Datenschutz versus Katastrophenschutz

Sebastian Bretthauer 2020-03-27T16:22:03

Einige Länder setzen Standortdaten jetzt schon gezielt ein, um die weitere Ausbreitung von Covid-19 einzudämmen. Ein Gesetzentwurf von Bundesgesundheitsminister *Jens Spahn*, der weitreichende Befugnisse vorsah, um mithilfe von Standortdaten Kontaktpersonen von Infizierten über deren Handys zu orten, stieß auf teilweise heftige Kritik. Der Gesetzentwurf wurde daraufhin zurückgezogen, ohne dass nähere Einzelheiten an die Öffentlichkeit gelangt sind. Ein genauer Blick zeigt jedoch, dass eine Verarbeitung von Standortgesundheitsdaten nicht nur tatsächlich nützlich sein kann, sondern auch rechtlich möglich ist.

Der Zweck entscheidet

Die Deutsche Telekom hat dem Robert Koch-Institut (RKI) bereits zwei Massendatensätze mit Standortdaten zur Verfügung gestellt. Diese Daten seien allesamt anonymisiert, sodass keine Rückschlüsse auf einzelne Nutzer möglich seien. Der Bundesdatenschutzbeauftragte, *Ulrich Kelber*, ließ über seinen Twitter-Account mitteilen, dass „die Weitergabe von Standortdaten durch die Deutsche Telekom an das Robert-Koch-Institut […] in der gewählten Form datenschutzrechtlich vertretbar [ist]“. In Folge dessen kamen erste Überlegungen auf, ob nicht mithilfe der generellen Zurverfügungstellung solcher Daten eine gezieltere und effektivere Bekämpfung der Corona-Pandemie möglich sei.

Der Einsatz von Standortdaten würde jedenfalls dann Sinn machen und einen echten Mehrwert stiften, wenn bekannt ist, dass sich eine infizierte Person zu einem bestimmten Zeitpunkt an einem konkreten Ort aufgehalten hat. Hat man darüber hinaus auch noch die Standortdaten sämtlicher anderer und bisher nicht infizierter Personen, so ließe sich über diese Angaben feststellen, ob die erkrankte Person mit weiteren Personen potentiell in Kontakt gekommen ist.

Die Daten könnten darüber hinaus aber auch noch für einen weiteren Zweck genutzt werden. So ließe sich mit der Datensammlung über die Bewegungsströme die Ausbreitung der Corona-Viren wesentlich besser nachverfolgen. Aber auch dies verlangt wenigstens, dass die infizierten Personen und deren Kontaktpersonen in den Datensätzen erkennbar sind. Denn damit könnten die mathematischen Modelle zur besseren Vorhersage der künftigen Ausdehnung der Corona-Pandemie angereichert werden und so passgenauere Vorhersagen ermöglichen. Eine exaktere wissenschaftliche Bewertung führt am Ende zu einer insgesamt besseren und wirksameren Bekämpfung der Corona-Pandemie für die Gesamtheit. Und damit letztendlich auch zu weniger Todesfällen.

Beide Zwecke in ihrer jeweiligen konkreten Ausgestaltung erweisen sich aber als besonders grundrechtsintensiv, da es nicht nur möglich wäre, umfassende Bewegungsprofile zu erstellen, sondern geradezu bezweckt wird. Eine solche Gestaltung ist darum überhaupt nur in besonders engen rechtsstaatlichen Grenzen möglich.

Rechtsanforderungen an die Standortdatenverarbeitung

Bei allen pandemischen Schrecknissen müssen grundlegende Werte beachtet werden. Dabei versteht sich von selbst, dass die Verarbeitung von Standortdaten einen besonders schwerwiegenden Grundrechtseingriff in fundamentale Grundrechte (Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG, Art. 8 GRCh) darstellt. Aber schon heute kennt das Recht – beispielsweise im Rahmen der Gefahrenabwehr (vgl. § 15a Abs. 3 HSOG) oder der Strafverfolgung (vgl. §§ 100g, i StPO) – Möglichkeiten, in engen, vom Gesetz definierten Grenzen, Standortdaten zu verarbeiten.

Gleichzeitig ist der Staat aber auch verpflichtet, seine Bürgerinnen und Bürger in Krisen- und Katastrophenzeiten effektiv zu schützen. Der Schutz der Gesundheit der gesamten Bevölkerung und nicht nur ausschließlich des Individuums muss besondere Bedeutung erlangen. Der Staat hat eine Schutzpflicht (Art. 2 Abs. 2 S. 1 GG, Art. 6 GRCh), die von ihm verlangt, die notwendigen Maßnahmen zu treffen. Auch hier kennt das Recht schon Maßnahmen, die dem Gesundheitsschutz der gesamten Bevölkerung dienen (vgl. etwa die Meldepflichten nach §§ 6 ff. IfSG).

In diesem Spannungsfeld ist also die Frage nach der Verarbeitung von Standortdaten angesiedelt.

Die Mär von anonymen Daten

Das Datenschutzrecht ist nur beim Vorliegen personenbezogener Daten anwendbar. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DSGVO). Dabei ist der Begriff weit auszulegen, wie schon das Bundesverfassungsgericht (BVerfG) im Volkszählungsurteil („Es gibt kein belangloses Datum“, Rn. 158) sowie auch der Europäische Gerichtshof (EuGH, Urt. v. 19.10.2016 – C-582/14, Rn. 38 ff.) konstatiert haben.

Nun wird hinsichtlich der Standortdaten zur Bekämpfung der Corona-Pandemie oftmals vorgetragen, dass es sich um anonyme Daten bzw. aggregierte Daten handele. Dementsprechend seien die datenschutzrechtlichen Vorschriften nicht anwendbar – was rechtlich so auch zutrifft (vgl. EG 26 S. 4 DSGVO und EG 162 S. 5 DSGVO). Allerdings ist die Vorstellung von anonymen Daten – und das gilt auch für aggregierte Daten – unter den heutigen Bedingungen moderner Daten- und Informationsverarbeitung im Zeitalter von BigData nur noch eine reine Illusion. Wissenschaftlerinnen und Wissenschaftler haben schon mehrfach nachgewiesen,

dass vermeintlich anonyme Daten de-anonymisiert werden können und vormals als verheißungsvoll angepriesene Anonymisierungsverfahren nachträglich versagen.

Im Übrigen fallen Standortdaten *de lege lata* schon in den Anwendungsbereich der datenschutzrechtlichen Vorschriften. Denn Art. 4 Nr. 1 DSGVO spricht ausdrücklich davon, dass „als identifizierbar […] eine natürliche Person angesehen [wird], die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie […] zu Standortdaten […], identifiziert werden kann“. Demnach muss sich die Auswertung der Standortdaten der mit Corona infizierten Personen als auch deren Kontaktpersonen an den datenschutzrechtlichen Vorschriften messen lassen. Gleiches gilt aber auch, wenn man die Standortdaten zur Verbesserung der Modellvorhersagen hinsichtlich der Ausbreitung der Corona-Pandemie einsetzen möchte. Denn diese Modelle können wesentlich genauere Vorhersagen treffen, wenn man bei ihnen ebenfalls bestimmen kann, welche Personen mit Corona infiziert sind und bei welchen Personen es sich um Kontaktpersonen handelt. Auch hier gilt, dass es keine anonymen Daten mehr gibt.

Die Metamorphose der Standortdaten

Standortdaten sind ganz allgemein Daten, die den Standort des Endgeräts eines Endnutzers eines öffentlich zugänglichen Telekommunikationsdienstes angeben. Dass die Europäische Datenschutzgrundverordnung (DSGVO) gegenüber dem Telekommunikationsgesetz (TKG) anwendbar ist, ist zwar auf den ersten Blick nicht offensichtlich, ergibt sich allerdings bei näherer Betrachtung aus Art. 95 DSGVO, da TKG und DSGVO im Bezug auf die vorliegende Standortdatenverarbeitung unterschiedliche Ziele verfolgen. Eine Datenverarbeitung ließe sich darum generell auf die Ermächtigungsgrundlagen nach Art. 6 Abs. 1 lit. a – lit. f DSGVO stützen.

Allerdings werden die Standortdaten nun aber mit dem Wissen angereichert, dass es sich entweder um eine mit dem Corona-Virus infizierte Person handelt oder eben nur um eine Kontaktperson, die ihrerseits aber noch gesund ist. Die zunächst für sich allein „unscheinbaren“ Standortdaten werden also um die Information ergänzt, dass eine Person krank oder gesund ist. Dieser neue Verwendungskontext lässt die Standortdaten zu einer besonderen Kategorie personenbezogener Daten werden, da nunmehr Gesundheitsdaten über die betroffenen Personen vorliegen. Denn Gesundheitsdaten sind personenbezogene Daten, die sich auf die körperliche Gesundheit einer natürlichen Person beziehen und aus denen Informationen über den Gesundheitszustand hervorgehen (vgl. Art. 4 Nr. 15 DSGVO). Davon erfasst sind auch positive oder neutrale Informationen zum Gesundheitszustand, also auch solche Informationen die generell beschreiben, dass eine Person gesund ist. Für die Kombination aus Standortdaten und Gesundheitsdaten – die so nun generierten „Standortgesundheitsdaten“ – müssen deshalb besonders hohe datenschutzrechtliche Anforderungen gelten.

Rechtskonforme Standortgesundheitsdatenverarbeitung

Eine Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) aller Nutzer von Mobiltelefonen einzuholen, ist rechtlich denkbar, dürfte aber schon aus rein tatsächlichen Gründen scheitern. Eine Ermächtigung für die Verarbeitung der Standortgesundheitsdaten kann sich aber auch aus Art. 9 DSGVO ergeben. Auch der Europäische Datenschutzbeauftragte, *Wojciech Wiewiórowski*,formulierte das schon so, wenn auch in allgemeinerer Form. In die gleiche Richtung geht eine Stellungnahme des Europäischen Datenschutzausschusses. Als Rechtsgrundlagen kommen insbesondere Art. 9 Abs. 2 lit. h DSGVO sowie Art. 9 Abs. 2 lit. i DSGVO in Betracht.

Beide Normen setzen ihrerseits voraus, dass die Datenverarbeitung in einer spezifischen Rechtsgrundlage im Unionsrecht oder nationalen Recht normiert ist. Weder im europäischen noch im deutschen Recht gibt es bisher eine derartige Rechtsgrundlage. Eine solche zu schaffen wäre aber – wie sich im Folgenden zeigen wird – rechtlich möglich.

Art. 9 Abs. 2 lit. h DSGVO kommt zunächst dann in Betracht, wenn die Verarbeitung der Standortgesundheitsdaten für Zwecke der Gesundheitsvorsorge oder die Versorgung oder Behandlung im Gesundheitsbereich erforderlich ist. Die Regelung normiert insbesondere solche Datenverarbeitungen, die im weitesten Sinne im Zusammenhang mit der Gesundheitsversorgung des Individuums stehen.

Der Einsatz der Standortgesundheitsdaten zur Bekämpfung der Corona-Pandemie lässt sich darum nur schwer mit der Intention von Art. 9 Abs. 2 lit. h DSGVO in Einklang bringen. Denn die Standortgesundheitsdaten werden verarbeitet, um insbesondere Personenbewegungen nachvollziehen zu können, sodass mit diesen Daten einerseits mögliche Kontaktpersonen von mit Corona infizierten Personen ausfindig gemacht werden können und andererseits die mathematischen Modelle zur Vorhersage der Ausbreitung des Virus verbessert werden können. Der individuelle Schutz, den Art. 9 Abs. 2 lit. h DSGVO adressiert, steht aber bei der Standortgesundheitsdatenauswertung nicht im Vordergrund der Maßnahme, da sie primär der Bevölkerungsgesundheit insgesamt dienen soll.

Vielmehr lässt sich eine Auswertung der Standortgesundheitsdaten aber auf Art. 9 Abs. 2 lit. i DSGVO stützen. Demnach ist eine Verarbeitung möglich, wenn sie aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren, erforderlich ist.

Generell sind damit Maßnahmen gemeint, die Gefahren für die öffentliche Gesundheit oder Gesundheitsrisiken abwehren sollen. Der Begriff der öffentlichen Gesundheit ist im Sinne von Art. 3 lit. c VO (EG) 1338/2008 zu verstehen (EG 54 S. 3 DSGVO), sodass „alle Elemente im Zusammenhang mit der Gesundheit“ hiervon erfasst werden. Er ist also weit auszulegen. In erster Linie dient Art. 9 Abs. 2 lit. i DSGVO dazu, Maßnahmen zum Gesundheitsschutz der Bevölkerung zu ermöglichen. Das Erforderlichkeitskriterium kommt schließlich als einschränkendes

Korrektiv zur Geltung. Dass die Corona-Pandemie eine schwerwiegende grenzüberschreitende Gesundheitsgefahr darstellt, bedarf angesichts der aktuellen Entwicklungen und Grenzschließungen weltweit keiner besonderen Begründung.

Gleichwohl mag es befremdlich anmuten, wenn ursprüngliche Standortdaten zum Gesundheitsschutz beitragen sollen. Klassischerweise werden hier nämlich Maßnahmen wie etwa Meldepflichten von besonders schweren Krankheiten nach §§ 6 ff. IfSG erfasst. Allerdings schaffen die heutigen technischen Gegebenheiten eben auch neue Möglichkeiten und Methoden, um Gesundheitsgefahren und -risiken auf neuen und teilweise noch unkonventionellen Wegen vorzubeugen und effektiv zu bekämpfen. Durch die Standortgesundheitsdaten von infizierten Personen können deren Kontaktpersonen ermittelt werden und gleichzeitig damit verbunden auch die mathematischen Modelle zur Vorhersage der weiteren Ausbreitung der Corona-Pandemie wesentlich verbessert werden. Diese Ergebnisse können sodann direkt in unmittelbare Maßnahmen zur Abwehr von Gefahren für die öffentliche Gesundheit einfließen und insgesamt zu einer wesentlich besseren Steuerung in der Corona-Pandemie Krise beitragen.

Flankierende Maßnahmen zum Schutz der informationellen Selbstbestimmung

Gleichwohl müssen daneben angemessene und spezifische Maßnahmen getroffen werden, um die Rechte und Freiheiten der betroffenen Personen zu wahren (Art. 9 Abs. 2 lit. i DSGVO).

Im Rahmen einer derartig sensiblen Datenverarbeitung müssen die datenschutzrechtlichen Grundsätze (Art. 5 DSGVO) eingehalten werden und hierfür besonders hohe Schutzstandards gelten. So ist sicherzustellen, dass die verarbeiteten Standortgesundheitsdaten ausschließlich für die Gefahrenabwehr gegen die Corona-Pandemie eingesetzt werden, um also Kontaktpersonen ausfindig zu machen und die mathematischen Modelle zur Vorhersage der weiteren Ausbreitung des Virus zu verbessern. Die strenge Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO) der Datenverarbeitung muss also durchgehend sichergestellt werden.

Besonders bedeutsam ist, dass die Standortgesundheitsdaten nach ihrer Zweckerreichung – spätestens also, wenn die Corona-Pandemie gebannt ist – gelöscht werden müssen. Deshalb sollte eine konkrete Frist festgelegt werden, beispielsweise eine dreimonatige Frist, die nochmals verlängert werden kann, wenn besondere Voraussetzungen vorliegen. Eine generelle Bevorratung dieser Standortgesundheitsdaten kommt ohnehin nicht in Betracht und würde auch schon jetzt gegen deutsches und europäisches Recht verstoßen.

Die Standortgesundheitsdaten müssen ferner transparent verarbeitet werden (Art. 5 Abs. 1 lit. a DSGVO). Die betroffenen Personen müssen ihre Rechte nach Art. 12 ff. DSGVO wirksam ausüben können, womit gleichzeitig auch Informationspflichten (Art. 14 DSGVO) des Datenverarbeiters – also des RKI – einhergehen. Hier sind transparente und leicht verständliche Erklärungen notwendig. Auch sind Ressourcen

vorzuhalten, um die Betroffenenrechte – etwa Auskunftsrechte (Art. 15 DSGVO) – effektiv erfüllen zu können.

Ferner sind besonders hohe Anforderungen bei der Sicherheit der Datenverarbeitung zu gewährleisten (Art. 32 DSGVO). So sind die Daten idealerweise zu pseudonymisieren und zu verschlüsseln. Dabei ist denkbar, dass die Standortgesundheitsdaten verschlüsselt abgelegt werden und der Schlüssel dazu auf mehrere Institutionen verteilt wird. Nur wenn alle beteiligten Akteure zustimmen, ist eine Verarbeitung dann denkbar.

Daneben sind die Datenschutzbeauftragten als unabhängige Stellen zu beteiligen. Ihnen sind umfangreiche Mitwirkungsrechte einzuräumen, um die Einhaltung der Vorschriften parallel zur Datenverarbeitung kontrollieren zu können. Neben dieser Kontrollfunktion sollten sie auch eine aktive Beratungsfunktion einnehmen dürfen, die neben rechtlicher Expertise auch das technische Wissen beisteuern kann. Als zusätzliche Absicherung wäre darüber hinaus denkbar, eine Standortgesundheitsdatenverarbeitung generell unter Richtervorbehalt zu stellen.

Schließlich ist nach erfolgreich überstandener Corona-Pandemie Krise zu evaluieren, ob und in welchem Maße die Auswertung der Standortgesundheitsdaten dazu beigetragen hat, die Ausbreitung des Virus einzuhegen. Hier bietet es sich an, eine Expertenkommission einzusetzen.
