
Zur Aktualität

Der gläserne Gast

Der Kanton Bern speichert Contact-Tracing-Daten von Restaurantbesuchern zentral ab – geliefert werden sollen sie von umstrittenen Apps. Mehrere Kantone wollen nun nachziehen. Aus Datenschutzsicht ist das verheerend.

Eine Recherche von [Adrienne Fichter](#) und [Florian Wüstholtz](#), 06.05.2021

Man kann an der Schweizer Pandemiepolitik vieles aussetzen: Den Datenschutz aber hat sie vorbildlich respektiert. Bis jetzt.

Erinnern Sie sich, wie zu Beginn der Pandemie heftig über die Contact-Tracing-App diskutiert wurde? Sie sollte datensparsam, freiwillig und dezentral funktionieren: Die Daten darüber, wer wen wo getroffen hat, sollten verschlüsselt auf den Smartphones bleiben, weder das Bundesamt für Gesundheit noch die Kantone sollten Zugriff darauf haben. Dies wurde sogar eigens im angepassten Epidemien-gesetz festgehalten, das die Grundlage für die App bildet.

Ein Jahr später werden diese hehren Grundsätze über Bord geworfen.

So entschied der Berner Regierungsrat letzte Woche, dass Restaurants, Bars und Clubs ab dem 10. Mai ihre Besucherdaten mit Check-in-Apps erfassen sollen. Und dass diese Daten permanent an eine zentrale Datenbank des Kantons übertragen werden sollen.

Bern schafft damit als erster Kanton eine gesetzliche Grundlage für die zentrale Speicherung von Kontaktdaten. Weitere Kantone sind kurz davor: In der Waadt und im Wallis gibt es zwar noch keine gesetzliche Regelung, doch die dortigen Gastroverbände schreiben die Nutzung von Apps wie «Social Pass» für den Restaurantbesuch vor.

Das Berner Modell

Wer ein Berner Restaurant besucht, muss nun also ab dem 10. Mai zwingend seine Kontaktdaten digital angeben. Eine analoge Variante auf Papier gibt es bald nur noch in Ausnahmefällen. Die Gastrobetriebe sollen die Daten der Besucherinnen täglich ans Gesundheitsamt des Kantons liefern, wo diese zentral gespeichert werden. Der Regierungsrat begründet dies damit, dass zuverlässige Kontaktdaten «aus epidemiologischer Sicht erforderlich» seien.

Vergangenes Jahr war mit «Lunchgate» bereits einmal eine Check-in-App mit einer sehr laschen Datenschutzpraxis aufgefallen. Warum nun der neue Fokus auf zentralisierte Datenbanken – und ausgerechnet in der Gastronomie?

Zum einen sind die Restaurantbesuche schlecht dokumentiert: viele Gäste hinterlassen Fantasienamen oder gar keine Kontaktdaten. Auch gehen

Listen verloren, oder sie sind unleserlich. Die Effektivität der Swiss-Covid-App ist zwar belegt, doch es harzt bei der Datenübertragung vor allem beim Faktor Mensch: Wenn die Gesundheitsämter mit der Ausstellung der Aktivierungscodes nicht nachkommen, wird niemand rechtzeitig gewarnt.

Zum anderen haben neuere Erkenntnisse zur Aerosol-Übertragung gezeigt, dass die 2-Meter-Regel nicht greift: *Alle* Personen, die sich in einem ungelüfteten Raum aufhalten, müssen benachrichtigt werden.

Deshalb ruhen die Hoffnungen beim Contact-Tracing also auf Check-in-Apps. In Bern können sich die Restaurants dabei aus einem bunten Strauss von Applikationen bedienen: «Social Pass», «Lunchgate», «Mindful» oder «Get-Entry» – der Branchenverband Gastro Suisse allein führt 16 verschiedene Apps auf seiner Website auf. Sie wurden allesamt weder öffentlichen Sicherheitstests unterzogen noch unabhängig auf Datenschutzrisiken überprüft, geschweige denn wurde der Quellcode publiziert. In der angepassten Berner Verordnung wird auch nichts dergleichen verlangt. Wie die Daten gesammelt und übertragen werden, ist Sache der Betriebe, solange sie täglich auf den Servern des Kantons landen.

Zum Vergleich: In Deutschland haben die Betreiber des dortigen Pendant – der viel kritisierten Luca-App – den Code publiziert. Prompt haben Security-Expertinnen entsprechende Sicherheitslücken entdeckt.

Diverse Kantone interessieren sich für das Berner Modell, bei dem der Kanton selbst eine Datenbank betreibt. Werden Restaurantbesucher damit zu gläsernen Bürgern? Nein, versichert der Sprecher des Berner Gesundheitsamts, Gundekar Giebel. «Es wird nur nach Betrieben, nicht nach Personennamen gesucht.» Doch eine technische Sicherheitshürde für personenbezogene Abfragen existiert nicht.

Sprich: Das Gesundheitsamt könnte also persönliche Bewegungsprofile erstellen – wenn es denn wollte.

Eine private Konkurrenzdatenbank

Als weitere Alternative zur datensparsamen offiziellen App des Bundes wird das Contact-Tracing seit Oktober auch von einer privaten Initiative vorangetrieben. Eine Gruppe von Gastroverbänden und App-Anbietern hat unter der Federführung von Jean-Paul Saija – Co-Chef der Firma Mindnow, deren Check-in-App «Mindful» bei über 6000 Gastrobetrieben im Einsatz ist – eine private Datenbank entwickelt: die «Swiss Contact Tracing Database».

Gemäss der Republik vorliegenden Dokumenten und öffentlich verfügbaren Informationen wäre diese Datenbank ein veritabler Datenschutzalbtraum: Besuchsdaten aus den führenden Schweizer Check-in-Apps flössen darin zusammen und liessen sich verschiedentlich analysieren: Es gäbe etwa eine Check-in-Historie der Besucherinnen, um *Forward Tracing*, *Backward Tracing* und Cluster-Erkennung zu ermöglichen. «Jeder Kanton könnte aus den Funktionen aussuchen und das verwenden, was für ihn Sinn ergibt», sagt Saija. Und er betont: Man lege hohen Wert auf Datenschutz und habe die Datenbank von externen Sicherheitsexperten prüfen lassen.

Bundesverwaltung und diverse Kantone haben Interesse an der Datenbank signalisiert. Das geht aus mehreren E-Mails und internen Dokumenten hervor, die der Republik vorliegen. Auch die Lobbyagentur Furrerhugi wirft sich dafür ins Zeug. Profitieren von einer Verbreitung würde unter anderem

die Firma Ticketcorner, die grösste Eventveranstalterin der Schweiz. Ihr gehört seit Dezember 2020 die App «Mindful».

Untersuchung gegen App-Anbieter Social Pass

Egal, ob sich die private Gastro-Lösung oder das Berner Modell durchsetzt: Mit der zentralen Datenspeicherung vollzieht sich ein Paradigmenwechsel.

Anders als beim Proximity-Tracing – das die Infektionswahrscheinlichkeit anhand von Distanzen misst – findet dazu aber keine politische Debatte statt. Reaktionen der netzpolitischen Zivilgesellschaft bleiben aus. Der Bundesrat gibt die Verantwortung an die Datenschutzbehörden ab: Diese sollen klären, ob die jeweiligen Apps die Privatsphäre achten oder nicht.

Mindestens bei einem Anbieter ist dies nicht der Fall. Die App «Social Pass», die bereits eine halbe Million Downloads verzeichnet, ist seit Dezember 2020 im Visier des eidgenössischen Datenschützers. Zurzeit findet eine «formelle Sachverhaltsabklärung» statt, wie Edöb-Sprecherin Silvia Böhlen bestätigt. Man untersuche Nutzungsbedingungen, die technische Sicherheit sowie die zentrale Datenhaltung. Die Ergebnisse dürften Signalwirkung haben.

Jean-Paul Saija, Co-Chef von Mindnow, sagt, eine dezentrale Lösung sei nicht automatisch besser als eine zentrale, insbesondere wenn Menschenleben und eine sichere Öffnung der Wirtschaft auf dem Spiel stünden. «Wir müssen solche Fragen ohne vereinfachende Schlagwörter sinnvoll abwägen. Es ist schade, dass wir diese Diskussion nicht sachlich führen können.»

Gefährliche Entwicklungen

Anders sieht dies Carmela Troncoso, Professorin an der Eidgenössischen Technischen Hochschule in Lausanne und Entwicklerin der Swiss-Covid-App. Sie ruft in einem Interview dazu auf, keine Infrastrukturen zur digitalen Überwachung aufzubauen, die womöglich unnötig und zeitlich nicht begrenzt sind sowie zweckentfremdet werden können.

Hintergrund von Troncosos Aufruf: Solche Strukturen wecken Begehrlichkeiten. Wie wird etwa sichergestellt, dass keine anderen Departemente und Behörden die Contact-Tracing-Daten für andere Zwecke nutzen – etwa für Ermittlungen der Polizei, wie bereits in Deutschland geschehen? De facto reicht ein Regierungsbeschluss, und die Daten werden plötzlich ganz anders als ursprünglich vorgesehen genutzt: zur Analyse, Prävention, Bestrafung.

Die Befürchtung, dass diese Daten auch in der Schweiz zweckentfremdet werden könnten, kommt nicht von ungefähr: In der Berner Verordnung steht nichts von der Vernichtung der Datenbank nach Pandemieende, ganz im Gegensatz zur Bundesverordnung zur Swiss-Covid-App.

Digitale Infrastrukturen sind wie Strassen, sagt die Datenschutzexpertin. Einmal gebaut, verschwinden sie nicht mehr.