Datenschutz und Datenethik: die Kontroverse um Contact-Tracing-Apps

Der Einsatz sogenannter Contact-Tracing-Apps zum Zweck der Eindämmung der Corona-Epidemie wird kontrovers diskutiert. Es ist letztlich eine Gefühlsfrage, welcher Ansatz – zentral oder dezentral – zu bevorzugen ist.

Von Dr. Thomas Steiner, LL.M., Rechtsanwalt

Mit der Rückverfolgung und Alarmierung von Kontakten einer infizierten Person können Infektionsketten unterbrochen und Epidemien wirksam eingedämmt werden. Während die Digitalisierung dieses sogenannten Contact- oder Proximity-Tracings die Privatsphäre sogar verbessern kann, geht es im öffentlichen Diskurs um die Gegenüberstellung verschiedener Implementierungsmodelle.

Expertenstreit um die Architektur

Ein Expertenstreit um die Architektur – **dezentraler oder zentraler Ansatz** – steht im Zentrum der Kontroverse und hat dazu beigetragen, dass der Einsatz von Contact-Tracing-Apps in der Schweiz, Deutschland und anderen europäischen Staaten in den letzten Monaten zuweilen emotional diskutiert wurde. Dieser Beitrag vergleicht den vom Schweizer Bundesamt für Gesundheit (BAG) zusammen mit der EPFL und der ETH gewählten Ansatz (Projekt «DP-3T») mit dem Ansatz, den das Projekt «PEPP-PT» verfolgt.

Zentraler Backend-Server ist Voraussetzung beider Ansätze

Um DP-3T und PEPP-PT zu vergleichen, muss man wissen, dass es sich bei beiden um Protokolle – das Protokoll ist abzugrenzen gegenüber der App, die das Protokoll implementiert – handelt, die symmetrische Verschlüsselung voraussetzen:

Symmetrische Verschlüsselung hat im Vergleich zu asymmetrischer Verschlüsselung diverse Nachteile aus Sicht des Schutzes der Privatsphäre, namentlich gegenüber sogenannten Snoopers und den eigenen Kontakten.

Asymmetrische Verschlüsselung verbessert den Schutz der Privatsphäre. Sie macht es aber z.B. notwendig, dass das Mobiltelefon von Bob nicht jederzeit versucht, Krankheitsmeldungen «in Echtzeit» zu erhalten, sondern z.B. jeweils erst, wenn das Mobiltelefon über das Ladekabel an der Steckdose aufgeladen wird.

Da beide Protokolle die für den Schutz der Privatsphäre nachteilige symmetrische Verschlüsselung voraussetzen, basieren mithin weder DP-3T noch PEPP-PT auf dem besten «Privacy-by-Design», das man sich vorstellen kann.

Beide Protokolle – wie es überhaupt für die meisten Tracing-Lösungen der Fall ist – setzen einen zentralen **Backend-Server** voraus. Er dient mindestens dazu, die Krankmeldung, die von Alice ausgeht, an Bob zu übermitteln.

Verschlüsselungsvorgang und Datenhaltung

Es geht beim Vergleich von PEPP-PT und DP-3T nur um die Fragen, wie der Backend-Server in den Verschlüsselungsvorgang eingebunden ist und wo Daten über Proximities (Treffen) gespeichert werden (Datenhaltung). Beide Modelle funktionieren wie folgt: Treffen sich zwei Mobiltelefone, tauschen sie je eine Kleinstdatei aus (Token). Diese ist verschlüsselt und somit primär nicht lesbar.

Verschlüsselungsvorgang: Der Schlüssel zur Ver- und Entschlüsselung der Tokens, welche die Mobiltelefone von Alice und Bob aussenden, liegt bei PEPP-PT auf dem Backend-Server und bei DP-3T auf dem Mobiltelefon von Alice. Bei PEPP-PT besteht somit die Gefahr der Zweckentfremdung: Heute benutzt die Regierung die Technologie für das Proximity-Tracing, aber für welche Überwachung morgen?

Datenhaltung: Ausserdem sind die verschlüsselten Angaben auf dem Backend-Server von PEPP-PT bestenfalls pseudonym. Verknüpfungen mit individualisierbaren Angaben (z.B. über eine Anfrage an Apple oder Google, die den App Store bzw. den Play Store stellen) sind möglich. Somit kann der zentrale Server umfangreiche Bewegungsprofile und den gesamten «Contact Graph» (Ereignisprotokoll darüber, wer wen getroffen hat) mitschreiben. Bei DP-3T soll das Übermitteln des Contact Graph an den zentralen Backend-Server zwar ebenfalls möglich, aber anders als bei PEPP-PT freiwillig sein.

Eine Vertrauensfrage

Es ist eine Vertrauensfrage: Ob das System «gut» ist, hängt davon ab, ob der Staat bzw. die sonstige Organisation, die den Backend-Server betreibt, «gut» ist. Das technische System von PEPP-PT selber vermittelt deutlich weniger Schutz als DP-3T (weniger Privacy-by-Design). Die Macher von PEPP-PT sind aber der Meinung, dass ihr Protokoll auch als sicher eingestuft werden kann, da es überaus unwahrscheinlich sei, dass sich mehrere Akteure in widerrechtlicher Weise zu-

sammentun würden, um den Überwachungsstaat zu realisieren.

Wie man dieses Argument bewertet, ist im Wesentlichen **eine stark subjektiv geprägte Vertrauensfrage.** Zum Vergleich: Es gibt eine Vielzahl von IT-Infrastrukturen, bei denen der Zugriff auf Daten «nur» durch mehrfach abgesicherte organisatorische Massnahmen geschützt wird. Auch diese gelten aus juristischer und gesellschaftlicher Sicht oft als ausreichend gesichert.

Wo Personendaten bearbeitet werden und wo nicht

In der Schweiz haben die Nationale Ethikkommission und der EDÖB den vom BAG gewählten Ansatz «datenschutzrechtlich» analysiert und für zulässig erachtet. Durchschnittliche **Nutzer können keine Ableitungen über andere Nutzer treffen** (das wäre bei DP-3T gleich wie bei PEPP-PT). **Dem BAG wird es nicht möglich sein, einzelne Nutzer der App zu identifizieren.**

Hier besteht «datenschutzrechtlich» ein Unterschied zwischen DP-3T und PEPP-PT: Anders als bei DP-3T (wo die Entschlüsselung nicht auf dem Backend vorgenommen wird und die Angaben somit auch für das BAG **anonyme Daten** darstellen) handelt es sich bei verschlüsselten Angaben auf dem Backend-Server von PEPP-PT um identifizierende oder bestenfalls um **pseudonyme Daten.** Pseudonyme Daten sind für diejenigen Behörden (z.B. Gesundheitsbehörden) oder Organisationen (z.B. Forschungseinrichtungen), die den Schlüssel zur Re-Identifizierung von Nutzern haben, **Personendaten.**

Recht und Ethik des Datenschutzes

Die Bearbeitung von Personendaten muss nach den Vorgaben des anwendbaren Datenschutzrechts erfolgen. Beim Implementierungsmodell PEPP-PT müssen folglich insbesondere die Grundsätze der Speicherbegrenzung und der Datenminimierung eingehalten werden, und es müssen Betroffenenrechte (z.B. das Auskunftsrecht) gewährt werden. Wo die DSGVO gilt oder bei Bearbeitungen durch Bundesbehörden in der Schweiz bräuchte die Bearbeitung zudem eine Rechtsgrundlage (die in der Schweiz mit Art. 33 und 58 des EPG gegeben wäre – eine Einwilligung ist nicht erforderlich).

Auch eine Implementierung basierend auf PEPP-PT liesse sich konform mit dem **Recht** des Datenschutzes gestalten. Fraglich ist indes, ob die App basierend auf dieser Implementierung auch der **Ethik** des Datenschutzes entspricht. Konkret: Fühlen sich Nutzerinnen und Nutzer auch «wohl», und akzeptieren sie es, wenn die App-Architektur einer staatlichen Behörde die Re-Identifizierung ermöglicht?

Es geht also stark um eine Gefühlsfrage: Wie verändert sich unser Verhalten, wenn wir nur schon das Gefühl haben, überwacht werden zu können? (Egal, ob eine solche Überwachung dann tatsächlich stattfindet oder nicht.)

Datenethik und Vertrauensbildung für dreifache Freiwilligkeit

Das BAG setzt beim Einsatz der Contact-Tracing-App auf eine **dreifache Freiwilligkeit:** Die Installation und Nutzung der App ist freiwillig. Für positiv getestete Nutzer ist es freiwillig, andere Nutzer (enge Kontakte) über die App zu benachrichtigen. Für benachrichtigte Nutzer ist es freiwillig, die in der App angegebene Infoline Coronavirus zum Zweck weiterer Abklärungen anzurufen.

Damit die App trotz Freiwilligkeit ihre Ziele erreicht (gemäss BAG müssten mindestens 60% der Bevölkerung die App nutzen), braucht sie die nötige Akzeptanz in der Bevölkerung. Die entsprechende **Akzeptanz** erfordert Vertrauen, und Vertrauen schafft man durch Transparenz über die Funktionsweise der App, durch Einhaltung anerkannter Datensicherheitsstandards und mit einer App-Architektur, die für die Privatsphäre (Privacy-by-Design) möglichst schonend ist.

Vor diesem Hintergrund ist es letztlich gar nicht entscheidend, bei welchen Implementierungsmodellen für Contact- oder Proximity-Tracing-Apps das **Datenschutzrecht** anwendbar ist und wie gegebenenfalls anwendbare Datenschutzanforderungen eingehalten werden können.

Die Diskussion sollte nicht nur im Lichte des Datenschutzrechts, sondern auch im Lichte der Datensicherheit und der **Datenethik** geführt werden. Datenethik (auch «digitale Ethik») befasst sich mit Fragen des vertrauenswürdigen, verantwortungsvollen und nachhaltigen Umgangs mit Daten unter Aufrechterhaltung demokratischer Werte und (bei Einsatz von Algorithmen und künstlicher Intelligenz) menschlicher Kontrolle über neue Technologien (vgl. z.B. dataethics.eu).

Datenethik und digitale Governance

Entsprechend sind Arbeiten auf Ebene der **digitalen Governance** zu forcieren. An einer entsprechenden Arbeit haben sich Mitglieder eines nationalen Netzwerks für digitale Selbstbestimmung beteiligt. In einem kurz gehaltenen Dokument zeigen die Autorinnen und Autoren auf, welche Akteure relevant sind und welche Datenhaltungen entstehen, wenn die Schweiz Applikationen für das Contact- bzw. Proximity-Tracing einsetzt.

Das Dokument enthält Empfehlungen auf technischer und politischer Ebene. Es stellt zudem allgemeine Mindestanforderungen auf, die sicherstellen sollen, dass solche Systeme vertrauenswürdig sind (vgl. https://devpost.com/software/covid-19-governanzmodell-fur-ein-digitales-proximity-tracing).

AUTOR

Thomas Steiner, Dr. iur., LL.M., RA, LAUX LAWYERS AG, ist überwiegend im Daten-, Kartell- und Technologierecht tätig.