Nr. 435 / April 2021
Analysen & Argumente

KONRAD ADENAUER STIFTUNG

Das uneingelöste Versprechen?

Daten, die Lockdowns hätten verhindern können

Pencho Kuzev

- Es gibt kein demokratisches Land auf der Welt, in dem allein Tracing-Apps zu spürbaren positiven Effekten im Kampf gegen Corona geführt haben.
- Vergleiche mit asiatischen Ländern führen nicht weiter und blenden oft wichtige Tatsachen aus. Taiwan etwa nutzt gar keine Contact-Tracing-App, während die Überwachungsmethoden in Südkorea nicht im Einklang mit unserer Rechtsordnung und unseren demokratischen Prinzipien stehen.
- Die von Apple und Google bestimmte Ausgangslage zum Design weltweit genutzter Corona-Apps macht die Kontaktnachverfolgung *de facto* unmöglich. Der sogenannte dezentrale datenschutzakzeptierte Ansatz schützt zwar die Privatsphäre der Menschen, liefert jedoch keine Erkenntnisse, die Fachleute des öffentlichen Gesundheitswesens und der Wissenschaft benötigen.
- In dieser Pandemie erleben wir das *Privacy Paradox* immer wieder. Den demokratisch legitimierten Organen ist es verwehrt, für einen eindeutig definierten Zweck, mit allen rechtsstaatlichen Garantien, die Standortdaten und die zentrale Datenspeicherung zu nutzen.
- Der Datenschutzton in dieser Pandemie ist leider nicht unbedingt kohäsiv. Dem Rechtsrahmen ist das nicht geschuldet.

Inhaltsverzeichnis

Einleitung

Datenbasierte Innovationen könnten zur Bekämpfung von Covid-19 beitragen – davon sind bis heute viele überzeugt. Doch nach mehr als einem Jahr Pandemie macht sich Ernüchterung breit: Weder ist man in Deutschland mit dem implementierten Modell der Corona-Warn-App zufrieden noch wurde in irgendeinem demokratischen Land eine Alternative entwickelt, die positive Effekte auf das Infektionsgeschehen gehabt hätte.

Kontaktverfolgungsinstrumente, die ihrem Namen gerecht werden

Unmittelbar nach Ausbruch der Pandemie implementierten mehrere asiatische Länder Kontaktverfolgungsinstrumente – sogenannte Tracing Apps, die ihrem Namen gerecht wurden. Unter Zuhilfenahme entsprechender QR-Codes, Tokens (Singapure), Check-In-Systeme, Überwachungskameras, GPS-Signale, Verkehrs- oder Kreditkartendaten (Südkorea) ermöglichten sie Rückschlüsse, wer, wann, wo das Virus verbreitet hat. Unbestritten ist jedoch, dass die so konzipierten Instrumente ein Missbrauchspotential haben und zu massiven Grundrechtseinschränkungen führen.

Die folgende Analyse dokumentiert im *ersten* Schritt die Bemühungen der Bundesregierung, mit dem Einsatz von digitalen Instrumenten zur Eindämmung der Pandemie beizutragen. Zugleich wird daran erinnert, was im bisherigen Pandemieverlauf nicht umgesetzt wurde. Rückblickend wird die Rolle der relevanten Protagonisten analysiert. Der *zweite* Teil widmet sich einer kritischen Würdigung der Bemühungen in Großbritannien und Australien. Es wird die Rolle der marktbeherrschenden Betriebssysteme von Google (Android) und Apple (iOS) beschrieben und deren Einfluss auf die weltweite Entwicklung von Tracing-Apps. *Abschließend* wird in politischen Handlungsempfehlungen formuliert, wie man den datenschutzpolitischen Diskurs in Deutschland versöhnen kann.

Die Verarbeitung personenbezogener Daten im Dienste der Menschheit

Das Recht auf Schutz der personenbezogenen Daten muss im Hinblick auf seine gesellschaftliche Funktion gesehen werden.

Bereits bei der Einführung der Datenschutz-Grundverordnung (DSGVO) stellte der europäische Gesetzgeber klar, dass „die Verarbeitung personenbezogener Daten im Dienste der Menschheit stehen sollte." Das Recht auf Schutz der personenbezogenen Daten ist kein uneingeschränktes Recht; es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden.[1] In Deutschland ist immer wieder der Eindruck entstanden, dass der Datenschutz ausgerechnet diese gesellschaftliche Funktion nicht erfüllt. Das ist jedoch nicht dem Rechtsrahmen geschuldet.

Ein Jahr nach Ausbruch der Pandemie hält die kontroverse Diskussion über die Rolle der Corona-Warn-App an. Viele sehen die Ursachen für ihre eingeschränkte Wirkung in einem

rigide umgesetzten Datenschutz.[2] Der Vorwurf lautet, die Datenschutzbehörden seien für die Ineffektivität der App verantwortlich, eine Kritik, die von prominenten Datenschützern postwendend zurückgewiesen wurde.[3]

Die DSGVO und der Kampf gegen die Pandemie – Kein Widerspruch

Trotz mancher Kritik an der DSGVO ist sie eine solide Grundlage für die gesellschaftliche Herausforderung unserer Zeit. Bereits im Gesetzgebungsprozess war man sich darüber im Klaren, welche Bedeutung Daten in einer Pandemie haben.[4]

Die DSGVO nimmt einen direkten Bezug auf eine pandemische Lage.

Ist die Verarbeitung von Daten zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erforderlich, braucht es dafür eine Grundlage im Unionsrecht oder im Recht eines Mitgliedstaats. Als Rechtsgrundlage für die Auswertung von Standortdaten zur Bekämpfung des Corona-Virus kommen mehrere rechtliche Vorgaben in Betracht: allen voran die Einwilligung zur Verarbeitung von Daten zum Schutz lebenswichtiger Interessen oder aufgrund des öffentlichen Interesses im Bereich der öffentlichen Gesundheit. Nach der DSGVO sollten personenbezogene Daten grundsätzlich nur dann wegen eines lebenswichtigen Interesses einer anderen Person verarbeitet werden, wenn dafür keine weitere Rechtsgrundlage herangezogen werden kann.[5] Mit etwa 15.000 Neuinfektionen pro Tag ist diese Hürde zweifelsohne genommen. Hinsichtlich der Erforderlichkeit nimmt die DSGVO sogar direkten Bezug auf eine pandemische Lage: So kann „die Verarbeitung (von Daten) für humanitäre Zwecke einschließlich der Überwachung von Epidemien und deren Ausbreitung (…) erforderlich sein."

Erforderlichkeit der Datennutzung

Gestützt auf diese Grundlagen, versuchte die Bundesregierung im März 2020 den datengetriebenen Kampf gegen die Pandemie durch gesetzliche Maßnahmen noch präziser zu gestalten. Doch der Versuch, die Arbeit der Gesundheitsbehörden zu erleichtern, scheiterte an massiven Widerständen in manchen gesellschaftlichen Kreisen und in der Politik[6]. Es fehlte die Überzeugung, dass die Nachverfolgung von Standortdaten einen Beitrag zur Bestimmung von Kontaktpersonen leistet[7], und dass eine solche Maßnahme durchaus im Geiste der DSGVO sein könnte. So hielt der Bundesbeauftragte für den Datenschutz, Ulrich Kelber, einen staatlich erzwungenen Zugriff auf die Handydaten von Infizierten für mehr als problematisch[8]. Neben der Frage, auf welcher Rechtsgrundlage ein entsprechendes Vorgehen erfolgen solle, müsse auch die Verhältnismäßigkeit des Eingriffs hinterfragt werden. Zu rechtfertigen sei eine derartige Maßnahme nur mit Zustimmung der Betroffenen, so Kelber weiter im Interview mit dem *Tagesspiegel*.

Infektionsschutzgesetz und die Nachverfolgung von Standortdaten

Mit eindeutigem Verweis auf die Erfahrungen in asiatischen Ländern legte das Bundesgesundheitsministerium den Entwurf des Infektionsschutzgesetzes (IfSG) vor. Darin hieß es: „Internationale Erfahrungen etwa im Rahmen der südkoreanischen Maßnahmen zur Eindämmung von Covid-19 zeigen, dass die Nachverfolgung von Standortdaten einen Beitrag zur Bestimmung von Kontaktpersonen leisten kann." Im Mittelpunkt des Gesetzesentwurfs stand § 5 IfSG-E mit der Überschrift „Epidemische Notlage von nationaler Tragweite, Verordnungsermächtigungen".[9] Die folgenden Regelungen mussten aufgrund vielfachen Widerspruchs ersatzlos gestrichen werden. Vollständigkeitshalber sei an dieser Stelle darauf hingewiesen:

> *„Für den Fall einer epidemischen Lage (…) kann die zuständige Behörde zum Zwecke der Nachverfolgung von Kontaktpersonen technische Mittel einsetzen, um Kontaktpersonen von erkrankten Personen zu ermitteln, sofern aufgrund epidemiologischer Erkenntnisse gesichert ist, dass dies zum Schutz der Bevölkerung vor einer Gefährdung durch schwerwiegende übertragbare Krankheiten erforderlich ist. Unter den Voraussetzungen nach Satz 1 kann die zuständige Behörde* von jedem (…) Dienstanbieter *die Herausgabe der vorhandenen Verkehrsda-*

ten, der für die Ermittlung des Standortes eines Mobilfunkgerätes erforderlichen spezifischen Kennungen und die (…) erforderlichen Daten der möglichen Kontaktpersonen von erkrankten Personen verlangen.[10] ***(…) Die zuständigen Behörden dürfen zu diesem Zweck personenbezogene Daten verarbeiten (…).“***

Zu diesem Zweck ist es ausreichend, dass die Dienstanbieter die Verkehrsdaten, die spezifischen Kennungen sowie Daten zur Verfügung stellen, die eine **Kontaktaufnahme zu betroffenen Personen ermöglicht**. Die Begründung stellt auch klar, dass von der Befugnis **keine Inhaltsdaten und keine Kommunikationsinhalte erfasst werden.**

Diese ursprünglich formulierte Regelung steht durchaus im Einklang mit der DSGVO. Sie stellte eine Befugnis zur Datenverarbeitung nach Artikel 6 Absatz 1 Buchstabe d und 2 sowie Artikel 9 Absatz 2 Buchstabe i DSGVO dar. Zwar können die Telefon-Standortprotokolle von Mobilfunkbetreibern keine hundertprozentige Genauigkeit liefern. Sie können jedoch in Verbindung mit anderen Daten für Modellanalysen und die Kontaktverfolgung nützlich sein – wie in Südkorea erfolgreich praktiziert.

Die Corona-Warn-App wurde bewusst nicht als Geo-Tracking-App entwickelt

Es mag verwundern, aber eine Standortverfolgung war nie erklärtes Ziel[11] bei der Konzipierung der Corona-Warn-App. Selbst wenn die Bundesregierung es gewollt hätte, eine Standortverfolgung ist mit Apple und Google nicht realisierbar. Dieser Aspekt kommt in der öffentlichen Diskussion kaum zur Sprache. Die Ausgangslage zum Design weltweit zum Einsatz kommender Corona-Apps ist wie folgt: Eine App zur Ermittlung von Kontaktpersonen **darf keine standortbasierten APIs verwenden, darf keine Bluetooth Funktionalität verwenden und darf keine Geräteinformationen sammeln, mit denen der genaue Standort von Benutzern zu identifizieren wäre**. So die Regelung in den Richtlinien von Apple[12]. Mit anderen Worten, alle Regierungen mussten ihre Corona-Warn-Apps entsprechend den Leitlinien der marktbeherrschenden Betriebssysteme konzipieren. Länder, die aus guter Überzeugung einen eigenständigen Weg gegangen sind, wie Australien und Großbritannien, konnten die technischen Barrieren der Gatekeeper Google und Apple nicht überwinden.

Die von Apple & Google bestimmte Ausgangslage zum Design der Corona-Apps

Privacy Paradox auch zu Pandemiezeiten

Während Google und Apple die Standortdaten uneingeschränkt für die eigenen kommerziellen Dienste nutzen, für beliebige Zwecke weiterverwerten und die Nutzer das stillschweigend zur Kenntnis nehmen, erleben wir am Beispiel der Corona-Warn-App, wie sich das *Privacy Paradox* wiederholt. Für einen eindeutig definierten Zweck, mit allen rechtsstaatlichen Garantien war und bleibt die Nutzung der Standortdaten und die zentrale Datenspeicherung den demokratisch legitimierten Organen verwehrt.

Eine Studie des US-Telekommunikationsunternehmens Cisco, die im vergangenen Jahr mit mehr als 2.600 Erwachsenen weltweit durchgeführt wurde, ergab, dass etwa ein Drittel der Befragten „datenschutzaktiv“ ist. Darunter sind Nutzerinnen und Nutzer zu verstehen, die aufgrund der Datenrichtlinien der Unternehmen Maßnahmen wie den Wechsel des Dienstanbieters ergreifen. Interessanterweise ist diese Gruppe mit Kompromissen einverstanden, z. B. mit der Weitergabe ihrer Kaufhistorie im Austausch für personalisierte Produkte und Dienstleistungen sowie der Weitergabe von Informationen aus Smart-Home-Lautsprechern im Austausch für Gesundheits- und Sicherheitswarnungen für die ganze Familie.[13]

Ein Reminder für eine nächste Pandemie

Keine Analysen möglich, die zu effektiveren politischen Reaktionen auf COVID-19 führen könnten

Es gibt im Wesentlichen zwei Arten von Ansätzen zur Nachverfolgung von Virus-Kontakten: dezentralisierte und zentralisierte.[14] **Epidemiologisch entscheidend ist zu wissen, wo Kontakte bzw. Ansteckungen stattfinden.** In dieser Krise wissen wir das oft nicht. Die Information, ob man eine infizierte Person im Supermarkt oder in der Buchhandlung getroffen hat, hat epidemiologisch einen Mehrwert[15], die die Datenschutzaufsicht in Deutschland scheinbar nicht nachvollziehen kann. Wenn man erfassen würde, wer sich an welchen Orten infiziert, wären Analysen möglich, die zu effektiveren und gerechteren politischen Reaktionen auf COVID-19 führen könnten.

Keine Erkenntnisse, die die Fachleute des öffentlichen Gesundheitswesens und der Wissenschaft benötigen

Der erste, dezentralisierte Ansatz, wie er von Apple und Google verfolgt wird und in Deutschland alternativlos als einzig richtiger datenschutzkonformer Weg proklamiert wurde, gibt den Nutzern komplette Kontrolle über „ihre" Daten. Unsere Corona-Warn-App alarmiert automatisch, ohne dass eine dritte Partei eingreifen muss. Inwieweit die Kontaktpersonen die Risikomeldungen wahrnehmen und wie sich die Freiwilligkeit bei der Datenübermittlung im Falle einer Infektion auswirkt, ist inzwischen bekannt. **Das deutsche Modell schützt die Privatsphäre. Entscheidend ist jedoch, dass es keine Erkenntnisse liefert, die die Fachleute des öffentlichen Gesundheitswesens und der Wissenschaft benötigen, um das Virus besser zu verwalten bzw. um es einzudämmen.**

Der zweite, zentrale Ansatz nimmt Daten von den Telefonen der Menschen und speichert sie in einem zentralen System. In Deutschland könnte diese Aufgabe dem RKI zukommen, dem die Fachleute vertrauen, dass es die Daten bestmöglich nutzt. **Das zentrale Modell liefert Erkenntnisse, die das öffentliche Gesundheitswesen benötigt, um das Virus besser zu verstehen, zu verwalten und rechtzeitig proaktive Maßnahmen zu ergreifen**. Meldet ein erkrankter Nutzer, eine erkrankte Nutzerin die Symptome, werden der Gesundheitsbehörde auch alle anonymen Kontakte, einschließlich einiger Details über die Art des Kontakts (etwa Dauer und Nähe) übermittelt. Mithilfe der geteilten Informationen kann die Gesundheitsbehörde anhand von Risikomodellen entscheiden, welche Kontaktpersonen am stärksten gefährdet sind und diese benachrichtigen, damit sie die erforderlichen Maßnahmen ergreifen. Die Gesundheitsbehörden können nachvollziehen, wie sich die Krankheit verbreitet. Trotz der Überlegenheit dieses Modells in der Nachvollziehbarkeit der Virusausbreitung und der Effizienz bei der Kontaktverfolgung, konnte es weder in Australien noch in Großbritannien umgesetzt werden – wegen der von Google und Apple gesetzten Einschränkungen.

Die Rolle der digitalen Gatekeeper Google und Apple

Die zentralisierte Version, die etwa auf der Isle of Wight getestet wurde, funktionierte bei der Bewertung der Entfernung zwischen zwei Benutzern gut, war aber schlecht im Erkennen von Apple-iPhones. Nach Aussage des britischen Gesundheitsministers Matt Hancock wäre man möglicherweise erfolgreicher gewesen, hätte Apple nicht die Nutzung von Bluetooth durch Drittanbieter-Apps eingeschränkt[16]: Die Regeln der marktbeherrschenden Plattformen verhindern, dass Apps von Drittanbietern im Hintergrund laufen und Bluetooth-Signale senden. Das hat zur Folge, dass man eine Kontaktverfolgungs-App ständig im Vordergrund geöffnet lassen muss, damit sie richtig funktioniert. Die Betriebssysteme von Apple und Google erlauben zwar Software wie der britischen NHS-Tracing-App und der australischen COVID-Safe-App, in einem speziellen Modus zu laufen, allerdings in engen Grenzen. Die Apps verkürzen die Akkulaufzeit eines Geräts stark. Und im Ergebnis nutzen die Menschen die App nicht, weil sie Strom sparen wollen.

Zwischenfazit

Gründe, warum die Apps in demokratischen Ländern weltweit gescheitert sind

Es gibt kein demokratisches Land auf der Welt, in dem Tracing-Apps spürbar positive Effekte im Kampf gegen Corona hatten. Wichtig ist allerdings festzuhalten, dass Vergleiche an unterschiedlichen Gegebenheiten scheitern: eine rigorose Überwachung der Quarantänemaßnahmen (Taiwan), Datenschutzkultur und Infrastruktur (Südkorea)[17] oder Ausmaß der Pandemie (Australien).

Im Wesentlichen gibt es zwei Gründe, warum die Apps in demokratischen Ländern weltweit gescheitert sind: der Datenschutz und die Rolle der digitalen Gatekeeper (Google (Android) und Apple (iOS)).

***Datenschutz*:** Erfolge bei der Kontaktnachverfolgung, wie in Südkorea, waren nur durch Eingriffe in den Datenschutz möglich. Die Eingriffe waren schwerwiegend[18], in einem demokratischen Rechtsstaat wie in den EU-Staaten wären solche Eingriffe rechtswidrig. Sensible personenbezogene Daten wurden aus mehreren Quellen zusammengeführt, und Fallnummern mit Bewegungsprofilen waren auf einer Website für jedermann einsehbar – erschreckende Überwachungsmethoden mit riesigem Gefahrenpotential.

Gesellschaftliches Umdenken, Daten zum Wohle der Allgemeinheit zu teilen

Eine anders gelagerte Frage ist, wie die Datenschutzpraxis (nicht der Rechtsrahmen) zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Europäischen Binnenmarkts sowie zum Wohlergehen der Bürgerinnen und Bürger beitragen kann. Eines ist evident: Der Datenschutzton in dieser Pandemie war nicht unbedingt kohäsiv. Ein grundsätzliches gesellschaftliches Umdenken, personenbezogene Daten – vor allem in nationalen Krisen – zum Wohle der Allgemeinheit zu teilen, ist derzeit in Deutschland wohl nicht zu erwarten. Doch der geltende Rechtsrahmen bietet deutlich mehr Spielraum zur Eindämmung der Pandemie mit innovativen Mitteln. Der politische Handlungsspielraum blieb ungenutzt, da der gesellschaftliche Druck durch aggressive Fehlinterpretation der DSGVO einfach zu groß ist.

In Deutschland gibt es weder eine gesellschaftliche noch eine politische Bereitschaft, geschweige denn den Willen, datenschutzrechtliche Prämissen in Frage zu stellen – trotz massiver Freiheitseinschränkungen und wirtschaftlicher Belastungen, die der gegenwärtige Shutdown mit sich bringt. Fast jedem Versuch, Dateninnovation als Mehrwert darzustellen, wird mit Skepsis begegnet. Jeder Vorstoß im Rahmen der Corona-Debatte hin zur besseren Nutzung von ausgewählten Daten wird prompt mit regelmäßigem Entsetzen im öffentlichen Diskurs begleitet. Der Ton ist meist laut und negativ konnotiert. Es sei an die Debatte um die Nutzung von gängigen Videokonferenzen-Tools im Bildungsbereich erinnert.

***Gatekeeper*:** Eine effektive Kontaktverfolgung ist nur unter Einbindung der marktbeherrschenden Plattformen möglich. Sie setzen die Regeln und bestimmen die Grundsätze, wie eine Corona-App zu funktionieren hat.[19] Großbritannien und Australien haben bittere Erfahrungen gemacht, als sie mit ihren Apps die Regeln von Google und Apple nicht eingehalten haben. Großbritannien konnte die technische Funktionalität seiner App nicht gewährleisten und wechselte in einer großen Kehrtwende zum dezentralen Modell, das auf der von Apple und Google bereitgestellten Technologie basiert. Die Funktionalität der australischen App ist trotz mehrerer Updates nach wie vor eingeschränkt.

Abhilfe zur dieser Abhängigkeit bietet vielleicht bereits der Entwurf des *Digital Market Act* in seinem Artikel 6, der unter anderem die Installation und die effektive Nutzung von Softwareanwendungen oder Softwareanwendungsspeichern von Drittanbietern regelt. Eine noch ziel-

genauere, regulatorische Lösung ist auch im Rahmen des angekündigten *Data Acts* noch in diesem Jahr möglich. Der *Data Act* soll die Förderung des Datenaustauschs zwischen Unternehmen sowie zwischen Unternehmen und Regierungen konkreter regeln. Die Erfahrungen mit den Corona-Apps sollen dabei zwingend berücksichtigt werden.

Fazit und Ausblick

Daten haben sich zu einem Synonym für eine ganze Reihe von Vorstellungen und Ängsten entwickelt, nicht zuletzt aufgrund mancher Äußerungen im datenschutzrechtlichen Diskurs während der Corona-Pandemie. Deutschland braucht, neben einer Reform der Datenschutzaufsicht hin zu mehr Kohärenz, einen gesellschaftlich funktionierenden Kompromiss zwischen persönlichen Daten auf der einen Seite sowie Innovationen und öffentlichem Interesse auf der anderen Seite. Wenn der nicht gelingt, werden Missverständnisse und Widerstände weiterbestehen. Wir müssen die datenpolitische Debatte mehr unter dem Gesichtspunkt gesellschaftlicher und wirtschaftlicher Potentiale von Daten führen. Und wir brauchen neue Institutionen wie ein Open-Data-Institut nach britischem Vorbild. Ein Open-Data-Institut würde diesen Diskurs bereichern und vorantreiben.

Viel mehr noch muss die Europäische Union sich in die Lage versetzen, unabhängiger von den Gatekeepern zu werden. Das kann nur gelingen, wenn die digitalen Märkte in Europa bestreitbar, also offen für einen freien Wettbewerb werden, was heute de facto nicht gegeben ist. Die zunehmende wirtschaftliche Macht und technologische Dominanz bei großen, nicht-europäischen Online-Plattformen verhindern nicht nur, dass sich europäische Geschäftsmodelle und Innovationskraft behaupten können, sondern dass wir vor allem in Krisensituationen unabhängig agieren. Ziel muss sein, dass wir als Europäische Union auch im digitalen Raum nach eigenen Werten und Interessen handeln können, ohne dabei von Zwängen weniger Unternehmen abhängig zu sein. Die klaren Verhaltensregeln und Normen des Digital Markets Act (DMA) sollen künftig das Level Playing Field wiederherstellen, eine zügige Verabschiedung des DMA ist im Interesse Europas. Auch neue Instrumente, wie Datentreuhänder, können auf diesem Weg hilfreich sein, vorausgesetzt, sie werden nicht regulatorisch überfrachtet. Sie sind wahrscheinlich das wichtigste Instrument im Rahmen des europäischen Data Governance Acts, der sich derzeit ebenso im gesetzgeberischen Verfahren befindet.

Die EU kann es sich nicht leisten, von den Gatekeepern abgehängt zu werden.

1 VO (EU) 2016/679 (Datenschutz-Grundverordnung), Erwg. 4.

2 Markus Söder bei Anne Will vom 29.11.2020, https://daserste.ndr.de/annewill/Soeder-Datenschutz,videoimport33016.html, ähnlich Boris Palmer https://www.bz-berlin.de/deutschland/tuebingen-buergermeister-palmer-geht-auf-corona-warn-app-los, sowie Kristina Schröder https://www.zdf.de/politik/maybrit-illner/keine-impfung-keine-lockerung-planlos-in-den-fruehling-sendung-am-4-februar-2021-100.html zuletzt abgerufen am 15.03.2021.

3 Woran die Wirksamkeit der Corona-Warn-App leidet, https://www.handelsblatt.com/politik/deutschland/pandemiebekaempfung-woran-die-wirksamkeit-der-corona-warn-app-leidet/26887560.html?share=twitter, zuletzt abgerufen am 15.03.2021.

4 VO (EU) 2016/679 (Datenschutz-Grundverordnung), Erwg. 46.

5 Ibid.

6 Christine Lambrecht (SPD): „Bevor es ‚tiefgreifende Einschnitte' in Freiheitsrechte und Bürgerrechte gebe, müsse deutlich werden, dass dies ‚absolut zwingend' erforderlich sei" (ZDF-Morgenmagazin), https://www.zeit.de/politik/deutschland/2020-03/corona-krise-infektionsschutz-gesetz-jens-spahn/seite-2?utm_referrer=https%3A%2F%2Fwww.google.com%2F, zuletzt abgerufen am 15.03.2021.

7 *Spiegel Online*, Weniger Datenschutz hilft auch nicht gegen Covid-19, Ein Gastbeitrag von Ulrich Kelber https://www.spiegel.de/netzwelt/netzpolitik/corona-warn-app-weniger-datenschutz-hilft-auch-nicht-gegen-covid-19-a-a3a31c6b-e876-44cb-bb84-baf95681b53f, zuletzt abgerufen am 15.03.2021.

8 *Tagesspiegel*, https://www.tagesspiegel.de/politik/mit-handydaten-gegen-das-coronavirus-zugriff-auf-bewegungsdaten-mehr-als-problematisch/25615368.html zuletzt abgerufen am 15.03.2021.

9 Entwurf eines Gesetzes zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite vom 20.03.2020.

10 Ibid. § 5 IfSG-E.

11 Vgl. Ulrich Kelber / *Spiegel Online*, https://www.spiegel.de/netzwelt/netzpolitik/corona-warn-app-weniger-datenschutz-hilft-auch-nicht-gegen-covid-19-a-a3a31c6b-e876-44cb-bb84-baf95681b53f, zuletzt abgerufen am 15.03.2021.

12 Exposure Notification APIs Addendum https://developer.apple.com/contact/request/download/Exposure_Notification_Addendum.pdf, zuletzt abgerufen am 15.03.2021.

13 Consumer Privacy Survey The growing imperative of getting data privacy right (Cisco Survey) (https://www.cisco.com/c/dam/global/en_uk/products/collateral/security/cybersecurity-series-2019-cps.pdf, zuletzt abgerufen am 15.03.2021.

14 Ian Levy, The security behind the NHS contact tracing app https://www.ncsc.gov.uk/blog-post/security-behind-nhs-contact-tracing-app zuletzt abgerufen am 15.03.2021.

15 Vgl. Serina Chang, Emma Pierson, Pang Wei Koh, Jaline Gerardin, Beth Redbird, David Grusky & Jure Leskovec, Mobility network models of COVID-19 explain inequities and inform reopening: „Our model predicts that a small minority of ‚superspreader' points of interest account for a large majority of the infections, and that restricting the maximum occupancy at each point of interest is more effective than uniformly reducing mobility." https://www.nature.com/articles/s41586-020-2923-3 zuletzt abrufbar am 15.03.2021.

16 UK abandons contact-tracing app for Apple and Google model https://www.theguardian.com/world/2020/jun/18/uk-poised-to-abandon-coronavirus-app-in-favour-of-apple-and-google-models, zuletzt abgerufen am 15.03.2021.

17 More scary than coronavirus: South Korea's health alerts expose private lives https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives, und Tech Tent: Can we learn about coronavirus-tracing from South Korea? https://www.bbc.com/news/technology-52681464 zuletzt abgerufen am 15.03.2021.

18 Ibid.

19 Vgl. Apple Addendum: „IF YOU DO NOT OR CANNOT ACCEPT THIS EXPOSURE NOTIFICATION APIS ADDENDUM, YOU ARE NOT PERMITTED TO USE THE APPLE SOFTWARE OR SERVICES" https://developer.apple.com/contact/request/download/Exposure_Notification_Addendum.pdf, zuletzt abgerufen am 15.03.2021.

Impressum

Der Autor

Dr. Pencho Kuzev LL.M. ist Policy Advisor in der Hauptabteilung Analyse und Beratung der Konrad-Adenauer-Stiftung. Er ist promovierter Jurist im Bereich Kartell- und Regulierungsrecht. Wichtige berufliche Erfahrungen sammelte er bei der Deutschen Telekom AG sowie in den Kanzleien TaylorWessing LLP und Wagner Legal in Hamburg. Seine besonderen Schwerpunkte sind die Datenökonomie und der Wettbewerbsrahmen in Europa.

Konrad-Adenauer-Stiftung e. V.

Dr. Pencho Kuzev
Datenpolitik
Analyse und Beratung
T +49 30 / 26 996-3247
pencho.kuzev@kas.de

Postanschrift: Konrad-Adenauer-Stiftung, 10907 Berlin

Herausgeberin: Konrad-Adenauer-Stiftung e. V. 2021, Berlin
Gestaltung: yellow too, Pasiek Horntrich GbR
Satz: Janine Höhle, Konrad-Adenauer-Stiftung e. V.
Druck: copy print Kopie & Druck GmbH, Berlin
Printed in Germany.
Hergestellt mit finanzieller Unterstützung der Bundesrepublik Deutschland.

ISBN 978-3-95721-910-7