Martin-Luther-Universität Halle-Wittenberg
Naturwissenschaftliche Fakultät III
Institut für Informatik

Seminar

Informatik und Gesellschaft

Sommersemester 2020

geleitet durch Prof. Dr. Paul Molitor

Datenschutz in Zeiten von Covid-19
Selbstzweck oder Grundbedingung?

Tim Gleichmann & Pascal Teubert

Inhaltsverzeichnis

1 Einleitung **4**

2 App-Einsatz in der Pandemiebekämpfung **5**
2.1 Intentionen des App-Einsatzes 5
2.2 Tracking versus Tracing 5
2.3 Das Robert Koch Institut und die Deutsche Telekom 7
2.4 Voraussetzungen für den Erfolg 7

3 Die Datenspende-App des RKI **8**
3.1 Verwirrung umd die Datenspende-App 8
3.2 Funktion und erhobene Daten 9
3.3 Datenschutz 10

4 Rechtliche Grundlagen **11**
4.1 BDSG und DSGVO 11
4.2 Gesetzentwurf des Gesundheitsministers Jens Spahn (März 2020) . . . 13
4.3 Infektionsschutzgesetz 14

5 Internationale Corona-Apps **15**
5.1 Israel 15
5.2 Polen 16
5.3 China 17
5.4 Südkorea 18
5.5 Tschechien und Slowakei 18

6 Deutsche Corona-Warn-App **19**
6.1 Das zähe Ringen um die App 19
6.2 Diskutierte Formen 20
6.2.1 PEPP-PT Initiative 20
6.2.2 DP-3T App 21
6.2.3 „STOPP-Corona“-App der accenture GmbH (Österreich) 22
6.3 Umsetzung in der finalen Version 23
6.4 Datenschutz 24

7 Diskussion und Fazit **25**

8 Literatur **25**

Gender-Hinweis: Die weibliche Form ist der männlichen Form in dieser Arbeit gleichgestellt; lediglich aus Gründen der Vereinfachung wurde an einigen Stellen nur die männliche Form gewählt.

Überarbeitung durch den Dozenten: Der vorliegende Text entspricht im Wesentlichen dem ursprünglichen durch Herrn Tim Gleichmann und Herrn Pascal Teubert erstellten Bericht. Der Dozent hat lediglich die sehr wenigen Schreib- und Kommatafehler entfernt, und die Formatierung an die Vorgaben angepasst.

1 Einleitung

Wir schreiben das Jahr 2020. Die ganze Welt befindet sich in Aufbruchstimmung in ein neues Jahrzehnt, es sollte das Jahr für viele werden: Klimakampf, die After-Britain-EU, vielleicht das Ende Trumps. Die ganze Welt? Nein! In der kleinen Metropole Wuhan im fernen China bricht Ende Januar ein Virus aus, das bereits seit Dezember bekannt war und doch bis dato unterschätzt wurde. Und noch immer belächelt man die drohende Gefahr, von einer Epidemie möchte kaum einer sprechen. Zwei Monate später, im März 2020, ist keine Rede mehr von einer Epidemie, was angesichts der weltweiten Ausbrüche auch völlig untertrieben wäre. Das Wort der Stunde heißt Pandemie!

Mittlerweile ist auch Deutschland betroffen, 60.000 Infizierte und fast 5.000 [1] neue Fälle täglich, die Dunkelziffer scheint deutlich höher zu sein. Auch wenn hierzulande die Letalität mit 0,9 Prozent und ca. 500 offiziell gemeldete Toten verhältnismäßig gering erscheint (Stand März 2020), so setzt man doch auf rigorose Maßnahmen: Kontaktsperren, Schließung von Schulen (man kann hier zu keinem Zeitpunkt von einem „Lockdown“ im eigentlichen Sinne reden, da z.B. die Produktion der Industrie jederzeit möglich war) und Ausgangsbeschränkungen. Die Maskenpflicht ist zu diesem Zeitpunkt noch keine Option, da die flächendeckende Versorgung mit Masken bereits für medizinisches Personal kaum gewährleistet werden kann. Ein Impfstoff ist ebenso weit entfernt wie ein wirksames Medikament gegen das Virus.

Und doch machen Experten und Politik der Bevölkerung leise Hoffnungen auf Besserung: Man wolle zeitnah denselben Weg gehen wie Südkorea, Ende März Vorreiter der Pandemiebekämpfung, das ostasiatische Land verzeichnet entgegen dem weltweiten Trend sinkende Infektionszahlen. Mit einer Corona-App soll wieder mehr Begegnung in Zeiten von Social Distancing möglich sein, vielfach ist von einer neuen Normalität mit dem Virus die Rede. Für die einen Hoffnungsträger, für die anderen eine Gefahr im Stil einer „NSA 2.0“, ähnlich schlimm wie die befürchtete „Zwangsimpfung“. Seit den Vorfällen, die Whistleblower Edward Snowden 2013 öffentlich machte, stehen die Deutschen dem Umgang mit ihren Daten kritischer gegenüber: Ist eine solche App sicher? Werden wir zukünftig überwacht, auf Schritt und Tritt überwacht? Viele waren skeptisch, das Ringen begann.

Im Folgenden blicken wir aus dem August des Jahres 2020 zurück auf vier Monate des Ringens um die App. Es soll geklärt werden, wie sicher die App geworden ist. Fand dabei eine Abwägung zu Gunsten von Infektions- oder Datenschutz als Prämisse des weiteren Handelns statt?

[1] Situationsbericht des Robert Koch Instituts (RKI) vom 31.03.2020

2 App-Einsatz in der Pandemiebekämpfung

2.1 Intentionen des App-Einsatzes

Der Einsatz von Smartphone-Apps bietet für die Bekämpfung oder Eindämmung von Pandemien eine Vielzahl von Möglichkeiten. Diese lassen sich grundsätzlich in drei große Funktionen einteilen, die allerdings nicht trennscharf betrachtet werden können: Prävention, Eindämmung und Überwachung.

Überwachung ist an dieser Stelle keineswegs auf die Bevölkerung oder einzelne Erkrankte zu beziehen. Sie meint vielmehr eine Datenerhebung zur Einschätzung verschiedener App-gestützter Pandemiefaktoren, die ihren Anteil zur Entscheidungsfindung über politische Maßnahmen der Viruseindämmung beitragen können. Bewegungsprofile sollen helfen, Verbreitungswege und besondere Personenkumulationen zu erkennen und gegebenenfalls zu unterbinden (siehe Kapitel 2.3). Gleichzeitig sollen Frühwarn- und Inzidenzsysteme geschaffen werden, die einerseits als Indikatoren einen Anstieg der Infektionszahlen schnellstmöglich anzeigen und andererseits besonders betroffene Regionen kennzeichnen sollen. Das Hauptziel dieser Pandemieüberwachung stellt also eine bessere Datenlage zur Einschätzung des jeweiligen Infektionsgeschehens dar, die ergänzend zu epidemiologischen Studien sind. (Kapitel 3.1) Dass diese Datenerhebung vorbeugende Maßnahmen ebenso unterstützt wie die Eindämmung, zeigt die elementare Verzahnung der einzelnen Ziele des App-Einsatzes. Über mögliche Kontaktwarnungen wird das Individuum selbst über eine möglicherweise erhöhte Infektionsgefahr nach Kontakt mit Infizierten informiert, um ihm die Möglichkeit zu geben, durch eine PCR-Testung eine Infektion auszuschließen und im Fall der Fälle einer Weitergabe durch Isolation vorzubeugen. (Kapitel 2.2) Gleichzeitig kann über den Einsatz von Apps die Einhaltung behördlich angeordneter Quarantäne erfolgen. (s. Kapitel 5.2) Den Gesundheitsämtern bieten sich dabei weitere Optionen: Einerseits die Nachverfolgung individueller Kontakte automatisiert per App, was die aufwändige telefonische Nachverfolgung durch einen Mitarbeiter ersetzt, und andererseits die Zeit des Meldeweges von der aufgetretenen Infektion bis zur Eintragung in die amtlichen Statistiken zu verkürzen.

2.2 Tracking versus Tracing

Bei der Debatte um das Für und Wider einer solchen App fielen sowohl die Begriffe des Trackings und des Tracings. Diese beiden Begriffe sind allerdings weder synonym noch äquivalent zu verwenden, sondern stellen zwei völlig verschiedene Ansätze der Nachverfolgung dar.

Das Tracking ist eine Methodik, die vorwiegend auf GPS-Standortdaten und denen der Funkmasten der Telefonanbieter basiert. Hierbei findet eine Echtzeit-Standortverfolgung statt,

über die mögliche Kontakte zu infizierten Personen nachverfolgt werden können. Dies funktioniert also nur, wenn persönliche Daten und der jeweilige Aufenthaltsort weitergegeben werden - was nicht unbedingt der Vorstellung von umfassendem Datenschutz entspricht. Des Weiteren existieren Zweifel an der Effektivität einer solchen Methodik: Zwar kann die Bewegung eines Individuums nachverfolgt werden, allerdings sind die GPS-Daten nur auf einige Meter genau - bei den Höhenmeter ist die Diskrepanz unter Umständen noch größer. Damit ist die Aussagekraft über mögliche Kontakte mit Infektionsgefahr stark limitiert.
Das Tracing hingegen ist - richtig angewendet – einerseits datenschutzkonformer und andererseits durchaus effektiver. Es geht hier nicht um das Sammeln persönlicher Daten durch Standortabgleich, sondern um die Warnung bei für eine Infektion ausreichendem Kontakt durch das eigene Smartphone. Dabei tauschen die Apps der Smartphones untereinander entsprechende Codes aus, wenn sie sich über einen bestimmten Zeitraum hinaus (zumeist 15 Minuten) in einem Radius von 3 Metern befinden. Wird bei einem Nutzer eine Infektion festgestellt, die dieser der eigenen App meldet, so werden die per Code bekannten Kontakte von ihrer App informiert, dass für sie durch den Kontakt ein erhöhtes Infektionsrisiko besteht. Man erfährt dabei allerdings nicht, wer der infizierte Kontakt war oder wo dieser stattfand. Dennoch ermöglicht dieses Verfahren den Nutzern nun, sich auf den begründeten Verdacht hin testen zu lassen und in Selbstisolation zu begeben.[2]
Der entscheidende Unterschied ist also: Während beim Tracking dauerhaft Daten weitergegeben werden, geschieht dies beim Tracing erst im Falle eines positiven Testes – vorher werden ausschließlich Erkennungscodes der Smartphones ohne Rückschluss auf den Nutzer ausgetauscht.[3]

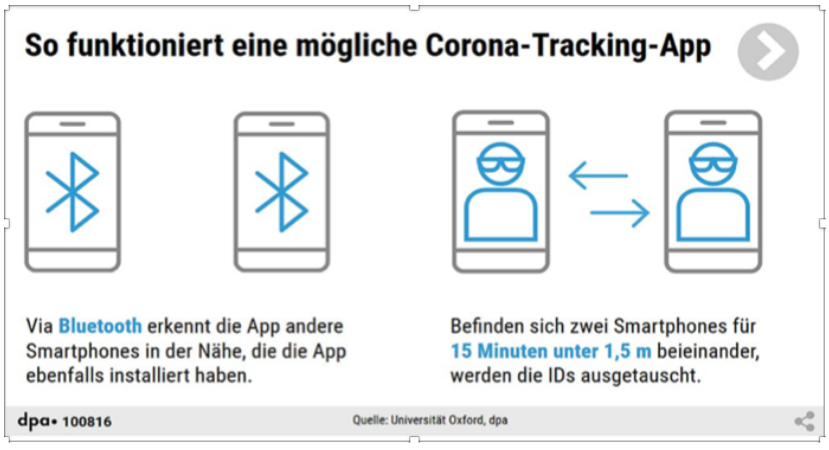

Abbildung 1: Funktionsweise der Corona-Tracing-App

[2]https://spiegel.de
[3]RBB:inforadio.de

2.3 Das Robert Koch Institut und die Deutsche Telekom

Doch der Einsatz von Smartphones im Kampf gegen die Pandemie begann nicht erst mit der Corona-Warn-App. Bereits seit Ende März 2020 liefert die Deutsche Telekom freiwillig Standortdaten anonymisiert an das Robert Koch Institut (RKI). Zu diesem Zeitpunkt nahmen die Verletzungen der seit dem 20. März geltenden Ausgangsbeschränkungen stärker zu, das RKI wollte „datenbasierte Entscheidungen“ treffen. Durch die Lieferung der Datensätze sollten potenzielle Hauptverbreitungswege im Sinne größerer Bewegungsströme festgestellt werden. Von großer Bedeutung ist dabei eben die Bewegung größerer Gruppen, die Daten lassen nach Angabe der Telekom dabei keine Rückschlüsse auf einzelne Bewegungsprofile zu, sondern bilden nur Personenströme anhand der Einwahl in die Funkzellen ab. Dies geschieht mit einer eher geringen Genauigkeit von 150 Metern bis zu mehreren Kilometern, auch abhängig von der Dichte der Funkzellen. Allerdings gab es Widerstand von der EU-Kommission: Der EU-Datenschutzbeauftragte Wojciech Wiewiorowski bemängelte, dass eine Rückverfolgung auf das Individuum keinesfalls ausgeschlossen sei. Und auch die Art und Weise der Weitergabe stieß auf Protest: Die einzelnen Telefon-Nutzer müssen vor der Weitergabe nicht gefragt werden, ihnen ist ausschließlich eine Widerspruchsmöglichkeit beim Anbieter vorbehalten, mit der eine Nutzung untersagt werden kann. Wiewiorowskis nationales Pendant in Deutschland, Ulrich Kelber, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), sieht dagegen keine Probleme: „Der BfDI sieht den Schutz der Daten bei Einhaltung der vorgegebenen technischen Voraussetzungen gewährleistet“. Entscheidend dabei: Das Prinzip ist nicht neu. Diese Daten werden seit Jahren kommerziell genutzt, kommen darüber hinaus in der Stadt- und Verkehrsplanung zum Einsatz. Es wird also ein bereits gut bekanntes und genutztes Verfahren angewandt, das keine weitere Verschärfung der Datenschutzsituation hervorruft.[4] [5]

2.4 Voraussetzungen für den Erfolg

Damit eine Corona-App nachhaltig zur Bewältigung der Krise beiträgt, sind bestimmte Parameter einzuhalten. Am wichtigsten ist eine umfassende Nutzung durch möglichst viele Smartphonebesitzer:innen, um die Funktionalität der App zu erhalten. In Deutschland besitzen mit 76 % der Menschen circa 63 Millionen Menschen ein Smartphone, damit liegt man im internationalen Vergleich auf Rang 16. Die Epidemiologen gehen davon aus, dass für einen Erfolg circa 65 % einer Gesellschaft die App herunterladen müssten. Das wären wiederum circa 54 Millionen Menschen. Daraus ergibt sich eine Toleranzgrenze für die Nichtnutzung von ma-

[4] https://www.br.de/nachrichten/netzwelt/handy-daten-sollen-beim-kampf-gegen-corona-helfen,Rtfml1G

[5] https://www.merkur.de/welt/coronavirus-telekom-handydaten-rki-covid-19-krise-bevoelkerung-massnahmen-deutschland-mobilfunk-zr-13606412.html

ximal 8, bei einer höheren angenommenen Rate von 70 % gar nur 3 Millionen Menschen. Diese Fenster ist klein, nur jeder 10. Smartphoneuser dürfte auf eine Installation verzichten.[6] Stand August 2020 nutzen in Deutschland 17,2 Millionen Menschen die Corona-Warn-App. Ob das genügt, bleibt abzuwarten. Zumal bisher lediglich 1.679 positive Testergebnisse in der App gemeldet wurden[7] - zum Vergleich: Allein am 19.08.2020 wurden 1.510[8] neue Fälle registriert, der Erfolg ist also bisher überschaubar.

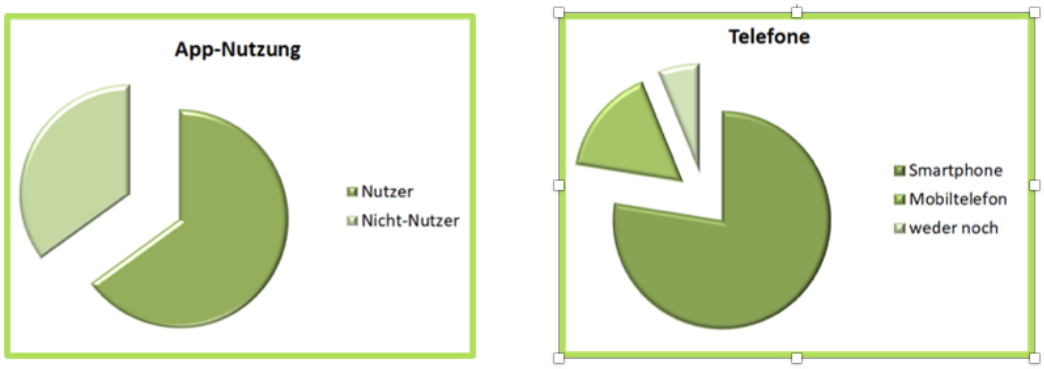

Abbildung 2: Benötigte Teilnehmer:innen für einen Erfolg der Corona-Warn-App (links). Verteilung der Smartphonebesitzer:innen (rechts).

3 Die Datenspende-App des RKI

3.1 Verwirrung umd die Datenspende-App

Man schrieb den 7. April 2020, mitten in der Hochphase der Pandemie im Frühjahr 2020. Das Robert Koch Institut hatte zu einer Pressekonferenz geladen, die fast schon gewöhnlich über die aktuelle Corona-Situation berichtete. So weit, so normal. Hätte der Präsident des RKI, Prof.Dr. Lothar Wieler, nicht zum Ende mit der Ankündigung einer App überrascht. Als diese dann nicht die seit Wochen angekündigte Warn-App, sondern eine zusätzliche Datenspende war, trug zur öffentlichen Verwirrung bei. Und dennoch stellte diese App fortan gewissermaßen einen Testlauf für die eigentliche App des Bundes dar.[9]

[6] https://www.handelsblatt.com/technik/gadgets/studie-zur-handynutzung-mehr-als-2-5-milliarden-menschen-besitzen-ein-smartphone/23955602.html?ticket=ST-113713-LUontaiqXxadfG9bgAQ1-ap4

[7] https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Kennzahlen.pdf?__blob=publicationFile

[8] https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Fallzahlen.html

[9] https://www.br.de/nachrichten/netzwelt/verwirrung-um-weitere-corona-app-des-rki,RvY9bci

3.2 Funktion und erhobene Daten

Die Datenspende-App des RKI sollte dem Institut eine breitere Datenbasis für die Modellierung von Inzidenz, Verbreitung und Hotspotlage bieten. Dafür erhebt sie folgende Daten: Alter*, Geschlecht, Postleitzahl, Gewicht*, Größe* sowie die entsprechenden Biodaten zu Gesundheit und Aktivität.[10] Das sind explizit Schlafverhalten, Herzfrequenz, Pulsschlag und Körpertemperatur, die in regelmäßigen Abständen erfasst und pseudonymisiert an das RKI weitergeleitet werden. Erhoben werden diese Daten ausschließlich über die Smartwatches der App-Nutzer, die die Daten dann über das Smartphone weitergeben. Stand August 2020 werden ausschließlich Smartwatches der fünf Hersteller Fitbit, Garmin, Polar, Withings und GoogleFit unterstützt.[11]

Innerhalb weniger Wochen ist die Zahl der Teilnehmenden bereits auf über eine halbe Million gewachsen, die geografische Verteilung der Teilnehmenden auf alle Kreise wurde immer besser. Nun soll zeitnah aus den langfristig erhobenen Ruhepuls- und Fieberwerten der Kreise ein Basiswert ermittelt werden, der die Erstellung einer sogenannten Fieberkarte ermöglicht. Auf dieser wären in bestimmten Regionen erhöhte Ruhepuls- oder Fieberwerte direkt und aktuell ablesbar, woraus Rückschlüsse auf Hotspots sowie die akute Inzidenz zu ziehen wären.[12]

Abbildung 3: Die Datenspende-App

[10] * entspricht der Erhebung in 5er-Schritten.
[11] RKI-APP Datenschutzinformationen
[12] https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Corona-Datenspende.html

3.3 Datenschutz

Bereits kurz nach der Veröffentlichung wurden kritische Stimmen, unter anderem der Experten des ChaosComputerClubs, laut: Die App sei unausgereift und nicht wirklich sicher, zumal das Robert Koch Institut den Quellcode seiner App damals nicht mit offen legte. Das RKI selbst verwies bei der Veröffentlichung auf die Datenschutzrichtlinien der App. Demnach werden ausschließlich anonymisierte Daten weitergeleitet, sodass „das RKI ohne die Hinzuziehung weiterer Informationen keinen Bezug zu meinem Namen (*Anm.:* des Nutzers) herstellen kann. Die App hat zu keinem Zeitpunkt Zugriff auf unmittelbar identifizierende Informationen wie Namen oder Adresse.“[13] Die Daten würden im nächsten Schritt ausschließlich auf deutsche Server weitergeleitet und zum Zwecke der Verarbeitung gespeichert. Man halte sich bei der maximalen Speicherzeit mit 10 Jahren an die Vorgaben der DFG (Deutsche Forschungsgemeinschaft). Alle nicht-personenbezogenen und repersonalisierbaren Daten verbleiben allerdings als anonymisierte Forschungsdaten dauerhaft beim RKI.[14]
Einigkeit besteht weitestgehend über den großen Nutzen dieser App, die Umsetzung hingegen lässt zu wünschen übrig. Neben der mangelhaften Anonymisierung stören auch bestimmte Berechtigungen der App. So greift die App wohl bei den AppleHealth-Konten ungefragt auf die bereits gespeicherten Daten zu, indem sie sich nach der aktiven Trennung neu verbindet - darin sind eben auch Bewegungs- und Standortdaten enthalten. Das RKI antwortete auf Anfrage von Deutschlandfunk: „Nach Auskunft des technischen Dienstleisters für die Corona-Datenspende-App hat die Trennung der App von Apple Health in Einzelfällen nicht zuverlässig funktioniert. Mit dem heute noch anstehenden Update der App wird ein zusätzlicher Hinweis integriert, wie die Nutzer die Datenfreigabe zurückziehen können.“ Da auch nicht bekannt ist, wie die einzelnen Schnittstellen zu den Benutzerkonten der Smartwatchanbieter implementiert wurden, bleiben Zweifel über die Datensicherheit auch an dieser Stelle offen. Denn ist nicht ausgeschlossen, dass durch den Zugriff auf in der Vergangenheit gesammelte Daten Missbrauch stattfindet, weil der zukünftige Umgang mit diesen Zugriffsberechtigungen unklar erscheint. Professor Hannes Federrath, Vorsitzender der Gesellschaft für Informatik e. V., äußerte infolge dieser Mängel scharfe Kritik und betont, „dass das Vertrauen in echte nützliche Apps, die dann jetzt auch die Infektionen eindämmen könnte, nicht untergraben werden darf etwa durch solche Datenspende-Apps.“ Dennoch darf eines nicht vergessen werden: Die nun über die Datenspende-App an das RKI übermittelten Daten sind dieselben, die von den Nutzern seit Jahren bedenkenlos an die Server der Smartwatchanbieter übermittelt werden - nur das Ziel ist eben nun eine staatliche Institution anstatt eines Unternehmens.[15]

[13] RKI-APP Datenschutzinformationen

[14] https://www.weser-kurier.de/themenwelt/technik-und-multimedia_artikel,-rki-mehr-als-halbe-million-teilnehmer-bei-datenspendeapp-_arid,1911811.html

[15] https://www.deutschlandfunk.de/covid-19-kritik-an-neuer-datenspende-app-des-rki.684.de.html?dram:article_id=474510

Abbildung 4: Übersicht der Daten, die durch die Datenspende-App übertragen werden.

4 Rechtliche Grundlagen

4.1 BDSG und DSGVO

Die rechtlichen Grundlagen für das Verarbeiten von personenbezogenen Daten regeln zum einen das Bundesdatenschutzgesetz (BDSG) und zum anderen die neuere Datenschutzgrundverordnung (DSGVO). Diese gelten für alle Dienstleistungen, welche persönliche Daten von Menschen analysieren, auswerten und ggf. weiterverwenden. Wichtig dabei zu unterscheiden ist, dass das Bundesdatenschutzgesetzt nur auf nationaler Ebene agiert, wobei die Datenschutzgrundverordnung den Gebrauch von Daten auf europäischer Ebene regelt. Damit steht

die DSVGO über dem BDSG, wodurch diese wirkungsvoller ist.
Das Bundesdatenschutzgesetz regelt die Nutzung von personenbezogenen Daten nur im Groben. Zu diesen zählen Daten wie Name, Alter, Anschrift, Telefonnummer, Aufenthaltsort, Kreditkartennummer und so weiter. Derzeit sind im BDSG kaum noch feste Gesetze zu finden. Die Hauptarbeitsfelder werden dabei auf die Datenschutzgrundverordnung verwiesen.
Die DSGVO betrachtet die Verarbeitung der personenbezogenen Daten im Artikel 5 „Rechtmäßigkeit der Verarbeitung“. In diesem Artikel wird definiert, wie das Verhältnis zwischen Datenverarbeiter und der Person, welche ihre Daten weitergibt, aussehen muss. Zusammenfassend müssen folgende Punkte zwischen ihnen beachtet werden:

- Die Person muss der Datenverarbeitung in einem oder mehreren Zwecken zustimmen.
- Die Verarbeitung erfolgt auf Grundlage eines Vertrages.
- Die Verarbeitung ist nur zulässig für die Erfüllung der rechtlichen Pflichten der Person.
- Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der Person oder einer anderen natürlichen Person zu schützen.[16]

In Hinblick auf die Datenverarbeitung der Corona-App sind die letzten beiden Punkte von Wichtigkeit. Nach der Annahme, dass eine erforderliche Verarbeitung bei Gefahr um Leib und Leben nötig ist, ließe sich darüber eine Corona-App abbilden. Ebenso könnte die Auslegung der „rechtlichen Pflicht“ geändert werden. Dies würde dazu führen, dass es eine rechtliche Pflicht wäre, Infektionsketten zu unterbinden und die übrigen Menschen zu schützen.
Ein weiterer Bezug von der Corona-App und der Datenverarbeitung findet sich im Artikel 9 der DSGVO. In diesem wird sich mit der „Verarbeitung besonderer Kategorien personenbezogener Daten“ auseinandergesetzt. Der Bundesbeauftragte für Datenschutz und Sicherheit gibt dabei den Hinweis, dass dieser Artikel eine Verbindung zwischen personenbezogenen Daten, also der Person und dem Gesundheitszustand dieser Person, herstellt. Damit werden außerdem die personenbezogenen Daten automatisch zu Gesundheitsdaten. Jedoch kann mit Hilfe des Artikel 9 im Falle der Corona-Pandemie eine Datenverarbeitung legitimiert werden. Der Datenschutzbeauftragte nennt dazu einige Beispiele, welche eintreten können und eine legale Verarbeitung von personenbezogenen Daten darstellen.

- Personenbezogene Daten von Arbeitgeber und Arbeitnehmer dürfen verarbeitet werden, um eine Eindämmung des Virus zu bewirken.
  - Dazu muss ein positiver Befund festgestellt werden
  - Die Person hat sich in einem vom RKI als Risikogebiet erklärtem Gebiet aufgehalten.

[16] https://dsgvo-gesetz.de/art-5-dsgvo/

- Verarbeitung von personenbezogenen Daten von Gästen und Besuchern (Gaststätten, Hotels, Bars, usw.) zur Feststellung,
  - ob die Personen selbst das Virus verbreiten oder mit infizierten Personen in Kontakt standen,
  - die Personen sich in einem vom RKI als Risikogebiet erklärtem Gebiet aufgehalten haben.[17]

Sollten diese Fällen eintreten, so sind die Behörden legitimiert, personenbezogene Daten zu verarbeiten, um Kontaktpersonen und damit etwaige Infektionsketten ausfindig zu machen. Vom heutigen Standpunkt aus gesehen wurden die Rechte innerhalb des Bundesdatenschutzgesetzes und der Datenschutzgrundverordnung nicht geändert. Die Verarbeitung der Daten erfolgt auf dem gleichen rechtlichen Fundament, wie auch vor der Corona-Zeit, nur dass der Bundesbeauftragte für Datenschutz und Sicherheit die rechtliche Grundlage für die Arbeit der Behörden offenlegt, diese jedoch schon immer vorhanden war.

4.2 Gesetzentwurf des Gesundheitsministers Jens Spahn (März 2020)

Mitte März 2020 legt der amtierende Gesundheitsminister Jens Spahn einen Gesetzentwurf für die Bekämpfung der Corona-Viren vor. Dazu nutzt er die Erneuerung des bestehenden Infektionsschutzgesetzes, um weitere Regelungen, speziell auf die steigenden Corona Infektionszahlen, zu reagieren. Ziel ist es, Infektionsketten nachverfolgen zu können und diese dann zu unterbrechen, um eine weitere Ausbreitung des Corona-Virus zu verhindern. Darin hieß es, dass personalisierte Bewegungsdaten an Behörden übergeben werden sollen. Die Technik, welche dazu benutzt werden sollte, ist das Handy-Tracking, also die GPS-Ortung aller Handys auf Bundesgebiet mit den zusätzlichen personenbezogenen Daten des Besitzers. Damit sollte eine unfreiwillige Rückverfolgung über die Bewegungsprofile der einzelnen Personen erreicht werden.
Der Vorschlag stieß auf sehr viel Kritik. Justizministerin Christine Lambrecht und Datenschützer Organisationen betitelten seinen Vorstoß als einen weitreichenden Eingriff in die Rechte der Bürger:innen. Auch seine eigenen Parteimitglieder kritisierten den Gesetzentwurf scharf. Es würde eine Art Dauerüberwachung geschaffen.[18]
Schlussendlich wurde der Gesetzentwurf gestrichen und nicht umgesetzt. Aus jetziger Sicht, August 2020, ist anzunehmen, dass das Konzept nicht umsetzbar gewesen wäre. Zum einen

[17] https://www.bfdi.bund.de/DE/Datenschutz/Themen/Gesundheit_Soziales/GesundheitSoziales-Artikel/Datenschutz-in-Corona-Pandemie.html
[18] |https://www.tagesschau.de/inland/corona-handydaten-103.html

gibt es in vielen Gebieten Deutschlands, vorrangig dem ländlichen Raum, zu wenig Funkzellen, um genaue Aussagen darüber zu treffen, ob sich zwei oder mehrere Menschen begegnet sind, und zum anderen wäre der Aufwand für die Analyse der Daten und der darauf sich ergebende Anstieg der Arbeit der Behörden zu hoch. Für uns ist es jedoch wichtig zu erwähnen, dass es diesen Ansatz gab, da dieser bei Umsetzung einen großen Einschnitt in die Privatsphäre aller Menschen in Deutschland dargestellt hätte.

4.3 Infektionsschutzgesetz

Das Infektionsschutzgesetz, kurz IfSG, stellt eine weitere Regelung für das Verarbeiten von persönlichen Daten in Bezug auf die Verbreitung von Krankheiten dar. Gelten tut es bereits seit dem Jahre 2001, gilt jedoch immer noch. Kerninhalt dieses Gesetzes ist es, dass speziell kategorisierte Krankheiten als meldepflichtig deklariert werden und dementsprechend bei einem positiven Labortest an die Behörden gemeldet werden müssen. Es legt also fest, welche Krankheiten und dementsprechende Krankheitsfälle den jeweiligen lokalen Gesundheitsämtern gemeldet werden müssen.[19] Damit sollen Infektionen frühzeitig erkannt, die Weiterverbreitung verhindert und somit übertragbaren Krankheiten vorgebeugt werden.
Der Staat kann mit Hilfe des Infektionsschutzgesetzes erweiterte Eingriffe in einige Rechte der Menschen vornehmen, sollte eine Pandemie auftreten. So kann er zum Beispiel in die folgenden Grundrechte eingreifen:

- der körperlichen Unversehrtheit
- die Freiheit der Person
- die Freizügigkeit von Personen
- die Versammlungsfreiheit
- das Brief- und Postgeheimnis
- Unverletzlichkeit der Wohnung.

Weiterhin ist es möglich, ein Arbeitsverbot für bestimmte Branchen oder sogar die gesamte Wirtschaft auszusprechen.[20]
Die Verarbeitung der Daten erfolgt nach zwei Prinzipien. Zum einen erfolgt eine namentliche Meldung des Krankheitsfalles, sofern dieser von einem Arzt oder Labor bestätigt wurde, an das zuständige Gesundheitsamt in der Nähe, zum anderen erfolgt eine anonymisierte Meldung

[19] https://www.rki.de/DE/Content/Infekt/IfSG/ifsg_node.html
[20] https://de.wikipedia.org/wiki/Infektionsschutzgesetz

an das Robert Koch Institut. Beide Meldungen enthalten die jeweils festgestellte Krankheit und erfolgen auf elektronischem Wege.[21]
Aufgrund der Corona-Pandemie wurde das Verfahren jedoch etwas verändert. Derzeit werden die Krankheitsfälle personalisiert an das entsprechende Gesundheitsamt gemeldet. Dieses meldet folgend die Corona-Erkrankung anonymisiert an das Institut für Umweltschutz und Agrikulturchemie, kurz IUA, weiter. Dort werden die Krankheitserreger nochmals analysiert und ausgewertet. Sollte sich der Corona-Fall bestätigen, wird das Robert Koch Institut ebenfalls über eine anonymisierte Meldung von dem Vorfall informiert. Abbildung 5 veranschaulicht den Ablauf.

Abbildung 5: Ablauf der Datenverarbeitung, P = personalisiert, A = anonymisiert

Die zuständigen Gesundheitsämter in unserer Umgebung sitzen in Magdeburg (Sachsen-Anhalt), Dresden (Sachsen) und Erfurt(Thüringen).

5 Internationale Corona-Apps

5.1 Israel

Schutzschild - so lautet der wohlklingende Name der Corona-Schutz-App Israels. Was bis hierher, wie eine reine Defensivmaßnahme, sehr nach Schutz klingt, entpuppte sich bereits im Frühjahr als weit einschneidendere Maßnahme gegen die Pandemie. Grundsätzlich verfolgt sie einen zwar freiwilligen, aber dennoch ungewöhnlich restriktiven Ansatz für eine Demokratie, galt demnach frühzeitig nicht mehr als Vorbild für eine deutsche Lösung. Denn sie arbeitet mit

[21] https://www.gesetze-im-internet.de/ifsg/___14.html

dem oben vorgestellten Konzept des Tracking. Sie erhebt also Standort- und Bewegungsdaten der Nutzer, um diese dann mit den durch die Behörden eingebrachten Daten der Infizierten abzugleichen. Entscheidend hierbei: Es folgt bei Kontakt keine ausschließliche Warnung der App an den Nutzer, stattdessen wird dieser durch eine SMS der Behörden gewarnt - bei dieser Form der Auswertung kennt der Staat die Infizierten also.[22]
So weit, so verkraftbar. Doch Israel ging einige Schritte weiter, der Polizei und Inlandsgeheimdienst *Schin Bet* wurde per Notverordnung ermächtigt, sich in die Telefone der Infizierten zu hacken, um auch diejenigen zu kontrollieren, die eine solche App nicht nutzen. Die Sicherheitsbehörden dürfen Telefone orten, Kontakte identifizieren und Internetdaten auswerten. Darüber hinaus wird die Einhaltung angeordneter Quarantäne zusätzlich zu Hausbesuchen der Polizei über die Standortdaten der Infizierten überwacht. Insgesamt 14 Sensoren werden neben den GPS eingesetzt, Bewegung, Beschleunigung, Lichtverhältnisse, Wlan-Zugang, Soziale Netzwerke und Emails - die abgerufenen Daten sind mehr als umfassend. Während dies auf Kritik der Datenschützer stieß, steht die Bevölkerung Israels mehrheitlich hinter der Maßnahme. Und doch hat der Oberste Gerichtshof entschieden, dass der Einsatz von App und Geheimdienst parlamentarisch überwacht werden muss - ein herber Rückschlag für die Regierung Netanjahu. Ein entscheidender Nachteil einer solchen App wurde allerdings bei der besonders stark betroffenen orthodoxen Minderheit deutlich: Weil gerade deren Angehörige oftmals kein Smartphone besitzen, läuft das Konzept an dieser Stelle ins Leere.
Zumindest ein positiver Aspekt bleibt: Die im Internet veröffentlichten Standortdaten der Infizierten, die dem eigenständigen Abgleich der Bevölkerung mit den eigenen Bewegungen dienen, werden anonymisiert. Allerdings ist klar: Im Gegensatz zum deutschen Modell werden die Daten keinesfalls freiwillig, sondern eben durch den Geheimdienst erhoben - nicht anonymisiert. Ein Konzept, das den Datenschutz ad absurdum führt. Ob damit das Ende der Fahnenstange erreicht ist, wird sich zeigen.
Gemeinsam mit einer israelischen Spionagefirma wurde noch im April angekündigt, man arbeite an einer Echtzeitüberwachung.[23] [24] [25]

5.2 Polen

In unserem Nachbarland Polen sind sogar zwei Apps seit März im Einsatz. Sie heißen *ProteGo Safe* und *Kwarantanna domowa* und erfüllen zwei differente Zwecke.
Letztere heißt übersetzt so viel wie Häusliche Quarantäne. Nachdem sich zwischenzeitlich bis

[22] https://corona-datenspende.de
[23] www.br.de/nachrichten/deutschland-welt/corona-apps-und-tracking-in-israel,Rw2L5uh
[24] https://www.daserste.de/information/politik-weltgeschehen/weltspiegel/sendung/israel-corona-ueberwachung-100.html
[25] https://www.tagesschau.de/ausland/israel-corona-101.html

zu 300.000 Menschen in Quarantäne befanden, veröffentlichten die Behörden am 19. März diese App, seit dem 1. April ist sie auch verpflichtend. Sie dient der Quarantäneüberwachung potentiell oder real Infizierter sowie der Urlaubsrückkehrer aus Risikogebieten. Der Beweis für die Einhaltung wird durch die Kombination von Standortdaten und Fotos realisiert. Die Isolierten können 24 Stunden am Tag eine Information mit Aufforderung zur Identifikation erhalten. Nun haben sie maximal 20 Minuten Zeit, durch die Aufnahme eines Fotos zu beweisen, dass sie sich gemeinsam mit ihrem Smartphone (das ja durch den Standort auf das eigene Zuhause überprüft werden kann) in der häuslichen Quarantäne befinden. Die Verbraucherzentrale Sachsen kritisiert die App der direkten Nachbarn: Sie schränke Persönlichkeitsrechte der Nutzer stark ein, sei auch für Urlauber aus anderen Ländern verpflichtend. Des Weiteren seien wesentliche Standards in den Datenschutzrichtlinien unklar, ebenso wie die letztendliche Verwendung und Dauer der Speicherung der Daten.
Ziemlich analog zur deutschen Corona-Warn-App ist die *ProteGo Safe* angelegt. Sie ist im Gegensatz zur Quarantäne-App freiwillig. Sie warnt per Tracing die Nutzer, wenn sie Kontakt zu potenziell Infizierten hatten, die Funktion ist fast identisch mit der der App in Deutschland (siehe Kapitel 6.3). Bisher sind die Apps länderübergreifend nicht kompatibel, woran allerdings gearbeitet wird, um vor allem im Grenzverkehr nicht die Nutzung zweier Apps voraussetzen zu müssen.[26]

5.3 China

Dass die Freiheit in einer kommunistischen Diktatur wie China erheblich zu kurz kommt, war bereits vor der Krise klar. Doch mit dem innerhalb kürzester Zeit entwickelten Konvolut an Pandemie-Apps hob man die Überwachung der eigenen Bevölkerung bereits während des Ausbruchs in Hangzhou auf ein ganz neues Niveau. Flaggschiff der Aktion ist dabei eine vom Internet-Konzern Alibaba innerhalb von drei Tagen entwickelte App zur Kontaktnachverfolgung. Anhand der individuellen Standort-, Mobilfunk und Internetdaten wird bestimmt, ob sich der Nutzer an Orten mit vielen Infizierten und dementsprechend hohem Risiko aufgehalten hat. In Kombination mit den bereits umfassend erhobenen Informationen aus der öffentlichen Gesichtserkennung und weiteren sensiblen Personendaten wird dem Nutzer so ein Barcode in den Farben Rot, Gelb oder Grün zugewiesen, der für das Betreten bestimmter öffentlicher Orte oder Reisen notwendig ist und über die Bewegungsfreiheit der Menschen bestimmt. Auch die Einhaltung der Quarantäne wird restriktiv der App überwacht.[27] Die gesammelten Daten werden zumeist zu kommerziellen Zwecken weiterverwendet und ungehindert weitergegeben, die Codes der Apps unter Verschluss gehalten und nicht veröffentlicht.

[26] https://www.saechsische.de/diese-corona-apps-nutzen-die-polen-5217114.html
[27] https://www.n-tv.de/wirtschaft/Chinas-Corona-App-Wunder-hat-viele-Haken-article21865963.html

Ein Modell - das für Deutschland geradezu undenkbar wäre.
Als wäre dies nicht genug, arbeitet man bereits an einer weiteren Anwendung für die Zeit nach der Pandemie: Eine App, die unter Anderem Ernährungs, Schlaf- und Bewegungsdaten überwacht und daraus eine Bewertung der Gesundheit auf einer Skala von 0 bis 100 vornimmt. Die Tendenz ist eindeutig: Die Überwachung wird in China nach Corona nicht abnehmen - im Gegenteil.[28]

5.4 Südkorea

Bereits Ende März schwang sich Südkorea zum globalen Vorreiter im Kampf gegen Covid19 auf. Während man in Europa noch über Maskenpflicht und „Lockdown“ diskutierte, ging in der jungen Demokratie die erste App an den Start. Die Koreaner waren bereit - wie sie der Links-Mitte Regierung bei der Parlamentswahl auch überwältigend bestätigten - die gerade aufgrund der noch deutlichen Erinnerungen an die Diktatur sehr geschätzte Freiheit zugunsten der Pandemiebekämpfung stark einzuschränken. Durch Handytracking sowie Mobilfunk- und Kreditkartendaten und Überwachungskameras an öffentlichen Plätzen gelang es frühzeitig, Infizierte und ihre Kontaktpersonen aufzuspüren, Infektionsketten, Hotspots und Inzidenzzahlen zu ermitteln. Somit konnte man schnellstmöglich potenziell Infizierte aufspüren und parallel Warnungen über erhöhtes Risiko an die Bevölkerung herausgeben. Dieses konsequente Vorgehen griff zwar in die Datenschutzrechte des Individuums ein, verhinderte aber eine Schließung von öffentlichen Plätzen wie dem Einzelhandel oder Freizeiteinrichtungen, ausschließlich Schulen, Universitäten und Einrichtungen für Großveranstaltungen blieben temporär geschlossen.[29]

5.5 Tschechien und Slowakei

Tschechien hat bereits im April einen anderen, deutlich liberaleren Ansatz vorgestellt: Mit *FreeMenvsCovid* sollen die Nutzer besonders stark frequentierte Plätze gar nicht erst besuchen, sondern präventiv meiden. Dafür werden anhand anonymisierter Bewegungsdaten Informationen über die Kumulation von Personen an bestimmten Orten gesammelt. Schaut der Nutzer also in die App, kann er entscheiden, den Supermarkt zu einer voraussichtlich weniger stark ausgelasteten Zeit zu besuchen und so das Ansteckungsrisiko minimieren.
Die Corona-App der Slowakei verbindet die beiden Einzelmodelle Polens, also die Kontaktwarnung und die Quarantänekontrolle. Wenn sich zwei Smartphones innerhalb eines Radius von 50 Metern befinden, tauschen sie anonymisierte Codes aus. Nur bei positivem Test ei-

[28] https://www.dw.com/de/gesundheits-app-sorgt-f%C3%BCr-aufregung-in-china/a-53576057
[29] www.sueddeutsche.de/gesundheit/krankheiten-zwickau-professor-in-suedkorea-ende-der-corona-pandemie-in-sicht-dpa.urn-newsml-dpa-com-20090101-200426-99-836386

nes Infizierten werden die Kontaktpersonen über diesen informiert, ohne dabei Zugriff auf die Personendaten zu gewähren. Nebenbei dient die App dazu, durch die Standortdaten der Infizierten deren Isolation zu überprüfen.

6 Deutsche Corona-Warn-App

6.1 Das zähe Ringen um die App

Bei der Idee einer App beim Vorgehen gegen die Corona-Pandemie stellte sich Deutschland im Vergleich zu anderen Ländern sehr weit hinten an. Die Politik ging dabei als ersten Weg, im März 2020, eine eigene App in Auftrag zu geben und diese über die Bundesbehörden entwickeln zu lassen. Um einen freien Markt zu garantieren, wurde dieses Vorhaben jedoch nach kurzer Zeit unterbrochen und ein Auftrag an alle Softwareunternehmen ausgeschrieben. Andere Länder, wie zum Beispiel Österreich, gingen diesen Weg bereits bei Beginn der steigenden Infektionszahlen. Dadurch verzögerte sich die Entwicklung einer App in Deutschland enorm.
Erst Mitte April wurde somit begonnen, eine App zu entwickeln. Konzepte und die Umsetzung wurden dabei in Absprache zwischen Regierung, Gesundheitsbehörden, dem Robert Koch Institut und dem Softwareunternehmen bewerkstelligt. Dies erforderte einen großen Aufwand. Zudem mussten verschiedene Konzepte besprochen werden,insbesondere ob die App ihre Daten zentral oder dezentral speichern soll. Nachdem der Gesetzentwurf von Jens Spahn gekippt wurde, war auch die Art der Kontakterfassung geklärt. Es sollte nicht mehr um das direkte Orten von Handys und Smartphones gehen, sondern viel mehr über das gegenseitige Austauschen von Informationen im kleinen Radius unter den Geräten selbst. In Österreich wurde dieses Konzept von Anfang an angedacht, Deutschland musste sich diesem jedoch erst bewusst werden.
Die Kosten für das Projekt einer Corona-App wurden vollends von der Bundesregierung übernommen. Zudem mussten von den großen Entwicklerfirmen Apple und Google, welche die beiden Hauptbetriebssysteme Android und iOS stellen, Schnittstellen implementiert werden, um eine Möglichkeit zu schaffen, Daten in kleinem Radius über die Bluetooth-Technologie zu übertragen. Dies alles verzögerte die Konzeptplanungen und Umsetzung der App. So konnte die erste Beta-Version erst im Juni 2020 starten, drei Monate nach dem Ausbruch der Corona Infektion in Deutschland.
Auf genauere Formen, welche für eine App diskutiert wurden und welcher Typ App am Ende veröffentlich wurde, darauf wollen wir im Folgenden eingehen. Genauso soll es um die Technologie und die Risiken der verschiedenen Formen gehen.

6.2 Diskutierte Formen

6.2.1 PEPP-PT Initiative

Als eine der in Betracht gezogenen Formen steht die PEPP-PT Initiative für Pan-European Privacy-Preserving Proximity Tracing. Wie der Name es schon verrät sollte das Konzept eine Corona-Warn-App darstellen, welche innerhalb der gesamten europäischen Union Einzug erhält. Die Entwickler der App sind 130 Mitglieder, darunter Wissenschaftler:innen und Entwickler:innen aus sieben verschiedenen europäischen Ländern.[30]
Das Konzept beruht auf der Bluetooth-Low Energy, kurz Bluetooth-LE, Technologie, welche es ermöglicht, kleine Datenmengen innerhalb von kurzen Distanzen zwischen zwei Bluetooth-Geräten auszutauschen. Dies erfolgt energiesparend und über die Signalstärke der Geräte kann eine Schätzung über die Entfernung zwischen ihnen abgegeben werden.
Die PEPP-PT App sollte nach der Vorstellung der Entwickler eine anonyme Registrierung bieten. Es sollten keine persönlichen Daten gespeichert oder verwendet werden. Zudem war geplant, dass die App im Hintergrund protokolliert mit welchen weiteren Geräten, die die App ebenfalls verwenden, sich der Besitzer getroffen hat. Damit sollte es möglich sein im Falle eines positiven Testergebnisses eine anonyme Nachverfolgung der Kontaktpersonen zu erlauben. Die Kontaktpersonen werden dann über die App benachrichtigt, dass sie Kontakt zu einer infizierten Person hatten und sich testen lassen sollten.
Technisch sollte die App anhand einer dynamischen Schlüsselgenerierung umgesetzt werden. Treffen sich zwei Geräte, so tauschen sie ihre Schlüssel untereinander aus und speichern diese für eine gewisse Dauer. Im Falle von Corona sind 14 Tage angedacht gewesen. Diese sollen von den Geräten auf einem zentralen Server gespeichert werden, von welchem sie ebenfalls informiert werden im Falle eines Kontaktes.[31] Das Testergebnis muss dabei hochgeladen werden, um Fehlinformationen zu vermeiden.
Mehrere Kritiker sahen als großes Problem die Vielfalt der Handys und Smartphones auf dem Markt. Nicht alle verwenden gleiche Standards und somit sind die Bluetooth-Daten je nach Gerät spezifisch anders. Daher scheint es schwierig, die genauen Abstände zwischen zwei Personen bzw. Geräten genau zu errechnen. Zudem wurde die zentrale Speicherung der Daten als großes Problem angesehen. Datenschützer befürchteten bei einem Angriff auf das System, dass sich durch die Schlüssel der Geräte und die erfassten Kontakte mit anderen Geräten, Rückschlüsse auf Bewegungsprofile der Personen ziehen lassen. Daher nahmen immer mehr Unterstützer Abstand von dem Projekt, wodurch es scheiterte und nicht umgesetzt wurde.

[30] ttps://www.heise.de/newsticker/meldung/Corona-Kontaktverfolgung-Bundesregierung-prueft-drei-App-Modelle-4706775.html
[31] https://www.heise.de/newsticker/meldung/Kontakt-Tracing-vs-Corona-Aderlass-beim-Pilotprojekt-PEPP-PT-geht-weiter-4705939.html

6.2.2 DP-3T App

Anstelle PEPP-PT Initiative wurde die DP-3T-App entwickelt. Sie steht für „Decentralized Privacy Preserving Proximity Tracing“. Sie arbeitet fast genauso wie die App der PEPP-PT, mit dem Unterschied, dass die Daten nicht zentral gespeichert werden, sondern dezentral auf den jeweiligen Geräten. Es ist zu erwähnen, dass es ebenfalls eine anonyme Registrierung gibt und die App genauso mit generiertem Schlüsselaustausch auf der Ebene von Bluetooth-LE Verbindungen funktioniert. Sollte nun eine Person angeben, sich mit dem Corona-Virus infiziert zu haben, werden alle gespeicherten Schlüssel informiert. Dafür wird der Schlüssel der infizierten Person auf dem Server hochgeladen und die Endgeräte von anderen Personen fragen ab, ob sie mit diesem Schlüssel in den letzten 14 Tagen Kontakt hatten, also ob dieser Schlüssel auf ihrem Gerät gespeichert ist. Sollte dies der Fall sein, wird diejenige Person darüber informiert. Es werden also keine Schlüssel auf Servern hochgeladen, nur bei positivem Testergebnis.

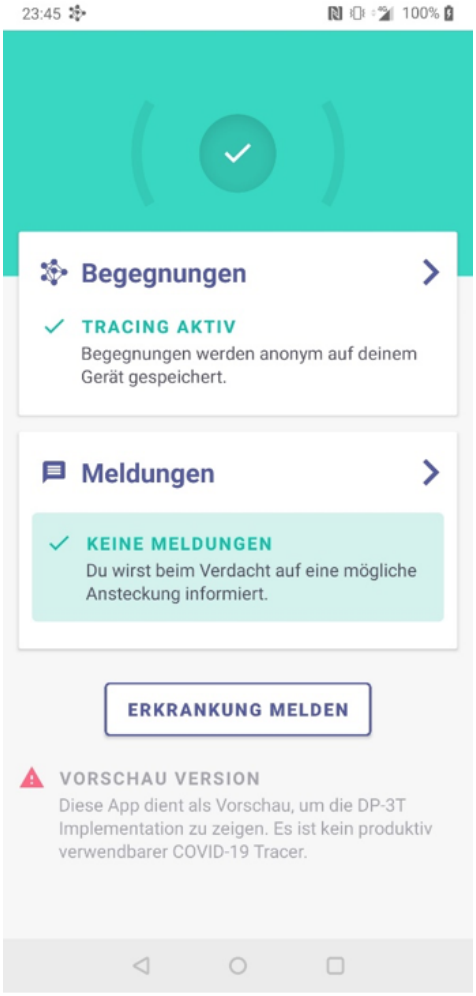

Abbildung 6: Frontend der DP-3T-App

Das Konzept der DP-3T App erschien für viele Datenschützer als richtiger Weg. Die Hauptmenge an Nutzern wird geschützt durch eine dezentrale Datenspeicherung. Nur die Schlüssel von Personen mit positivem Corona-Test werden hochgeladen. Dadurch kann kein Bewegungsprofil erzeugt werden, wenn die Daten von dem Server durch einen Hacker-Angriff entwendet werden, da die Kontakte nur auf den jeweiligen Endgeräten festgehalten werden und nicht wie bei der PEPP-PT App auf den Servern. Zudem gab es von dieser Variante bereits einen lauffähigen Test (siehe Abb.6). Der Code der App wurde zudem Open-Source zur Verfügung gestellt.[32]

[32]https://www.golem.de/news/d3-pt-vs-pepp-pt-worum-es-im-streit-um-die-corona-app-geht-2004-148002.html

6.2.3 „STOPP-Corona“-App der accenture GmbH (Österreich)

Die accenture GmbH hat in Österreich die „STOPP-Corona“-App für das rote Kreuz entwickelt. Veröffentlicht wurde die App im April 2020 als eine der ersten im Kampf gegen die sich immer weiter ausbreitende Corona-Pandemie. Genauso wie die anderen bereits erwähnten App-Konzepte arbeitet die „STOPP-Corona“-App über eine Kontaktverfolgung per Bluetooth-LE. Die Registrierung erfolgt dabei unter einem Pseudonym. Der Speichertyp ist dezentral gelöst. Die Daten werden nur auf dem jeweiligen Smartphone gespeichert und, genau wie bei der DP-3T Lösung, nur die Schlüssel auf Server geladen, welche nachweislich einen positiven Corona-Test hochgeladen haben.
Ein großer Unterschied zu den anderen Lösungen ist, dass die „STOPP-Corona“-App mit zwei Methoden arbeiten kann, wovon sich der Benutzer eine aussuchen muss. So gibt es zum einen die automatische Kontakterkennung und zum anderen die manuelle Kontakterkennung. Wird die App auf die automatische Erkennung gestellt, so protokolliert sie im Hintergrund die Kontakte mit anderen Endgeräten, wie es auch PEPP-PT und DP-3T tun. Der Unterschied liegt in der manuellen Erkennung. Der Nutzer kann damit selbst entscheiden, ob das Treffen mit einem anderen Kontakt protokolliert werden soll oder nicht. Vorteil davon ist, dass eine gewisse Privatsphäre in einigen Momenten erhalten bleibt, Nachteil dagegen, dass im Falle einer Infektion der Infektionsweg nicht komplett nachvollziehbar wäre, wenn der Nutzer nicht preisgeben will, mit wem er sich alles getroffen hat.

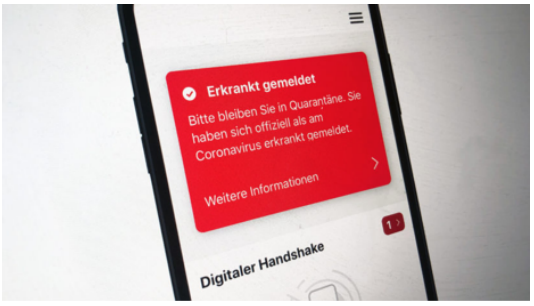

Abbildung 7: Die „STOPP-Corona“-App

In Österreich wurde die App innerhalb der ersten Woche fast 400.000-mal heruntergeladen. Eine genaue Auswertung, inwiefern sie zur Reduktion der Verbreitung des Corona-Virus in Österreich beigetragen hat lässt sich zum jetzigen Zeitpunkt jedoch noch nicht abschätzen. Die „STOPP-Corona“-App wurde von Datenschützern begrüßt, da sie dezentral arbeitet und jeder theoretisch selbst entscheiden könnte, wann er welche Kontakte freigibt. Ein weiteres Feature der App ist ein Symptomcheck. Mit Hilfe von diesem erhalten die Benutzer alle wichtigen Informationen und Symptomstrukturen der Krankheit auf einen Blick. Zudem ist es möglich, falls Symptome auf einen selbst zutreffen, seine Kontakte zu warnen, dass diese ihren Körper ebenfalls beobachten sollen auf Symptome der Krankheit. Sollte der anschließende Corona-Test beim Arzt/Labor jedoch ein negatives Ergebnis zeigen, so können die Benutzer eine Entwarnung an ihre bereits informierten Kon-

takte senden.[33]

6.3 Umsetzung in der finalen Version

Seit dem 16. Juni 2020 ist die deutsche Version der Corona-App in allen gängigen Stores für mobile Endgeräte verfügbar. Geschaffen wurde sie durch die Zusammenarbeit der Firma SAP und der Deutschen Telekom für einen Preis von rund 20 Millionen Euro.[34]
Verwaltet wird die App durch das Robert Koch Institut in Kooperation mit dem Hersteller und der Bundesregierung. Zudem wurden zwei Hotlines eingerichtet, eine für technische Probleme und die andere muss von positiv getesteten Personen angerufen werden, um ihren positiven Befund zu verifizieren. Ziel ist es, damit etwaige Falschmeldungen so gut es geht auszuschließen.[35] Pro Tag erfolgen nach Angaben des Robert Koch Institutes rund 2.300 Anrufe auf beide Hotlines zusammen (Durchschnittswerte vom 10. bis 17. August 2020). Insgesamt wurde die App bereits 17,2 Millionen Mal heruntergeladen, was fast ein Viertel der deutschen Bevölkerung darstellt. Das Robert Koch Institut verwendet zur Verifizierung von positiv getesteten Personen ein TAN-Verfahren. Seit dem Start der App am 16. Juni wurden 1.679 TANs herausgegeben.[36]

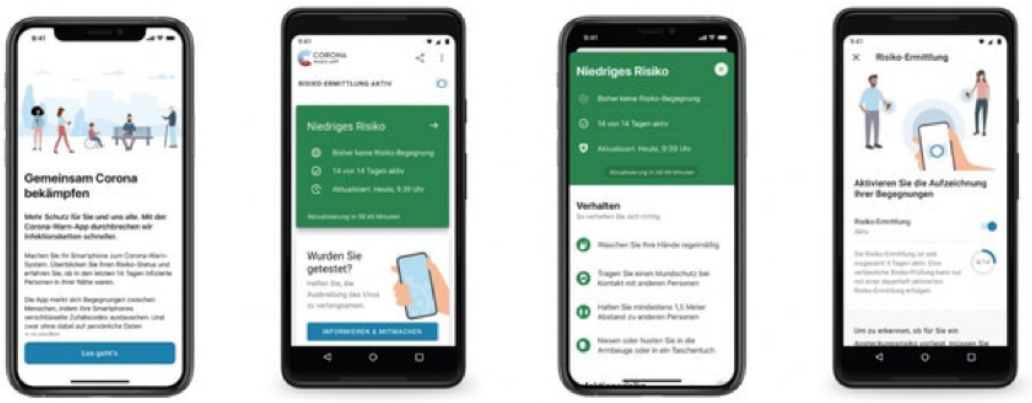

Abbildung 8: Die Corona-App für Android und iOS

Doch wie arbeitet die Corona-App? Eigentlich ist sie eine Mischung aus den diskutierten Formen. Die Datenspeicherung erfolgt dezentral auf dem jeweiligen Endgerät und nur die Schlüssel der positiv getesteten Menschen werden hochgeladen, sodass die Endgeräte darauf zugreifen und selbst überprüfen, ob sie mit dem Infizierten Kontakt hatten. Die Registrierung erfolgt zudem anonym. Ein weiterer, wie auch in den diskutierten Formen enthaltener, Bestandteil ist die Bluetooth-LE Technologie, um Kontakt

[33] https://www.profil.at/oesterreich/stopp-corona-app-ingrid-brodnig-rotes-kreuz-11461093
[34] https://www.zeit.de/digital/2020-06/corona-app-entwicklungskosten-betriebskosten-sap-telekom
[35] https://www.zeit.de/digital/datenschutz/2020-06/tracing-app-corona-warn-app-smartphone-virus-ausbreitung-deutschland
[36] https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Kennzahlen.pdf?___blob=publicationFile

auf geringer Distanz zwischen den Geräten herzustellen und zu überprüfen, ob diese sich weniger als zwei Meter entfernt befanden. Der Programmcode der App ist zudem öffentlich einsehbar, also Open-Source.
Sollte ein Kontakt mit einer infizierten Person innerhalb der letzten 14 Tage bestanden haben, so zeigt die App ein erhöhtes Risiko für den Benutzer an. Zudem sieht er, wann er dem Infizierten begegnet ist, und die App empfiehlt, soziale Kontakte ab sofort zu vermeiden und sich testen zu lassen. Damit soll der Benutzer als selbstständiger Mensch Rücksicht auf sein Umfeld nehmen. Überprüft wird dies jedoch nicht. Ein weiterer Fall, welcher eintreten kann, ist, dass es Kontakt mit einem Infizierten gab, dieser aber zu weit entfernt war oder der Kontakt zu kurz. Der Schwellenwert für ein „erhöhtes Risiko“ wurde damit nicht überschritten. Der dritte Fall ist, dass es keinen Kontakt zu einer infizierten Person innerhalb der letzten 14 Tage gab und damit ein „niedriges Risiko“ besteht.[37]

6.4 Datenschutz

In Bezug auf den Datenschutz können wir nun zwei Formen der Datenspeicherung aus den diskutierten Formen und der letztendlichen Umsetzung der App ableiten.
Die Form der zentralen Datenspeicherung der Schlüssel auf einem Servernetz, welches angegriffen werden könnte, wurde durch die Entwickler zum Glück nicht in Betracht gezogen. Zu groß wäre der Datenverlust, wenn die Server einem Hackerangriff zum Opfer fielen. Zudem könnten sich aus den gespeicherten Daten Bewegungsprofile der Benutzer ableiten lassen.
Die dezentrale Speicherung ist dagegen sicherer. Durch die alleinige Speicherung der Daten auf den Endgeräten müssten erst alle von ihnen gehacked werden, damit sich Bewegungsprofile nachvollziehen lassen für Außenstehende. Trotzdem müssen auch in dieser Variante einzelne Daten auf einem zentralen Server gespeichert werden. Wer positiv getestet wurde, dessen Daten werden hochgeladen und von allen anderen Endgeräten abgefragt. Daher könnten Angreifer nur deren Daten abgreifen.
Da die Registrierung anonym erfolgt, gibt es von dieser auch keine Rückschlüsse auf die Person dahinter. Dies ebnet den Weg für Menschen, welche durch ihren Beruf zwei Endgeräte benutzen und daher auf beiden die App installiert haben. Dadurch erhöhen sie die Nutzerzahl aber nicht tatsächlich.
Schlussendlich können alle Skeptiker auch den Quellcode der App auf Github einsehen. Dort ist dieser frei zugänglich für jede Person, welche einen Computer besitzt und die nötige Programmiersprache versteht.

[37] https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Funktion_Detail.pdf?__blob=publicationFile

7 Diskussion und Fazit

Die Corona-Applikationen sind mittlerweile globaler Standard, gelten weithin als anerkanntes Mittel gegen die Pandemie. Und doch hat sich während unserer Recherche ein Bild in unseren Köpfen verfestigt: Dieses Mittel ist doch mindestens fragwürdig. Zum einen bleiben große Zweifel an der Effektivität dieser Apps, die Erfolge der Vorreiter um Südkorea sind nicht ohne die weiteren, parallel laufenden Maßnahmen und Freiheitsaufgaben zu denken, in vielen anderen Ländern inklusive Deutschland muss sich die jeweilige Corona-Warn-App noch beweisen. Stand heute - Ende August 2020, ein halbes Jahr nach Ausbruch der Pandemie - sind hierzulande noch kaum positive Auswirkungen zu verzeichnen. Zum anderen muss auch der Preis für den Einsatz einer solchen Applikation gesehen werden: Die Aufgabe von Persönlichkeitsrechten im Sinne der Freigabe von persönlichen Daten scheint in einer Demokratie auf den ersten Blick wenig gefährlich. Doch die Beispiele Israels und Chinas zeigen, dass an dieser Stelle ein ungeheures Potential für Missbrauch besteht. Was in China nur eine Verschärfung bereits bestehender Repressionen des autoritären Staates darstellt, äußerte sich in Israel im bisher unbekannten Einsatz der Geheimdienste gegen die eigene Zivilgesellschaft. Die Bundesrepublik profitierte 2020 von einer funktionierenden Demokratie - einem potentiellen Missbrauch der durch die Corona-Warn-App erhobenen Daten wurde frühzeitig durch Gesellschaft, IT-Experten wie dem Chaos-Computer-Club und Datenschützern entgegengetreten, am Ende eine scheinbar sichere Version präsentiert. An dieser Stelle musste eine Abwägung stattfinden: Epidemiologie versus Datenschutz, Fremd- und Gemeinschaftsschutz versus Selbstschutz. Deutschland entschied sich für letztere Option - angesichts des gut kontrollierbaren Infektionsgeschehens wohl die richtige Entscheidung. Doch man darf dabei nicht vergessen: Die Entwicklung der deutschen App war langwierig und teuer, und sie ist aus epidemiologischer Perspektive ein Kompromiss: Das Beispiel Südkorea zeigt, dass weitere Mittel möglich gewesen wären. Ohne das moderate Infektionsgeschehen hätte die viel zu lange andauernde Entwicklung dieser sehr datenschutzkonformen App zu spät kommen - und Leben kosten können.
Es bleibt also festzuhalten: Der Datenschutz ist keinesfalls nur Selbstzweck, er dient der Erhaltung der Grundpfeiler einer Demokratie. Andererseits sollte man auch bereit sein, diese augenscheinliche Grundbedingung temporär zu überdenken, wenn der praktische Einsatz dies bei der Rettung von Leben erfordert. Die Leitfrage dieses Aufsatzes: „Selbstzweck oder Grundbedingung?“ lässt sich insofern also nicht klar beantworten, ihre Entscheidung muss immer auf einer Abwägung zwischen epidemiologischen und datenschutzrechtlichen Aspekten beruhen.

8 Literatur

Die Zitierungen finden sich in Fußnoten auf den entsprechenden Seiten.