Die Aufzeichnung von Bewegungsprofilen mit Tracking-Apps ist auch unter Wahrung des Datenschutzes möglich.

Fotos: rcfotostock/Stock.adobe.com

Anonymisiertes Tracking

Tracking-Apps ermöglichen es, das Bewegungsprofil eines Menschen aufzuzeichnen, wie etwa im Fall der Corona-Krise diskutiert wird. Eine Möglichkeit, dabei den Datenschutz zu wahren, besteht in der Pseudonymisierung und Anonymisierung der Daten.

In Zusammenhang mit Gesichtserkennung sowie Identifikation über Bewegungsanalyse und ähnliche Technologien entstehen berechtigterweise Ängste vor einer Überwachung. Die rechtlichen Schutzvorgaben für persönliche Daten durch das Datenschutzrecht wirken einer Überwachung entgegen.

Seit Ende März 2020 ist in Österreich eine App in Verwendung, die Kontakte auf persönlicher Ebene trackt und nachträglich Zusammentreffen mit anderen Personen nachvollziehbar macht, um mögliche Ansteckungswege sichtbar zu machen. Es wurden Befürchtungen laut, dass auf Basis dieser App Kontaktprofile von Personen erstellt werden könnten.

Tracking. Es gibt derzeit verschiedene Ansätze, das Tracking der Kontakte durchzuführen. Das „Pan-European Privacy-Preserving-Proximity-Tracing-Projekt“ vertritt den Ansatz, der auch von *Apple* und *Google* unterstützt wird: Bei Kontakten werden zufällige Geheimzahlen beiderseits gespeichert und für eine bestimmte Zeit aufgehoben. Wird eine Person positiv getestet, überträgt diese ihre relevanten Kontaktcodes an eine zentrale Stelle.

Täglich erhalten alle Nutzer eine Liste aller Kontaktcodes, die von positiv getesteten Personen stammen, die App stellt lokal eine mögliche Übereinstimmung fest. Der Nachteil ist dabei, dass potenziell mehrere MB Daten pro Übertragung anfallen können und die positiv getestete Person identifizierbar wird.

Lösungen mit zentraler Datenspeicherung, die das Übertragungsproblem lösen würden, werden derzeit vermieden, aus Gründen des Datenschutzes. Doch ist es möglich, eine datenschutzkonforme, vollends pseudonymisierte Form des Tracking zu verwenden, die zentral speichert. Mit kryptografischen Methoden kann ein Erstellen von Bewegungs- und Kontaktmustern unter Wahrung der Rechte des Einzelnen erreicht werden.

Sicherung einer CoViD-19-Tracking-App. Eine Methode, die Daten einer CoViD-19-Tracking App datenschutzkonform zu gestalten, kann darin bestehen, nicht Telefonnummern oder Namen beim Zusammentreffen mit anderen Personen zu speichern, sondern nur kryptografische Hashes. Kryptografische Hashes sind „Einweg-Identifikatoren“: Bei einem Hash wird von Daten ein „kryptografischer Fingerabdruck“ erzeugt, der deshalb zuverlässig ist, weil er aus einem unvorstellbar großen Zahlenraum „zufällige“ Identifikatoren errechnet. Diese können nicht zurückgerechnet werden, also die ursprünglichen Daten verraten.

Kryptografische Hashes kann ein einigermaßen modernes Mobiltelefon errechnen. Die Kommunikations-App *Signal.org* beispielsweise, macht das bereits mit den Telefonnummern im persönlichen Telefonbuch auf dem Mobiltelefon und verwendet die Hashes der Nummern, um herauszufinden, ob eine bestimmte Person bereits *Signal.org* verwendet. Durch die Verwendung von Hashes weiß *Signal.org* selbst nie, wer mit wem verknüpft ist.

Eine derartige Lösung wäre auch für eine CoViD-19-Kontakt-Tracking-App denkbar. Wenn jedes Mobiltelefon, das mit dieser App verwendet wird, beim Kontakt mit einem anderen Mobiltelefon nur dessen selbsterrechneten Hash verwendet und die beiden Hashes, den eigenen und den des Kontakts, an die zentrale Datenverwaltung der App sendet, dann werden keine persönlichen Daten gespeichert. In die Daten, die zu einem Hash verarbeitet werden, fügt jedes Mobiltelefon zusätzlich eine nur dem Mobiltelefon bekannten Zufallszahl sowie eine Zeitmarke ein, um das Pseudonym sicher zu schützen.

Ohne Mitwirkung der Betroffenen kann auch der Verlauf der Kontakte, also die Identifikation der Kontaktpersonen, nicht nachvollzogen werden. Es

Tracking: Die Kontakte könnten anonym über Hashes hergestellt werden.

darf dabei nicht die Telefonnummer des Senders oder andere identifizierende Daten mitgespeichert werden.

Wird nun ein positiver Virustest durchgeführt oder zweifelsfrei eine Infektion festgestellt, wird das zu dem Hash vermerkt. Da die App auf jedem Mobiltelefon regelmäßig mit der zentralen Datenbank kommuniziert und dabei den Status der Hashes von Kontaktpersonen überprüft, kann der Nutzer alarmiert werden, wenn eine Kontaktperson im gefährdenden Zeitraum positiv diagnostiziert oder erkrankt ist.

Unter der Prämisse, dass nur diese Hashes gespeichert werden, kann nur das Kontaktverhalten einer anonymisierten Person nachvollzogen werden, nicht aber eine oder mehrere der Personen identifiziert werden.

Verschiedene Maßnahmen zum weiteren Schutz der Pseudonyme sollten zusätzlich zum Einsatz kommen, sind aber hier nicht detailliert beschrieben, wie etwa Kollisions- und Fälschungsschutz, Passwort-Verwendung, Vermischung von echter Kommunikation und Scheinkommunikation, um Kontakthäufigkeiten, Positivmeldungen und Kontaktabfragen zu verschleiern.

Sollte es aus behördlichen Gründen die Notwendigkeit geben, eine bestimmte Person zu identifizieren, kann das wie bisher nur über eine Anfrage beim Mobilfunk-Provider unter den entsprechenden rechtlichen Voraussetzungen erfolgen, und nicht einfach durch Auslesen der Daten, die die App speichert. *Michael Werzowa*

Der Autor ist Experte für Netzwerk- und Datensicherheit, IoT Austria – The Austrian Internet of Things Network.

PSEUDONYMISIERUNG UND ANONYMISIERUNG

Unterschiede

Im Sinne des Datenschutzes müssen Daten für statistische Auswertungen oder die Verarbeitung im Bereich von „Big Data“ anonymisiert werden. Wichtig ist, dass das einfache Weglassen von Identifikatoren wie Namen, Versicherungsnummern, Mitgliedsnummern oder Ähnlichem nicht ausreichen muss, um Anonymität herzustellen. Ein Beispiel lässt sich schnell konstruieren: Wenn ein Mobilfunkbetreiber Bewegungsmuster von Personen anonymisiert weitergibt, muss dieser darauf achten, dass bestimmte Kennzeichen und Eigenschaften nicht bereits alleine für sich eine Identifikation einer Person ermöglichen. Wenn ein alleinstehender Hof, eine Berghütte oder ein Betriebsgelände derzeit nur von einer oder wenigen Personen frequentiert wird – Bauernfamilie, Hüttenwirtin oder Wachpersonal am Betriebsgelände – kann ein Bewegungsprofil leicht mit einer dieser Personen in Beziehung gebracht werden. Ebenso könnten Ärzte, Betreiber von Taxiservices oder Lieferdiensten leicht identifiziert werden. Daher müssen bei einer zuverlässigen Anonymisierung Daten, die sich einzeln abheben, entfernt werden: Wenn also in einer Funkzelle derzeit immer nur die gleichen zwei Mobiltelefone eingeloggt sind, müssen diese Daten ausgeschieden werden. Jedenfalls gilt, dass alle Informationen, die eine eindeutige Identifizierung einer Person ermöglichen, aus dem anonymisierten Datenbestand entfernt werden müssen, damit tatsächlich eine Anonymisierung erfolgt ist. Nur unter diesen Umständen ist eine Rückführung der Ergebnisse auf bestimmte Individuen nicht mehr möglich.

Pseudonymisierung. Im Sinne des Datenschutzes liegt eine Pseudonymisierung vor, wenn zwar eindeutige Kennzeichen vorhanden sind, diese aber nicht einer bestimmten Person zugeordnet werden können. Eine typische Pseudonymisierung kann durch die Auswahl eines selbstgewählten Kennzeichens erfolgen, das idealerweise eine möglichst zufällige Zeichenkette sein sollte. Der Sinn einer Pseudonymisierung liegt darin, auf die pseudonymisierten Daten weiterhin individuell zugreifen zu können, etwa, um sie zu verändern. Im Bereich der medizinischen Verwaltung werden sinnvollerweise pseudonymisierte Daten verwendet. Auch dabei ist darauf zu achten, dass nicht zu viele Daten unter einem Pseudonym zusammengefasst sind. Daher sollten lieber mehrere Pseudonyme für eine Person verwendet werden, sodass auch eine „Rasterung“ durch Zusammenführung aller Daten zu einem Pseudonym nicht mehr möglich ist. Eine geeignete technische Form der Pseudonymisierung ist die Verwendung von Hashes, die über Kennzeichen gerechnet werden. *Michael Werzowa*