



Handy-Tracking vs. Corona

(Stand 31.03.2020)

Die Corona-Pandemie ist beispiellos und es verwundert nicht, dass entsprechend unserer heutigen Möglichkeiten über eine digitale Bekämpfung nachgedacht wird. Hierbei rückt die zentrale Frage der Demokratie in den Vordergrund, inwieweit die Einschränkung von Freiheit unter der Zwecksetzung Sicherheit gehen kann.

Handy-Tracking im Kampf gegen Corona, was ist hierunter zu verstehen? Gemeint ist hiermit, dass staatliche Stellen Verkehrsdaten von Mobilfunkanbietern erhalten (d.h. Standortdaten, Datum/Uhrzeit Telefonnummer, Geräte-IDs, Kommunikationspartner), was beispielsweise die Erstellung von Bewegungsprofilen oder die Kontrolle der Einhaltung von Quarantänevorschriften ermöglichen soll.

Bestehende Rechtsgrundlage

Festzuhalten ist hierbei zunächst, dass das deutsche Recht die Erhebung von Standortdaten ohne Einwilligung des Betroffenen explizit lediglich im Rahmen der Strafprozessordnung zu repressiven Zwecken (§ 100g StPO) oder in den Polizeigesetzen der Länder zu präventiven Zwecken gestattet (z.B. § 31 e Polizei- und Ordnungsbehördengesetz Rheinland-Pfalz). Im Rahmen dieser Normen werden erhöhte Anforderungen für eine derartige Datenverarbeitung gestellt, was zum einen die europäische und bundesverfassungsrechtliche Rechtsprechung zur Vorratsdatenspeicherung aufgreift und zum anderen widerspiegelt, dass es sich hierbei um schwerwiegende und nicht mehr rückgängig zu machende Eingriffe in das Fernmeldegeheimnis sowie die informationelle Selbstbestimmung handelt.

Derartige Eingriffe sind auf das absolut Notwendige zu beschränken, da nicht zuletzt die Geschichte belegt, dass einmal erfolgte Freiheitsbeschränkungen nur bedingt wieder zurückgenommen werden. Hinzu kommt, dass derart weitreichende Datensammlungen wie sie bei der Sammlung von Verkehrsdaten entstehen auch Ziel von Hackern sein können und behördliche Fehler schnell Zugriff zu hochsensiblen personenbezogenen Daten gewähren würden. Insofern überrascht es nicht, dass die Erhebung von Verkehrsdaten zum Zwecke der Pandemiebekämpfung eine breite politische und gesellschaftliche Diskussion in Deutschland auslöst. Mit der zunächst insoweit zurückgestellten Gesetzesinitiative, im Rahmen der Änderung des Infektionsschutzgesetzes die Nutzung von Standortdaten bei der Änderung des Infektionsschutzgesetzes einzubeziehen, ist diese Diskussion noch nicht beendet.

Entwicklungen im Ausland

Südkorea, als eines der ersten Länder welches das Handytracking in der Corona-Krise genutzt hat, wird als Positivbeispiel für die Wirksamkeit zur Eindämmung unter Aufrechterhaltung des



öffentlichen Lebens genannt. Taiwan, Hongkong, Singapur und China beschreiten ähnliche, allerdings im Einzelnen dann doch unterschiedliche Wege. Allerdings wurden derartige Maßnahmen zu einem sehr frühen Zeitpunkt und eingebettet in andere einschneidende Maßnahmen eingesetzt. Hinzu kommt, dass in diesen Ländern nicht allein Verkehrsdaten von Handynutzern erhoben wurden, um die Kurve der Neuinfektionen zum Abflachen zu bringen. Laut Medienberichten wurden ebenso anderweitige Daten erhoben. In Südkorea sollen Bewegungsprofile aus Einreisedaten, Kreditkarteninformationen sowie GPS-Daten von Smartphones und Autos erstellt worden sein, um Infizierte zu überwachen. Auch Daten aus der Videoüberwachung kamen zum Einsatz sowie eine Website, die anzeigt, wo sich Infizierte in den vergangenen Wochen aufgehalten haben. In China kamen beispielsweise Apps zum Einsatz, die auf Basis von Datenauswertung den Gesundheitsstatus farbcodiert ausgaben und deren Vorzeigen nötig war, um Zugang zu U-Bahnen oder anderen öffentlichen Orten zu bekommen.

Andere Länder wie Österreich und Großbritannien gehen ebenfalls die zentrale Auswertung von Handydaten an. In Österreich hat das Rote Kreuz darüber hinaus eine „Stopp Corona-App“ entwickelt, um das Auffinden von Infizierten zu verbessern und Infektionsketten zu unterbrechen. Kernstück ist ein Kontakt-Tagebuch, in dem persönliche Begegnungen jenseits der engeren Familie mittels „digitalem Handshake“ anonymisiert gespeichert werden. Diese App soll ohne die Verarbeitung von personenbezogenen Daten funktionieren und ihre Installation und Nutzung erfolgt allein auf freiwilliger Basis.

Entwicklungen im Inland

In Deutschland übermittelte die Deutsche Telekom erstmals fünf Gigabyte Telefondaten an die Forscher des Robert-Koch-Instituts. Diese Übermittlung erfolgte auf freiwilliger Basis, anonymisiert und zu nicht-kommerziellen Zwecken entsprechend der aktuellen Datenschutzbestimmungen. Mit diesen Gruppen-Daten soll die Wirksamkeit der eingesetzten politischen Maßnahmen überprüft werden, einen darüber hinausgehenden Mehrwert liefern sie nicht, insbesondere sind sie aufgrund des nur grob erkennbaren Standorts für die Nachvollziehbarkeit individueller Kontakte und Infektionsketten ungeeignet.

Das Robert-Koch-Institut arbeitet aktuell an einer App, um auch individuelle Handydaten auswerten zu können. Diese soll allein auf „Einwilligungsbasis“ installiert werden und es ermöglichen, die Nähe und die Dauer des Kontakts zwischen Personen in den vergangenen zwei Wochen zu erfassen und auf dem Handy anonym abzuspeichern. Bislang ist allerdings nicht bekannt, wie genau eine derartige App konkret arbeiten soll.

Die App soll in der Nähe befindliche Mobiltelefone erkennen und diese für einen gewissen Zeitraum speichern. Dies ist möglich über die Bluetooth- und WLAN-Funktion; in diesem Zusammenhang wäre auch ohne GPS die Bestimmung von Standortdaten möglich (z.B. über das aktuelle WLAN-Netz in dem sich das Handy befindet). Da die App auf freiwilliger Basis eingesetzt werden soll, ist davon auszugehen, dass die für die gewünschte Zielsetzung nötige Funktionalität auf dem Handy aktiviert wird bzw. die App die dazu nötigen Berechtigungen erhält.



Jedes Handy verfügt über eine eindeutige Geräte-ID sowie weitere individuelle Kennungen, die ggf. ausgelesen werden können (Mac Adressen). Dies sind technische Angaben, über die jedoch ggf. ein Personenbezug hergestellt werden kann. Unklar ist gegenwärtig, wie im Fall einer Infektion oder eines Verdachts die zurückliegenden Handy-Kontakte informiert werden sollen. Unabhängig davon, wie die konkrete technische Ausgestaltung am Ende aussieht, ergeben sich fünf datenschutzrechtliche Kernanforderungen, denen Rechnung getragen werden muss:

- Die Freiwilligkeit der Teilnahme auf Basis einer informierten Einwilligung und eine jederzeitige Widerrufsmöglichkeit müssen gegeben sein,
- für die Bewegungs- und Kontaktdaten muss eine enge Zweckbegrenzung gelten,
- die bereitgestellten personenbezogenen Daten (Kontaktdaten, IDs, MAC-Adressen etc.) müssen wirksam pseudonymisiert und gesichert übertragen werden,
- die Lösung sollte soweit möglich auf einer dezentralen Speicherung auf den mobilen Endgeräten basieren,
- nach Ablauf der Quarantänefrist von 14 Tagen muss eine Löschung der Daten erfolgen.

Datenschutz vs. Gesundheitsschutz

Zum Zwecke des Gesundheitsschutzes erscheint es zunächst konsequent über eine „Nicht-Anonymisierung“ von Verkehrsdaten der Mobilfunkanbieter nachzudenken. Hierbei muss man sich allerdings fragen, ob dieser Zweck einen derart starken Eingriff in wesentliche Grundrechte wie das Fernmeldegeheimnis und das Datenschutzrecht rechtfertigt. Dabei ist zu überlegen, ob und inwieweit dieser Zweck noch konkretisiert werden kann. Unser Recht auf vertrauliche Kommunikation und darauf, selbstbestimmt zu entscheiden, mit wem wir unsere Daten teilen wollen, steht auf dem Spiel. Von daher stellt sich die Frage nach dem Nutzen einer derartigen Maßnahme. Schon die Geeignetheit bedarf eingehender Begründung.

Es fehlt bislang der Nachweis, dass individuelle Standortdaten der Mobilfunkanbieter einen Beitrag leisten könnten, Kontaktpersonen zu ermitteln. Die Daten der Mobilfunkanbieter würden auf Funkzellenabfragen basieren. Problematisch hieran ist, dass diese nur ungenaue Informationen liefern und den Standort einzelner Nutzer selbst in Großstädten, wo es mehr Funkmasten gibt, nur auf einige hundert Meter genau bestimmen können. Die Varianz liegt zwischen 100 m und 35 km. Um herauszufinden, wen eine infizierte Person möglicherweise angesteckt haben könnte, eignen sich diese Daten damit nicht.

Mit einem speziellen Verfahren, der sogenannten Triangulation, ließe sich der Aufenthaltsort genauer eingrenzen. Bei dieser Methode werden Daten mehrerer Mobilfunkmasten miteinander abgeglichen. Sie ist aber aufwendig und weniger exakt als GPS-Daten, die auf dem Handy selbst gespeichert werden. Hinzu kommt, dass sich aus der Erkenntnis welche Funkzellen genutzt worden sind, schwerlich herausfiltern lässt, wer mit der infizierten Person Kontakt hatte. Im Übrigen soll es auch Leute geben, die ihr Handy ausschalten, einen leeren Akku haben oder es einfach zuhause vergessen, was bei einem „aufgezwungenen Tracking“ wohl durchaus öfter der Fall sein würde. In die Betrachtung miteinzustellen ist daneben, dass ein Verkehrsdatenabruf eine



erhebliche Streubreite aufweist, da er neben der Zielperson des Auskunftersuchens auch deren Kommunikationspartner erfasst, also vielfach Personen, die keinen persönlichen Kontakt mit der infizierten Person hatten und damit nicht als Multiplikatoren für das Coronavirus in Betracht kommen. Im Ergebnis kann die Erhebung von Verkehrsdaten der Mobilfunkanbieter in dieser Form damit wohl nicht als effektives und erforderliches Mittel zur Bekämpfung der Pandemie gelten und es ist zu begrüßen, dass der Vorschlag zur Schaffung einer Ermächtigungsgrundlage im Infektionsschutzgesetz, die staatlichen Stellen die Rechtsgrundlage für den Abruf von Verkehrsdaten liefern sollte, nicht umgesetzt wurde.

Teils werden andere technische Maßnahmen vorgeschlagen, die auf eine temporäre Speicherung der Verkehrsdaten von Handys mittels Bluetooth hinauslaufen, die näher als 2m in Reichweite des speichernden Handys waren. Das System zur Kontaktnachverfolgung in Anlehnung an das Vorbild Singapur erfordert das Herunterladen einer App. Es werden sicher noch diese und andere Vorschläge diskutiert. Die Entscheidung des Gesetzgebers bei Schaffung einer Rechtsgrundlage muss in jedem Fall ebenso wohl abgewogen sein wie die Entscheidung der Nutzerin und Nutzer, ob sie eine entsprechende App nutzen möchten.