COVID-19: Gouvernanzmodell für ein digitales Proximity Tracing

Kernelemente eines Gouvernanzmodelles für ein digitales Tracing- und Alarmierungssystem

Ein Resultat einer Arbeitsgruppe des Netzwerks «Digitale Selbstbestimmung»

erstellt im Rahmen des Hackathons VersusVirus (https://www.versusvirus.ch)
vom 3. – 5. April 2020

Autor*innen[1]:

Roger Dubach
Andrin Eichin
André Golliez
Dominique Keller
Christian Laux
Thomas Schneider
Martin Steiger

[1] Die Autor*innen haben dieses Papier in ihrer persönlichen Kapazität verfasst.

A. Vision

Digitale Technologien, wie beispielsweise Anwendungen für Mobiltelefone (**Apps**), sind wichtige Instrumente im Kampf gegen die COVID-19-Krise.

In digitalen Technologien liegt die **Chance** begründet, dass sie andere – teilweise bereits existierende – politische und epidemiologischen Massnahmen ergänzen und verstärken können. Insbesondere im Hinblick auf eine mögliche Exit-Strategie und der damit einhergehenden Lockerung bestehender Massnahmen werden digitale Technologien zur Eindämmung des Coronavirus, beispielsweise Tracing-Apps, an Bedeutung gewinnen. Mit solchen Apps könnte man gezielt einzelne Personen frühzeitig über mögliche Infektionen warnen. Dadurch werden Massnahmen zur Isolation von Menschen möglich, was dazu beitragen kann, das Risiko einer weiteren Infektionswelle zu minimieren. Eine entsprechende Risikoverminderung könnte eine Lockerung von Einschränkungen der Bewegungs- oder Wirtschaftsfreiheit begünstigen. Damit digitale Technologien eine solche Wirkung haben können, müssen sie weite *Verbreitung* finden. Dies bedingt jedoch *Vertrauen* der Bevölkerung. Zudem müssen die App ebenso wie die zugrundeliegenden Konzepte *einfach verständlich und genauso einfach anwendbar* sein.

Digitale Technologien können mit **Risiken** verbunden sein. Bereits vor der Krise haben unkontrollierte Datensammlung und -nutzung begründete Ängste und Bedenken ausgelöst. Im Kontext einer Krise sind diese Bedenken bezüglich Überwachung durch Staat und Unternehmen und den damit einhergehende Befürchtungen von grundlegendem Freiheitsverlust besonders relevant. Es besteht die Befürchtung, dass unsere Gesellschaft Apps, welche auf Überwachungsmassnahmen hinauslaufen oder in solche münden, nach Bewältigung der Krise nicht mehr los wird. Dieser Preis wäre zu hoch: Freiheit würde eingetauscht gegen Gesundheit.

Wir sind der festen Überzeugung, dass der Einsatz von digitalen Technologien zur Bekämpfung dieser Krise **keine Wahl zwischen Freiheit und Gesundheit** ist. Wir sollen sowohl grundlegende Freiheitsrechte wie Privatheit als auch Gesundheit garantieren und geniessen können. In der Schweiz sollen die Menschen im Zentrum der digitalen Transformation stehen – auch in Zeiten von Corona. Die Entwicklung digitaler Hilfsmittel im Kampf gegen das Virus sollte zu Gunsten und zur Ermächtigung aller Menschen genutzt werden. Dafür braucht es neue Strukturen, die dem Individuum eine aktive Steuerung der digitalen Transformation in der COVID-19-Krise ermöglichen.

Der Einsatz von digitalen Hilfsmitteln erfordert einen Rahmen, der eine solche Balance garantiert und alle Menschen dazu ermächtigt, digital selbstbestimmt handeln zu können. Das vorliegende Dokument definiert **Kernelemente für die Schaffung eines solchen Gouvernanzmodells** im Rahmen der COVID-19-Krise. Es soll dazu beitragen, ein effizientes Tracing- und Alarmierungssystem gegen Infektionen aufzubauen und die für eine möglichst weite Verbreitung nötige Akzeptanz schaffen. Diese Kernelemente sind einerseits *genereller Natur* und orientieren sich andererseits an den verschiedenen Wirkungsebenen von digitalen Anwendungen, namentlich an der *technischen Ebene*, der *innenpolitischen Ebene* und der *internationalen Ebene*.

Die Grundsätze der digitalen Selbstbestimmung sind in der **bundesrätlichen Strategie «Digitale Schweiz»** festgelegt. Im Kontext dieser Grundsätze hat sich das Netzwerk «Digitale Selbstbestimmung» formiert, um Bürger*innen, Unternehmen und öffentliche Einrichtungen eine Nutzung der Datenwirtschaft auf der Basis freiheitlich-demokratischer Grundwerte zu ermöglichen. Mit den vorliegenden Kernelemente zu einem Gouvernanzmodell wollen wir dazu beitragen, dass diese Werte auch im Kontext der COVID-19-Krise bestmöglich respektiert werden können.

B. Erklärungen

Als **Tracing- und Alarmierungssystem** bezeichnen wir in diesem Dokument das Zusammenspiel zwischen Apps, Protokollen und IT-Infrastrukturen (Rechenzentren, Geräte, Server, Betriebssoftware, etc.) zur Rückverfolgung möglicher Ansteckungen («Tracing») und Alarmierung der betreffenden Personen. Damit ein solches System seine gewünschte Wirkung entfalten kann, muss es in einen Gesamtkontext eingebettet sein, welcher verschiedene Datenräume, Akteure, Abläufe und Massnahmen umfasst. Es geht um die Einbindung der nachfolgend «Akteure» genannten Stellen in die Abläufe, die auf technischen Lösungen basieren.

1. COVID-19-relevante Datenräume

Als **Datenräume** werden hier zentrale Datenhaltungen mit einem abgrenzbaren Zugriffskonzept bezeichnet. Innerhalb des Gesamtsystems wird von folgenden Datenräumen ausgegangen: a) vom Datenraum des Tracing- und Alarmierungssystems, b) jenem mit direkt-identifizierenden Personendaten sowie c) jenem mit weiteren in der aktuellen Situation relevanten Daten. Die Bezugspunkte, an denen Daten erfasst, gesammelt und unter Umständen bearbeitet werden, werden als **Datenquellen** bezeichnet.

a) Datenraum des Tracing- und Alarmierungssystems

Wenn ein Staat eine App für Tracing und Alarmierung einsetzt, wird diese App Daten (1) einerseits auf dem Mobiltelefon des Nutzers und (2) andererseits auf einer zentralen Infrastruktur generieren. Es geht namentlich um zufällig generierte (idealerweise verschlüsselte) Identifikationsdaten des mobilen Endgerätes sowie allenfalls weitere Angaben (z.B., aber je nach Lösung nicht vorgesehen: Datum, Uhrzeit, Dauer, Standort, Nähe). Dabei werden nur Kontakte aus den letzten *n* Tagen[2] gespeichert, in welchen eine Infektion hätte stattfinden können. Ältere Kontakte werden fortlaufend gelöscht.

b) Datenraum mit direkt-identifizierenden Personendaten

Ausserhalb der Tracing- und Alarmierungs-App können im Rahmen der Bekämpfung des Coronavirus zusätzliche Daten erhoben werden, beispielsweise durch das Gesundheitssystem oder durch freiwillig übermittelte Angaben von Nutzer*innen. Je nach Datenquelle kann es sich um Daten zur Identifikation des Individuums (Name, Geschlecht, Alter, Wohnort etc.) oder zu dessen Gesundheitszustand (Testergebnisse, medizinische Informationen über den allgemeinen Gesundheitszustand oder Vorerkrankungen) handeln.

c) Datenraum mit weiteren relevanten Angaben

Zum Datenraum mit weiteren Angaben gehören alle weiteren für das Ziel der Verfolgung und Eindämmung des Coronavirus relevanten Daten. Quelle können sowohl Individuen als auch andere Datensammlungen sein, die Grundlage für aggregierte Daten bilden. Diese Daten sind aus gesamtgesellschaftlicher Sicht ebenfalls relevant. Dazu gehören z.B. Geo- und Bewegungsdaten der Individuen (Reisewege, Aufenthaltsorte sowie Angaben über Kontakte mit anderen Personen etc.).

d) Verknüpfte Datenräume

Die bereits bezeichneten Datenräumen können prinzipiell miteinander verknüpft und somit neu erschlossen werden. Diese Verknüpfungen und die daraus entstehenden Datenhaltungen können

[2] Diese Grösse muss epidemiologisch wirkungsvoll und wissenschaftlich abgestützt definiert werden. Aus diesem Grund verzichtet dieses Papier darauf eine Referenzangabe zu nennen.

heute noch nicht konkret vorausgesehen werden. Aus diesem Grund sind konkrete Risikoabschätzungen für diese noch nicht möglich. Eine greifende Gouvernanz verlangt jedoch auch eine Methode zur Kontrolle solcher Verknüpfungen. Hier gilt der Grundsatz, dass versteckte Datennutzungen zu verhindern sind: Zusätzliche Verknüpfungen von Daten dürfen erst hergestellt werden, wenn die Risiken im Rahmen eines Umsetzungsprojekts identifiziert, bewertet und transparent kommuniziert wurden. Umsetzungsprojekte müssen das Gouvernanzmodell einhalten.

2. Akteure

Das nationale Tracing- und Alarmierungssystem bedingt verschiedene Akteure auf nationaler, auf internationaler und auf transnationaler Ebene.

a) Nationale Akteure

Zu den nationalen Akteuren gehört zunächst die **Bundesverwaltung** (insbesondere das Eidgenössische Departement des Inneren [EDI] und das Bundesamt für Gesundheit [BAG]). Die Bundesverwaltung ist für die Koordination zuständig. Weitere Akteure sind die Betreiberorganisationen für das Tracing- und Alarmierungssystem, kantonale Behörden, Forschungsinstitutionen und verschiedene Akteure des Gesundheitssystems.

Zudem soll ein nationaler **Datentreuhänder**[3] (National Data Trust oder Trust Center) den Rahmen sicherstellen, damit Daten vertrauenswürdig erhoben, verwaltet, ausgetauscht und genutzt werden können. Der Datentreuhänder hat die Hauptaufgabe, die Einhaltung des Gouvernanzmodells sicherzustellen. Im Kontext des Epidemiengesetz (EpG) sollten bei der weiteren Rollenbeschreibung Art. 54 f. EpG und Art. 58 ff. EpG berücksichtigt werden.[4] Als Datentreuhänder könnte bereits gemäss Art. 58 Abs. 1 EpG auch ein geeigneter Dritter beauftragt werden. In Zusammenwirkung mit dem Gouvernanzmodell gewährleistet der Datentreuhänder, dass die Bevölkerung dem System vertraut und bereit ist, relevante und nützliche Daten der Allgemeinheit digital selbstbestimmt zur Verfügung zu stellen.

b) Internationale Akteure

Das Gouvernanzmodell muss ermöglichen, dass die Schweiz ihre Beziehungen zu **anderen Staaten** bei der Umsetzung digitaler Massnahmen im Kampf gegen COVID-19 auf operativer und kommunikativer Ebene im Sinne der Digitalen Selbstbestimmung sichern und koordinieren kann.

Dasselbe gilt für die Beziehungen zu **Internationalen Organisationen** (z.B. UNO-Ökosystem, Standardisierungsorganisationen etc.).

[3] Im Rahmen der digitalen Selbstbestimmung kann ein Datentreuhänder über sehr unterschiedliche Kompetenzen verfügen und sowohl ein privatrechtliches als auch öffentlich-rechtliches Konstrukt sein. Im vorliegenden Fall wurde für den Datentreuhänder eine Form gewählt, die sich eng am EpG orientiert.

[4] Gemäss heutiger Gesetzeslage ist das vorliegende Governanzmodell gesamthaft im Lichte des Bundesgesetzes über die Bekämpfung übertragbarer Krankheiten des Menschen (EpG) zu lesen: Bestimmungen zur Bearbeitung und Bekanntgabe von Personendaten sowie über das Informationssystem, inklusive Verantwortlichkeiten zur Einhaltung des Datenschutzes sind für den Epidemiefall unter anderem im EpG unter Kapitel 7, Abschnitt 2, insbesondere Art. 58-60 sowie in der konkretisierenden Verordnung über die Bekämpfung übertragbarer Krankheiten des Menschen (Epidemienverordnung, EpV) unter Kapitel 6, Abschnitt 4 (Art. 88) und Abschnitt 5 (Art. 89–99) geregelt. Mittelfristig könnte das hier skizzierte Gouvernanzmodell jedoch in das EpG aufgenommen werden und, soweit dies erforderlich sein oder als wünschbar angesehen werden sollte, im Rahmen einer Gesetzesänderung an das vorliegende Gouvernanzmodell angepasst werden).

c) Transnationale Akteure

Ein Gouvernanzmodell ist erst vollständig, wenn es berücksichtigt, dass die Handlungsfreiheit der Schweiz auch von weiteren, **transnational agierenden Dritten** beeinflusst oder in Frage gestellt werden kann. Zu nennen sind Anbieter von Protokollen (z.B. Pan-European Privacy-Preserving Proximity Tracing, PEPP-PT) oder von technischen Lösungen (z.B. Technologieunternehmen) und Vertreter der Wissenschaft. Auch Massnahmen zum Schutz gegen **widerrechtlich handelnde Angreifer** sind zu berücksichtigen.

C. Empfehlungen

Damit das Tracing- und Alarmierungssystem sowie das Gesamtsystem funktionieren und sowohl Datennutzer als auch Datensubjekte darin Vertrauen haben, braucht es eine klare Gouvernanz. Im Folgenden schlagen wir im Sinne von Empfehlungen **Kernsätze** für diese Gouvernanz vor:

- Systeme: Die Kernsätze sollen zunächst helfen, alle technischen Systeme (Apps, Netzwerke und weitere IT-Infrastrukturen) zur Bekämpfung des Coronavirus und die zum Betrieb dieser Systeme eingesetzten Organe im Sinne der Digitalen Selbstbestimmung auszugestalten.
- Datenräume: Es werden Datenräume entstehen, die auf diesen technischen Systeme beruhen. Diese müssen einer Kontrolle unterworfen werden, welche Digitale Selbstbestimmung gewährleisten kann.
- Akteure: Zudem soll das Gouvernanzmodell die Grundlage für die Kontrolle und Koordination der an den Systemen und Datenräumen beteiligten Akteure bilden. Auch für diese Aspekte stellt das vorliegende Dokument Kernsätze zur Verfügung.

Im Sinne der Vision zielen die Empfehlungen darauf ab, Vertrauen zu schaffen und in der Bevölkerung eine möglichst breite Bereitschaft zu wecken, ihre Daten dem System zur Verfügung zu stellen und dieses zum eigenen Wohl wie demjenigen der ganzen Gesellschaft zu nutzen. Zielsetzung ist entsprechend ein möglichst einfaches Gouvernanzmodell: Es soll eine leicht verständliche Orientierungshilfe sein und maximalen Schutz der Bevölkerung ermöglichen.

Die Empfehlungen differenzieren nach drei Handlungsebenen: (a) der technischen, (b) der nationalen und (c) der internationalen Ebene. Generelle Empfehlungen werden vorangestellt; diese sind als Kerngehalt der Gouvernanz stets einzuhalten und haben die Stellung von Leitmotiven.

1. Generelle Empfehlungen

Generelle Kernsätze	
1.1	Der Einsatz von digitalen Technologien zur Bekämpfung der COVID-19-Krise darf nicht auf eine Wahl zwischen Freiheit und Gesundheit hinauslaufen. Insbesondere das Tracing- und Alarmierungssystem darf in keinem Fall dazu führen, dass Bürger*innen überwacht werden (weder durch den Staat noch durch Private).
1.2	Bürger*innen haben im Rahmen der Rechtsordnung grösstmögliche Kontrolle über ihre Daten und die darauf basierenden Prozesse und Entscheidungen im digitalen Raum.

1.3	Bürger*innen können die Auswirkungen ihres Handelns im digitalen Raum abschätzen. Es besteht Transparenz, wie und wozu ihre Daten erfasst, verarbeitet und genutzt, in welchen Datenräumen die Daten gehalten, wie und durch wen sie verwaltet werden und wer auf die Daten zugreift.
1.4	Die Nutzung von digitalen Anwendungen basiert auf Freiwilligkeit. Bürger*innen sollen die Möglichkeit haben, aus freiem Willen Daten weiterzugeben.
1.5	Das Recht auf Kopie und die weiteren Betroffenenrechte nach Datenschutzrecht (namentlich Auskunft, Einsicht, Berichtigung und Löschung) sind gewährleistet.

2. Technische Handlungsebene

Auf der technischen Handlungsebene finden sich Empfehlungen, die sich auf die konkrete Ausgestaltung des Tracing- und Alarmierungssystem beziehen. Dieses besteht konzeptionell aus den drei folgenden Bausteinen: erstens aus einem *Basisprotokoll*, zweitens aus einer *Softwareentwicklung* (App, entweder integriert in eine bestehende Anwendung oder als neu zu entwickelnde Lösung) und *drittens* aus einer *Betriebsinfrastruktur mit Betriebsorganisation*.

Kernsätze zum Basisprotokoll des Tracing- und Alarmierungssystems	
2.1	Das Basisprotokoll darf nicht dazu führen, dass das Tracing- und Alarmierungssystem zum Überwachungsinstrument wird (weder durch den Staat noch durch Private).
2.2	Das Basisprotokoll gewährleistet Anonymität und ist datenschutzrechtlich zulässig.
2.3	Alle Daten, die anonymisiert bzw. verschlüsselt werden können, ohne die Ziele des Tracing und der Alarmierung zu verunmöglichen, werden anonymisiert bzw. verschlüsselt. Daten werden grundsätzlich dezentral auf dem Endgerät der Nutzer*innen gespeichert.
2.4	Das Basisprotokoll sieht die Preisgabe von Daten (dazu gehört auch der Upload in einen Datenraum oder die Übermittlung an andere Teilnehmer*innen) nur vor, wenn dies zwingend notwendig ist. Es gilt die Regel, dass Daten nur mit expliziter Einwilligung der Nutzer*innen zentralisiert werden.[5] Auch nach Einwilligung sind Nutzer*innen bestmöglich zu schützen.
2.5	Eine Alarmierung kann nur durch eine berechtigte Fachperson (z.B. Arzt) ausgelöst werden.

Kernsätze zu den Apps, in welche das Alarmierungssystem eingebettet ist	
2.6	Die App darf nicht dazu führen, dass das Tracing- und Alarmierungssystem zum Überwachungsinstrument wird (weder durch den Staat noch durch Private).
2.7	Die App gewährleistet Anonymität und darf nicht gegen Datenschutzrecht verstossen. Sofern sich aus der Herkunft der App aus einem App-Store Verknüpfungen zu Personen ableiten lassen, hat der Staat entsprechende Massnahmen zu treffen.

[5] Speicherung in zentrale Datenräume soll es nur geben, wenn hierfür ein wichtiges epidemiologisches Bedürfnis besteht und die generellen Empfehlungen (Kernsätze 1.1–1.5) dadurch nicht ausgehöhlt werden. Vor Implementierung ist die Öffentlichkeit angemessen zu konsultieren.

2.8	Die Nutzung der App sowie die Preisgabe von Daten erfolgt auf freiwilliger Basis. Die App befolgt die zentralen Prinzipien des Datenschutzrechts: Datenminimierung und Privacy by Design. Die App sieht freiwillige und transparent erläuterte Einwilligungen ("Opt-ins") vor. Datenräume sind jederzeit so auszugestalten, dass der Widerruf der Einwilligungen auch auf der Datenebene umgehend und automatisiert umgesetzt werden.
2.9	Nutzer*innen müssen einfach und verständlich über Zweck, technische Funktionalität und juristische Konsequenzen einer Nutzung der App informiert sein. Nutzungsbedingungen und Abläufe müssen einfach sein (siehe auch Kernsatz 3.15).
2.10	Der Source Code der App (unter Einschluss des Basisprotokolls) ist frei verfügbar und kann unter Vorbehalt der Pflicht zur Quellenangabe frei verändert und verwendet werden.

Kernsätze zur Betriebsinfrastruktur und -organisation	
2.11	Die Betriebsorganisation unterwirft sich dem hier definierten Gouvernanzmodell. Die vorstehenden Kernsätze sind durchwegs einzuhalten. Zusätzlich gelten die Kernsätze 2.12 und 2.13.
2.12	Es gilt der Grundsatz der Datenminimierung. Er wird dadurch umgesetzt, dass Daten automatisch gelöscht werden, sofern Nutzer*innen nicht ausdrücklich der verlängerten Speicherung für eine im Voraus auf kurze Dauer limitierte Zeitspanne zustimmen (gilt sowohl für Datenspeicherungen auf dem Mobiltelefon sowie für Datenspeicherungen in Datenräumen, sofern solche überhaupt vorkommen).
2.13	IT-Infrastrukturen zum Betrieb von App und / oder von Datenräumen sind von den Betreibern gegen den unbefugten Zugriff von Seiten Dritter oder eigenen Personals zu sichern.

3. Nationale Handlungsebene

Auf der nationalen Handlungsebene sind die Empfehlungen für die Institutionen des Bundes und weiterer Stellen in der Schweiz angesiedelt. Empfehlungen zur Ausgestaltung des Datentreuhänders sind auf dieser Handlungsebene zentral.

Kernsätze zur Verantwortung und Rolle der Bundesbehörden und der kantonalen Behörden	
3.1	Die Oberaufsicht und -verantwortung liegt bei den Behörden des Bundes und der Kantone gemäss der geltenden Kompetenzregelung. Die Rollen zur Sicherung der Koordination auf Bundes- und Kantonsebene sind von den zuständigen Stellen wahrzunehmen.
3.2	Der Grundsatz der Verhältnismässigkeit ist konsequent einzuhalten und sowohl auf der planenden als auch auf der umsetzenden Ebene zu leben (insbesondere Erforderlichkeit, Eignung und Güterabwägung).
3.3	Wenn eine aus der Optik der Freiheit mildere Massnahme möglich ist, ist diese zu wählen, auch wenn andere Ziele damit nicht mehr umgesetzt werden können. Ziffer 3.4 ist vorbehalten.

3.4	Falls der Schutz der Freiheit dazu führt, dass der Einsatz eines Tracing- und Alarmsystems deswegen nicht mehr möglich oder sinnvoll ist, prüft die Behörde im Sinn der Verhältnismässigkeit mögliche Eingriffe in die Freiheit. Es braucht dann aber flankierende Massnahmen. Der Eingriff muss strikt zeitlich limitiert sein und vollständig rückgängig gemacht werden können.
3.5	Die Behörden sorgen im Rahmen ihrer Zuständigkeiten für die Durchsetzung des Gouvernanzmodells.

Kernsätze zum Nationalen Datentreuhänder (National Data Trust oder Trust Center)	
3.6	Die Rolle des Datentreuhänders wird durch den Bund oder die Kantone oder durch von diesen beauftragte Dritte ausgeübt.
3.7	Der Datentreuhänder verwaltet die Datenräume, welche im Sinne der vorstehenden Bestimmungen als gerechtfertigt gelten und entsprechend umgesetzt werden.
3.8	Der Datentreuhänder hält sich jederzeit an die limitierte Zweckbestimmung, dass Daten ausschliesslich für die Zwecke des anonymen Tracings und der anonymen Alarmierung (Alarmierung ohne namentliche Ansprache und ohne Erfassung der angeschriebenen Person in einem Verzeichnis als Verdachtsfall) verarbeitet werden.
3.9	Der Datentreuhänder stellt sicher, dass die von ihm verwalteten Daten vor Zugriff durch Unberechtigte geschützt sind.
3.10	Der Datentreuhänder stellt sicher, dass Betreiberorganisationen und Apps als Träger für Tracing- und Alarmierungssysteme geeignet sind. Diese Eignung muss verifizierbar sein und fortlaufend verifiziert werden.

Kernsätze zum nationalen Datenaustausch innerhalb der Schweiz	
3.11	Der Datenaustausch muss nach Möglichkeit automatisierbar über Systemschnittstellen (Application Programming Interfaces, APIs) möglich sein.
3.12	Die Weiternutzung von Daten über den ursprünglichen Zweck (Tracing- und Alarmierungssystem) hinaus, ist sowohl dem Staat als auch Dritten verboten, solange die Nutzer*innen für die sie betreffenden Nutzungen ihre Zustimmung nicht erteilt haben.
3.13	Die Weiternutzung von Daten soll möglichst ohne weitere technische Umsetzungsmassnahmen möglich sein, wenn Nutzer*innen ihre Zustimmung freiwillig erteilt haben. Nutzer*innen können ihre Zustimmung jederzeit widerrufen (Kernsatz Ziffer 2.8 gilt entsprechend).
3.14	Wer eine Weiternutzung von Daten gemäss diesem Gouvernanzmodell vornehmen möchte, muss sich diesem Gouvernanzmodell unterwerfen. Wer weiternutzt unterstellt sich der Kontrolle des nationalen Datentreuhänders (National Data Trust / Trust Center).
3.15	Jede Weiternutzung wird einfach und transparent und dabei in den wesentlichen Zügen vollständig so dargelegt, dass die betroffenen Personen jederzeit sachgerecht beurteilen können, inwiefern ihnen aus der Zustimmung der Datenweiternutzung Nachteile erwachsen könnten.

4. Internationale Handlungsebene

Auf der dritten Handlungsebene stehen Empfehlungen zur Koordination und zum Erfahrungsaustausch mit internationalen Akteuren sowie Mechanismen zur Förderung der digitalen Selbstbestimmung auf globaler Ebene.

Kernsätze zur Koordination und Austausch mit internationalen Akteuren	
4.1	Die Schweiz soll aktiv die Koordination mit anderen Ländern (allen voran unseren Nachbarländern sowie anderen Ländern mit hohem ein- oder ausreisenden Verkehr) sowie internationalen Organisation (bspw. der WHO) suchen, um die Interoperabilität technischer Anwendungen, insbesondere des Tracing- und Alarmierungssystems, zu garantieren.
4.2	Gegenüber Staaten, welche das Gouvernanzmodell der Schweiz nicht gewährleisten können, werden Systemgrenzen errichtet. Diese können besonderen Bedürfnissen anderer Staaten Rechnung tragen, sofern diese Bedürfnisse und die daraus resultierenden Risiken für Nutzer*innen transparent und verlässlich kommuniziert werden.
4.3	Die Schweiz soll den Austausch von Erfahrungen in der Verwendung digitaler Anwendungen zur Bekämpfung von COVID-19 mit anderen Ländern aktiv fördern, selbst ihre Erfahrungen einbringen und Erfahrungen anderer Länder einholen. Dafür können bestehende internationale Gremien und Foren genutzt werden, um einen raschen Wissenstransfer zu ermöglichen.
4.4	Um den Risiken der internationalen Mobilität entgegenzutreten, sollten auf internationaler Ebene Regelungen abgestimmt werden, damit nicht jedes Land sein eigenes Einreiseregime einführt. Hier wird davon ausgegangen, dass die Systemintegration zwischen nationalen Systemen über Systembrücken ermöglicht wird («Data Feeds»).
4.5	Die Schweiz steht dafür ein, dass die allgemeinen Kernsätze (Ziffer 1.1 – 1.5) sowie die Kernsätze unter Ziffer 2 auch im internationalen Verhältnis zum Durchbruch kommen.

Kernsätze zum internationalen Datenaustausch	
4.6	Der Austausch von Daten mit spezifischem oder potenziellem Personenbezug zwischen Staaten soll anonym erfolgen und ausschliesslich dem Zweck der Benachrichtigung («Alarmierung») potenziell infizierter Personen dienen. Der Datenaustausch darf nicht dazu führen, dass das Alarmierungssystem zum Überwachungsinstrument eines Staates wird.
4.7	Die Schweiz schliesst mit ausländischen Partnern eine internationale Vereinbarung, welche regelt, unter welchen Bedingungen Daten zwischen nationalen Systemen ausgetauscht werden können.
4.8	Die Schweiz legt anderen Staaten das Basisprotokoll ihres Tracing- und Alarmierungssystems transparent offen und verlangt Entsprechendes im Gegenzug.

4.9	Die Schweiz sorgt nach Möglichkeit für die Einhaltung des vorliegenden Gouvernanzmodells. In jedem Fall dürfen die Kernsätze in den Ziffern 1.1 – 1.5 nicht ausgehöhlt werden.
4.10	Die Schweiz sorgt dafür, dass andere Staaten sich auf die Einhaltung der vorliegenden Kernsätze verpflichten. Der andere Staat darf Daten nicht entgegen der Zweckbestimmung gemäss Kernsatz Ziffer 3.8 verwenden; Ziffer 3.11 – 3.15 sind vorbehalten. In jedem Fall muss die Datenaufbewahrung (siehe Kernsatz 2.12) limitiert sein.

Kernsätze zur Definition von Unabhängigkeit gegenüber Dritten	
4.11	Das Gouvernanzmodell sorgt für Methoden zur Einhaltung der Cyber-Sicherheit mit Mitteln, die einer demokratisch legitimierten Kontrolle unterstehen.
4.12	Technische Angebote von ausländischen Anbietern sind auf ihre Kompatibilität mit dem Gouvernanzmodell zu prüfen. Dabei ist auf Transparenz zu achten und eine demokratisch legitimierte Nachkontrolle muss vorgenommen werden.
4.13	Protokolldefinitionen sind auf ihre Kompatibilität mit dem Gouvernanzmodell zu prüfen. Dabei ist auf Transparenz zu achten. Eine demokratisch legitimierte Nachkontrolle muss vorgenommen werden.
4.14	Etablierte Meinungen der Wissenschaft sind proaktiv einzubinden, wobei auch hier Grundsätze der Transparenz und der demokratisch legitimierten Nachkontrolle beachtet werden.
4.15.	Die Schweiz führt bei Bedarf neue Strafnormen ein, wenn dies nötig sein sollte, um Dritte wirksam abzuschrecken in Bezug auf das Mithören des Datenaustauschs über die Bluetooth-Schnittstelle auf dem Mobiltelefon.

* * *

Anhang

1. Technische und funktional bedingte Abläufe eines Tracing- und Alarmierungssystems

Ein Tracing- und Alarmierungssystem funktioniert vereinfacht ausgedrückt wie folgt: Über Bluetooth bzw. Bluetooth Low Energy Bluetooth LE, BLE) tauschen die mobilen Geräte, welche dem System angeschlossen sind und sich länger als eine kritische Zeit in kritischer Nähe[6] zueinander befunden haben, ihre verschlüsselten Geräte-Identitäten aus. Damit trägt man sich gegenseitig in die Benachrichtigungsliste des Gegenübers ein. Sobald ein User des Systems positiv auf das Corona-Virus getestet wurde, sendet er nach Freigabe durch den zuständigen Arzt über einen nationalen Trust Service einen Alarm an alle Einträge auf seiner Benachrichtigungsliste. Je nach Protokolldefinition enthält diese Nachricht Standort des Zusammentreffens und einen Zeitstempel.[7]

2. Ablauf bei symmetrischer Verschlüsselung

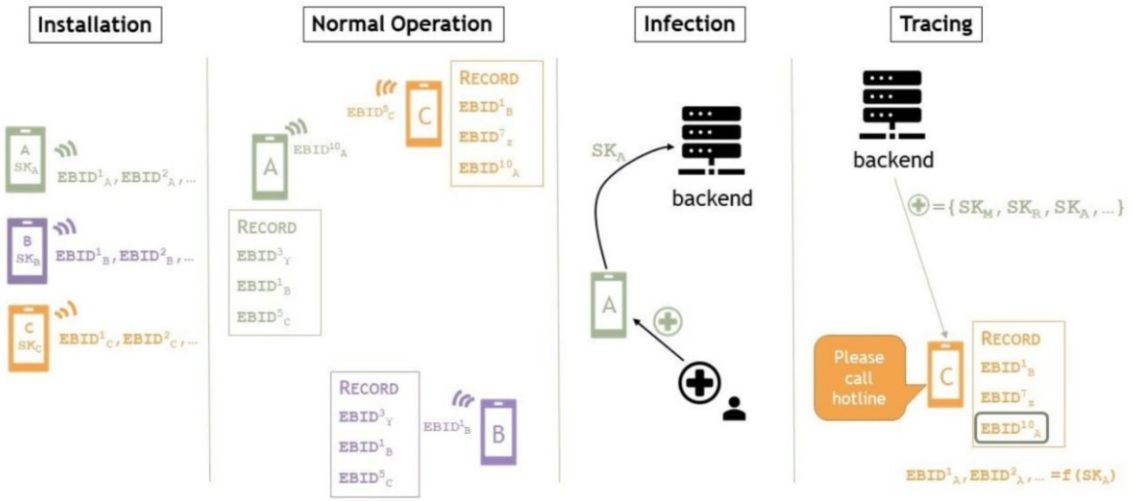

Figure 1: Phases in the decentralized proximity tracing system

(**Quelle:** documents/DP3T - Data Protection and Security.pdf at master · DP-3T/documents.)

Erläuterung zum Schritt «Installation» in Figure 1: Im Kern der symmetrischen Verschlüsselung stehen kleine, sich laufend ändernde Identifizierungsdateien («Tokens»), die in rascher Zahl von einem Hauptschlüssel auf dem Handy ausgegeben werden.

Erläuterung zum Schritt «Normal Operation» in Figure 1: Das Mobiltelefon sendet den jeweils aktuellsten Token laufend über Bluetooth an die Öffentlichkeit, so dass eine Person in physischer Nähe sie auf ihrem Mobiltelefon speichern kann. So wird «Proximity» als Ausgangspunkt festgestellt.

[6] «Epidemiologically sufficient proximity in epidemiologically sufficient period of time» (https://www.pepp-pt.org/content).
[7] Für ausführlichere Informationen zu PEPP-PT siehe https://github.com/DP-3T/documents.

Erläuterung zum Ablaufschritt «Infection» in Figure 1: Wer sich als infiziert meldet (bzw. erst nach Prüfung durch einen Arzt als infiziert melden darf), publiziert nunmehr den Hauptschlüssel ins Netzwerk.[8]

Erläuterung zum Ablaufschritt «Tracing» in Figure 1: «Subscribers» in den «Newsletter» der als infiziert gemeldeten Person (in Figure 1 ist dies die Person A) erhalten nun eine Nachricht (zum Beispiel: «Please call hotline now» (im Beispiel in Figure 1 ist Person C ein solcher Empfänger). So können alle, die sich für genügend lange Zeit in der Nähe der dannzumal an COVID-19 erkrankten Person aufgehalten haben, erkennen, dass sie sich ebenfalls angesteckt haben könnten.

3. Diskussion eines Protokolls auf Basis der symmetrischen Verschlüsselung

Veröffentlichung des Bewegungsprofils an einen offenen Empfängerkreis: Jeder Empfänger, der passiv einen der unzähligen Tokens erhalten hat, kann das Bewegungsprofil des Absenders (meist für die zurückliegenden 14 Tage) rekonstruieren; denn dieses hängt üblicherweise als Ganzes am Hauptschlüssel.

Snooping: Eine Folge der symmetrischen Verschlüsselung besteht darin, dass eine leistungsfähige, in der Nähe eines öffentlichen Platzes aufgestellte Antenne den Datenverkehr über die Bluetooth-Schnittstelle passiv mitschneiden kann. Da sie somit den Token der dannzumal infizierten Person kennt, kann auch diese Antenne das Bewegungsprofil der Person rekonstruieren. Wer sich eine Antenne leisten kann, kann also reinschnüffeln.

Fazit: Ein Protokoll mit symmetrischer Verschlüsselung erfüllt somit mindestens zwei der Anforderungen gemäss der Arbeit von *Cho / Ippolito / Yu* nicht (siehe Cho / Ippolito / Yu, Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs).

4. Diskussion von Protokollen mit zentraler Datenhaltung

Keine Anonymität: Soweit die Datenhaltung nicht rein lokal besteht und somit zentral gespeicherte Daten entstehen, wird von Bedeutung, dass eine App, die aus einem App-Store heruntergeladen wird, mit einer Person in Verbindung gebracht werden kann (Re-Identifizierbarkeit aus Sicht der Schweizerischen Eidgenossenschaft). Es liegt somit keine Anonymisierung vor.

Profilbildung: Sofern zentrale Daten hinterlegt werden, ist eine Profilbildung möglich. Dies ist im Licht des Verbots von Überwachungen oder Massnahmen mit gleicher Wirkung zu würdigen.

[8] «If the user of phone A has been confirmed to be SARS-CoV-2 positive, the health authorities will contact user A and provide a TAN code to the user that ensures potential malware cannot inject incorrect infection information into the PEPP-PT system. The user uses this TAN code to voluntarily provide information to the national trust service that permits the notification of PEPP-PT apps recorded in the proximity history and hence potentially infected. Since this history contains anonymous identifiers, neither person can be aware of the other's identity.» (https://www.pepp-pt.org/content).