Alexander Dix

Die deutsche Corona Warn-App – ein gelungenes Beispiel für Privacy by Design?

Bei der Vorstellung der Corona Warn-App am 16. Juni 2020 zeigte sich Kanzleramtsminister Helge Braun „ziemlich überzeugt", dass die deutsche App die beste weltweit sei.[1] Ob dies zutrifft, kann zuverlässig nur aufgrund einer umfassenden vergleichenden Untersuchung der zahlreichen weltweit zur Eindämmung der COVID 19-Pandemie eingesetzten Apps beurteilt werden, die hier nicht zu leisten ist. Dagegen soll die Frage im Vordergrund stehen, ob die in Deutschland mittlerweile in fast 20 Millionen Fällen heruntergeladene App[2] den Vorgaben des europäischen Datenschutzrechts genügt.

Bei der datenschutzrechtlichen Beurteilung müssen alle mit der Nutzung der App ausgelösten Datenflüsse auch mit den Anbietern der Betriebssysteme in den Blick genommen werden, was bei der bisherigen Diskussion in Deutschland noch nicht hinreichend berücksichtigt wurde.

1 Datenerzeugung und Datenflüsse

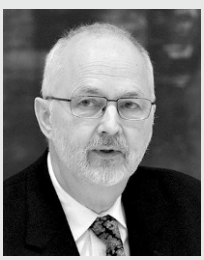
Nach der insofern sehr detaillierten Information des Robert-Koch-Instituts[3] generiert die App auf dem Smartphone des Nutzers, der sie installiert hat, zwei Arten von Zufallscodes: einen Tages- oder Geräteschlüssel und eine aus diesem erzeugte Bluetooth-ID, die kryptografisch aus dem Tagesschlüssel erzeugt wird und der Begegnungsaufzeichnung mittels Bluetooth Low Energy (LE) dient. Die Warn-App misst auf diesem Weg, ob der Nutzer einer anderen Person, die die App aktiviert hat, nahe genug gekommen ist, und tauscht in diesem Fall mit deren Smartphone die verschlüsselten Bluetooth-IDs aus. Während der Tages- bzw. Geräteschlüssel alle 24 Stunden wechselt, also neu erzeugt wird, wird die Bluetooth-ID schon nach 10-15 Minuten ausgetauscht. Damit soll sichergestellt werden, dass durch die Nutzung der Corona-Warn-App keine längerfristigen Bewegungsprofile des Nutzers angelegt werden können. Solange der Nutzer keinem anderen Nutzer der App für einen bestimmten Zeitraum nahe genug gekommen ist, der positiv getestet wurde und sein Testergebnis geteilt hat, verlassen die Geräteschlüssel (im Gegensatz zu den Bluetooth-IDs) das Smartphone des Nutzers nicht und auf sie wird auch nicht zugegriffen. Auch wenn für die Zwecke der Begegnungsregistrierung die Lokalisierung über GPS eingeschaltet sein muss, werden von der Warn-App keine Standortdaten gespeichert.[4] Wer positiv getestet wurde, kann dieses Ergebnis mittels eines QR-Codes oder einer teleTAN in die App eingeben. Den QR-Code erhält er bei der Probenentnahme, damit missbräuchliche Meldungen (Fehlalarme) vermieden werden. Demselben Zweck dient die teleTAN, die über eine Hotline abgefragt werden kann. Wird der positive Test in die App eingeben und verifiziert, werden gleichzeitig die eigenen Tagesschlüssel maximal der letzten 14 Tage an den Server beim Robert-Koch-Institut übertragen (nicht jedoch die Schlüssel der App-Nutzer, die dem Infizierten begegnet sind). Am nächsten Tag wird auch der aktuelle Tagesschlüssel übertragen. Um zu verhindern, dass einzelne Infizierte identifiziert werden können, werden in diesem Prozess den übertragenen Schlüsseln vom System erzeugte weitere Schlüssel beigemischt. Deshalb gibt es keine Zahlen über die tatsächlich übermittelten Tagesschlüssel. Alle aktiven Warn-Apps rufen mehrfach täglich Positivmeldungen vom Server des Robert-Koch-Instituts ab und gleichen sie mit den lokal gespeicherten temporären Zufallscodes ab. Werden Treffer festgestellt, so findet

1 https://www.rnd.de/politik/beste-corona-app-weltweit-minister-feiern-entwicklung-deutscher-warn-app-TCOMAVYUCN7MGVBKJZNEZHXR7E.html (zul. abgerufen am 18.8.2020).

2 Die App wurde bis Oktober 2020 in rund 19,6 Millionen Fällen heruntergeladen. Man geht davon aus, dass rund 16 Millionen Menschen die App aktiv nutzen (https://www.heise.de/news/EU-zahlt-angeblich-7-Millionen-Euro-an-SAP-und-Telekom-fuer-Corona-Warn-App-4931465.html?wt_mc=nl.red.ho.ho-nl-daily.2020-10-19.link.link, zul abgerufen am 19.10.2020).

3 So funktioniert die Corona-Warn-App im Detail, https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Warn_App.html (zul. abgerufen am 19.8.2020).

4 https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-faq-1758392 (zul. Abgerufen am 24.8.2020).



Dr. Alexander Dix, LL.M.

Ehem. Landesbeauftragter für Datenschutz und das Recht auf Akteneinsicht in Brandenburg (1998-2005) und Berliner Beauftragter für Datenschutz und Informationsfreiheit (2005-2016), stellv. Vorsitzender des Vorstands der Europäischen Akademie für Informationsfreiheit und Datenschutz Berlin.
E-Mail: dix@eaid-berlin.de

eine mehrstufige Risikoermittlung statt. Darin fließt sowohl die Zeit ein, die seit der Begegnung vergangen ist, als auch die Dauer des Kontakts, der gemessene Abstand (Grad der Nähe) und das Übertragungsrisiko der positiv getesteten Person[5]. Überschreitet der so ermittelte Risikopunktestand (Risk Score) einen definierten Schwellenwert, so erhält der Nutzer eine entsprechende Warnmeldung („Erhöhtes Risiko"). Darin wird dem Nutzer mitgeteilt, vor wie vielen Tagen[6] die Begegnung mit der positiv getesteten Person stattgefunden hat, nicht aber wer diese Person ist und wo die Begegnung erfolgte. Umgekehrt erfährt die Corona-infizierte Person nicht, welche Personen einen Warnhinweis erhalten haben. Die Kontaktperson wird mit der Warnung aufgefordert, persönliche Kontakte zu reduzieren und bei Symptomen den Hausarzt, den kassenärztlichen Bereitschaftsdienst oder das Gesundheitsamt zu kontaktieren, die darüber entscheiden, ob ein Test durchgeführt werden soll. Wurde der Schwellenwert trotz der Begegnung mit einer positiv getesteten Person nicht überschritten (z.B. wegen zu großen Abstands oder zur kurzer Dauer), so erhält der Nutzer einen Hinweis hierauf („Niedriges Risiko trotz Risiko-Begegnung"), der keinen zusätzlichen Handlungsbedarf (abgesehen von den allgemeinen Hygiene-Regeln) auslöst.

Die deutsche Corona-Warn-App ist angesichts der sich ausbreitenden Pandemie unter hohem Zeitdruck und in relativ kurzer Zeit entwickelt und bereitgestellt worden. Dieser Zeitraum wurde durch die Kontroverse zwischen den Befürwortern einer zentralen Lösung nach dem Modell des Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) und einer dezentralen Lösung (Decentralized Privacy-Preserving Proximity Tracing – DP-3T) etwas verlängert, bis die Bundesregierung sich schließlich für das dezentrale Modell entschied. Auch in diesem Modell bedarf es allerdings eines zentralen Servers, der aber ausschließlich die Aufgabe hat, die pseudonymisierten und verifizierten Positivmeldungen an die Nutzer zu verteilen, auf deren Endgeräten der Abgleich mit den dokumentierten Begegnungen stattfindet. Dieser Server speichert keine weiteren personenbezogenen Daten zentral.[7] Mit der Entscheidung für das dezentrale Modell hat die Bundesregierung bewusst im Interesse einer höheren Akzeptanz darauf verzichtet, mithilfe der Corona-App weitergehende epidemiologische Daten zu gewinnen. Diese sollen getrennt über andere Kanäle, z.B. die bereits vor der Warn-App gestartete (und zuweilen mit ihr verwechselte) Datenspende-App des Robert-Koch-Instituts gewonnen werden. Auch sollen die Nutzer die Möglichkeit erhalten, auf freiwilliger Basis an der Evaluation der Warn-App und damit zusammenhängenden Forschungsprojekten teilzunehmen.[8]

Der hohe Zeitdruck bei der Entwicklung der Warn-App und die Notwendigkeit einer schnellen Verfügbarkeit für eine möglichst hohe Zahl von Smartphone-Nutzern hat auch dazu geführt, dass die von der Bundesregierung beauftragten Unternehmen SAP und T-Systems mit den beiden großen Anbietern von Betriebssystemen für Mobilfunkgeräte, Apple und Google, zusammengearbeitet haben, die gemeinsam das dezentrale Modell der App unterstützten.[9] Die Corona-Warn-App ist als zweiteiliges System zu verstehen, bei dem die App auf dem Endgerät des Nutzers als „Client" fungiert, während die beiden am weitesten verbreiteten Betriebssysteme Android und iOS mit dem Google/Apple Exposition Notification Service (GAEN) eine zweite wesentliche Komponente bereitstellen, ohne die die Benachrichtigung der Nutzer (Kontaktaufzeichnung-Funktion, COVID-19-Kontaktprotokoll) nicht möglich wäre.[10] Dieser Dienst wird bei Android-Geräten von Google verantwortet und ist Teil der App Google Play Services.[11] Ohne die Nutzung dieser App kann der Besitzer eines Android-Smartphones die Corona-Warn-App zumindest bisher nicht nutzen. Google hat lediglich angekündigt, dass man die entsprechende Schnittstelle in den Open-Source-Teil von Android (im Rahmen des Android Open-Source-Projekts) einbauen wolle.[12] Irische Wissenschaftler haben festgestellt, dass die App Google Play Services etwa alle 20 Minuten Kontakt mit den Google-Servern aufnimmt. Dabei übermittelt sie neben der IP-Adresse die IMEI (International Mobile Equiment Identification, die eindeutige Seriennummer jedes mobilen Endgerätes), die Mobilfunknummer, die WiFi-MAC-Adresse und die E-Mail-Adresse des Nutzers beim Playstore sowie detaillierte Daten über die übrigen auf diesem Endgerät genutzten Apps.[13] Das gilt in gleicher Weise für die in anderen europäischen Staaten genutzten Corona-Apps, die in das Google-Betriebssystem eingebettet sind. Schon die Übermittlung der IP-Adresse ermöglicht es Google, detaillierte Profile des Nutzers zu erstellen.[14]

Die Einbettung der Corona-Warn-App in die am meisten genutzten mobilen Betriebssysteme hat sicher dazu beigetragen, dass die App in Deutschland relativ häufig heruntergeladen wurde. Zugleich hat sich die Bundesregierung damit aber in eine gewisse Abhängigkeit von dem Duopol Google/Apple begeben, was etwa die französische Regierung von vornherein abgelehnt hat. Diese hat andererseits eine – weniger datenschutzfreundliche – zentrale Server-Lösung realisiert, was die beiden wichtigsten Betriebssystem-Anbieter abgelehnt haben. Die Parallelität der Corona-Warn-App mit dem Betriebssystem iOS hat beispielsweise auch dazu geführt, dass Apple-Nutzer Push-Nachrichten von ihrem Betriebssystem erhielten, die den Warnmeldungen der Corona-Warn-App widersprachen und eine höhere Anzahl von Risiko-Begegnungen anzeigten als diese. Dazu wurden keine weiteren Erläuterungen gegeben.[15] Google und Apple haben außerdem erklärt, alsbald die Kontaktverfolgung ausschließlich auf der Basis ihrer Betriebssysteme ermöglichen zu wollen, so dass dafür keine besondere App erforderlich wäre. Diese müsste nur in-

5 Wie dieses Übertragungsrisiko im Einzelnen ermittelt wird, teilt das Robert-Koch-Institut auf seiner Website nicht mit.

6 Eine genaue Uhrzeit wird nicht mitgeteilt.

7 https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-faq-1758392 (zul. abgerufen am 20.8.2020).

8 https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Warn_App.html (zul. abgerufen am 21.8.2020).

9 Demgegenüber hat die französische Regierung die Kooperation mit Google und Apple abgelehnt, weil sie eine zentrale App-Lösung favorisierte.

10 Auf diese Zweiteilung weist das Robert-Koch-Institut in seinen Datenschutz-Informationen zur App ausdrücklich hin.

11 Leith/Farrell, Contact Tracing App Privacy: What Data Is Shared By Europe's GAEN Contact Tracing Apps (2020), 9. Eine entsprechende Untersuchung der Benachrichtigung bei Apple-Endgeräten steht noch aus.

12 https://www.heise.de/news/Fragen-und-Antworten-zur-Corona-Warn-App-der-Bundesregierung-4784570.html?seite=5 (zul. abgerufen am 20.8.2020).

13 Eingehend dazu Leith/Farrell (FN 14), 9 f.

14 Das Robert-Koch-Institut erläutert zwar in seinen FAQs, wie Nutzer von Android-Geräten die Übermittlung von Nutzungs- und Diagnosedaten an Google unterbinden können. Selbst ein solcher Schritt würde aber das von Leith/Farrell beschriebene Problem nicht vollständig lösen.

15 https://www.zdf.de/nachrichten/politik/corona-app-risikoanalyse-100.html (zul. abgerufen am 24.8.2020).

stalliert werden, um positive Testergebnisse den Gesundheitsbehörden mitzuteilen.[16]

2 Personenbezug und Sensitivität

Regeln des Datenschutzrechts, insbesondere die Datenschutz-Grundverordnung, finden nur Anwendung, soweit personenbezogene Daten verarbeitet werden. Personenbezogen sind Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt […] identifiziert werden kann.[17] Inwieweit dies bei Nutzung der Corona-Warn-App geschieht, ist zunächst bezogen auf die verschiedenen Phasen der App-Nutzung zu beurteilen. In der ersten Phase tauschen die Nutzer ausschließlich/einerseits temporäre Zufallscodes (Geräteschlüssel und Bluetooth-IDs) untereinander aus. Zu diesen Zufallscodes hat sich die Bundesregierung widersprüchlich geäußert: in ihren FAQs sichert sie den Nutzern einerseits zu, dass sie bei Nutzung der App „jederzeit anonym" bleiben.[18] Andererseits spricht sie an derselben Stelle von einer „vollumfänglichen Pseudonymisierung". Handelte es sich um anonyme Daten, so wäre die Datenschutz-Grundverordnung auf die Nutzung der Warn-App insgesamt nicht anwendbar, während pseudonymisierte Daten demgegenüber als personenbezogen anzusehen sind und dem Datenschutzrecht unterliegen.[19]

Die Feststellung des Personenbezugs erfordert stets eine Risikoanalyse[20], bei der auch der Informationsgehalt der in Rede stehenden Daten zu berücksichtigen ist. Insbesondere bei sensitiven Daten (Gesundheitsdaten, dazu näher unten) wird man keine zu hohen Anforderungen an die Identifizierbarkeit stellen dürfen.[21] Richtigerweise wird man die Zufalls-Codes im Hinblick auf ihre Nutzung nach Meldung einer Infektion als Pseudonyme anzusehen haben, denn es ist gerade ihr Zweck, nach einer Infektion alle App-Nutzer, die der infizierten Person begegnet sind, gezielt zu warnen.[22] Die Information, wer wem begegnet ist, kann Rückschlüsse auf die einzelne Person selbst dann ermöglichen, wenn nichts über den genauen Standort der Personen bekannt ist.[23] Jedenfalls nach Meldung einer Infektion an das Robert-Koch-Institut und nach dem lokalen Abgleich mit dieser verifizierten Infektion durch die Endgeräte aller App-Nutzer findet eine Verarbeitung personenbezogener Daten statt.[24] Auch wenn man vor der ersten dem Robert-Koch-Institut mitgeteilten Infektion die auf den Endgeräten erzeugten und übermittelten Zufallscodes noch als anonym bezeichnen könnte, so würde durch den Abgleich mit erfolgten Infektionsmeldungen der gesamte Prozess zu einer Verarbeitung personenbezogener Daten, weil die anonymen Daten nicht sinnvoll von den personenbezogenen Positivmeldungen getrennt werden können. Deren Personenbezug „infiziert" gewissermaßen den gesamten Verarbeitungsprozess.[25] Ohne Frage personenbezogen sind auch die IP-Adressen, die regelmäßig durch den Exposition Notification Service (s.o.) an Google übermittelt werden. Zumindest Google verfügt selbst bei nicht-registrierten Nutzern über genügend Zusatzwissen, um den jeweiligen Nutzer der Warn-App zu identifizieren.

Bei den Infektionsmeldungen handelt es sich zudem um personenbezogene Gesundheitsdaten i.S.d. Art. 4 Nr. 15 DS-GVO. Das gilt in gleicher Weise für die Risikowarnungen an Kontaktpersonen, auch wenn bei ihnen (bis zu einem Test) noch nicht sicher ist, ob sie sich mit dem Virus infiziert haben. Selbst Wahrscheinlichkeitsaussagen über den möglichen zukünftigen Gesundheitszustand eines Menschen gehören zu den sensitiven personenbezogenen Daten nach der DS-GVO.[26] Auch hier strahlt diese besondere Qualität eines Teils der verarbeiteten Daten auf alle anderen, für sich genommen nicht sensitiven Daten wie die Zufallscodes auf den Endgeräten Nicht-Infizierter aus.

3 Verantwortlichkeit

Da die Datenschutz-Grundverordnung auf die mit der Warn-App ausgelöste Datenverarbeitung anwendbar ist, stellt sich die Frage nach der Verantwortung. In erster Linie wird man das Robert-Koch-Institut als verantwortliche Stelle i.S.d. Art. 4 Nr. 7 DS-GVO anzusehen haben.[27] Nach dessen eigenen Angaben nimmt das Institut eine Doppelrolle wahr: zum einen leistet es einen fachlichen Beitrag bei der Ausgestaltung der App und ist zugleich als „Herausgeber" dafür verantwortlich, die Anforderungen an Datenschutz und Datensicherheit „sorgfältig zu prüfen".[28] Da dieses Institut auch den zentralen Server betreibt, der die Informationen über infizierte App-Nutzer zum Abruf bereithält, bestimmt es über die Zwecke und Mittel der Verarbeitung jedenfalls insoweit, als es die positiven Test-Ergebnisse speichert und zugleich Warnmeldungen und Hinweise an die App-Nutzer versendet.

Parallel dazu finden allerdings zumindest bei Nutzern von Android-Geräten Datenflüsse statt, die der Google/Apple Exposition Notification Service auslöst, auf dem die Kontaktaufzeichnungs-Funktion basiert (s.o.). Auch hier stellt sich die Frage der datenschutzrechtlichen Verantwortlichkeit. Das Robert-Koch-Institut weist in den App-Informationen zum Datenschutz (Datenschutzerklärung) ausdrücklich darauf hin, dass die Kontaktaufzeichnungs-Funktion als Bestandteil des Betriebssystems des Smartphones vom Duopol Apple und Google bereitgestellt wird und den „Datenschutzbestimmungen dieser Unternehmen" unterliegt. Sie liege außerhalb des Einflussbereichs des Robert-Koch-Instituts. Umgekehrt weist auch Google in der vom Robert-Koch-Institut verlinkten Android-Hilfe darauf hin, dass die App nicht von Google oder Apple entwickelt wurde.[29] Nun müssen diese bloßen Er-

16 https://netzpolitik.org/2020/update-bei-google-und-apple-kontaktverfolgung-soll-bald-auch-ohne-app-klappen/ (zul. abgerufen am 31.8.2020). Die von Apple bereitgestellte Tracing-Funktion wird in einzelnen US-Bundesstaaten bereits angeboten, https://www.heise.de/news/iOS-13-7-verfuegbar-Corona-Tracking-direkt-im-Betriebssystem-4883586.html (zul. abgerufen am 3.9.2020).

17 Art. 4 Nr. 1 DS-GVO.

18 https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-faq-1758392 (Welche personenbezogenen Daten speichert die Corona- Warn-App?) (zul. abgerufen am 24.8.2020).

19 Art. 4 Nr. 5 DS-GVO; ErwG 26 S. 2 DS-GVO.

20 Klar/Kühling in Kühling/Buchner, DS-GVO-BDSG, 3. Aufl. 2020, Art. 4 Nr. 1 Rn. 22.

21 Vgl. Klar/Kühling in Kühling/Buchner, DS-GVO-BDSG, 3. Aufl. 2020, Art. 4 Nr. 1 Rn. 29.

22 So auch Kuhlmann, GSZ 2020, 115, 117 f.

23 Kuhlmann, ebda.

24 Kühling/Schildbach, NJW 2020, 1545, 1549.

25 Kühling/Schildbach, ebda., sprechen von „Kontaminierung".

26 Weichert in Kühling/Buchner, DS-GVO-BDSG, 3. Aufl. 2020, Art. 4 Nr. 15 Rn. 3a.

27 So auch die Datenschutzhinweise zur Corona-Warn-App.

28 https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Warn_App.html (Warum die Daten der Nutzer sicher und geschützt sind) (zul. abgerufen am 25.8.2020).

29 https://support.google.com/android/answer/9888358?hl=de (zul. abgerufen am 31.8.2020).

klärungen die rechtliche Bewertung nicht notwendig präjudizieren. Fern liegt allerdings die Annahme einer Auftragsdatenverarbeitung durch die Betriebssystem-Anbieter. Google und Apple haben sich auf die Einbettung der Warn-App in ihre Betriebssysteme Android und iOS verständigt. Sie sind aber weder von Weisungen des Robert-Koch-Instituts noch der betroffenen App-Nutzer abhängig (Art. 28 Abs. 3 DS-GVO). Näher liegt die Annahme einer gemeinsamen Verantwortung des jeweiligen Betriebssystem-Anbieters und des Robert-Koch-Instituts nach Art. 26 DS-GVO. Allerdings fehlt es an der vorgeschriebenen Vereinbarung, in der die gemeinsam Verantwortlichen in transparenter Form die jeweiligen Pflichten gegenüber den Betroffenen festlegen. Man wird deshalb von einer getrennten Verantwortung des Robert-Koch-Instituts für die durch die App selbst ausgelösten Datenflüsse zwischen den Nutzern und dem zentralen Server einerseits und von Google und Apple für die durch die Betriebssysteme ausgelösten Datenflüsse andererseits auszugehen haben. Auch für die Betriebssysteme gilt allerdings – abweichend von den Angaben des Robert-Koch-Instituts – die Datenschutz-Grundverordnung[30], und es gelten nicht lediglich die Datenschutzbestimmungen von Google und Apple.

4 Transparenz

Wer personenbezogene Daten verarbeitet, unterliegt zahlreichen Informations- und Transparenzpflichten, deren Erfüllung auch Auswirkungen auf die Rechtmäßigkeit der Datenverarbeitung hat. Die vom Robert-Koch-Institut und der Bundesregierung bereitgestellten Informationen über die Funktionsweise der App selbst, über die Verantwortlichkeiten und den Umfang der Datenverarbeitung sind detailliert und genügen im Wesentlichen den Vorgaben der Datenschutz-Grundverordnung.[31] Allerdings fehlen entsprechende Informationen bezüglich des Google/Apple Exposition Notification Service, der zumindest bei Android-Endgeräten zusätzliche Datenflüsse zwischen den Nutzern und Google-Servern auslöst (s.o.). Ohne diesen Dienst kann die Corona-Warn-App bisher nicht genutzt werden. In der Android-Hilfe wird lediglich betont, dass die Identität des Nutzers nicht an Google weitergegeben und sein Standort nicht erfasst wird. Die dennoch bei jeder Nutzung des Google Play Services ausgelösten personenbezogenen Datenflüsse (z.B. die IP-Adresse, E-Mail-Adresse und Mobilfunknummer des Nutzers) werden weder erwähnt noch erläutert. Das ist mit den Informationspflichten der Datenschutz-Grundverordnung (Art. 13) nicht vereinbar. Leith/Farrell halten darüber hinaus sogar die Koppelung der in Europa eingesetzten Corona-Warn-Apps (einschließlich der deutschen App) für unzulässig.[32] Sie fordern jedenfalls zu Recht, dass eine nutzerfreundliche Dokumentation zugänglich gemacht wird, die eine möglichst datenschutzfreundliche Einstellung von Google Play Services erläutert. Zudem müsste die Möglichkeit einer Nutzung der Warn-App geschaffen werden, ohne dass ständig Daten über Google Play Services an Google fließen. Schließlich müssten Google und Apple die Funktionsweise von Google Play Services (und des entsprechenden Dienstes bei Apple) transparent machen und sie einer Datenschutzfolgenabschätzung unterziehen.[33]

5 Rechtsgrundlage

Die Nutzung der Corona-Warn-App ist in jeder Phase freiwillig. Man kann den Austausch der lokal gespeicherten Schlüssel (Geräteschlüssel, Blutooth-ID) zulassen. Auch die Mitteilung eines positiven Testergebnisses erfolgt erst, wenn der betroffene Nutzer dem ausdrücklich zustimmt. Es ist also möglich, die Warn-App lediglich passiv zu nutzen und keine Informationen über den eigenen Gesundheitszustand preiszugeben. Die Bundesregierung hat bewusst davon abgesehen, eine gesetzliche Verpflichtung zur Nutzung der App einzuführen. Dabei dürften Akzeptanz- und Praktikabilitätsüberlegungen eher im Vordergrund gestanden haben als rechtliche Gesichtspunkte. Schon rein praktisch hätte eine Nutzungspflicht zu kurz gegriffen, da nur Besitzer von Smartphones mit einer modernen Betriebssystem-Version die App nutzen können und der Erwerb eines solchen Smartphones nicht generell vorgeschrieben werden kann.

Die Rechtsgrundlage für die Datenverarbeitung im Zusammenhang mit der Corona-Warn-App könnte sich unmittelbar aus der Datenschutz-Grundverordnung ergeben, wo die informierte und – im Fall der Gesundheitsdaten – ausdrückliche Einwilligung als Erlaubnistatbestand genannt wird.[34] Dessen Voraussetzungen wird man für die eigentliche App, also die Datenverarbeitung des Robert-Koch-Instituts, bejahen können. Dieses hat die notwendigen Informationen in verständlicher Weise bereitgestellt, so dass eine wirksame Einwilligung der App-Nutzer i.S.d. Art. 7 Abs. 1 DS-GVO nachzuweisen ist. Daran ändert auch die Möglichkeit nichts, dass in der sozialen Realität die Gewährung von Vorteilen und die Teilhabe am Wirtschaftsleben von der Nutzung der App abhängig gemacht werden könnte. Denn ein solches Vorgehen z.B. von Arbeitgebern oder Gastwirten wäre rechtswidrig, weil darin eine unzulässige Zweckentfremdung der mit der Corona-Warn-App erhobenen Daten läge. Deren Nutzer haben einer Verarbeitung ihrer Daten zum Zweck der Unterbrechung von Infektionsketten durch die Gesundheitsbehörden zugestimmt. Damit wäre eine Nutzung durch Arbeitgeber, Restaurants oder andere Unternehmen nicht vereinbar; sie könnte auch nicht durch eine gesonderte Einwilligung legitimiert werden, weil gerade etwa bei einer Stellenbesetzung oder bei der Nutzung des öffentlichen Nahverkehrs die Freiwilligkeit fehlen würde.[35]

Dagegen fehlt es bei den in den Betriebssystemen angelegten Datenflüssen (jedenfalls bei Android-Endgeräten) an der vorgeschriebenen umfassenden Information (s.o.), so dass insoweit die Einwilligung nicht „informiert" und damit tragfähig ist. Die Nutzer haben keine Wahl, als diese – im Einzelnen nicht transparenten – Datenflüsse bei der Nutzung der App mit in Kauf zu nehmen.

Damit stellt sich die Frage, welche anderen Rechtsgrundlagen neben oder zusätzlich zur Einwilligung herangezogen werden können. Die Datenschutz-Grundverordnung sieht eine Reihe von Verarbeitungserlaubnissen und Öffnungsklauseln vor, die hier einschlägig sein könnten. Sie sind aber entweder zu allgemein gehalten, um die Verarbeitung teils sensitiver Daten zu rechtfertigen, oder der deutsche Gesetzgeber hat sie bisher nicht in der gebotenen Normenklarheit ausgeschöpft.

Die Regelungen der Datenverarbeitung zur Erfüllung rechtlicher Verpflichtungen des Verantwortlichen (Art. 6 Abs. 1 lit. c DS-

30 Art. 3 Abs. 2 DS-GVO.
31 Insbesondere Art. 13 DS-GVO.
32 Leith/Farrell (FN 14), 3.
33 Ebda.
34 Art. 6 Abs. 1 lit. a; Art. 9 Abs. 2 lit. a DS-GVO.
35 BayLDA, ZD Fokus, 9/2020, XII; Saarl. VerfGH, Beschl. v. 28.8.2020 (Lv 15/20), 29.

GVO), zum Schutz lebenswichtiger Interessen von Personen (Art 6 Abs. 1 lit. d DS-GVO), zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe (Art. 6 Abs. 1 lit. e DS-GVO) und zur Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f DS-GVO) enthalten teilweise eigene Befugnisse, teilweise aber auch nur Begrenzungen anderweitig durch Unionsrecht oder mitgliedstaatliches Recht geregelter Befugnisse zur Datenverarbeitung.[36] Nur die Tatbestände des Art. 6 Abs. 1 lit. c und e DS-GVO setzen wie der hier vor allem einschlägige Art. 9 Abs. 2 lit. i DS-GVO gesonderte Regelungen durch das Recht der Union oder der Mitgliedstaaten voraus.[37] Bei der Verarbeitung zum Schutz lebenswichtiger Interessen von Personen und zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten ist dies nicht der Fall.

Auf die allgemeine Abwägungsklausel des Art. 6 Abs. 1 lit. f DS-GVO können Behörden wie das Robert-Koch-Institut und die Gesundheitsämter sich nicht berufen (Art. 6 Abs. 1 S. 2 DS-GVO).[38] Gleiches muss für die privaten Anbieter der Betriebssysteme gelten, die die Kontaktaufzeichnungsfunktion bereitstellen. Diese können im Zusammenhang mit der zum Zweck des öffentlichen Gesundheitsschutzes bereitgestellten Corona-Warn-App keine weitergehenden Befugnisse reklamieren als die Gesundheitsbehörden.

Darüber hinaus ist aber grundsätzlich zu bezweifeln, ob die Tatbestände des Art. 6 Abs. 1 DS-GVO auf die hier in Rede stehenden Datenverarbeitungsprozesse anwendbar sind. Seitdem der erste positiv getestete Nutzer der Corona-Warn-App sein Ergebnis dem Robert-Koch-Institut mitgeteilt hat, werden ständig sensitive Daten zwischen dem zentralen Server und den Nutzern zum Zweck des Abgleichs ausgetauscht. Damit aber hat bei einer ganzheitlichen Betrachtung der durch die Corona-Warn-App ausgelösten Datenflüsse Art. 9 DS-GVO mit seinen Ausnahmetatbeständen als speziellere Vorschrift Vorrang vor den allgemeinen Regelungen des Art. 6 Abs. 1 DS-GVO.[39] Dem steht auch Erwägungsgrund 46 der Grundverordnung nicht entgegen, der davon spricht, dass die „Überwachung von Epidemien und deren Ausbreitung" sowohl als wichtiger Grund des öffentlichen Interesses als auch als lebenswichtiges Interesse der betroffenen Person angesehen werden kann, denn diesen Interessen kann auch ohne die Verarbeitung sensitiver Daten (z.B. durch die Auswertung von Standortdaten bei der Bekämpfung von Epidemien) Rechnung getragen werden.

Deshalb kommt als einzige Legitimationsgrundlage Art. 9 Abs. 2 lit. i DS-GVO in Frage, wonach unabhängig von der ausdrücklichen Einwilligung des Betroffenen Gesundheitsdaten verarbeitet werden dürfen, wenn dies „aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren […] auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person […] vorsieht, erforderlich" ist. Diese Regelung setzt ihrerseits eine besondere Rechtsgrundlage im Unionsrecht oder im Recht eines Mitgliedstaates voraus. Teilweise wird eine solche Rechtsgrundlage in § 22 Abs. 1 lit. c BDSG gesehen.[40] Diese Vorschrift begnügt sich allerdings damit, den Wortlaut des Art. 9 Abs. 2 lit. i DS-GVO zu wiederholen und ist damit zu wenig normenklar und präzise, um die durch die Nutzung der Warn-App ausgelösten Datenflüsse auch ohne Einwilligung der Betroffenen rechtfertigen zu können.[41] Das Infektionsschutzgesetz wiederum enthält bisher nur Regelungen, die den Gesundheitsämtern eine analoge und verdachtsabhängige Kontaktverfolgung erlauben.[42]

Art. 9 Abs. 2 lit. i DS-GVO würde zwar prinzipiell auch die Einführung einer Pflicht zur Nutzung der Corona-Warn-App zulassen. Allerdings müsste diese zugleich den verfassungsrechtlichen Anforderungen des deutschen Grundrechtskataloges genügen, die nach der Rechtsprechung des Bundesverfassungsgerichts in diesem europaweit nicht vollständig harmonisierten Rechtsbereich zur Anwendung kommen.[43] Dabei stellt sich die Frage der Verhältnismäßigkeit in mehrfacher Hinsicht: zunächst ist zu fragen, ob nicht mit der Einführung der App auf freiwilliger Basis ein weniger weitreichender Grundrechtseingriff möglich ist, der das mildere Mittel darstellt und dessen Wirkung durch die zwangsweise Einführung nicht entscheidend übertroffen würde.[44] Zum anderen wäre es mit einer Nutzungspflicht nicht getan: sie müsste nicht nur ergänzt werden durch ein „Bluetooth-Abschaltverbot",[45] sondern auch durch eine Pflicht zur Anschaffung und Nutzung eines genügend modernen Smartphones für die gesamte Bevölkerung. In der Gesamtschau würden diese Eingriffe das verfassungsrechtliche Übermaßverbot verletzen, zumal vor dem Hintergrund der entstehenden Vollzugsprobleme unklar wäre, wie effektiv die Warn-App zur Eindämmung der Pandemie beitragen würde.[46]

Festzuhalten bleibt, dass die mit der Corona-Warn-App zusammenhängende Datenverarbeitung insoweit durch die informierte Einwilligung der Nutzer legitimiert wird[47], als der Austausch von Zufallscodes mit anderen Nutzern und der Abgleich mit Positivmeldungen betroffen ist, die das Robert-Koch-Institut bereitstellt. Für die Datenflüsse zu den Anbietern der Betriebssysteme (Google und Apple) gilt dies solange nicht, wie diese keine umfassenden Informationen über den Google/Apple Exposition Notification Service bereitstellen.

Davon zu trennen ist die Frage, ob nicht trotz der freiwilligen Nutzung der App eine gesetzliche Regelung bestimmter Aspekte des Umgangs mit der App geboten oder zumindest ratsam ist, zumal die Datenschutz-Grundverordnung selbst in mehreren einschlägigen Bestimmungen die Notwendigkeit einer solchen Regelung unterstreicht.[48] So ist insbesondere die Zweckbindung der erhobenen Daten in Deutschland nicht hinreichend gesichert. Das aber ist ein wesentlicher Aspekt, den der Gesetzgeber nach dem

36 Anders der Saarl. VerfGH, Beschl. v. 28.8.2020 (Lv 15/20), 30 f., der generell davon ausgeht, dass die in Art. 6 Abs. 1 DS-GVO enthaltenen Regelungen keine eigenen Befugnisse enthalten.

37 Vgl. Art. 6 Abs. 3 Satz 1 DS-GVO.

38 Das übersieht Kuhlmann, GSZ 2020, 115, 120 f.

39 So für das Verhältnis zwischen Art. 6 Abs. 1 lit. d und Art. 9 Abs. 2 lit. c DS-GVO auch Buchner/Petri in Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, Art. 6 Rn. 110. Vgl. auch Kühling/Schildbach, NJW 2020, 1545, 1547. A.A. Kuhlmann, GSZ 2020, 115, 119 ff.; Schmitz, ZD-Aktuell 2020, 04404.

40 Kuhlmann, GSZ 2020, 115, 120.

41 So auch Kühling/Schildbach, NJW 2020, 1545, 1549. Krit. zu § 22 BDSG generell Weichert in Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, § 22 BDSG Rn. 20.

42 Kühling/Schildbach, NJW 2020, 1545, 1548. Weitergehend offenbar Kuhlmann, GSZ 2020, 115, 120.

43 BVerfG, Beschl. v. 6.11.2019 (1 BvR 16/13) („Recht auf Vergessen I"), dazu Dix in Blatt/Dix/Kelber/Kloepfer/Kugelmann/Schaar/Schoch (Hrsg.), Informationsfreiheit und Informationsrecht – Jahrbuch 2019, 145, 147 ff., sowie Kühling/Schildbach, NJW 2020, 1545, 1547.

44 Kühling/Schildbach, NJW 2020, 1545, 1550.

45 Kühling/Schildbach, ebda.

46 Ebenso Kühling/Schildbach, ebda. A.A. Kuhlmann, GSZ 2020, 115, 121 f. sowie Schmitz, ZD-Aktuell 2020, 04404.

47 Art. 6 Abs. 1 lit. a, Art. 9 Abs. 2 lit. a DS-GVO, auf die auch die Datenschutzerklärung der Corona-Warn-App hinweist.

48 Art. 6 Abs. 1 lit. c und e, Art. 9 Abs. 2 lit. i DS-GVO.

Rechtsstaatsprinzip und dem Vorbehalt des Gesetzes selbst regeln muss.[49] Zwar willigen die App-Nutzer in die Verarbeitung ihrer Daten nur zu dem Zweck ein, dass Infektionsketten zeitnah erkannt und unterbrochen werden. Das schließt aber nicht aus, dass Endgeräte mit lokal gespeicherten Geräteschlüsseln, Bluetooth-IDs und Informationen über positiv getestete Personen, denen der Nutzer begegnet ist, beschlagnahmt werden, wenn die Strafverfolgungsbehörden dies für Ermittlungszwecke für zielführend halten sollten. Hier wäre es dringend geboten, dass der Gesetzgeber nach dem Vorbild des Autobahn-Mautgesetzes[50] ein Beschlagnahmeverbot statuiert, um sicherzustellen, dass die bei der Corona-Warn-App anfallenden sensitiven Daten nicht zweckentfremdet werden.[51] Die Diskussion um den polizeilichen Zugriff auf die zur Infektionseindämmung vorgeschriebenen Gästelisten in Restaurants hat gezeigt, wie schnell die Akzeptanz und Bereitschaft, wahre Angaben zu machen, sinkt, wenn solche Daten sogar zur Verfolgung von Kleinkriminalität genutzt werden sollen.[52] Im Fall der Corona-Warn-App geht es zwar nicht um die Angabe von personenbezogenen Daten durch die Betroffenen, gleichwohl würde die Bereitschaft zur Nutzung der App möglicherweise noch gesteigert werden, wenn eine Nutzung der dabei anfallenden Daten für Zwecke der Strafverfolgung ausgeschlossen wäre. Zwar wären gesellschaftliche Zwänge zur Nutzung der Corona-Warn-App durch Arbeitgeber, Restaurantbesitzer und andere Unternehmer, die den Abschluss von Verträgen von der Nutzung der App abhängig machen könnten, bereits jetzt rechtlich problematisch (s.o.), dem damit einhergehenden Diskriminierungsrisiko könnte aber durch eine explizite gesetzliche Regelung mit entsprechender Sanktionsbewehrung effektiver begegnet werden.[53]

6 Privacy by Design

Insgesamt ist der deutschen Corona-Warn-App zu attestieren, dass sie hierzulande das erste Beispiel für eine staatlich geförderte Anwendung ist, bei der die Grundsätze des Privacy by Design and by Default i.S.d. Art. 25 DS-GVO bereits im Stadium der Gestaltung weitestgehend berücksichtigt wurden. Der Umfang der personenbezogenen Daten ist – jedenfalls im Verhältnis zwischen den Betroffenen und dem Robert-Koch-Institut – auf ein Minimum beschränkt und durch die Nutzung von Pseudonymisierungsmechanismen sowie die primär dezentral organisierte Datenverarbeitung wurde eine im Vergleich zu zentralen Verfahren datenschutzfreundlichere Systemkonfiguration[54] gewählt, die zur erhöhten Akzeptanz beigetragen haben dürfte.

Das heißt nicht, dass die Corona-Warn-App in ihrer gegenwärtigen Form und abgesehen von vielfältigen praktischen Problemen[55] ein datenschutzrechtliches Optimum darstellt. Auf die rechtlich relevanten Transparenzmängel und Koppelungsprobleme bei den Anbietern der Betriebssysteme Android und iOS wurde bereits hingewiesen. Auch eine vorherige Datenschutz-Folgenabschätzung, wie sie der Europäische Datenschutzausschuss gefordert hat,[56] steht bisher aus. Darüber hinaus wird auch über eine Weiterentwicklung sowohl in Deutschland als auch in Europa diskutiert.

7 Weiterentwicklung auf nationaler und europäischer Ebene

Die Bundesregierung hat stets betont, dass die Corona-Warn-App nicht die „Wunderwaffe" (silver bullet), wohl aber ein wesentlicher Baustein im Kampf gegen die Pandemie sein kann, wenn hinreichend viele Menschen sie nutzen. Die Zahl der Nutzer könnte durch eine Reihe von Maßnahmen weiter erhöht werden. Zum einen ist bisher nicht evaluiert worden, welchen konkreten Nutzen die Warn-App bei der Eindämmung der Pandemie tatsächlich hat. Entsprechende Untersuchungen sind zu Recht gefordert worden[57] und könnten – falls sie zu positiven Ergebnissen führen – die Bereitschaft zur Nutzung der App weiter erhöhen. Experten zufolge muss sich die Zahl der Nutzer zumindest verdoppeln, um Infektionen wirksam nachverfolgen zu können.[58] Das Robert-Koch-Institut hat angekündigt, dass es die Möglichkeit zur Evaluation unter Beteiligung anderer wissenschaftlicher Institutionen in einer der nachfolgenden Ausbaustufen der App zur Verfügung stellen will. Dann sollen sich auch die Nutzer freiwillig an einer solchen Evaluation und an den damit zusammenhängenden Forschungsfragen zur COVID-19-Situation in Deutschland beteiligen können.[59] Es ist zu hoffen, dass das Robert-Koch-Institut dabei die Fehler vermeidet, die es bezüglich der Transparenz und Datensi-

49 Johannes, ZD-Aktuell 2020, 07114. Vgl. auch Lichdi, SächsVBl. 2020, 273 ff. Die Schweiz hat ihr Epidemiengesetz (entspricht dem Infektionsschutzgesetz) am 19.6.2020 um entsprechende Regelungen zum Einsatz der (der deutschen Warn-App ähnelnden) COVIDApp ergänzt.

50 § 4j Abs. 3 Satz 2 des Gesetzes über die Erhebung von streckenbezogenen Gebühren für die Benutzung von Bundesautobahnen und Bundesfernstaßen i.d.F. v. 20.11.2019.

51 Vgl. die entsprechende Regelung in § 60a Abs. 2 Satz 2 des schweizerischen Epidemiengesetzes sowie § 6 Satz 2 des Gesetzentwurfs der Fraktion BÜNDNIS 90/DIE GRÜNEN zur zivil-, arbeits- und dienstrechtlichen Sicherung der Freiwilligkeit der Nutzung und zur Zweckbindung mobiler elektronischer Anwendungen zur Nachverfolgung von Infektionsrisiken v. 16.6.2020 (BT-Drs. 19/20037).

52 https://www.heise.de/newsticker/meldung/Bayerische-Polizei-Mit-Corona-Gaestelisten-gegen-Kleinkriminalitaet-4885096.html (zul. abgerufen am 4.9.2020); krit. dazu mit Recht Fährmann/Arzt/Aden, https://verfassungsblog.de/corona-gaestelisten-masslose-polizeiliche-datennutzung/ (zul. abgerufen am 10.9.2020). Eingehend zur polizeilichen Nutzung von Corona-Daten durch die Polizei Fährmann/Arzt in diesem Heft.

53 Vgl. den Gesetzentwurf der Fraktion BÜNDNIS 90/DIE GRÜNEN (FN. 53) und Johannes, ZD-Aktuell 2020, 07114.

54 Auch die zentrale Lösung, wie sie etwa in Frankreich gewählt wurde, kann nach Auffassung des Europäischen Datenschutzausschusses (EDSA) mit der DS-GVO im Einklang stehen, s. EDSA, Leitlinien 4/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19 v. 21.4.2020, Rn. 42.

55 Es wird immer wieder über Probleme bei der Hintergrundaktualisierung und bei der Information über die Bedeutung einzelner Warnhinweise und den dadurch entstehenden Beratungsbedarf berichtet, s. z.B. https://www.tagesspiegel.de/wirtschaft/corona-warn-app-immer-noch-stoeranfaellig-zwei-kniffe-und-ein-update-sollen-jetzt-helfen/26158106.html (zul. abgerufen am 4.9.2020). Außerdem hat die Warn-App vor allem in der Anfangsphase dazu geführt, dass die personell ohnehin mangelhaft ausgestatteten Gesundheitsämter, die zudem bei der Entwicklung der App nicht einbezogen waren, mit einer Flut von Anrufen verunsicherter App-Nutzer fertig werden mussten, https://www.spiegel.de/netzwelt/apps/corona-warn-app-wer-von-der-app-alarmiert-wird-soll-auch-ohne-symptome-getestet-werden-a-f27b4dfc-c5e3-4073-91eb-145cf890d894 (zul. aufgerufen am 7.9.2020).

56 EDSA, Leitlinien 4/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19 v. 21.4.2020, Rn. 39 (https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en (zul. abgerufen am 8.9.2020)).

57 Leith/Farrell, https://www.sciencemediacenter.de/alle-angebote/rapid-reaction/details/news/was-haben-corona-apps-bisher-gebracht/ (zul. abgerufen am 7.9.2020).

58 https://www.zeit.de/wissen/gesundheit/2020-08/corona-warn-app-contact-tracing-downloads-nutzung-niedrig (zul. abgerufen am 8.9.2020).

59 https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Warn_App.html (Wie die Corona-Warn-App weiterentwickelt wird) (zul. abgerufen am 7.9.2020).

cherheit bei seiner Corona-Datenspende-App gemacht hat,[60] mit der Nutzer von Fitness-Armbändern dazu veranlasst werden sollen, dem Institut Vitaldaten zur Verfügung zu stellen, die Aufschluss über den Verlauf der Pandemie geben könnten. Zur Weiterentwicklung der App ist zudem vorgeschlagen worden, dass infizierte Nutzer auf freiwilliger Basis zusätzliche Daten wie etwa den genauen Zeitpunkt der Begegnung mit Kontaktpersonen machen und mithilfe der App ein digitales Kontakttagebuch über Begegnungen mit Menschen führen können, die die App nicht nutzen oder kein Smartphone besitzen.[61] Das führt zu einem grundsätzlichen Problem, das bisher nicht ausreichend adressiert wurde: Da die Corona-Warn-App nur auf bestimmten Smartphones funktioniert, sind Menschen mit älteren Endgeräten oder ohne Smartphone von ihrer Nutzung ausgeschlossen. Das betrifft möglicherweise ältere Menschen, die mit der digitalen Technik weniger vertraut sind und zugleich einer Risikogruppe angehören. Hier wäre es sinnvoll, Token (z.B. Armbänder) zu entwickeln und kostengünstig bereitzustellen, die Bluetooth-Signale verarbeiten und die Corona-Warn-App unterstützen können.

Angesichts des grenzüberschreitenden Charakters der Pandemie ist überdies die Entwicklung einer europaweit nutzbaren Warn-App notwendig. Hierzu haben sowohl der Europäische Datenschutzausschuss als auch die Europäische Kommission Leitlinien und Empfehlungen veröffentlicht.[62] Die Europäische Kommission hat zudem T-Systems und SAP, die die deutsche Warn-App entwickelt haben, den Auftrag erteilt, eine Software-Plattform für die Verknüpfung europäischer Warn-Apps zu entwickeln, die Ende September 2020 bereitstehen soll.[63] Als Länder, die sich an dieser testweisen Verknüpfung seit Mitte September beteiligen, gehören neben Deutschland Dänemark, Irland, Italien, Lettland und Tschechien.[64] Das wirft die Frage nach der Kompatibilität der nationalen Warn-Apps auf. Google und Apple unterstützen mit ihren Betriebssystemen dezentrale Warn-Systeme auch auf europäischer Ebene. Frankreich und Ungarn haben sich dagegen für eine zentrale Speicherlösung entschieden und dürften damit für eine Verknüpfungsplattform ausscheiden. Aber auch in Ländern mit einem dezentralen System werden teilweise erheblich invasivere technologische Konzepte verfolgt. So ist etwa in Polen die Nutzung der entsprechenden App, die zugleich der Quarantäne-Überwachung dient, verpflichtend. Es werden Techniken der Gesichtserkennung und Geolokalisierung genutzt.[65] Bevor eine technische Verknüpfung zwischen europäischen Ländern ermöglicht wird, muss deshalb die Frage geklärt werden, wie verhindert werden kann, dass datenschutzfreundliche Voreinstellungen etwa in der deutschen Warn-App durch eine Nutzung in anderen Ländern mit datenschutzrechtlich problematischen Funktionen unterlaufen werden. Ebenso wenig dürfen in Deutschland Gesundheits- oder Bewegungsdaten von Bürgern anderer Länder in einer Weise verarbeitet werden, die deutschem und europäischem Datenschutzrecht widerspricht. Hier ist der Europäische Datenschutzausschuss aufgefordert, seine Leitlinien für mobile Apps zur Eindämmung der Pandemie zu präzisieren. Letztlich ist auch aus diesem Grund die Schaffung einer europäischen Rechtsgrundlage zum Einsatz technischer Mittel zur Bekämpfung grenzüberschreitender Gesundheitsgefahren wünschenswert.

8 Fazit

Insgesamt lässt sich festhalten, dass die deutsche Corona-Warn-App insofern Modellcharakter hat, als sie tatsächlich in weiten Teilen den Ansprüchen des Prinzips Privacy by Design genügt. Zum ersten Mal wurde mit Unterstützung der Bundesregierung ein Datenverarbeitungsprojekt entwickelt, bei dem der Datenschutz explizit im Vordergrund stand. Insofern hat die Corona-Warn-App für die Entwicklung des Datenschutzes eine mindestens so große Bedeutung wie für die Bekämpfung des Virus. Auch wenn die Nutzerzahlen noch nicht hoch genug sind, um der App zu der erforderlichen Wirksamkeit im epidemiologischen Sinn zu verhelfen, sind die Nutzerzahlen sicher durch die dezentrale und datensparsame Konfiguration begünstigt worden. Ein Zwang zur Nutzung der App hingegen wäre verfassungsrechtlich problematisch.

Allerdings gibt es datenschutzrechtliche Defizite bei den beiden vorherrschenden Betriebssystemen, deren Kontaktaufzeichnungsfunktion Voraussetzung für die Nutzung der Corona-Warn-App ist. Google und Apple müssen die erforderliche Transparenz über die ausgelösten Datenflüsse vom Endgerät des Nutzers zu ihren Servern herstellen und es muss darüber hinaus möglich sein, die Warn-App zu nutzen, ohne dass personenbezogene Daten dabei an Google oder Apple übermittelt werden.

Letztlich ist eine europaweite Nutzbarkeit von Corona-Warn-Apps anzustreben. Der Weg dahin ist allerdings angesichts der in den einzelnen Staaten der Europäischen Union sehr unterschiedlichen technischen Konzepte nicht trivial. Oberstes Ziel muss es mit den Worten des Europäischen Datenschutzausschusses sein, die wirksame Reaktion auf die Pandemie und den Schutz der Grundrechte nicht gegeneinander auszuspielen. Beides ist nicht nur miteinander vereinbar, sondern ein wirksamer Datenschutz kann sogar eine wichtige Rolle bei der Bekämpfung des Virus spielen.[66] Ein technischer „Solutionismus", bei dem wie z.B. in China der Einsatz von Überwachungsinstrumenten auch im Gesundheitsbereich zum Normalzustand wird,[67] darf in Europa nicht Platz greifen.

60 Vgl. dazu die Stellungnahme der Gesellschaft für Informatik, https://gi.de/meldung/gi-kritisiert-datenspende-app-des-robert-koch-instituts (zul. abgerufen am 7.9.2020).

61 Mit der Version 1.5 können seit dem 19.1.2020 in der Corona-Warn-App auf freiwilliger Basis in einer Art Tagebuch Krankheitssymptome erfasst werden, um die Risikoeinstufung zu erleichtern. https://www.zeit.de/digital/2020-08/corona-warn-app-coronavirus-eindaemmung-karl-lauterbach-henning-tillmann (zul. abgerufen am 8.9.2020).

62 EDSA, Leitlinien 3/2020 für die Verarbeitung von Gesundheitsdaten für wissenschaftliche Forschungszwecke im Zusammenhang mit dem COVID-19-Ausbruch v. 21.4.2020, Leitlinien 4/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19 v. 21.4.2020 (beide abrufbar unter https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en (zul. abgerufen am 8.9.2020)); Empfehlung (EU) 2020/518 der Europäischen Kommission v. 8.4.2020 für ein gemeinsames Instrumentarium der Union für den Einsatz von Technik und Daten zur Bekämpfung und Überwindung der COVID-19-Krise, insbesondere im Hinblick auf Mobil-Apps und die Verwendung anonymisierter Mobilitätsdaten, ABl. EU L 114/7 v. 14.4.2020.

63 https://www.tagesspiegel.de/wirtschaft/corona-warn-app-immer-noch-stoeranfaellig-zwei-kniffe-und-ein-update-sollen-jetzt-helfen/26158106.html (zul. abgerufen am 8.9.2020).

64 https://www.heise.de/news/Corona-Warn-Apps-EU-Staaten-testen-grenzueberschreitende-Funktion-4893643.html (zul. abgerufen am 15.9.2020).

65 Mileszyk/Tarkowski in Algorithm Watch/Bertelsmann Stiftung (Hrsg.), Automated Decision-Making Systems in the COVID-19 Pandemic: A European Perspective (2020), 26 f.

66 EDSA, Leitlinien 4/2020, Rn. 49 (https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en) (zul. abgerufen am 8.9.2020).

67 Dazu näher Algorithm Watch/Bertelsmann Stiftung (Hrsg.) (FN 67), 13 ff.