Ausarbeitung

Handytracking in Deutschland

Grundrechte und Datenschutzrecht

Handytracking in Deutschland
Grundrechte und Datenschutzrecht

Aktenzeichen: WD 3 - 3000 - 097/20
Abschluss der Arbeit: 9. April 2020
Fachbereich: WD 3: Verfassung und Verwaltung

Inhaltsverzeichnis

1. Fragestellung

Gefragt wird nach einer Beurteilung des sogenannten Handy-Trackings zur Eindämmung der Infektionen mit dem Coronavirus. Diese beinhaltet hier sowohl eine datenschutzrechtliche Prüfung, als auch eine solche bezüglich der Vereinbarkeit mit den Grundrechten.

Zugrunde liegen die öffentlich zugänglichen Angaben zu einer Handy-App, die im Rahmen des Projekts „Pan-European Privacy-Preserving Proximity Tracing“ (PEPP-PT) entwickelt wird. Teil der Initiative sind unter anderem das Heinrich-Hertz-Institut des Fraunhofer-Instituts, das Robert-Koch-Institut und Vodafone.[1]

2. Handy-Tracking nach PEPP-PT

Die Funktionsweise der App, die nach den Vorarbeiten des PEPP-PT entwickelt wird, ist wie folgt zu skizzieren. Hinzuweisen ist jedoch vorab darauf, dass bislang nicht alle Funktionsdetails veröffentlicht sind.

Auf den Handys, die die App nutzen, wird in regelmäßigen zeitlichen Abständen **eine individuelle ID** erzeugt und gespeichert. Diese besteht aus einer Zahlen-Buchstaben-Kombination und soll eindeutig sein, aber keine Rückschlüsse auf die Person des Handyinhabers zulassen. Hält sich eine Person mit einem Abstand von weniger als (wahrscheinlich) zwei Metern zu einer anderen Person auf und geschieht dies für einen gewissen Zeitraum (wahrscheinlich 15 Minuten), werden die IDs der jeweiligen Nutzer untereinander ausgetauscht und **lokal** auf dem jeweiligen Handy **verschlüsselt gespeichert**. Wenn anschließend eine der beiden Personen positiv auf das Coronavirus getestet werden sollte, kann sie dies mit Hilfe einer Tan-Nummer in der App angeben. Das Konzept sieht dann – anders als in den Anwendungen anderer Länder – vor, dass die Liste mit den Kontakten einer positiv getesteten Person auf einen gesicherten **Server des Robert-Koch-Instituts** hochgeladen wird. Das Institut warnt dann seinerseits die Kontaktpersonen. Auch auf dem Server sollen die Daten jedoch anonymisiert bleiben.2 In keinem Fall werden persönliche Daten oder der Aufenthalts- und Begegnungsort gespeichert oder irgendwie bekannt gegeben. Die Nutzer würden mit der Benachrichtigung gebeten werden, sich testen zu lassen und bis zu einem Testergebnis in häusliche Isolation zu begeben.[3]

Die App-Nutzung soll dabei ebenso **freiwillig** sein, wie die Bekanntgabe eines positiven Testergebnisses und das Hochladen der Kontaktdaten auf den Server. **Ziel** der App soll es sein, durch eine schnelle und einfache Rückverfolgbarkeit von Kontakten die **Ausbreitung von Infektionen** zu **verhindern** bzw. deutlich zu vermindern, was wiederum dem Gesundheits- und Lebensschutz der ganzen Bevölkerung dienen soll.

---

1 Eine Selbstbeschreibung findet sich unter https://www.pepp-pt.org (zuletzt aufgerufen am 6.4.2020).

2 Benrath/Mihm/Neuscheler, „Wenn das Handy zum Corona-Schutz wird“, FAZ vom 3.4.2020, S. 22.

3 Vgl. zur Funktionsweise: Budras/Freidel, „Technik gegen die Seuche“, FAS vom 5.4.2020, S. 3.

Die Abstandsmessung soll über Sensoren des Handys mittels **Bluetooth** erfolgen. Bluetooth hat nur eine geringe Reichweite. Kritisiert wird aber, dass diese geringe Reichweite je nach äußeren Umständen deutlich variieren kann. Teilweise kann sie unter einem Meter liegen, im günstigsten Fall aber auch bis zu 100 Metern weit reichen. Insbesondere kann ein Signal mitunter auch durch Wände oder Glasscheiben hindurch gehen. Es besteht also einerseits die Möglichkeit, dass ansteckungsrelevante Kontakte nicht erfasst werden. Andererseits ist nicht auszuschließen, dass aufgrund von größerer Entfernung oder Barrieren sichere Abstände fälschlicherweise als relevanten Kontakt gespeichert werden.[4] Zudem können absichtliche oder zufällige Falschmeldungen nicht ausgeschlossen werden. Die Entwickler bauen insoweit darauf, dass die Nutzer mit der App verantwortungsvoll umgehen.[5]

3. Grundrechte

3.1. Fernmeldegeheimnis – Art. 10 Abs. 1 GG

Der Schutzbereich des **Fernmeldegeheimnisses** nach Art. 10 Abs. 1 GG ist **nicht eröffnet**. Das Fernmeldegeheimnis – oder auch Telekommunikationsgeheimnis genannt – schützt die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit der Hilfe des Telekommunikationsverkehrs.[6] Geschützt sind dabei sowohl der Kommunikationsinhalt als auch die Kommunikationsumstände.[7] Kommunikation kann insofern aber nur als konkret **menschlich veranlassten Informationsaustausch** oder -aussendung verstanden werden, also einen Vorgang, bei dem ein Mensch willentlich mit einer konkretisierten anderen Person in den Kontakt tritt. Dies wird zum einen auch an dem Tatbestandsmerkmal des „individuellen Empfängers“ deutlich. Zum anderen knüpft auch die Rechtsprechung zum Fernmeldegeheimnis bislang stets an eine zielgerichtete Informationsübermittlung an, etwa das Versenden einer E-Mail,[8] die Kommunikation über Telefone oder das Aufrufen von Internetseiten.[9] Die automatisierte Sendung von Daten eines Handys zu einem anderen ohne weitere menschliche Beteiligung kann daher nicht unter den Schutzbereich subsumiert werden. Die Installation der entsprechenden App reicht insofern als Anknüpfungspunkt nicht aus.

---

4 Budras/Freidel, „Technik gegen die Seuche“, FAS vom 5.4.2020, S. 3.

5 Vgl. dazu auch bzgl. der in Österreich verwendeten App: Benrath/Mihm/Neuscheler, „Wenn das Handy zum Corona-Schutz wird“, FAZ vom 3.4.2020, S. 22.

6 BVerfG, Urteil vom 16.6.2009 – 2 BvR 902/06, BVerfGE 124, 43, 54; BVerfG, Urteil vom 2.3.2006 – 2 BvR 2099/04, BVerfGE 115, 166, 182.

7 BVerfG, Urteil vom 16.6.2009 – 2 BvR 902/06, BVerfGE 124, 43, 54; Ogorek, in: Epping/Hillgruber (Hrsg.), BeckOK Grundgesetz, 42. Edition, Stand: 1.12.2019, Art. 10, Rn. 35-38.

8 BVerfG, Urteil vom 16.6.2009 – 2 BvR 902/06, BVerfGE 124, 43, 54.

9 BVerfG, Urteil vom 2.3.2010 – 1 BvR 256/08 BVerfGE 125, 260.

3.2. Recht auf informationelle Selbstbestimmung – Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

In Betracht kommt eine Verletzung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Aus dem Allgemeinen Persönlichkeitsrecht wird auch das **Recht auf informationelle Selbstbestimmung** abgeleitet.

3.2.1. Schutzbereich und Eingriff

Das Recht auf informationelle Selbstbestimmung umfasst das Recht des Einzelnen, grundsätzlich selbst zu entscheiden, wann und gegenüber wem er zu welchem Zweck Lebenssachverhalte im Allgemeinen und personenbezogene Daten im Besonderen offenbart.[10] Da die Erfassung von Kontakten auch zu diesen Lebenssachverhalten gehören kann, deren Kundgabe zu den Rechten des Einzelnen gehört, kann man annehmen, dass der **Schutzbereich** des Grundrechts eröffnet ist.

Fraglich ist aber, ob ein **Eingriff** in diesen Schutzbereich vorliegt. Im Sinne des klassischen Eingriffsbegriffs liegt ein Eingriff vor, wenn er final, unmittelbar, durch Rechtsakt sowie mit Befehl und Zwang gegenüber dem Einzelnen angeordnet bzw. durchgesetzt wird.[11] Durch den neuen Eingriffsbegriff wurde diese Definition erweitert. Nunmehr ist als Eingriff jedes staatliche Handeln umfasst, das ein grundrechtlich geschütztes Verhalten erschwert oder unmöglich macht bzw. ein grundrechtlich geschütztes Rechtsgut beeinträchtigt. Umfasst sind auch mittelbare und faktische Eingriffe.[12] Durch die **Freiwilligkeit der Verwendung der App** kann aber jede Person frei entscheiden, ob sie eine für sie individuell und regelmäßig wechselnde ID mit anderen Personen teilen will oder nicht. Ebenso ist das spätere Teilen der Information über einen positiven Coronatest freiwillig. Insofern kann weder final, imperativ noch mittelbar oder faktisch ein Eingriff erkannt werden.

Auch das Argument, dass die Freiwilligkeit der **App-Nutzung erzwungen** sei, weil der soziale Druck zu deren Nutzung zu hoch sei,[13] ist nicht überzeugend. In Deutschland nutzten 2018 **81 Prozent** der über 14-Jährigen ein Smartphone. Bei den über 65-Jährigen nutzte jeder Vierte ein Smartphone.[14] Insofern steht für alle Beteiligten von Vornherein fest, dass nicht die ganze Bevölkerung diese App

---

10 BVerfG, Urteil vom 4.4.2006 – 1 BvR 518/02, BVerfGE 115, 320, 341; Dreier, in: ders. (Hrsg.), Grundgesetz-Kommentar, 3. Auflage 2013, Art. 2 Abs. 1, Rn. 79.

11 Ipsen, Staatsrecht II, 21. Auflage 2018, Rn. 143; Voßkuhle/Kaiser, JuS 2009, 313.

12 Voßkuhle/Kaiser, JuS 2009, 313.

13 Brink/Henning, „Warum freiwilliges Handy-Tracking nicht funktioniert“, vom 3.4.2020, abrufbar unter https://netzpolitik.org/2020/warum-freiwilliges-handy-tracking- nicht-funktioniert/ (zuletzt aufgerufen am 8.4.2020).

14 Statista, Anteil der Smartphone-Nutzer in Deutschland bis 2018, veröffentlicht von F. Tenzer, 5.11.2019, Erhebung durch Bitkom Research, abrufbar unter https://de.statista.com/statistik/daten/studie/585883/umfrage/anteil-der-smartphone-nutzer-in-deutschland/ (zuletzt aufgerufen am 8.4.2020).

nutzen kann und wird. Weitere diskutierte Wege, für Nicht-Smartphonenutzer einen Schlüsselanhänger mit einer vergleichbaren Funktion anzubieten,[15] sind derzeit wohl noch nicht weiter entwickelt. Zudem wird auch kommuniziert, dass der Nutzungsgrad von **60 Prozent der Bevölkerung angestrebt** wird.[16] Laut ersten Umfragen würden 50 bis 70 Prozent der Deutschen eine solche Tracking-App nutzen.[17] Mithin wird auch von Beginn an kein erheblicher Druck ausgeübt, dass alle Smartphoneinhaber die App auch nutzen müssten.

Zudem könnte in der Speicherung von Daten, die die Erstellung eines umfassenden **Bewegungsprofils** ermöglicht, ein Grundrechtseingriff liegen.[18] Da durch die geplante Handy-App aber weder der Ort noch die genaue Länge einer Begegnung gespeichert werden, sondern nur eine Aussage darüber gespeichert werden soll, ob sich eine Person länger als eine zuvor definierte Zeit in einem gewissen Abstand zu einer anderen Person befunden hat, ist das Erstellen eines solchen Bewegungsprofils nicht möglich.

Inwieweit doch irgendwelche Möglichkeiten bestehen könnten, entgegen den Angaben der Entwickler eine ID durch Dritte einer konkreten Person zuzuordnen, kann nicht beurteilt und somit auch nicht in die Prüfung einbezogen werden.

Ein Eingriff könnte nur bei einer verpflichtenden Nutzung der App angenommen werden.

3.2.2. Verhältnismäßigkeit

Auch wenn, wie dargestellt, kein Eingriff in die Grundrechte bei einer freiwilligen Nutzung der App angenommen werden kann, sollen einige Hinweise zur Verhältnismäßigkeit der Maßnahmen gegeben werden. Für die Annahme der **Verhältnismäßigkeit** eines Eingriffs bedarf es eines legetimen Zwecks, der mit der Maßnahme erreicht werden soll, wobei diese geeignet, erforderlich und angemessen sein muss, um diesen Zweck auch zu erreichen.

Legitimer Zweck: Mit der Verwendung und weiten Verbreitung der Nutzung der App zum Handy-Tracking wird das Ziel des **Infektionsschutzes** und damit des **Lebensschutzes** verbunden. Durch die schnelle und unbürokratische Feststellung eines infektionsrelevanten Kontakts soll zum einen die **Ausbreitung** des Virus und damit zugleich eine **Überlastung des Gesundheitssystems** verhindert werden, die dazu führen könnte, dass nicht allen infizierten Personen adäquat geholfen werden

---

15 So wird es derzeit in Österreich diskutiert. Vgl. Münch/Muth, Debatte um Pflicht zu Corona-App-Nutzung, SZ am 6.4.2020, abrufbar unter: https://www.sueddeutsche.de/politik/corona-app-pepp-pt-tracing-oesterreich-deutschland-1.4868497 (zuletzt abgerufen am 8.4.2020).

16 Vgl. u.a. Benrath/Mihm/Neuscheler, „Wenn das Handy zum Corona-Schutz wird“, FAZ vom 3.4.2020, S. 22.

17 Banse, „Wie Handy-Tracking funktioniert“, Deutschlandfunk vom 1.4.2020, abrufbar unter https://www.deutschlandfunk.de/kampf-gegen-coronavirus-ausbreitung-wie-handy-tracking.2897.de.html?dram:article_id=473614 (zuletzt aufgerufen am 9.4.2020).

18 Vgl. BVerfG, Urteil vom 2.3.2010 – 1 BvR 256/08 BVerfGE 125, 260, Rn. 211 f.; vgl. auch Appell der Europäischen Akademie für Informationsfreiheit und Datenschutz: Corona – Pandemie bekämpfen, Bürgerrechte und Datenschutz wahren!, vom 26.3.2020, abrufbar unter https://www.eaid-berlin.de/appell-der-europaeischen- akademie-fuer-informationsfreiheit-und-datenschutz-corona-pandemie-bekaempfen-buergerrechte-und- datenschutz-wahren/ (zuletzt aufgerufen am 8.4.2020).

könnte. Darüber hinaus könnte die Verwendung der App und die dadurch verbesserte Infektionskontrolle eine **Lockerung** der bisherigen **Infektionsschutzmaßnahmen** (zum Beispiel Kontaktsperren und Schließungen von Geschäften und Restaurants) begünstigen. Dies wiederum könnte die wirtschaftlichen Folgen der Epidemie abmildern. Bei beiden Zwecken handelt es sich um solche, die dem Schutz der Grundrechte der Bevölkerung dienen und somit um legitime Zwecke.

Geeignetheit: Die unmittelbare **Information** über einen Kontakt mit einer positiv getesteten Person kann dazu führen, dass auch die Kontaktperson sich einerseits schnell **isoliert** und so, falls sie infiziert ist, das Virus nicht selbst weiterverbreitet. Zudem könnte gegenüber dieser Person umgehend nach einem ebenfalls positiven Coronatest eine Quarantäneanordnung erlassen werden. Insofern kann von einer grundsätzlichen Eignung des Handy-Trackings zum **Infektionsschutz** ausgegangen werden.

Insbesondere die bekannten Ungenauigkeiten der Bluetooth-Technologie und die damit bestehende Gefahr von Falschwarnungen bzw. unterbliebenen Warnungen bei gleichzeitigem Vertrauen auf die Funktion der App, könnten die Geeignetheit in Frage stellen. Ebenso die Problematik der durch die Freiwilligkeit der App-Nutzung nicht vollständigen Erfassung aller möglichen Infektionsherde.[19] Jedoch führen diese Maßnahmen nur zu einer möglichen Einschränkung der Bewegungsfreiheit durch eine erhöhte Quote nicht notwendiger Selbstisolation. Der Lebensschutz und die grundrechtsrelevanten Aspekte der Lockerung der derzeitigen Infektionsschutzmaßnahmen werden dadurch gerade nicht beeinträchtigt.

Zudem ist zu beachten, dass die Erreichung des Ziels mit dem Handy-Tracking massiv damit zusammenhängt, dass genügend Testmöglichkeiten bestehen, nachdem ein Nutzer die Nachricht über einen Kontakt mit einer infizierten Person erhalten hat. Zum einen kann nur dann er selbst seinerseits die Information seiner Kontakte veranlassen, zum andern muss davon ausgegangen werden, dass im Laufe der Zeit die Zahl der Infizierten und damit auch der Kontakte steigt. Insofern könnten sich solche Benachrichtigungen bei einzelnen Personen häufen.[20] Um deren Bereitschaft zur wiederholten freiwilligen vorläufigen Selbstisolation nicht zu gefährden, bedarf es schneller und zahlreicher Testkapazitäten.

Erforderlichkeit: Eine Maßnahme ist dann erforderlich, wenn keine **anderen Mittel** zur Verfügung stehen, die in gleicher oder sogar besserer Weise das Ziel erreichen könnten. Im Rahmen des Infektionsschutzes kommen mehrere Möglichkeiten zum Lebensschutz in Betracht. Dazu zählen vor allem die bisher ergriffenen **Kontaktbeschränkungen, Wirtschaftsbeschränkungen**, Einreiseverbote, Versammlungsverbote, etc. Bei diesen handelt es sich aber einerseits um sehr grundrechtssensible Maßnahmen, zum andern führen diese zu erheblichen Auswirkungen auf die inländische

19 Vgl. zu Bedenken hinsichtlich der Geeignetheit auch: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, Handy-Tracking vs. Corona (Stand 31.03.2020), abrufbar unter https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Handy-Tracking_vs._Corona.pdf (zuletzt aufgerufen am 7.4.2020).

20 Ähnlich Bedenken äußern auch: Brink/Henning, „Warum freiwilliges Handy-Tracking nicht funktioniert“, vom 3.4.2020, abrufbar unter https://netzpolitik.org/2020/warum-freiwilliges-handy-tracking- nicht-funktioniert/ (zuletzt aufgerufen am 8.4.2020).

Wirtschaft. Eine weitere Maßnahme könnten regelmäßige **flächendeckende Tests** auf das Coronavirus sein, mit denen Erkrankte schnell erkannt werden können und dann entsprechende Maßnahmen der Quarantäne ergriffen werden können. Jedoch stehen derzeit in Deutschland noch keine ausreichenden Testmöglichkeiten und Laborkapazitäten bzw. Schnelltests dafür zur Verfügung. Zudem würde ein verpflichtender Test mit dem **Recht auf Nichtwissen** als negativer Variante des Rechts auf informationelle Selbstbestimmung[21] kollidieren. Mithin sind zunächst keine anderen ebenso geeigneten Mittel ersichtlich und die Erforderlichkeit der Maßnahme wäre gegeben.

Angemessenheit: Eine Maßnahme ist nur dann angemessen, wenn die mit der Maßnahme verbundenen Nachteile nicht vollkommen außer Verhältnis der damit verbundenen Vorteile stehen. Dies ist schon aufgrund der auf Grundrechtsebene nicht vorhandenen Annahme eines Eingriffs bei einem **freiwilligen Handy-Tracking** als gegeben anzunehmen. Auch aus der weiteren verfassungsgerichtlichen Rechtsprechung können keine Anhaltspunkte entnommen werden, die gegen die Angemessenheit sprechen würden.

Die im Urteil des Bundesverfassungsgerichts (BVerfG) zur Vorratsdatenspeicherung[22] getroffenen Aussagen lassen sich auf die geplante Tracking-App nur peripher übertragen. Insbesondere die Grundunterscheidung, dass die relevanten Daten nicht bei dem Telekommunikations- oder App-Anbieter gespeichert werden, sondern auf dem Handy des jeweiligen App-Nutzers selbst, und dass er bei einer positiven Coronainfektion selbst über die Weitergabe der Daten entscheiden kann, führen zu erheblichen Unterschieden.

Das BVerfG machte in seiner Entscheidung zur Vorratsdatenspeicherung die Aspekte der Datensicherheit und der **Transparenz der Datenübermittlung** zu Teilen der Verhältnismäßigkeitsabwägung des Grundrechtseingriffs. Die durch das BVerfG aufgestellten Anforderungen an die **Datensicherheit**[23] der gespeicherten Kontaktdaten scheinen zunächst in Bezug auf die Speicherung der Daten auf dem Gerät des App-Verwenders gewährleistet. Jedoch ist das Pendant der einzelnen Kontaktdaten auch stets auf dem Handy einer anderen Person gespeichert. Dies könnte Missbrauchsmöglichkeiten eröffnen. Jedoch sind auch dieser Person nicht die einzelnen Kontakte im konkreten bekannt, sondern nur eine ID, die sie selbst in der Regel keiner anderen Person zuordnen kann. Ausnahmen könnten nur dann bestehen, wenn die Kontakte nur mit einer oder sehr wenigen Personen bestanden. Fraglich ist, ob die App so konzipiert sein soll, dass die einzelne Person die weiteren gespeicherten IDs sehen kann. Wenn dies nicht der Fall ist, ist auch hier eine Identifikation ausgeschlossen.

Auch die Datenübermittlung ist im Sinne des BVerfG **transparent**.[24] Sie erfolgt nur im Zusammenhang der Meldung einer Kontaktperson als auf das Virus positiv getestet und führt unmittelbar über den Server zu einer Mitteilung an die Kontaktpersonen. Insofern erlangt man von jeder Übermittlung der eigenen IDs von Dritten an den Server Kenntnis.

---

21 Di Fabio, in: Maunz/Dürig (Hrsg.), Grundgesetz-Kommentar, 89. EL Oktober 2019, Art. 2 Abs. 1 GG, Rn. 192.

22 BVerfG, Urteil vom 2.3.2010 – 1 BvR 256/08 BVerfGE 125, 260.

23 BVerfG, Urteil vom 2.3.2010 – 1 BvR 256/08 BVerfGE 125, 260, Rn. 221 ff.

24 BVerfG, Urteil vom 2.3.2010 – 1 BvR 256/08 BVerfGE 125, 260.

Fraglich ist, inwieweit die unter 2. geschilderte mögliche Ungenauigkeit der Bluetooth-Technologie zu einem anderen Ergebnis der Angemessenheitsprüfung führen kann. Dies müsste im Wesentlichen davon abhängig gemacht werden, wie hoch die Fehlerquote tatsächlich ist. Um die Fehlerquote entsprechend zu verringern, führen die Entwickler derzeit umfassende Tests mit Hilfe der Bundeswehr durch. Solange keine genauen Angaben zur Fehlerquote vorliegen, können diese vorläufig das Abwägungsergebnis nicht in Frage stellen. Eventuell könnte auch mittels eines entsprechenden Hinweises an die App-Nutzer über gewisse Fehlerquellen einschneidenden Folgen von Falschmeldungen begegnet werden.

3.3. Hinweis auf potentielle Grundrechtseingriffe

Über die genaue Ausgestaltung der Infektionswarnung, die seitens des Robert-Koch-Instituts an die Handys mit entsprechendem Kontakt zu Coronapositiv-Getesteten gesendet werden würde, ist bislang wenig bekannt. Da beispielsweise eine Quarantäneanordnung nach § 30 Infektionsschutzgesetz nur durch die zuständige Behörde und damit in der Regel das Gesundheitsamt erlassen werden kann, ist davon auszugehen, dass seitens des Robert-Koch-Instituts nur ein Hinweis bzw. eine Bitte zur Isolation und zum Test erfolgt, ohne dass aus dieser Nachricht konkrete Rechtsfolgen resultieren. Es können auch mangels des Vorliegens personenbezogener Daten keine an das Gesundheitsamt gemeldet werden, damit dieses entsprechende Maßnahmen einleitet. Mithin kann auch in der Information über einen entsprechenden Kontakt kein Eingriff in ein Grundrecht liegen.

Fraglich ist auch, wie die Maßnahme des Handy-Trackings mit den Grundrechten zu vereinbaren wäre, wenn an die **Nutzung** der entsprechenden Handy-App die Teilnahme an bestimmten Teilen des **öffentlichen Lebens**, wie zum Beispiel Restaurantbesuche **geknüpft** wird.[25] Ein solcher Ausschluss von Nicht-App-Nutzern könnten zwar wohl als Schutzmaßnahmen auf der Grundlage von § 28 Abs. 1 Infektionsschutzgesetz angeordnet werden, sie würden jedoch auch einen Eingriff in die allgemeine Handlungsfreiheit, Berufs-, Gewerbe- und Eigentumsfreiheit sowie in den allgemeinen Gleichbehandlungsgrundsatz darstellen. Eine Rechtfertigung dessen scheint ohne einen leicht zugänglichen Ersatz (s.o. zum Beispiel Schlüsselanhänger) für Personen, die kein Smartphone nutzen, nicht möglich.

3.4. Zwischenergebnis

Im **Ergebnis** führt die Abwägung also zu folgendem Ergebnis: Wenn durch das Handy-Tracking die Ausbreitung des Virus vermindert und einer Überlastung des Gesundheitssystems entgegengewirkt werden kann, dann sind bestimmte Eingriffe in die Privatsphäre durchaus gerechtfertigt.[26]

---

25 So der Vorschlag von Löffler, „Ins Restaurant nur mit Corona-App?“, LTO vom 8.4.2020, abrufbar unter https://www.lto.de/recht/hintergruende/h/corona-app-diskriminierung-milderes-mittel-auflage-ende-ausgangssperre-exit-strategie/ (zuletzt aufgerufen am 8.4.2020).

26 Im Ergebnis auch: Buermeyer, „Ein Richter erklärt, wie die Corona-App aussehen müsste“, Der Tagesspiegel, 31.3.2020, abrufbar unter https://www.tagesspiegel.de/politik/eine-zwangs-app-darf-es-nicht-geben-ein-richter-erklaert-wie-die-corona-app-aussehen-muesste/25699280.html (zuletzt aufgerufen am 8.4.2020).

4. Datenschutzrecht

4.1. Keine Anwendbarkeit des Datenschutzrechts

Die Anwendbarkeit des Datenschutzrechts (EU-Datenschutzgrundverordnung (DSGVO) sowie Bundesdatenschutzgesetz) erfordert, dass die Verarbeitung **personenbezogener Daten** in Rede steht. Nach Art. 4 Abs. 1 Nr. 1 DSGVO sind „personenbezogene Daten“:

> „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden "betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“.

Die Identifizierbarkeit der Person anhand dieser Daten genügt also. Fraglich ist, ob dies auch bei einer in regelmäßigen Zeitabständen **wechselnden ID** auf einem Handy der Fall ist.

Der EuGH entschied zu einer ähnlich gelagerten Konstellation von dynamisch wechselnden IP-Adressen eines Online-Mediendienstes:

> „1. Eine dynamische IP-Adresse stellt keine Information dar, die sich auf eine ‚bestimmte natürliche Person‘ bezieht, da sich aus ihr unmittelbar weder die Identität der natürlichen Person ergibt, der der Computer gehört, von dem aus eine Website abgerufen wird, noch die Identität einer anderen Person, die diesen Computer benutzen könnte. […]
>
> 3. Dass über die zur **Identifizierung des Nutzers** einer Website erforderlichen Zusatzinformationen nicht der Anbieter von Online-Mediendiensten, sondern der Internetzugangsanbieter dieses Nutzers verfügt, vermag nicht auszuschließen, dass die von einem Anbieter von Online-Mediendiensten gespeicherten dynamischen IP-Adressen für ihn **personenbezogene Daten** im Sinne von Art. 2 Buchst. a der Richtlinie 95/46 darstellen. Maßgeblich hierfür ist jedoch, ob für den Anbieter von Online-Mediendiensten die Möglichkeit, eine dynamische IP-Adresse mit den **Zusatzinformationen zu verknüpfen**, über die der Internetzugangsanbieter verfügt, ein Mittel darstellt, das vernünftigerweise zur Bestimmung der betreffenden Person eingesetzt werden kann. Dies ist nicht der Fall, wenn die **Identifizierung** der betreffenden Person **gesetzlich verboten** oder **praktisch nicht durchführbar** wäre, z. B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, so dass das Risiko einer Identifizierung de facto vernachlässigbar erschiene.“[27]

27 EuGH, Urteil vom 19.10.2016 - C-582/14, redaktionelle Leitsätze 1 und 3 nach MIR, abrufbar unter https://medien-internet-und-recht.de/volltext.php?mir_dok_id=2791 (zuletzt aufgerufen am 9.4.2020), Hervorhebung nur hier.

Die gleichen Grundsätze gelten nach Erwägungsgrund 26 zur DSGVO auch nach der aktuellen Rechtslage für pseudonymisierte Daten.[28] Nach den bisher bekannten Parametern für das Handy-Tracking nach PEPP-PT muss davon ausgegangen werden, dass keine personenbezogenen Daten verwendet werden. Es sollen bei der App-Nutzung **keine persönlichen Daten** eingegeben oder gespeichert werden. Möglichkeiten der **Verknüpfung** mit weiteren bekannten Daten sind zunächst **nicht ersichtlich**, solange die App **autark** arbeitet und ihrerseits ebenfalls auf keine weiteren anderen Hilfsdienste zurückgreift,[29] wie es die Entwickler vorsehen.[30] Insofern läge die Anwendung des Handy-Trackings nach dem geschilderten Konzept außerhalb der Anwendung des Datenschutzrechts.

Zweifel äußert insofern der Datenschutzbeauftragte des Landes Baden-Württemberg, der die Information für Pseudonyme, also einer Person zuordenbaren Daten hält. Jedoch räumt auch dieser ein, die Funktionsweisen der App nicht genau zu kennen und daher nicht überprüfen zu können.[31] Er verlangt jedoch eine umfassende **Datenschutz-Folgenabschätzung** nach Art. 35 DSGVO. In diese ließen sich sowohl die im Rahmen der Grundrechtsabwägung genannten Aspekte, als auch die folgenden ergänzenden Erwägungen einbeziehen.

4.2. Ergänzende Erwägungen

Auch wenn das Datenschutzrecht hier nicht für anwendbar gehalten wird, sind noch einige allgemeine Erwägungen aus dem datenschutzrechtlichen Kontext sinnvoll.

Zunächst ist darauf hinzuweisen, dass durch den Verzicht der App auf die Eingabe persönlicher Daten dem Grundsatz der **Datensparsamkeit** entsprochen wird. Dafür ist auch notwendig, dass eine Frist zur **Löschung** der Kontaktdaten auf den Handys der einzelnen Nutzer festgelegt wird. Diese könnte zum Beispiel dem Ablauf der als Quarantänefrist festgelegten 14 Tage entsprechen.[32]

Fraglich ist, ob es sich bei den zu verarbeitenden Daten um sog. **„Gesundheitsdaten“** handelt, die einem **besonderen Schutz** (Art. 9 Abs. 1 DSGVO) unterliegen. Nach Art. 4 Nr. 15 DSGVO sind „Gesundheitsdaten“:

---

28 Amtsblatt der Europäischen Union L 119/1 vom 4.5.2016, S. 5.

29 In Forenbeiträgen als problematisch diskutiert wird das eventuelle Zurückgreifen der Tracking-App auf einen Client zur Benachrichtigung mit einer Push-Nachricht bei einem positiv-getesteten Kontakt. Inwieweit hier die Notwendigkeit besteht, auf eine andere Software zurückzugreifen, kann jedoch technisch nicht beurteilt werden.

30 Buermeyer als Antwort in den Kommentaren zu https://netzpolitik.org/2020/corona-tracking-datenschutz-kein-notwendiger-widerspruch/ (zuletzt aufgerufen am 9.4.2020).

31 Vgl. Brink/Henning, „Warum freiwilliges Handy-Tracking nicht funktioniert“, vom 3.4.2020, abrufbar unter https://netzpolitik.org/2020/warum-freiwilliges-handy-tracking-nicht-funktioniert/ (zuletzt aufgerufen am 9.4.2020).

32 So auch: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, Handy-Tracking vs. Corona (Stand 31.3.2020), abrufbar unter https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Handy-Tracking_vs._Corona.pdf (zuletzt aufgerufen am 7.4.2020).

> „personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“.

Dies kann für die gespeicherten Kontaktdaten nicht angenommen werden. Jedoch könnte die Meldung der einzelnen Person, dass sie positiv auf das Virus getestet wurde, eine solche Information darstellen. Erheblich ist an dieser Stelle aber erneut, ob die gemeldete ID hier als personenbezogenes Datum erkannt wird. Falls nein, dann ist die alleinige Information, dass der Inhaber einer bestimmten ID das Coronavirus hat, noch kein Gesundheitsdatum im Sinne der DSGVO.

Schließlich ist darauf hinzuweisen, dass die Verarbeitung eines personenbezogenen Datums nach Art. 6 Abs. 1 a) DSGVO dann rechtmäßig ist, wenn die betroffene Person ihre **Einwilligung** zu der Verarbeitung für einen oder mehrere bestimmte Zwecke gegeben hat. Eine solche Einwilligung könnte im Zusammenhang mit der Installation der App abgefragt werden. Auch an dieser Stelle kommt insofern die Freiwilligkeit der Nutzung des Handy-Trackings zum tragen.

***