Presseinformation Forum Privatheit

2. April 2020

Handy-Daten für Kontaktverfolgung bei Corona: Vertrauen in staatliches Handeln ist in Krisenzeiten besonders wichtig

Aktuell wird in der Bundesrepublik Deutschland viel getan, um die Verbreitung des Corona-Virus einzudämmen. Unter anderem sind der Zugriff auf Mobilfunk-Ortsdaten und Apps für eine Kontaktnachverfolgung im Gespräch, um bei später festgestellten Infektionen die Kontakte informieren zu können. Jüngst wurden von der Initiative PEPP-PT Arbeiten an App-Komponenten vorgestellt. Eine voraussichtlich ab Mitte April verfügbare App soll eine datenschutzkonforme Kontaktnachverfolgung ermöglichen – ohne eine massenhafte Sammlung von Bewegungsdaten. Welche Fragen sich hier im Hinblick auf den Datenschutz stellen, erläutern Marit Hansen und Alexander Roßnagel vom BMBF-geförderten Forschungsverbund „Forum Privatheit“.

Um die Verbreitung des Corona-Virus einzudämmen, setzt das Robert Koch-Institut (RKI) unter anderem auf die Analyse der Bewegungsdaten von rund 46 Millionen Mobilfunkkundinnen und -kunden, bereitgestellt von der Deutschen Telekom. So sollen Erkenntnisse darüber gewonnen werden, ob die Maßnahmen des Bundes und der Länder zur Einschränkung der Mobilität der Bevölkerung Wirkung zeigen. Der Schutz der Gesundheit von Bürgerinnen und Bürgern ist zweifelsohne eine der wichtigsten staatlichen Aufgaben. Zugleich gelten aber die Grundsätze des Datenschutzes, um die Rechte und Freiheiten der Bürgerinnen und Bürger zu schützen. Marit Hansen, Leiterin des ULD Schleswig-Holstein, erläutert, warum dies in der aktuellen Krise ein Zielkonflikt sein kann: „Bewegungsdaten können unterschiedlich detailliert sein. Wenn es nur um Muster geht, wie sich große Ströme von Menschen bewegen, ist dies datenschutzrechtlich weniger kritisch als individuell zurechenbare Positionsbestimmungen. Mit dieser absichtlich eingeführten Unschärfe erfährt man nichts über die einzelnen Menschen. Im konkreten Fall hat der zuständige Bundesbeauftragte für den Datenschutz die Weitergabe der Daten in der gewählten Form für vertretbar gehalten.“

Die Herausgabe personenbezogener Daten erfordert eine Rechtsgrundlage

Das Datenschutzrecht setzt beim Personenbezug an und gilt nicht für vollständig anonyme Daten. Für alle personenbezogenen Daten – also auch ursprüngliche Telekommunikationsdaten – gelten die Datenschutz-Grundsätze. Das heißt insbesondere: Es ist eine Rechtsgrundlage nötig, es dürfen nur die für einen legitimen Zweck erforderlichen Daten in einem transparenten und sicheren Verfahren verarbeitet werden. Die Datenschutz-Grundsätze gelten auch in Krisenzeiten. „Der Zweck Infektionsschutz heiligt keineswegs alle Mittel“, so Hansen. Der Schlüssel liege in der Gestaltung. Wichtig sei auch, dass alle Maßnahmen geeignet, verhältnismäßig, überprüfbar und in der Zeit nach der Krise reversibel seien.

Bei Standort- und Bewegungsdaten ist eine effektive Anonymisierung nicht trivial

Besonders bei Standort- und Bewegungsdaten sei eine effektive Anonymisierung nicht trivial. Hansen nennt ein Beispiel: „Ein Nutzer, der sich morgens vom Ort A nach B, dann am späten Nachmittag weiter zu C und abends wieder zu A bewegt, wohnt vermutlich an Ort A, der Arbeitsort ist B, Einkaufen oder Freizeitgestaltungen wären dann bei C zu vermuten. Hat man genaue Ortsdaten, zum Beispiel per GPS, kann man in den meisten Fällen herausfinden, um wen es sich handelt. Bei unschärferen Daten – zum

Beispiel ‚irgendwo in dieser Funkzelle' – wird es schwieriger, den Personenbezug herzustellen." Unter der Unschärfe kann allerdings die Nutzbarkeit leiden – es wird daran geforscht, wie man gleichzeitig eine Anonymisierung und die Nutzbarkeit für den gewünschten Zweck erreicht.

Reine Bewegungsdaten sind für eine exakte Kontaktnachverfolgung ungeeignet

Hinzu kommt: Aggregierte Bewegungsdaten liefern zwar einige Hinweise, zum Beispiel wie viel weniger die Bevölkerung nun auf den Straßen oder im ÖPNV unterwegs ist. Für eine exakte Kontaktnachverfolgung sind solche Daten aber ungeeignet. Funktionieren könnten laut Hansen zum Beispiel Apps auf Basis des jüngst vorgestellten Verfahrens, bei denen eine Art elektronisches Tagebuch auf dem Handy gespeichert wird. Eine infizierte Person könnte dann dort nachsehen und die getroffenen Bekannten selbst informieren oder bei der Teilnahme an Veranstaltungen dem Gesundheitsamt Bescheid geben. Das Hochladen der eigenen Bewegungsdaten auf eine Datenanalyseplattform hingegen sei keine geeignete Lösung, so Marit Hansen, denn die Daten seien viel zu ungenau, um Kontakte im Nahabstand festzustellen, die zu einer Infektion geführt haben könnten. Das wiederum wäre aber möglich auf Basis von Bluetooth: In einer datenschutzfreundlichen Realisierung könnte eine App die möglicherweise Betroffenen informieren, ohne dass überhaupt Ortsdaten erfasst würden. Eine solche App ließe sich so gestalten, dass zentrale Datensammlungen vollständig vermieden würden und Unbefugte die Daten nicht auswerten könnten.

Vertrauen in staatliches Handeln kann diszipliniertes und vernünftiges Handeln unterstützen

Auch nach Ansicht von Alexander Roßnagel, Sprecher des Forschungsverbunds „Forum Privatheit" und Professor für Technikrecht an der Universität Kassel, sollte die Sammlung und Analyse von Massendaten auf ein mögliches Minimum beschränkt werden. „Gerade in Krisenzeiten ist es besonders notwendig, dass die Bürger dem Staat vertrauen. Dies können sie umso eher, je stärker er durch seine Regelungen zeigt, dass er ihre Grundrechte schützt und durch Gestaltungsmaßnahmen in Einklang mit anderen Zielsetzungen – wie jetzt der Virusbekämpfung – bringt", so Roßnagel. „Eine App, die freiwillig genutzt wird, die keine zentrale staatliche Datensammlung bewirkt, die auch ausschließt, dass Google oder Apple über ihre Betriebssysteme auf die Daten zugreifen können, die eine anonyme Information potenziell infizierter Personen bewirkt und nach kurzer Zeit die Kontaktdaten löscht, kann Virusbekämpfung und Grundrechtsschutz gleichzeitig bewirken. Dann werden die Menschen in einer offenen Demokratie in solchen Krisenzeiten eher zu diszipliniertem, vernünftigem und gemeinwohlorientiertem Verhalten bereit sein, als wenn sie einseitig orientiertem Handeln des Staates grundsätzlich misstrauen müssen."

Interview mit Marit Hansen: „Datenschutzgrundsätze gelten auch in Krisenzeiten"

Im Forum Privatheit setzen sich Expertinnen und Experten aus sieben wissenschaftlichen Institutionen interdisziplinär, kritisch und unabhängig mit Fragestellungen zum Schutz der Privatheit auseinander. Das Projekt wird vom Fraunhofer ISI koordiniert. Weitere Partner sind das Fraunhofer SIT, die Universität Duisburg-Essen, das Wissenschaftliche Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel, die Eberhard Karls Universität Tübingen, die Ludwig-Maximilians-Universität München sowie das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein. Das BMBF fördert das Forum Privatheit, um den öffentlichen Diskurs zu den Themen Privatheit und Datenschutz anzuregen.

Sprecher „Forum Privatheit“:
Prof. Dr. Alexander Roßnagel
Fachgebiet Öffentliches Recht
Universität Kassel
a.roßnagel@uni-kassel.de
Pressefoto Alexander Roßnagel

Partnerin „Forum Privatheit“:
Marit Hansen, Diplom-Informatikerin
Landesbeauftragte für Datenschutz Schleswig-Holstein
marit.hansen@datenschutzzentrum.de
Pressefotos Marit Hansen

Projektkoordination „Forum Privatheit“:
Dr. Michael Friedewald
Fraunhofer-Institut für System- und Innovationsforschung ISI
Competence Center Neue Technologien
michael.friedewald@isi-fraunhofer.de

Presse und Kommunikation „Forum Privatheit“:
Barbara Ferrarese, M.A.
Fraunhofer-Institut für System- und Innovationsforschung ISI
+49 (0) 0721 / 6809-678
barbara.ferrarese@forum-privatheit.de

„Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt“
https://www.forum-privatheit.de
Twitter: @ForumPrivatheit