärztin untersucht den User und befindet eine positive COVID-19 Erkrankung. Sie erstellt eine von einer lokalen Gesundheitsbehörde (in der Schweiz dem BAG) erstellten einmaligen Autorisierungscode, beispielsweise in Form eines QR Codes. Der User erhält den QR Code zugestellt, etwa in Form einer E-Mail, SMS oder einem Link zu einer Webseite einer lokalen Gesundheitsbehörde.

b) Der User scannt den QR Code und übermittelt damit den Autorisierungscode an die PT-App.

c) Damit öffnet sich eine sichere, d.h. für Dritte nicht einsehbare Verbindung zum Backend.[47] Diese kann beispielsweise durch eine verschlüsselte Verbindung hergestellt werden. Die PT-App übermittelt den von der Ärztin erhaltenen Autorisierungscode, die EphID, den SK sowie die Angabe des Ansteckungszeitraums. Letzterer kann entweder im Autorisierungscode selbst eingebettet sein oder vom User im App manuell eingegeben werden.[48]

d) Der Backend erlaubt das Hochladen und die Speicherung der Information einer potenziell COVID-19 erkrankten Person nur, wenn ein gültiger Autorisierungscode verifiziert werden konnte. Ist dieser gültig, speichert der Backend den Autorisierungscode, die EphID sowie den SK. Für die in der Schweiz vorgeschlagene PT-App werden keine weiteren Daten auf dem Backend gespeichert. Sobald der Autorisierungscode und die EphID einer positiv COVID-19 erkrankten Person an den Backend gesendet wurde, generiert die PT-App des Absenders eine neue EphID.[49]

32

Durch den Zwischenschritt des zuerst zur Verfügung gestellten Autorisierungscodes und der anschliessenden Verifizierung auf dem Backend ist sichergestellt, dass nur Daten von potenziell COVID-19 erkrankten Personen hochgeladen werden, die medizinisch untersucht wurden.

2. Die Einwilligung in die Übertragung der EphID an den Backend

33

Die Rechtsgrundlage für die Datenbearbeitung ist länderspezifisch definiert. Für die Schweiz kann die PT-App auf freiwilliger Basis installiert werden. Es gibt entsprechend keinen Zwang die App zu installieren.[50] Das bedeutet, dass Personen, welche die App, aus welchen Gründen auch immer, nicht installieren, keinen Nachteil erleiden sollen. Umgekehrt können sie auch nicht von möglichen Vorteilen profitieren, welche die App als Service zur Verfügung stellt, nämlich rasch über eine mögliche COVID-19 Infektion informiert zu werden.

3. Die COVID-19-Verordnung für die PT-App

34

Dass die PT-App freiwillig genutzt, aber nicht von einer Behörde hoheitlich angeordnet wird, bedeutet nicht zwingend, dass die Rechtsgrundlage für eine solche Datenbearbeitung auf einer datenschutzrechtlichen Einwilligung beruht. Es ist also zu unterscheiden, ob der Staat individuell-konkret verfügt, dass eine betroffene Person eine PT-App nutzen muss, oder ob es zu hoheitlichen Massnahmen gegen diese Person kommt (z.B. das Aussprechen einer Busse). Die PT-App in der Schweiz verfolgt den Ansatz, dass die Installation der PT-App freiwillig erfolgt.[51] Falls User die App installieren, besteht eine gesetzliche Grundlage, die definiert, welche Daten zu welchem Zweck bearbeitet werden und wer für diese Datenbearbeitung verantwortlich ist (Art. 17 Abs. 1 DSG). Die COVID-19-Verordnung des

Bundesrates vom 24.Juni 2020 bildet ebendiese Rechtsgrundlage.[52] Diese gesetzliche Grundlage wird in der erforderlichen Änderung des Epidemiengesetzes[53] bestehen.

4. Die nicht-personenbezogene Datenbearbeitung von EphIDs bei PT-Apps

35

Unabhängig davon, ob der Backend personenbezogene Daten bearbeitet, erlaubt Art. 45c FMG die Bearbeitung von Informationen auf fremden Geräten durch z.B. Bluetooth nur dann, wenn a) dies für die Fernmeldedienste und ihre Abrechnung erfolgt oder b) wenn die User über den Bearbeitungszweck informiert wurden und die Bearbeitung ablehnen können. Ein Personenbezug, wie es das DSG vorsieht, ist entsprechend für die Anwendbarkeit des FMG nicht vorausgesetzt. Das FMG ist auch dann anwendbar, wenn keine personenbezogenen Daten bearbeitet werden (Art. 3 lit. a FMG).

36

Selbst wenn eine Re-Identifikation nicht möglich sein sollte, fällt somit die Bearbeitung der EphID unter das FMG. Das setzt voraus, dass User über den Bearbeitungszweck informiert wurden und die Datenbearbeitung ablehnen können. Die Information kann über Nutzungsbedingungen erfolgen, die bei der Installation der PT-App zur Verfügung gestellt werden. Eine Ablehnung ist möglich, indem die PT-App entweder gar nicht installiert oder aber nach erfolgter Installation wieder gelöscht wird.

VII. Das Matching mit anderen PT-App Usern

37

Eine PT-App benachrichtigt die User, wenn eine relevante unmittelbare physische Nähe zu einer positiv COVID-19 erkrankten Person bestand. Damit diese Benachrichtigung gewährleistet werden kann, muss a) eine positiv an COVID-19 erkrankte Person ihre EphID auf den Backend hochladen, b) die PT-App der anderen User den Backend regelmässig über die von anderen Usern hochgeladene EphID abfragen und dieses Datum auf dem eigenen Smartphone speichern sowie schliesslich c) die heruntergeladene, als COVID-19 bestätigte EphID, mit den auf dem Smartphone bereits vorhandenen EphIDs verglichen werden. Stimmen beide

EphIDs überein, weiss die Userin, dass sie sich in relevanter physischer Nähe zu einer positiv an COVID-19 erkrankten Person befunden hat.

1. Risk Scoring

38

Der Backend speichert demnach sämtliche EphIDs von Usern, die an COVID-19 erkrankt sind. In einem dezentralen Modell besteht die Funktion des Backend einzig darin, diese ‚infizierten' EphIDs regelmässig an alle User der PT-App zu senden. Jeder Empfänger vergleicht diese vom Backend gesendete infizierte EphID mit auf dem Smartphone bereits gespeicherten EphIDs. Stimmen zwei EphIDs überein, besteht eine gewisse Wahrscheinlichkeit, dass sich eine Person infiziert hat. Diese vergangenheitsbezogene Aussage ist nicht zwingend zutreffend, sondern von verschiedenen Variablen abhängig: a) dem Abstand zwischen Usern, b) der Dauer des Kontakts zwischen den Usern, c) der Messgenauigkeit der Bluetooth-Funktion, d) der Einschätzung des Infektionszeitraums. Basierend auf diesen Angaben berechnet ein Algorithmus der PT-App auf dem Smartphone des Users einen Risk Score. Erreicht der Risk Score eine von der Gesundheitsbehörde definierte Grenze, löst sie die Benachrichtigung einer potenziellen COVID-19 Erkrankung aus.[54]

2. Benachrichtigung über eine potenzielle COVID-19 Ansteckung

39

Ab diesem Zeitpunkt können sich User entscheiden, eine Gesundheitsstelle zu kontaktieren, um sich medizinisch zu untersuchen. Allenfalls sind auf der PT-App auch bereits erste Sofortmassnahmen ersichtlich, etwa sich in Selbst-Isolation zu begeben oder eben sich medizinisch untersuchen zu lassen.[55] Falls die PT-App so ausgestaltet ist, dass eine Rechtsfolge daraus resultiert, etwa eine COVID-19 Test zu machen (was möglicherweise zur Offenlegung an eine lokale Gesundheitsbehörde führt), zu Hause zu bleiben oder nicht mehr den Öffentlichen Verkehr zu benutzen, liegt damit ein automatisierter Einzelentscheid vor.

3. Die API von Google und Apple

40

Damit die Push-Benachrichtigung der PT-App im Fall einer bestätigten COVID-19 Erkrankung funktioniert, sendet die PT-App die Benachrichtigungsidentifier (die EphID, den SK und den Autorisierungscode) an den Backend. Der Backend sendet die ‚infizierte' EphID, also die EphID einer positiv getesteten COVID-19 Person, an

alle PT-App User. Durch die API erhalten Apple und Google Kenntnis, dass User die PT-App installiert und die Push-Benachrichtigungen aktiviert haben.[56] Zusätzlich erhalten sie Kenntnis der Daten, die zwischen dem Backend und der PT-App ausgetauscht werden, also den Benachrichtigungsidentifier (die EphID, den SK und den Autorisierungscode).[57] Weitere Informationen, insbesondere über den Gesundheitszustand eines Users, werden soweit ersichtlich jedoch keine ausgetauscht.[58] Wie für alle Smartphone-Apps besteht potenziell die Möglichkeit, dass Google und Apple anonyme Daten zu Statistikzwecken verwenden.

Fussnoten:

1. Bundesamt für Gesundheit BAG, «Die Swiss PT-App hilft, das Coronavirus in Schach zu halten», Faktenblatt vom 8. Mai 2020, https://www.bag.admin.ch/dam/bag/de/ dokumente/cc/kom/covid-19-faktenblatt-swiss-pt-app.pdf.download.pdf/BAG_ Faktenblatt_Coronavirus_Swiss-PT-App.pdf, besucht am: 31. Mai 2020, S. 1. ↑

2. Bundesamt für Gesundheit, Erläuterungen zur Verordnung über das Proximity-Tracing-System für das Coronavirus SARS-CoV-2 (VPTS) vom 29. Juni 2020, Art. 5 Abs. 2 Bst. e. ↑

3. Vgl. «Catch Me If You Can», www.imdb.com (titles/catch me if you can 2002), https://www.imdb.com/title/tt0264464/, besucht am: 24.05.2020. ↑

4. Vgl. beispielsweise Australien's «COVIDSafe app», https://www.health.gov.au/ resources/apps-and-tools/covidsafe-app, besucht am: 1. Juni 2020; für Grossbritannien vgl. «Contact-tracing apps: Why the NHS said no to Apple and Google's plan», https://www.zdnet.com/article/contact-tracing-apps-why-the-nhs-said-no-to-apple-and-googles-plan/, besucht am: 1. Juni 2020; für Österreich vgl. die «Stopp Corona-App», https://participate.roteskreuz.at/faq_stopp_corona_app/, besucht am 1. Juni 2020; für Deutschland die «Corona Warn-App», https://www.coronawarn.app/de/, besucht am: 1. Juni 2020. ↑

5. Verordnung über das Proximity-Tracing-System für das Coronavirus SARS-CoV-2 (VPTS) vom 24. Juni 2020, SR 818.101.25. ↑

6. BAG Faktenblatt [Fn. 1], S. 1. ↑

7. Bundesamt für Gesundheit, Erläuterungen zur Verordnung über das Proximity-Tracing-System für das Coronavirus SARS-CoV-2 (VPTS) vom 29. Juni 2020, Ziff. 1.1. ↑

8. BAG-Erläuterungen [Fn 7]. ↑

9. BAG [Fn. 5]; BAG Erläuterungen [Fn. 7], Art. 6 und 12. ↑
10. BAG-Erläuterungen [Fn. 2], ↑

11. Bugnion Edouard/Jaccard Michel/Jotterand Alexandre, DPIA Report – DP^3TS, https://github.com/DP-3T/documents/blob/master/data_protection/DP-3T%20Model%20DPIA.pdf., besucht am: 1. Juni 2020, S. 6. ↑

12. Troncoso Carmela/Payer Mathias/Hubaux Jean-Pierre (et al.), Decentralized Privacy-Preserving Proximity Tracing, Version vom 25. Mai 2020, https://github.com/ DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf, besucht am 1. Juni 2020, S. 16; Bugnion Edouard/Jaccard Michel/Jotterand Alexandre, [Fn. 10], S. 6. ↑

13. «Apple and Google partner on COVID-19 contact tracing technology», https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/, besucht am: 30. Mai 2020. ↑

14. Bugnion Edouard/Jaccard Michel/Jotterand Alexandre, [Fn. 11], S. 30. ↑

15. BAG-Erläuterungen [Fn. 2], ↑

16. Recher Patrick/Traussnig Anna, «So funktioniert eine Corona-Tracing-App die Ihre Privatsphäre schützt», https://www.republik.ch/2020/04/16/so-funktioniert-eine-corona-tracing-app-die-ihre-privatsphaere-schuetzt, besucht am: 1. Juni 2020; in allgemeiner Weise dargestellt in «DP37 API Documentation» vom 20. April 2020, https://github.com/DP-3T/dp3t-sdk-backend/blob/develop/documentation/ documentation.pdf, besucht am: 1. Juni 2020, S. 4. ↑

17. Troncoso Carmela/Payer Mathias/Hubaux Jean-Pierre (et al.), [Fn. 12], S. 15. ↑

18. BAG Fragen und Antworten [Fn. 2], Fragen 1–2 Seite 1; Troncoso Carmela/Payer Mathias/Hubaux Jean-Pierre (et al.), [Fn. 12], S. 15 f., die jedoch von einer Speicherdauer von 14 Tagen ausgehen; Bugnion Edouard/Jaccard Michel/Jotterand Alexandre, [Fn. 10], S. 13. ↑

19. Bugnion Edouard/Jaccard Michel/Jotterand Alexandre, [Fn. 11], S. 4; Troncoso Carmela/Payer Mathias/Hubaux Jean-Pierre (et al.), [Fn. 12], S. 15. ↑

20. Siehe hierzu hinten, Rz. 24. ↑

21. Troncoso Carmela/Payer Mathias/Hubaux Jean-Pierre (et al.), [Fn. 12], S. 16. ↑

22. Es gibt keine allgemeingültige Definition, ab wann ‚grosse Mengen an Daten' bearbeitet werden, doch liegt ein umfangreicher Datenbestand oder eine grosse Datenmenge aktuell im Tera- bis Zettabytebereich. Erst ab rund 100 Terabyte können Daten nicht mehr auf klassischen, relationalen Datenbanken operativ stabil und konsistent bearbeitet werden, vgl. ausführlich Meier Andreas/Kaufmann Michael, SQL- & NoSQL-Datenbanken, 8. Aufl., Berlin/Heidelberg 2016, S. 148 f. ↑

23. Siehe grundlegend die Ausführungen von Meier Andreas, Datamanagement mit SQL und NoSQL, in: Meier Andreas/Fasel Daniel (Hrsg.), HMD 51/2014, S. 17–38. ↑

24. Troncoso Carmela/Payer Mathias/Hubaux Jean-Pierre (et al.), [Fn. 12], S. 15 f. ↑

25. Bugnion Edouard/Jaccard Michel/Jotterand Alexandre, [Fn. 11], S. 13 f., die für die Zeitangabe einen Zeitraum von mindestens 6 Stundens empfehlen. ↑

26. BAG Erläuterungen [Fn. 2], ↑

27. Bundesamt für Gesundheit BAG, Erläuterungen zur Verordnung über das Proximity-Tracing-System für das Coronavirus SARS-CoV-2 (VPTS) vom 29. Juni 2020, Artikel 4. ↑

28. Bugnion Edouard/Jaccard Michel/Jotterand Alexandre, [Fn. 11], S. 9. ↑

29. Vgl. die Übersicht bei Bugnion Edouard/Jaccard Michel/Jotterand Alexandre, [Fn. 11], S. 3. ↑

30. «Das grosse soziale Experiment», Republik vom 16. April 2020, https://www.republik.ch/2020/04/16/das-grosse-sozial-digitale-experiment, besucht am: 30. Mai 2020. ↑

31. Bundesamt für Gesundheit BAG, Erläuterungen zur Verordnung über das Proximity-Tracing-System für das Coronavirus SARS-CoV-2 (VPTS) vom 29. Juni 2020, Artikel 2.↑

32. Troncoso Carmela/Payer Mathias/Hubaux Jean-Pierre (et al.), [Fn. 12], S. 15. ↑

33. Bugnion Edouard/Jaccard Michel/Jotterand Alexandre, [Fn. 10], S. 29; BAG Faktenblatt [Fn. 1], S. 1. ↑

34. Bugnion Edouard/Jaccard Michel/Jotterand Alexandre, [Fn. 11], S. 9. ↑

35. Troncoso Carmela/Payer Mathias/Hubaux Jean-Pierre (et al.), [Fn. 12], S. 15. ↑

36. Troncoso Carmela/Payer Mathias/Hubaux Jean-Pierre (et al.), [Fn. 12], S. 15. ↑

37. Vgl. Bundesamt für Gesundheit BAG, Erläuterungen zur Verordnung über das Proximity-Tracing-System für das Coronavirus SARS-CoV-2 (VPTS) vom 29. Juni 2020, Artikel 2. ↑

38. Vgl. Bugnion Edouard/Jaccard Michel/Jotterand Alexandre, [Fn. 11], S. 7. ↑

39. Bugnion Edouard/Jaccard Michel/Jotterand Alexandre, [Fn. 11], S. 5; Bundesamt für Gesundheit BAG, Erläuterungen zur Verordnung über das Proximity-Tracing-System für das Coronavirus SARS-CoV-2 (VPTS) vom 29. Juni 2020, Artikel 2 und Artikel 3. ↑

40. Siehe zum Personenbezug im Datenschutzrecht ausführlich, Heuberger, Rz. 89 ff. ↑

41. Fernmeldegesetz vom 30. April 1997 (FMG), SR 784.10; siehe zum FMG sogleich hinten, Rz. 35. ↑

42. Heuberger Olivier, Profiling im Persönlichkeits- und Datenschutzrecht der Schweiz, Luzerner Beiträge zur Rechtswissenschaft Band 144, Zürich/Basel/Genf 2020, Rz. 129. ↑

43. BAG-Erläuterungen [Fn. 2], ↑

44. Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG), SR 235.1. ↑

45. Botschaft zum Bundesgesetz über den Datenschutz vom 23. März 1988, BBl 1988 II, S. 446; Rosenthal David, in: Rosenthal David/Jöhri Yvonne (Hrsg.), Handkommentar DSG, Zürich 2008, Art. 3 N 48. ↑

46. Heuberger, [Fn. 38], Rz. 165. ↑

47. Bugnion Edouard/Jaccard Michel/Jotterand Alexandre, [Fn. 11], S. 10. ↑

48. BAG Fragen und Antworten [Fn. 2], Frage 24 S.4.; Bugnion Edouard/Jaccard Michel/Jotterand Alexandre, [Fn. 10], S. 5. ↑

49. Troncoso Carmela/Payer Mathias/Hubaux Jean-Pierre (et al.), [Fn. 12], S. 16. ↑

50. BAG Faktenblatt [Fn. 1], S. 2. ↑

51. Verordnung über das Proximity-Tracing-System für das Coronavirus Sars-CoV-2 (VPTS) vom 24. Juni 2020, SR 818.101.25, Art. 3.↑

52. Verordnung über das Proximity-Tracing-System für das Coronavirus Sars-CoV-2 (VPTS) vom 24. Juni 2020, SR 818.101.25 ↑

53. Bundesgesetz über die Bekämpfung übertragbarer Krankheiten des Menschen vom 28. September 2012 (EpG), SR 818.101. ↑

54. Troncoso Carmela/Payer Mathias/Hubaux Jean-Pierre (et al.), [Fn. 12], S. 26. ↑
55. Bugnion Edouard/Jaccard Michel/Jotterand Alexandre, [Fn. 11], S. 5. ↑

56. «Android Contact Tracing API» Version 0.4 vom April 2020, S. 2 f., https://blog.google/documents/55/Android_Contact_Tracing_API.pdf, besucht am: 1. Juni 2020. ↑

57. Bugnion Edouard/Jaccard Michel/Jotterand Alexandre, [Fn. 11], S. 30; vgl. die Übersicht bei Bundesamt für Gesundheit BAG, Technische Information, SwissCovid App: Einsatz von Bluetooth un den API von Apple und Google, S. 1. ↑

58. Vgl. Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB, Stellungnahme nach Art. 17a DSG zum Pilotversuch mit dem Swiss Proximity-Tracing-System (SPTS), Schreiben vom 11. Mai 2020 an das Bundesamt für Gesundheit, S. 5. ↑