Ausarbeitung für Mobile Security

# Datenschutz und Sicherheit von Kontaktnachverfolgungs-Apps zur Eindämmung der Corona-Pandemie


Veranstaltung: Mobile Security bei Prof. Dr.-Ing. E. Eren

Meike Henschen-Bolte
Matrikelnr.: **********
E-Mail: hello@frollein-web.de

29.8.2021

# Inhaltsverzeichnis

# Abkürzungsverzeichnis

| | |
|---|---|
| **BLE** | Bluetooth Low Energie |
| **CCC** | Chaos Computer Club |
| **CDN** | Content Delivery Network |
| **CRNG** | Cryptographic random number generator |
| **CWA** | Corona-Warn-App |
| **DP3T** | Decentralized Privacy Preserving Proximity Tracing Protocol |
| **DSGVO** | Datenschutz Grundverordnung |
| **ENS** | Exposure Notification Framework |
| **EU** | Europäische Union |
| **FifF** | Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FifF) e.V. |
| **GPS** | Global Positioning System |
| **PCR** | Polymerase Chain Reaction |
| **QR** | Quick Response |
| **RKI** | Robert Koch Institut |
| **RPI** | Rolling Proximity Identifier |
| **RPIK** | Rolling Proximity Identifier Key |
| **RSSI** | Received Signal Strength Indication |
| **WLAN** | Wireless Local Area Network |

# Abbildungsverzeichnis

# 1 Einleitung

Angesichts der weltweiten Corona-Pandemie werden Möglichkeiten und Ansätze gesucht, diese einzudämmen. Durch das Aufdecken von Infektionswegen der Viruserkrankung und das Identifizieren massenhafter Übertragungsereignisse könnten infizierte Personen isoliert und Übertragungsketten unterbunden oder zumindest eingedämmt werden. Schnelles und gezieltes Vorgehen ist dabei gefragt.

Im Frühjahr 2020 wurde die Kontaktnachverfolgung zunächst pragmatisch über einfache Papierlisten, welche in Cafés und anderen öffentlichen Orten verpflichtend wurden, umgesetzt. Auch in Befragungen zu den Kontakten von mit Corona infizierten Personen durch Gesundheitsämter waren solchen Listen hilfreich. Die digitale Lösung von Kontaktnachverfolgung in Form von Kontaktnachverfolgungs-Apps oder -systemen wurde daraufhin nicht nur in Deutschland diskutiert. Die Hoffnung dabei war, das persönliche Infektionsrisiko einer Person mit Unterstützung technischer Verfahren schneller ermitteln zu können.

Der Blick in andere Länder bot bereits zu diesem Zeitpunkt eine Vielzahl von unterschiedlichen Ansätzen. Einige davon greifen sehr weit in die Privatsphäre der Menschen ein: Die verpflichtende Smartphone-App TraceTogether, die in Singapur eingesetzt wird, wertet Bewegungsdaten und Kontakte per Bluetooth aus und ordnet über eine Meldung auf das Smartphone Quarantäne für den/die Nutzer:in an. Die Einhaltung dieser wird mit Hilfe von GPS-Daten überwacht, zusätzlich müssen Infizierte sie mit spontan abgefragten Fotos ihrer Wohnungsumgebung nachweisen. Der Ansatz der israelischen Regierung hingegen ist es, sämtliche Standort- und Bewegungsdaten sowie auch Finanzdaten von möglicherweise Infizierten zentral auszuwerten.[1] In Europa regelt die DSGVO, dass derart weitreichende Eingriffe in die Privatsphäre der Bürger:innen nicht so einfach möglich sind.

In dieser Arbeit werden zunächst einige grundlegende Begriffe, Konzepte und Technologien erläutert. Anschließend werden die beiden wichtigsten Kontaktnachverfolgungs-Apps in Deutschland, die Corona-Warn-App und die luca-App vorgestellt, ihre technische Umsetzung im Detail betrachtet und ihre Vor- bzw. Nachteile dargelegt. Bestehende Sicherheitslücken werden aufgezeigt und Kritikpunkte erörtert. Außerdem werden die beiden Apps miteinander verglichen und diskutiert, ob Kontaktnachverfolgungs-Apps und die damit einhergehend erfassten Daten, im Kampf gegen die Corona-Pandemie überhaupt eine Wirkung entfalten konnten oder das in Zukunft können.

Abschließend wird die generelle Zunahme von Digitalisierung, ausgelöst durch die Corona-Pandemie skizziert und der kürzlich eingeführte digitale Impfnachweis vorgestellt.

[1] Vgl. Reh20, S. 16

## 1.1 Grundlegendes

### 1.1.1 Epidemiologisch relevante Ereignisse

Zu Beginn der Corona-Pandemie bzw. im Frühjahr 2020 gingen Virolog:innen davon aus, eine Ansteckung fände überwiegend im direkten Kontakt statt, beispielsweise während eines ausreichend langen Gesprächs mit einem infizierten Gegenüber. Einen geringeren Anteil der Übertragungswege vermutete man über Schmierinfektionen.[2]

Superspreading-Events oder Cluster-Situationen, also einzelne Veranstaltungen, bei denen sich viele Menschen anstecken, konnten ebenfalls schon früh als aus epidemiologischer Sicht kritisch eingestuft werden.[3]

Heute, ein Jahr später, halten Forscher:innen zusätzlich Ansteckungsszenarien für möglich, in denen die infektiösen Aerosole in geschlossenen Räumen über einen längeren Zeitraum ansteckend bleiben. Sogar auch dann noch, wenn die infizierte Person gar nicht mehr anwesend ist. Demnach könnten Ansteckungen auch ohne den direkten Kontakt erfolgen. Insbesondere ist dieses Szenario vorstellbar in kleinen Räumen, wie Cafés oder Fahrstühlen, in denen wenig gelüftet wird.[4]

Ansteckungen im Freien finden demgegenüber so gut wie gar nicht statt. Die Luftverdünnung und Zerstreuung der Aerosole außerhalb geschlossener Räume machen eine Infektion unwahrscheinlich. Ausnahme: Viele Menschen kommen an einem windgeschützten Ort zusammen.[5]

### 1.1.2 Tracing vs. Tracking

Der Begriff Tracking (engl. Verfolgen) meint eine permanente möglichst lücken- und pausenlose Überwachung. Beim GPS-Tracking, also der Verfolgung und Aufzeichnung von Ortsdaten zu einer Person oder beim Web-Tracking, der Überwachung von Aktivitäten einer Person im Internet, erfolgt die Erfassung der Bewegungsdaten so umfassend wie möglich. Tracing (engl. Aufspüren) bedeutet, dass Informationen ganz oder teilweise im Nachhinein anhand von Spuren rekonstruiert werden.

In den „Leitlinien zur Gewährleistung der uneingeschränkten Einhaltung der Datenschutzstandards durch Mobil-Apps zur Bekämpfung der Pandemie“ der Europäischen Kommission aus April 2020 wird hervorgehoben, „dass Standortdaten für die Ermittlung von Kontaktpersonen nicht erforderlich sind und dafür auch nicht verwendet werden sollten“.[6] In den Leitlinien wird deutlich, dass die Kommission damals aus epidemiologischer Sicht das Kontaktereignis an sich als wichtig einschätzt, nicht aber den Ort an dem dieses stattgefunden hat. Mit dieser Einschränkung sollte ein Tracking von Personen über GPS-Daten oder eine Ortung über WLAN nicht das Mittel der Wahl sein. Das „Aufspüren“ eines Kontaktereignisses könnte stattdessen über die Entfernung zweier Mobilgeräte voneinander erfolgen.[7]

Ansteckungsszenarien, in denen sich der/die Infektiöse und der/die sich neu Infizierende nicht getroffen haben, sondern die Infektion über verbliebene Aerosole in der Luft stattgefunden hat (siehe Abschnitt 1.1.1), ließen sich über diesen Weg allerdings nicht

[2] Vgl. RKI21a, Chr20
[3] Vgl. dpa20b
[4] Vgl. Sch21a, RKI21a
[5] Vgl. Sch21a
[6] EU-20b
[7] Vgl. Sch20a

aufdecken. Trotzdem würde umfassendes Bewegungs-Tracking von Personen nicht notwendig werden. Zwar ist relevant, ob eine infektiöse Person sich über einen längeren Zeitraum an einem Ort aufgehalten hat. Gleiches gilt für die Information, ob andere Kontakte sich zur selben Zeit oder innerhalb einer gewissen Zeitspanne im Anschluss am selben Ort aufgehalten haben. Entsprechend der aktuellen Forschung wäre der Aufenthalt aber nur an Orten relevant, die aufgrund ihrer Umgebungsvariablen eine Infektionsgefahr bieten. Dies sind geschlossene Räume, in denen viele Menschen ein und aus gehen und/oder sich über einen längeren Zeitraum aufhalten.[8] Die Erfassung von Daten, die ein Tracing dieser Szenarien im Nachhinein möglich machen, ist ausreichend

### 1.1.3 Bluetooth Low Energy und Ortungsdienste

Mit den Technologien GPS, WLAN und seit einigen Jahren auch iBeacon, das die Technologie Bluetooth Low Energy (Bluetooth LE oder BLE) verwendet, ist eine unterschiedlich genaue Standortbestimmung möglich. GPS ist satellitengestützt, allerdings in der Standortermittlung eher grob und im Indoorbereich nicht sinnvoll.[9] WLAN-Ortung berücksichtigt die Ausbreitungsmuster von WLAN-Netzwerken und bestimmt mittels Lateration die Position eines Smartphones auf einen halben Meter genau. WLAN-Ortung ermöglicht sogar die Navigation innerhalb von Gebäuden, beispielsweise setzt das Museum Industriekultur in Nürnberg diese Technologie unter anderem in ihrem Führungssystem ein.[10] Ähnlich funktioniert auch das Prinzip von iBeacons (Apple) und vergleichbare Entwicklungen. Hierbei werden kleine BLE-Sender physisch platziert, die die Standortbestimmung eines empfangenden BLE-Moduls mittels Lateration erlauben. Mit Hilfe dieser Technik kann der Standort eines Geräts theoretisch auf wenige Zentimeter genau bestimmt werden.[11]

Die Funktionsweise von Bluetooth beruht auf dem Aussenden elektromagnetischer Wellen aus demselben Spektrum wie auch Radio-Wellen oder WLAN. Um sich mit einem anderen bluetoothfähigen Gerät zu verbinden, sendet es wiederholt Signale aus, um seinen aktiven Status zu broadcasten.

Bluetooth ist nicht gleich Bluetooth. Bluetooth Low Energy ist eine Bluetooth-Variante die stromsparender agiert als das klassische Bluetooth. Allerdings ist sie langsamer und hat eine geringere Reichweite als das klassische Bluetooth. BLE ist nicht kompatibel zu klassischem Bluetooth und ab der Version 4.0 optionaler Bestandteil des Bluetooth-Standards.[12]

Aufgrund dieser Eigenschaften wurde BLE zur Hoffnung der Technologiebranche zur Bekämpfung der Corona-Pandemie. Der Grundgedanke: Anhand des ausgesendeten Signals einer BLE-Zelle kann festgestellt werden, dass sich zwei Smartphones erreichen können. Anhand der Signalstärke kann theoretisch bestimmt werden, auf wie viel Meter nahe sich die Geräte genau kommen.[13] Die Idee dabei ist, dass ein Kontakt mit einer später positiv getesteten Person als Rückmeldung oder Warnung auf dem Smartphone erscheint.

In der Praxis führen allerdings die massenhaft verschiedenen Versionen der genutzten Mobilgeräte und die Platzierung der Zellen im Gerät, aber auch die Ausrichtung des

[8] Vgl. Sch21a
[9] Vgl. Mer19
[10] Vgl. Int18
[11] Vgl. Kau14
[12] Vgl. MS19, Mut20
[13] Vgl. Bid20

Geräts, zu Diskrepanzen in der Entfernungsmessung.[14] Zudem verbreiten sich elektromagnetische Wellen in alle Richtungen und können von Hindernissen in ihrem Weg behindert, geschluckt und reflektiert werden. So wird ein Signal unter idealen Bedingungen besser empfangen, als wenn das Mobilgerät z.B. in einer Handtasche unter einem Tisch in einem vollen Café Signale aussendet. Die Signalstärke wird in der Einheit Received Signal Strength Indication (RSSI) gemessen. Je nach Umgebung kann ein Smartphone das zwei Meter entfernt ist anhand des RSSI-Werts auf eine Entfernung von 20 Meter geschätzt werden.[15]

Auch die beiden Entwickler Jaap Haartsen und Sven Mattisson, die Bluetooth gemeinsam während ihrer Zeit bei telekcom Ericsson erfunden haben, vermuten, dass Bluetooth für diesen Zweck zu ungenau ist. Es würden Triangulation oder Lateration wie bei Radar benötigt, um genauere Aussagen zu der Entfernung von zwei Geräten treffen zu können. Um diesem Problem zu begegnen haben die Unternehmen Google und Apple mit einem Softwareupdate die Informationen in dem Bluetooth Broadcast Signal angepasst. Ein kleines Fragment in den Daten gibt Informationen über die Signalstärke des Broadcasts und soll so dabei helfen zu bestimmen, wie viel auf dem Weg verloren gegangen ist.[16]

Wesentlich bei der Ungenauigkeit in der Entfernungsmessung ist im Kontext der Kontaktnachverfolgungs-Apps die Gefahr von falsch-positiven oder falsch-negativen Risiko-Begegnungen. Einerseits würden Personen die keine Risikobegegnung mit einer infizierten Person hatten ggf. unnötig in Quarantäne isoliert, inklusive aller Einschränkungen und sozialer Stigmatisierung die damit einhergehen. Noch kritischer hinsichtlich der Ausbreitung des Virus ist aber die falsch-negative Begegnung, bei der eine infizierte Person sich nicht testet, in falscher Sicherheit wiegt und andere anstecken kann.

Bluetooth und Bluetooth LE gehören nicht zu den sichersten Technologien. Da in der Praxis häufig die notwendigen Sicherheitsmechanismen nicht aktiviert sind bzw. immer wieder neue Sicherheitslücken auftauchen, ist die Technologie anfällig für Angriffe. Problematisch sind insbesondere Implementierungsfehler oder Fehler im SDK. Außerdem können kryptografisch relevante Daten leicht abgegriffen werden.[17]

### 1.1.4 Zentralität vs. Dezentralität der Daten

Die Entscheidung zwischen einem zentralen und einem dezentralen Architekturansatz ist grundlegend für die Implementierung einer Kontaktnachverfolgungs-App.

Im Fall der zentralisierten Architektur werden die gesammelten Daten aller Nutzer:innen auf zentraler Ebene der Betreiber:innen und/oder Behörden zusammengeführt. Dies betrifft sowohl Gesundheitsdaten der natürlichen Personen als auch ihre Kontakthistorie. Diese Daten werden vor unbefugtem Zugriff geschützt und nur zweckgebunden verwendet. Zusätzlich werden die Daten bei ihrer Verwendung im größtmöglichen Maße anonymisiert. Dies ergibt sich aus gesetzlichen Vorgaben und Leitlinien.[18] Eine zentrale Datenhaltung ermöglicht die gemeinsame Auswertung und Analyse, um weiterreichende Erkenntnisse über die Pandemie zu gewinnen. Dennoch ist es bei diesem Modell unerlässlich, auf die "Vertrauenswürdigkeit und Kompetenz des Betreibers von zentraler

[14] Mut20, al20
[15] Vgl. Bid20
[16] Vgl. Bid20
[17] Vgl. Mik13
[18] Vgl. Rat16, EU-20b

Infrastruktur zu vertrauen, die Privatsphäre der Nutzer schon ausreichend zu schützen."[19]

Als Argument für den zentralisierten Ansatz werden insbesondere die sich hinsichtlich der Epidemie möglichen zu ergreifenden Maßnahmen genannt. Grundgedanke ist die Idee, an zentraler Stelle Cluster und Superspreading-Events zu erkennen und in der Supervision besser kontrollieren zu können. Andererseits ist aus der Praxis bekannt, dass diese Erkenntnisse aus den Daten nur langsam während einer ausführlichen Analyse gewonnen werden.[20]

Die dezentralisierte Architektur unterstützt die Strategie, so viele Daten wie möglich auf dem Gerät der Nutzer:in zu belassen. Zwar ist im Falle einer Kontaktnachverfolgungs-App trotzdem eine zentrale Instanz nötig, über welche im Falle einer infizierten Teilnehmer:in die Information an die Kontakte übermittelt werden kann.[21] Da er nur diese losgelösten Daten - und keine Geheimnisse - vorhält, muss diesem Server nicht vertraut werden. Es gibt keinen „central point of trust for security and privacy“.[22] Bis zu dem Zeitpunkt der Bekanntmachung einer Infektion über die App verbleiben alle Daten auf dem Smartphone der Nutzer:innen.

Das von unabhängigen europäischen Forscher:innen entwickelte Projekt Decentralized Privacy Preserving Proximity Tracing Protocol (DP3T) veröffentlichte eine quelloffene Implementierung dieses Ansatzes auf Github. „The system aims to minimise privacy and security risks for individuals and communities and guarantees the highest level of data protection“.[23] Der Gruppe gehören Expert:innen aus den Bereichen Technologie und Entwicklung an sowie Rechtswissenschaftler:innnen und Epidemiolog:innen.

Hinsichtlich der Wahrung der Privatsphäre ist der dezentrale Architekturansatz zu bevorzugen. In dieser Weise äußern sich nicht nur der Chaos Computer Club[24] sowie zahlreiche Datenschützer:innen.[25] Auch Google und Apple befürworten Apps, die dezentrale Architekturen implementieren. Jedoch stehen hierbei womöglich nicht nur die Aspekte des Datenschutzes sondern ebenso wirtschaftliche Aspekte im Vordergrund.[26]

### 1.1.5 Kooperation mit Google und Apple

Die Marktmacht von Google und Apple verschaffte den beiden Technologie-Giganten eine besondere Rolle bei der weltweiten Entwicklung von Kontaktnachverfolgungs-Apps zur Bekämpfung der Corona-Pandemie. Um in den offiziellen App Store (Apple) bzw. Google Play Store aufgenommen zu werden, muss eine App sich den Richtlinien und Vorgaben der Unternehmen beugen. Die Hersteller stellen auf Betriebssystemebene nur

[19] Vgl. Neu20
[20] Vgl. Bun21b
[21] Vgl. Sch20a
[22] Vgl. Git20b
[23] Vgl. Git20a
[24] Vgl. Neu20
[25] Vgl. Sch20c
[26] Vgl. ZDF20

gewisse Dienste und Schnittstellen zur Verfügung, welche App-Entwickler nutzen können.

Um die Entwicklung von Kontaktnachverfolgungs-Apps möglich zu machen, haben sich die beiden Unternehmen zusammengeschlossen, „um Regierungen mit einem System für COVID-19- Benachrichtigungen zu unterstützen“.[27]

Laut eigener Aussage haben sie dabei den Datenschutz im Blick und versprechen: „Deine Identität wird vom System niemals mit anderen Nutzern, Apple, Google oder Behörden geteilt.“[28] Ähnlich wie vom Projekt DP3T vorgeschlagen, setzen sie auf eine dezentrale Architektur und schaffen mit der Entwicklung des Exposure Notification Framework (ENF) die notwendige Schnittstelle zur effizienten Implementierung einer Kontaktnachverfolgungs-App. Deren Verwendung wird allerdings nur gegen die Beachtung und Umsetzung gewisser Datenschutzregeln gewährt.[29] Werden diese missachtet, verhindern die Markt-Giganten auch schon mal ein Update.[30] Um sicherzustellen, dass es nicht eine große Auswahl verschiedener Tracing-Apps auf dem Markt gibt, sondern eine große Verbreitung einer einzigen App - aus epidemiologischer Sicht ist dies unbedingt sinnvoll - wurde außerdem von den Unternehmen festgelegt, dass pro Land nur eine App Zugriff auf die Schnittstelle bekommen soll. Dies soll unter der Verantwortung der Gesundheitsbehörden eines Landes geschehen.[31]

Einmalig an der hier dargestellten Situation ist sicherlich nicht nur die Tatsache, dass die zwei größten Konkurrenten auf dem Betriebssystem-Markt für Mobilgeräte im Angesicht der Corona-Pandemie eine Kooperation eingegangen sind. Bemerkenswert ist sicherlich auch, dass zwei private Unternehmen aufgrund ihrer Position Regierungen in ihre Schranken weisen können und eigene Regeln definiert haben, welche von Datenschützern hingenommen werden. Deutschlands Gesundheitsminister Jens Spahn hatte sich in diesem Zusammenhang kritisch geäußert, über den offenbar verbreiteten „Grundglauben daran, dass Daten bei Apple und Google besser aufgehoben sind“ als „auf staatlichen Servern in Deutschland“.[32]

Technische Details des Exposure Notification Framework von Google und Apple werden in Abschnitt 2.1.1 genauer vorgestellt.

## 1.2 Definitionen

**Datensicherheit**

Datensicherheit gewährleistet die technische Sicherheit von Daten, also den Schutz gegen Verlust oder unerlaubte Veränderung von Daten. Datensicherheit ist eine Voraussetzung für einen effektiven Datenschutz.

**Datenschutz**

Im Rahmen des Datenschutzes werden insbesondere die Privatsphäre und das Recht auf informationelle Selbstbestimmung einzelner Personen sichergestellt. Die Vertraulichkeit, Verfügbarkeit und Integrität von persönlichen aber auch wissenschaftlichen oder

[27] Vgl. Goo20b
[28] Goo20b
[29] Vgl. Kre20
[30] Vgl. Hol21
[31] Vgl. EU-20a, EU-20b und Kre20
[32] Vgl. Kre20

Unternehmens-Daten wird dabei gewährleistet. Hierbei werden neben technischen Aspekten auch organisatorische bzw. rechtliche Gegebenheiten relevant.

**Informationssicherheit**

Informationssicherheit stellt die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicher. In der Informationstheorie nach Shannon handelt es sich immer dann um Informationen, wenn durch vorliegende Daten neues Wissen erlangt werden kann. Datensicherheit und Datenschutz stellen somit einen Teilbereich der Informationssicherheit dar.[33]

# 2 Analyse

Im Folgenden werden zwei konkrete Umsetzungen von Kontaktnachverfolgungs-Apps betrachtet, die sich im wesentlichen Punkt der dezentralen bzw. zentralen Datenverarbeitung unterscheiden.

## 2.1 Die Corona-Warn-App (CWA) der deutschen Bundesregierung

Das Robert Koch-Institut (RKI) - die zentrale Einrichtung des Bundes im Bereich der öffentlichen Gesundheit - erhielt den Auftrag zur Entwicklung einer Corona-Warn-App für die Bundesrepublik Deutschland durch die deutsche Bundesregierung. Die Corona-Warn-App stellte in der ersten Version einige grundsätzliche Funktionalitäten bereit, wie die anonymisierte Kontaktnachverfolgung, das Veröffentlichen eines positiven Testergebnisses, das Melden des individuellen Risikos und eine digitale Unterstützung beim Führen eines Kontakttagebuchs.

Die Grundfunktionalität der Corona-Warn-App des RKI basiert auf der vorgestellten BLE-Technologie und dem Exposure Notification Framework (ENS) von Apple und Google. Nach langer Diskussion im Frühjahr 2020[34] wurde seitens der Bundesregierung und des RKI festgelegt, mit der App den Ansatz der Dezentralität zu verfolgen, wie im Projekt D3PT erarbeitet und durch Google und Apple vorgegeben.[35] Sie hat das Ziel, Nutzer:innen über ihr persönliches Infektionsrisiko zu informieren. Bei der Installation der App müssen keinerlei personenbezogene Daten angegeben werden.

Entwickelt wird die App unter der Leitung des Robert Koch-Instituts (RKI) durch eine Kooperation der Unternehmen SAP und Deutsche Telekom und 25 weiteren Kooperationspartnern.[36] Die Entwickler:innen-Teams haben laut eigener Aussage „mit der App den Prozess für eine erfolgreiche Unterbrechung der Infektionskette im Hinblick auf die Covid-19-Pandemie digitalisiert: von einer möglichen Infizierung bis hin zur Warnung möglicher Kontaktpersonen, vom Smartphone bis ins Labor.“[37] Die App wurde innerhalb von 50 Tagen entwickelt und im Juni 2020 erstmalig zum Download bereitgestellt. Die Entwickler:innen betonen den transparenten Entwicklungsprozess und heben hervor, dass er zu jedem Zeitpunkt auf der Plattform Github einsehbar und vollständig Open Source ist. Es hat von mehr als 109.000 Einzelbesuchern Einsichten in den Code sowie

[33] Vgl. Böh20
[34] Vgl. Kri20
[35] Vgl. RKI21b
[36] Vgl. Mül20
[37] Vgl. New20

ca. 7.250 Beteiligungen durch Community- und Projektmitglieder gegeben.[38] Zusätzlich gab es einen technischen Audit durch den TÜV-IT. Hierbei wurden zwar keine Anomalien, Hintertüren oder versteckte Funktionen entdeckt, allerdings erklärte der TÜV, dass der Testauftrag zeitlich und inhaltlich begrenzt gewesen sei. So war der anberaumte Testzeitraum nur klein. Eine Prüfung der Verschlüsselung oder ein Test der bereitgestellten Schnittstelle ENF war nicht gewünscht.[39]

Der Chaos Computer Club findet lobende Worte für die App und sieht seine zehn Prüfsteine für die Beurteilung von Kontaktnachverfolgungs-Apps, die das Netzwerk im Frühjahr 2020 veröffentlichte, fast vollständig erfüllt. Linus Neumann lobt unter anderem den transparenten Entwicklungsprozess und die Annahme von Vorschlägen aus der Community: „Die App ist das erste große öffentlich finanzierte Open Source Projekt in Deutschland. Da kann sich die Bundesregierung doch auch mal auf die Schulter klopfen.“[40]

### 2.1.1 Grundsätzliche Funktionsweise und Implementierung unter Verwendung des Exposure Notification Frameworks

Zur Ermittlung des „Kontakts“ von Personen wird mittels BLE festgestellt, ob sich Smartphones nahegekommen sind. Dabei fungieren die einzelnen Smartphones als „Beacons“, die ständig ihre eigene temporäre Zufallskennung broadcasten, während sie gleichzeitig auf Zufallskennungen anderer Smartphones lauschen. Die gesendeten IDs sind nur temporär und verändern sich alle 10 bis 20 Minuten.[41]

Die gesammelten Zufallskennungen anderer App-Nutzer:innen werden lokal auf jedem einzelnen Smartphone gespeichert. Aufgrund der empfangenen Signalstärke und -länge lässt sich grob abschätzen, wie weit das andere Gerät entfernt ist. Außerdem wird erfasst, wie lange der Kontakt besteht. Diese Daten werden später in die Risikoberechnung[42] für den/die Nutzer:in des Systems einbezogen.[43] Was hierbei nicht aufgedeckt werden kann, ist ob sich beispielsweise eine Glasscheibe oder eine Wand zwischen zwei Personen und ihren Smartphones befunden hat. In diesem Fall wäre der „Kontakt“ bezüglich der Ausbreitung des Corona-Virus nicht weiter relevant, da ein geringes oder kein Infektionsrisiko besteht.[44]

[38] Vgl. New20
[39] Vgl. Sch20b
[40] Vgl. Dom20
[41] Vgl. Goo20b, Goo20a
[42] Die Risikoberechnung ermittelt im Falle eines Kontakts mit einer positiv getesteten Person das vermutlich bestehende Risiko. Die Parameter zur Berechnung sind Übertragungsrisiko, Tage seit der Begegnung, Dauer der Begegnung und der Dämpfungswert. Sie werden gewichtet einberechnet. Die möglichen errechneten Risiken sind niedriges Risiko, niedriges Risiko trotz einer Begegnung mit einer positiv getesteten Person und erhöhtes Risiko. (Vgl. Ins20)
[43] Vgl. Ins20
[44] Vgl. Ins20, dpa20a

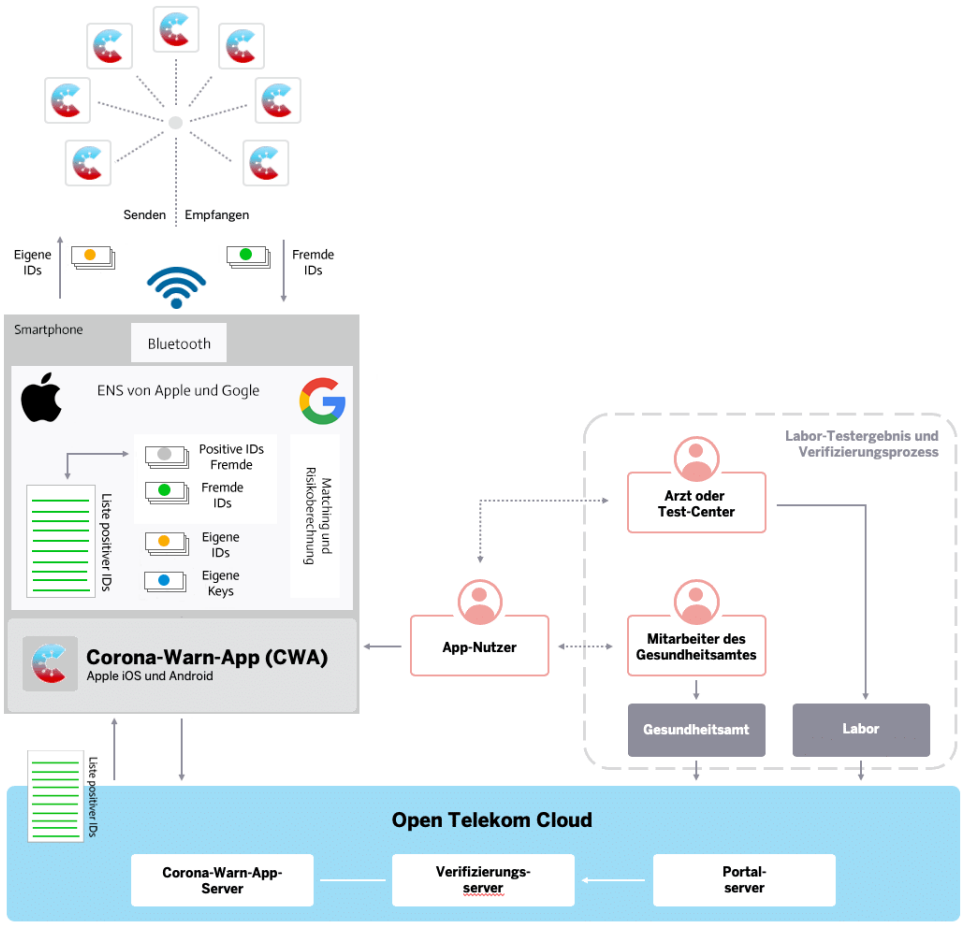


**Abbildung 1: Zusammenspiel von CWA und ENS auf dem Smartphone und der weiteren System-Architektur**

Die Zufallskennungen werden von einem Schlüssel, dem Temporary Exposure Key, kryptografisch abgeleitet: Der Temporary Exposure Key wird über einen CRNG[45] unabhängig generiert und alle 24 Stunden erneuert. Hieraus wird zunächst mit Hilfe der Schlüsselerzeugungsfunktion HKDF[46] ein weiterer Schlüssel (RPIK, Rolling Proximity Identifier Key) erzeugt. Mit diesem werden schließlich in einem definierten Zeitintervall die Zufallskennungen (RPI, Rolling Proximity Identifier), erzeugt.[47] Das Verfahren stellt sicher, dass weder durch die Temporary Exposure Keys noch durch die Rolling Proximity Identifier auf ein bestimmtes (Bluetooth-)Gerät oder eine Person geschlossen werden kann. Die temporären Zufallskennungen stellen sicher, dass Nutzer:innen nicht wiedererkannt oder Bewegungsmuster für sie erstellt werden können.[48]

Es werden jeweils die Temporary Exposure Keys und die daraus abgeleiteten Zufallskennungen des eigenen Systems als auch die gesammelten RPIs anderer Geräte der letzten 14 Tage auf dem Smartphone gespeichert. Dieser Zeitraum wurde auf Basis von medizinischen Studien festgelegt, die davon ausgehen, dass infizierte Personen maximal 14 Tage lang ansteckend sind.[49]

[45] Cryptographic Random Number Generator
[46] Eine Schlüsselableitungsfunktion basierend auf einem HMAC; ermöglicht Integritätscheck und Authentifizierung
[47] Vgl. Goo20c, RKI21c
[48] Vgl. Goo20b, Goo20c, Mül20
[49] Vgl. RKI21c, Sch20a, Mül20

Im Falle eines auf SARS-CoV-2 positiven PCR-Tests können Nutzer:innen der App eine Verifizierung ihres positiven Tests zur Verfügung stellen.[50] Ihre Temporary Exposure Keys der letzten 14 Tage werden daraufhin in Diagnosis Keys umbenannt und auf einen zentralen Server geladen. Der Server kann währenddessen sehen, von welchem Mobilgerät die Daten geladen werden, kann darüber hinaus aber keine Rückschlüsse auf die Person ziehen.[51] In der Dokumentation von Apple und Google wird bestimmt, dass der Server keine Meta-Daten des Client-Geräts speichern darf.[52] Wird die Person nicht positiv getestet oder veröffentlicht sie diese Information nicht über die App, verbleiben alle Daten auf dem Smartphone und werden nach Ablauf von 14 Tagen vollständig gelöscht.[53]

Alle Diagnosis Keys werden auf dem zentralen Server gesammelt und allen Nutzer:innen der App zur Verfügung gestellt. Um Millionen von Smartphones erreichen zu können, werden die aggregierten Daten über ein Content Delivery Network (CDN) bereitgestellt.[54] Mit Hilfe der Daten bestimmt das Exposure Notification Framework auf einem Smartphone, ob eine der gesammelten RPIs zu den Diagnosis Keys passt - ob also ein Kontakt innerhalb des relevanten Zeitraums stattgefunden hat.[55] Die App ermittelt nun lokal das Risiko eines erfolgten Kontakts und meldet dieses an den/die Nutzer:in. Auch diese Information verbleibt auf dem Smartphone der Nutzer:innen und wird nicht aktiv an andere weitergegeben.[56]

Für den erfolgreichen Einsatz der App ist Eigenverantwortung der Nutzer:innen gefragt. Sie sollten je nach Einschätzung ihres Risikos entsprechende Maßnahmen ergreifen, z.B. ein Testzentrum aufsuchen bzw. im Falle eines positiven Testergebnisses dieses in der App vermerken. Da keine zentrale Instanz involviert ist und der Prozess vollständig anonymisiert abläuft, wird nicht eingegriffen und beispielsweise von extern eine Quarantäne verhängt. Lediglich allgemeine Handlungshinweise können gegeben werden. Diese umzusetzen liegt aber im Ermessen und in der Eigenverantwortung jeder Bürger:in.[57]

Im Fall einer Infektion und um dem Gesundheitsamt Kontaktinformationen mitteilen zu können, ist die Funktion des digitalen Kontakttagebuchs hilfreich.[58]

### 2.1.2 Corona-Warn-App 2.0: Funktionserweiterung Event-Registrierung

Wie in Abschnitt 1.1.1 dargestellt, geschehen epidemiologisch relevante Ereignisse nicht immer nur im direkten Kontakt. Mit dem Versions-Update und der Funktionserweiterung im April 2021 zur „Cluster-Erkennung“ ermöglicht die App einen Check-In bei einem Event oder an einem Ort durch Scannen eines QR-Codes, Nutzer:innen müssen den Zeitpunkt des Verlassens selbständig erfassen. Veranstaltungsort und Zeitraum des Aufenthalts werden innerhalb eines Kontakttagebuchs 16 Tage lang gespeichert oder bis die Veranstaltung manuell aus der Historie entfernt wird. Nutzer:innen der App, deren Aufenthaltszeitraum sich mit dem einer positiv getesteten Person ausreichend über-

[50] Zur Verhinderung von Missbrauch muss die Person über eine Hotline eine TAN zu dem Test anfordern.
[51] Vgl. Sch20a
[52] Vgl. Goo20b
[53] Vgl. Ins20
[54] Vgl. Mül20
[55] Vgl. Sch20a
[56] Vgl. Goo20b, Ins20
[57] Vgl. Sch20a, Goo20b
[58] Vgl. Bun21b

schneidet, können über die App gewarnt werden. Dies geschieht als wesentliche Neuerung auch dann, wenn kein direkter Kontakt aufgezeichnet wurde.[59]

Wichtig dabei ist, dass die Dezentralität und die bekannte Methodik beibehalten werden. Alle Daten verbleiben auf den Smartphones. Die Veranstaltungen mit erhöhtem Infektionsrisiko werden durch das Verteilen der relevanten Event-IDs an die Apps gemeldet und das Risiko für die Nutzer:innen wird im Einzelnen lokal berechnet. Weder Gesundheitsämter noch Veranstalter:innen erhalten Kenntnis über die Daten.[60] Der Bundesbeauftragte für Datenschutz und Informationsfreiheit Ulrich Kelber (SPD) erklärte im Ausschuss Digitale Agenda im Mai 2021, die Corona-Warn-App habe seit dem Update eine „gut funktionierende und datenschutzfreundliche Clustererkennung".[61] Der SAP-Entwickler Martin Fassunge stellte im gleichen Ausschuss heraus, dass es epidemiologisch gesehen vor allem auf Schnelligkeit ankomme, um die Pandemie einzudämmen. Die neuen Funktionen der App würden gut von Nutzer:innen angenommen.[62]

### 2.1.3 Weitere Sicherheitsbetrachtung und Kritik

Kurz nach Veröffentlichung der CWA wurde ein Fehler im ENS bekannt, welcher die Hintergrundfunktion auf iPhones einschränkte und die App dadurch im Prinzip nutzlos machte. Das Problem betraf die Implementierung des ENS auf Seiten von Apple, so dass die direkte Handlungsfähigkeit der Entwickler:innen der CWA eingeschränkt war. Dies wurde allerdings nicht kommuniziert. Eine offenere Kommunikation hätte der Glaubwürdigkeit des Projekts gut getan. Außerdem hätten die Nutzer:innen durch einfache Maßnahmen (z.B. durch tägliches Öffnen der App) die Funktionalität leicht wiederherstellen können.[63]

Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FifF) e.V. bemängelte schon früh das Fehlen einer Datenschutzfolgenabschätzung, zu welcher die DSGVO Betreiber:innen umfangreicher Datenverarbeitungssysteme verpflichtet.[64] Kurzerhand veröffentlichten sie hierzu ein eigenes Dokument, in dem eine dezentral aufgebaute Kontaktnachverfolgungs-App analysiert wird.

Hierin wird betont, dass „die wesentlichen Risiken der Datenverarbeitung von den Betreiber:innen eines Datenverarbeitungssystems ausgehen." Die Hürde zu einer missbräuchlichen Verarbeitung der Daten sollte in einer wirksamen Kombination von rechtlichen, technischen und organisatorischen Maßnahmen bestehen, welche prüfbar und dokumentiert vorliegen müssen. Eine quelloffene Entwicklung wird als substanziell beschrieben, um die Transparenz nicht nur für Behörden sondern auch für die Zivilgesellschaft zu gewährleisten.[65]

Darüber hinaus werden einige mögliche Schwachstellen und Angriffe hinsichtlich Datenschutz beschrieben. Ein besonders kritischer Punkt, der bereits in 2.1.1 angesprochen wurde, ist die Deanonymisierung von positiv getesteten Personen zum Zeitpunkt der Veröffentlichung ihrer Infektion bzw. der temporären Schlüssel aus der Kontakthistorie. Zum Zeitpunkt des Uploads der Daten auf den zentralen Server, können Nutzer:innen anhand ihrer Geräteinformationen oder der IP-Adresse identifiziert

[59] Vgl. Len21, RKI21d
[60] Vgl. Bun21a, RKI21d, Len21
[61] Vgl. Bun21b
[62] Vgl. Bun21b
[63] Vgl. Lau20
[64] Vgl. Reh20
[65] Vgl. Reh20

werden.[66] Zwar wird in der Spezifikation des ENS bestimmt, dass der Server keine Meta-Daten des Client-Geräts speichern darf, zusätzlich ist der Quellcode der App öffentlich. Dennoch besteht das Risiko, dass Betreiber:innen Daten sammeln. Die Nutzung der App setzt demnach Vertrauen in den/die Betreiber:in voraus.

Hinsichtlich dessen vertraut Linus Neumann vom CCC darauf, dass Apple und Google den Zugriff auf z.B. die Locationdaten nicht erlauben werden. Sehr strenge Kriterien müssen eingehalten werden, damit eine solche App überhaupt zugelassen wird.[67] Außerdem hält er einen weiteren Aspekt für wichtig: „Was ich glaube was tatsächlich die Rolle spielt ist, dass niemand bei einem solchen Mammutprojekt [...] das Risiko der Gesundheitsdaten an zentraler Stelle haben wollte. Ich glaube nicht, dass diese beiden Unternehmen besondere Kämpfer für die Privatsphäre sind, ich glaube sie haben für sich ökonomisch und pragmatisch die Entscheidungen getroffen dieses Risiko nicht haben zu wollen.“[68]

Dieser vermuteten Datensparsamkeit widerspricht das Papier einer Arbeitsgruppe zu Kontaktnachverfolgungs-Apps des Trinity College Dublin. Hierin stellen die Autoren fest, dass Google alle 20 Minuten in großem Umfang Daten auf die eigenen Server weiterleitet. Dabei handelt es sich um detaillierte Geräteinformationen, Nutzer:innendaten sowie die IP-Adresse des Smartphones.[69] Allerdings: Diese Daten werden nicht im Rahmen des ENS erhoben, sondern zur „Sicherstellung der Funktionalität des Gerätes“. Dies ist bereits langjährige Praxis, abgesichert durch die Datenschutzerklärung von Google.[70] Es ist also nicht zu unterschätzen, welche Daten die Betriebssystemhersteller abseits des ENS sammeln und speichern.

Neben den grundsätzlichen Einschätzungen zu Privatsphäre und Datenschutz des FIfF zu Kontaktnachverfolgungs-Apps beschreibt eine Forschungsarbeit von Wissenschaftler:innen deutscher Universitäten zur konkreten Implementierung des ENS Probleme des Frameworks. Die Wissenschaftler:innen haben mit Hilfe eines Experiments bewiesen, dass es möglich ist, Bewegungsprofile infizierter Personen anhand aufgezeichneter Bluetoothdaten zu erstellen.[71] In derselben Forschungsarbeit werden Wurmloch-Angriffe beschrieben, welche angewendet werden könnten, um ein höheres Infektionsrisiko für Nutzer:innen der CWA fälschlicherweise zu erzeugen. Die mit der Version 2.0 hinzugekommene Check-In-Funktion eröffnet weitere Schwachstellen, die zur Erstellung von Bewegungsprofilen ausgenutzt werden können. Dies immer dann wenn Daten aufgrund einer positiven Infektion an den Server übertragen werden.[72]

Einen kritischen Standpunkt zur Corona-Warn-App nehmen einige Stimmen aus der Politik ein. Kritikpunkte sind, insbesondere dass die Nutzung der App freiwillig ist sowie die eingeschränkte Funktionalität resultierend aus Beachtung des Datenschutzes. Deshalb wird die Effektivität der CWA hinsichtlich der Eindämmung des epidemiologischen Geschehens angezweifelt.[73] Die Vorsitzende des Ethikrats Alena Buyx hält es für sinnvoll, den Datenschutz zur Pandemie-Bekämpfung einzuschränken und sieht in der Corona-Warn-App noch mehr Potential. In einem Interview mit dem ZDF äußert sie sich kritisch: „Stärkeren Datenschutz in der Umsetzung, das gibt’s kaum und deswegen kann die App auch ganz viel nicht. Und da muss man so langsam wirklich fragen - und

[66] Vgl. Reh20
[67] Vgl. Kut21
[68] Vgl. Kut21
[69] Vgl. Dou20
[70] Vgl. Goo21, Kut21
[71] Vgl. al20
[72] Vgl. Len21
[73] Vgl. Kut21

da bin ich nicht die Einzige - wir schränken so viele Grundrechte ein und den Datenschutz so gar nicht? Bei dem sind wir bis auf Punkt und Komma extrem präzise?“[74]

## 2.2 Die luca-App

Im Frühjahr 2021 wurde die luca-App des privaten Unternehmen Culture4life als neue App zur Kontaktnachverfolgung in öffentlichen Nachrichtensendungen und Medien bekannt gemacht und regelrecht beworben. Politiker:innen und prominente Künstler:innen wie die Fantastischen Vier unterstützen und empfehlen die App. Einige Bundesländer denken sogar über eine Pflicht der App im Rahmen von Lockerungsmaßnahmen nach. Herausgestellt wird dabei jeweils, dass die Dokumentationspflicht der Kontakte in Restaurants und Kulturstätten mit der App erleichtert, die „Zettelwirtschaft“ durch sie obsolet wird.[75] Sogar private Treffen können mit der luca-App erfasst werden.[76]

Die luca-App verfolgt einen zentralen Ansatz. Nutzer:innen registrieren sich in der App mit ihrer Telefonnummer und ihren Kontaktdaten, beim „Check-In“ an einem Ort werden die Daten erfasst. Im Falle einer bestätigten Infektion erfolgt ein Austausch der Daten mit dem zuständigen Gesundheitsamt und eröffnet so den Weg zur kontrollierten Kontaktnachverfolgung. Die App möchte „eine direkte Schnittstelle zu den Gesundheitsämtern sein und diese damit entlasten“.[77] Der luca-Server ist der zentrale Knotenpunkt, an dem alle Daten zusammengeführt werden und der in alle Prozesse von der Verifizierung der Teilnehmer:innen, über die Datenspeicherung bis hin zum Datenaustausch eingebunden ist.[78]

Erste Einschätzungen von Datenschützern:innen stufen die App als Erfolg ein. „luca leistet einen wichtigen Beitrag bei der Nachverfolgung von Kontakten während der Pandemie und erfüllt dabei unseren hohen Datenschutz-Standard“, äußert sich beispielsweise der Datenschutz-Beauftragte des Landes Baden-Württemberg.[79] luca selbst versichert bei der Installation „luca hilft dir bei der sicheren und verschlüsselten Angabe deiner Kontaktdaten. Du musst dir keine Sorgen um deine Daten mehr machen, wenn du Veranstaltungen, Kulturstätten, Restaurants, Cafés oder Bars besuchst.“[80] Durch das Zusammenführen der Informationen bei einem/einer Mitarbeiter:in des Gesundheitsamts versprechen sich die Unterstützer:innen der App eine bessere Clustererkennung und die Eingrenzung der Kontaktnachverfolgung auf bestimmte Bereiche bzw. gezielt ermittelte Personen. Zudem stellt das System verifizierte Kontaktdaten zur Verfügung.[81]

Bald gerät die App allerdings massiv in die Kritik. Der CCC kritisiert die Vergabepraxis, den intransparenten Entwicklungsprozess der App, den zentralisierten Ansatz des Systems als solchen und stellt sogar den grundsätzlichen Nutzen der App in Frage.[82] Andere sind noch deutlicher. Der Datenschützer Christian Köhntopp twittert: „luca-App ist im günstigsten Fall ein digitales Globuli. Im schlimmsten Fall eine unkontrollierte Jauchegrube für personenbezogene Daten und eine Ermutigung, Ansteckungsrisiken einzugehen.“[83]

[74] Vgl. ZDF20
[75] Vgl. dpa21, Fak21
[76] Vgl. Cul21e
[77] Vgl. Sch21c, dpa21
[78] Vgl. Cul21d
[79] Sch21c
[80] Cul21a
[81] Vgl. Cul21e
[82] Vgl. Neu21
[83] Köh21

Bei der Kritik dreht es sich zunächst um konzeptuelle Themen hinsichtlich Datenschutz und Privatsphäre. Bald werden aber auch Sicherheitslücken für aktive Angriffe bekannt, bei denen gezielt Daten abgegriffen werden können.[84] Culture4life reagiert und lässt eigene Penetration Tests auf das System durchführen, um die Sicherheit des Systems zu verbessern und Sicherheitslücken zu schließen.[85] Nach eigener Aussage ist das luca zugrunde liegende Krypto- und Verschlüsselungskonzept gemeinsam mit verschiedenen Unternehmen konzipiert, abgestimmt und entwickelt. Aufgezählt werden dabei Prof. Dr. Marian Margraf von Fraunhofer AISEC, SSE, CORE, neXenio und das Hasso-Plattner-Institut. Die Anbindung an die Gesundheitsämter und der Support erfolgen beim landesweiten Rollout durch die Bundesdruckerei.[86]

### 2.2.1 Grundsätzliche Funktionsweise und Implementierung

Für ein funktionierendes luca-System müssen sich zunächst alle Teilnehmenden während des „onboarding-Prozesses“ in der luca-Umgebung registrieren. Dazu gehören neben den nachzuverfolgenden Personen die jeweils zuständigen Gesundheitsämter und die Veranstaltungsorte selbst.

Für den überwiegenden Teil der kryptografischen Operationen im luca-System wird asymmetrische Verschlüsselung verwendet. Die Gesundheitsämter erhalten nach ihrer Registrierung offline ein Zertifikat sowie ein Schlüsselpaar zum Signieren und ein weiteres Schlüsselpaar („Health Department Encryption Keypair“) zum Verschlüsseln von Geheimnissen. Der öffentliche Schlüssel dieses Paares wird signiert auf den luca-Servern bereitgestellt, der private Schlüssel lokal im Gesundheitsamt gespeichert.

Ein Veranstaltungsort erhält nach seiner Anmeldung ein Schlüsselpaar, welches lokal im System des Veranstaltungsorts gespeichert wird. Bei seiner Registrierung gibt der Veranstaltungsort seine Geo-Koordinaten bekannt sowie einen „Check-In-Radius“ und weitere Daten zum Veranstaltungsort.[87]

Bei der Registrierung einer Person wird eine User-ID und ein Schlüsselpaar erzeugt. Die auf dem Smartphone zur Registrierung eingegebenen Daten der Nutzer:innen werden damit verschlüsselt und in der App sowie auf dem luca-Server hinterlegt.[88] Die Telefonnummer wird einmalig, zur Verifizierung per SMS, unverschlüsselt genutzt. Nutzer:innen werden aufgefordert, die hinterlegten Informationen richtig und aktuell zu halten. Die Eigentumsrechte der zur Verfügung gestellten Daten und der infolge der Nutzung entstehenden Daten verbleiben bei der Person, welche die App nutzt. Es wird luca nur ein Nutzungsrecht gewährt. Dies beinhaltet allerdings in „erforderlichem Maß auch über die Beendigung dieses Nutzungsvertrags hinaus, die Inhalte und Nutzerdaten in dem für die Erbringung der Dienste notwendigem Maße zu nutzen“.[89]

Vor der Eingabe der Daten wird durch die App versichert „Deine Daten werden verschlüsselt. Nur Gesundheitsämter können Sie im Rahmen einer Kontaktnachverfolgung wieder entschlüsseln.“[90] Die verschlüsselten Daten können laut luca nur vom zuständigen Gesundheitsamt gelesen werden „um Infektionsketten zurückzuverfolgen. Veranstalter oder andere Personen können diese Daten niemals entschlüsseln, lesen, oder etwas anderes damit anfangen.“[91] Auch der App-Anbieter hat keinen Zugriff darauf.

[84] Vgl. Neu21, al21b, Köv21a, Reu21
[85] Vgl. Cul21e
[86] Vgl. Cul21e
[87] Vgl. Cul21d
[88] Vgl. Cul21d
[89] Vgl. Cul21c
[90] Cul21a
[91] Fak21

Zur Entschlüsselung freigegeben werden die Daten erst durch das bewusste Teilen der Nutzer:in mit den Gesundheitsämtern.[92]

Die verschlüsselten personenbezogenen Daten verbleiben bis zum Einchecken auf dem Smartphone des/der Nutzer:in bzw. im Speicher der App.[93] Aus den Daten wird ein sich minütlich ändernder QR-Code erstellt. Mit diesem ist das Einchecken in Lokalen, Veranstaltungsstätten oder Geschäften etc. möglich. Dazu wird entweder vor Ort der generierte QR-Code eingescannt oder aber die Betreiber:innen stellen selbst einen QR-Code ihres Orts zur Verfügung, den die Nutzer:innen einscannen, um ihre Anwesenheit zu speichern. Für Personen die kein Smartphone besitzen, stellt das Unternehmen einen Schlüsselanhänger mit einem QR-Code bereit, der zum Check-In an einem Veranstaltungsort genutzt werden kann.[94] Der offensichtliche Nachteil ist hier, dass dieser QR-Code einmalig vergeben wird und daher statisch ist.

Beim Einchecken mit der luca-App wird das Nutzer:innengeheimnis zunächst mit einem täglich wechselnden öffentlichen Schlüssel des zuständigen Gesundheitsamts verschlüsselt. Der private Schlüssel des „Daily Keypair“ wird asymmetrisch mit dem öffentlichen „Health Department Encryption Key“ verschlüsselt. Damit wird sichergestellt, dass nur das zuständige Gesundheitsamt die Daten auch wieder entschlüsseln kann.[95] In einem zweiten Schritt werden die Check-In-Daten mit dem öffentlichen Schlüssel des Veranstaltungsorts ein weiteres Mal verschlüsselt, der zugehörige private Schlüssel wird lokal gespeichert.[96] Die sichere Verwahrung dieses Schlüssels und der gesammelten Daten liegen in der Verantwortung des/der Veranstalter:in.[97] Durch die Verschlüsselung werden die vorliegenden Daten dort geheim gehalten – ein Vorteil gegenüber Einträgen auf Papier. Die verschlüsselten Daten können nur auf Anfrage des zuständigen Gesundheitsamts über das luca-System freigegeben werden.[98]

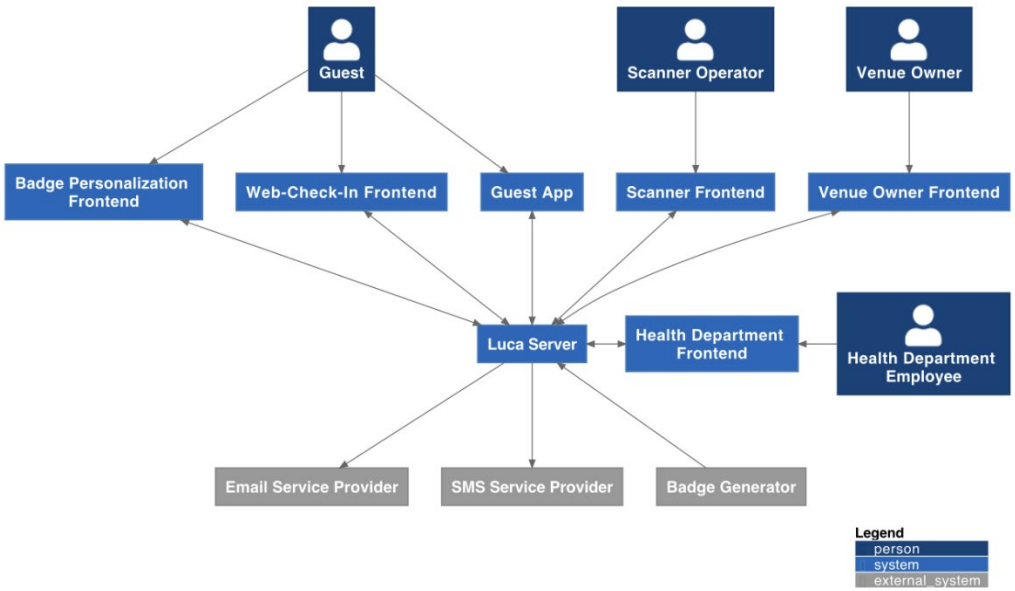


**Abbildung 2: Zusammenspiel von Komponenten und Akteuren**

[92] Vgl. Sch21c
[93] Vgl. Cul21b
[94] Vgl. Cul21e
[95] Vgl. Cul21d
[96] Vgl. Cul21d
[97] Vgl. Cul21b
[98] Vgl. Cul21d

Allerdings wird bei jedem Check-In oder Check-Out an einem Veranstaltungsort in einer direkten Verbindung zum luca-Server die aktuelle Trace-ID bereitgestellt. Dabei werden die aktuelle IP-Adresse und möglicherweise weitere Informationen, wie z.B. der Typ des Endgeräts oder die verwendete luca-App-Version, übermittelt. Wie bei der CWA muss dem/der Betreiber:in des Systems vertraut werden, dass diese Daten nicht gesammelt und/oder anderweitig verwendet werden.

Im Fall einer Infektion teilt die Person ihre Check-In-Historie mit dem zuständigen Gesundheitsamt. Die Historie wird im Gesundheitsamt geprüft und Veranstaltungen aus dem epidemiologisch relevantem Zeitraum[99] werden rekonstruiert.[100] Über den luca-Server wird nun angefragt, ob bei der Kontaktnachverfolgung unterstützt werden darf. Wenn der/die Veranstalter:in hier zustimmt, werden mit Hilfe der lokal gespeicherten Schlüssel die angefragten Daten entschlüsselt und an die zuständige Stelle im Gesundheitsamt übermittelt. Diese kann mit den privaten Schlüsseln ihrer Institution die Datenreferenzen entschlüsseln. Mit einem weiteren Zugriff auf den luca-Server können die zugehörigen Schlüssel zu den konkreten Kontaktdaten der potenziellen Kontakte entschlüsselt werden.[101]

Zur Gewährleistung, dass nur die epidemiologisch relevanten Kontaktereignisse entschlüsselt werden können, werden private Schlüssel, die älter sind als vier Wochen, automatisiert vom luca-Server gelöscht.[102]

### 2.2.2 Sicherheitsbetrachtung und Kritik

Kurz nachdem luca veröffentlicht wurde und die IT-Community und Datenschützer:innen anfingen, sich mit der App zu beschäftigen, wurden eine Vielzahl an unterschiedlichen Sicherheitslücken bekannt. Der Schlüsselanhänger mit dem statischen QR-Code geriet sofort in den Fokus, denn mit ihm lassen sich von Unbefugten, die in Besitz einer Kopie des QR-Codes (z.B. eines Foto des Anhängers) sind, Bewegungsprofile von Nutzer:innen erstellen.[103] Anhand dieser Metadaten, also der Informationen, wer zu welchem Zeitpunkt wo war, kann die Identität einer Person rekonstruiert werden, da die luca-App mittlerweile sehr weitreichend eingesetzt wird. So ist in einigen Bundesländern die luca-App nicht nur für das Einkaufen oder den Museumsbesuch notwendig, sondern auch der Besuch von Kirchen, Moscheen, Schulen, Selbsthilfegruppen etc. und privaten Veranstaltungen soll per luca-App dokumentiert werden.[104]

Grundsätzlich kann die luca-App einfach missbraucht werden. Der Moderator Jan Böhmermann verbreitete im April Fotos des QR-Codes des Osnabrücker Zoos und eines Modehauses in Bohmte (Landkreis Osnabrück) via Twitter. Anschließend checkten sich Menschen von überall her an diesen beiden Orten ein, so dass laut luca mehr als 43.000 Menschen in dem Modehaus waren, mehr als 100 besuchten nachts den Osnabrücker Zoo.[105]

In einer Studienarbeit der Universität EPFL in Lausanne werden weitergehende Konsequenzen dieser Sicherheitslücke abseits des satirischen Spaßes beleuchtet. Beispielsweise könnte ein:e Angreifer:in sich gezielt bei einem Event einloggen und anschließend eine positive Corona-Infektion melden. Um dem Event die nötige Relevanz zu verleihen, könnte durch vielfache Check-Ins (beispielsweise durch das Mitwirken

[99] i.d.R. wie gehabt 14 Tage
[100] Vgl. Cul21d
[101] Vgl. Cul21d, Cul21b
[102] Vgl. Cul21d
[103] Vgl. Köv21b
[104] Vgl. Mec21
[105] Vgl. cul21f, NDR21

einer Community wie oben beschrieben) die Teilnehmer:innenzahl künstlich in die Höhe getrieben werden. Dies könnte zu Stigmatisierung und Benachteiligungen bestimmter Personengruppen führen. Gleiches gilt für bestimmte Veranstaltungsorte: Eine Bar, bei der immer wieder positive Infektionen gemeldet werden, würde in Folge der Konsequenzen vermutlich den wirtschaftlichen Ruin erleiden.[106]

Des Weiteren werden in der Arbeit folgende Sicherheitsprobleme genannt: „Das System ist im Kern ein vertrauensbasiertes System“, sagt Carmela Troncoso, eine der Autor:innen. Alle Sicherheitseigenschaften hängen davon ab, dass der zentrale Server von luca, auf dem wie auf einer Drehscheibe große Mengen an sensiblen Daten zusammenlaufen, und diejenigen, die darauf Zugriff haben sich korrekt verhalten.[107] In der Vergangenheit hatte es bereits Zugriffe der Polizei auf die analogen Kontaktnachverfolgungslisten gegeben, um Straftaten aufzuklären.[108] luca liefert eine weit umfassendere digitale Datenbasis.

Mit Hilfe der Metadaten (wie möglicherweise die IP-Adresse) die vom luca-Server ggf. über App-Nutzer:innen gesammelt werden könnten, lassen sich theoretisch - wie bereits in 2.1.3 dargestellt - Bewegungsprofile erstellen. Ebenso werden auf dem zentralen System Informationen über Veranstaltungsorte gesammelt. Diese umfassen sensible Daten wie den Ort und die Zeit der Veranstaltung, die Anzahl Personen die teilgenommen hat, sowie Kontaktdaten des/der Veranstalter:in. Hieraus lassen sich indirekt zahlreiche Informationen ableiten über die Art und Hintergründe der Zusammenkunft. Schließlich kann auch hier eine Stigmatisierung von Einzelpersonen befürchtet werden, da die Daten über positive Infektionen über den zentralen Server bekanntgegeben werden.[109]

Im Mai 2021 wurde von Sicherheitsforscher Marcus Mengs eine weitere Sicherheitslücke gefunden. Ein Angriff war möglich, bei dem die Infrastruktur der luca-App über eine Code Injection nicht nur zum Auslesen von persönlichen Daten anderer Nutzer:innen genutzt werden kann, sondern es bestand sogar die Möglichkeit, Schadcode auf einem Rechner des Gesundheitsamts zu hinterlegen. Welche Reichweite ein solcher Angriff haben kann, beispielsweise durch das Einschleusen von Ransomware, ist offensichtlich.[110]

Da Vertrauen in den/die Betreiber:in insbesondere beim zentralen Systemansatz der wesentliche Faktor ist, ist der Umgang des Unternehmens hinter der luca-App mit der angebrachten Kritik bemerkenswert. Einige der eklatanten Sicherheitsprobleme werden abgestritten oder klein geredet[111], andere zunächst ignoriert, bis sie schließlich ansatzweise gefixt werden. In Bezug auf die von Sicherheitsforscher Mengs gefundene Sicherheitslücke beispielsweise sehen die Verantwortlichen von Culture4Life die Probleme auf der Seite von Microsoft Excel und den Mitarbeitern der Gesundheitsämter.[112]

Unabhängig davon ob dem Unternehmen selbst eine unlautere Strategie unterstellt wird oder ob die Sicherheit des Systems an sich in Frage gestellt werden muss: das Verhalten von Culture4Life ist nicht vertrauensfördernd.[113]

[106] Vgl. al21b
[107] Vgl. Köv21a
[108] Vgl. Lau21
[109] Vgl. al21b
[110] Vgl. Tod21
[111] Vgl. cul21f, cul21g
[112] Vgl. Köv21a, Reu21, Lau21
[113] Vgl. Reu21

## 2.3 Die CWA und die luca-App im Vergleich

Ab der Version 2.0 enthält die Corona-Warn-App alle Instrumente zur Pandemiebekämpfung, die auch die luca-App bereitstellt. Zusätzlich erfasst sie direkte Kontakte im privaten Bereich bzw. an Orten ohne Check-In, wie private Feiern oder Arbeitsplatz. Dabei ist sie datensparsam und punktet hinsichtlich des Datenschutzes durch ihre dezentrale Architektur.

Die unabhängige Datenschutzaufsichtsbehörde des Bundes und der Länder empfiehlt in einer öffentlichen Entschließung ihrer Konferenz vom 29. April 2021 den Bundesländern, die Corona-Warn-App „jedenfalls als ergänzende Möglichkeit zur Benachrichtigung potenziell infizierter Personen und zur Clustererkennung in ihren Konzepten zur Pandemiebekämpfung zu berücksichtigen“. Mit den in Version 2.0 eröffneten „datensparsameren Möglichkeiten der pseudonymisierten Clustererkennung und Kontaktbenachrichtigung“ könne die CWA Grundrechtseingriffe im Bereich des Datenschutzes minimieren. Durch die Vernetzung über die App seien Personen zudem unmittelbarer und dadurch schneller als über die Gesundheitsämter erreichbar.[114]

In einer gemeinsamen Stellungnahme von 70 führenden deutschen IT-Sicherheitsforscher:innen wird die luca-App deutlich kritisiert. Die vier definierten Kriterien, Zweckbindung[115], Offenheit und Transparenz[116], Freiwilligkeit[117] und Risikoabwägung[118] würden von der Corona-Warn-App größtenteils vorbildlich umgesetzt, die luca-App erfülle hingegen keine dieser Kriterien.[119] Trotz der anhaltenden Kritik setzen Bund und Länder wieter auf die luca-App. 318 von insgesamt 400 Gesundheitsämtern in Deutschland sind mittlerweile im luca-System registriert, 315 davon haben die App im vergangenen Monat zur Kontaktnachverfolgung verwendet[120]. Es ist offensichtlich: Der Ansatz der CWA kann auch als Nachteil und der zentrale Architekturansatz der luca-App als ihr Vorteil angesehen werden. Der dezentrale datensparsame Ansatz ist gleichzeitig ein liberaler Ansatz und setzt auf verantwortliches Handeln der Menschen gegenüber sich selbst und der Gesellschaft. Die zentrale Zusammenführung der Daten sowie die Einbindung der Gesundheitsämter in die Kontrollmechanismen im Pandemiegeschehen sind davon nicht abhängig.

Durch die zentrale Autorität können Maßnahmen angeordnet und ihre Einhaltung geprüft werden. Weltweit gibt es eine Vielzahl von Kontaktnachverfolgungs-Apps mit zentraler

[114] Vgl. Kon21
[115] „Das einzige Ziel muss die Pandemiebekämpfung sein. Eine Verknüpfung mit anderen Geschäftsmodellen, Anwendungsmöglichkeiten und Profitinteressen muss ausgeschlossen, idealerweise technisch unmöglich sein.“ (al21a)
[116] „Fachleuten, IT-Sicherheits- und Datenschutzexpert:innen muss frühzeitig die Möglichkeit gegeben werden, sich konstruktiv am Entwicklungsprozess zu beteiligen oder diesen unabhängig zu begutachten.“ (al21a)
[117] „Die Nutzung bestimmter Werkzeuge zur digitalen Kontaktverfolgung muss freiwillig sein. Bürger:innen, die das Werkzeug nicht benutzen möchten, dürfen nicht von sozialen Aktivitäten, dem Zutritt zu öffentlichen Gebäuden, Geschäften usw. ausgeschlossen werden.“ (al21a)
[118] „Die Beurteilung des Nutzens und der Risiken einer solchen Lösung muss im Vorfeld unabhängig und öffentlich geprüft werden können. Dies gilt ganz besonders dann, wenn der Effekt der technischen Lösung in wesentlichem Umfang auf dem Vertrauen der Bürger:innen basiert.“ (al21a)
[119] Vgl. al21a
[120] Daten abgerufen am 14. Juli 2021 auf https://luca.denken.io/. Die Website ist vom IT-Experten Ralf Rottmann, der Luca vehement kritisiert, ins Leben gerufen worden. Er stellt auf dieser Webseite Daten dar, die er über eine öffentliche Schnittstelle des Systems abruft.

Architektur, welche weit umfassendere Daten sammeln und weit mehr Kontrollmechanismen implementieren als die hier behandelte luca-App.[121]

## 2.4 Wirksamkeit von Kontaktnachverfolgungs-Apps

Die Wirksamkeit von Kontaktnachverfolgungs-Apps ist bis heute, rund ein Jahr nach der Einführung verschiedenster technischer Lösungen, umstritten.

In den vorangegangenen Kapiteln wurde aufgezeigt, wie eine Kontaktnachverfolgung technisch sauber und datenschutzkonform aussehen könnte. Es wurde insbesondere betrachtet, wie die Privatsphäre der Menschen ausreichend geschützt wird und welche Probleme entstehen, wenn dies nicht der Fall ist. Dabei wurde in der Regel vorausgesetzt, dass die Benutzer:innen der App sich ideal verhalten. Leider ist dies in der realen Welt oft nicht der Fall. Personen handeln aus verschiedenen Gründen nicht wie erwartet, was Einfluss haben kann auf die Wirksamkeit der Apps bis hin zu den Extremen: Nichtnutzung der App oder ein trügerisches Sicherheitsgefühl und daraus resultierendes Handeln. Weiterhin kann aufgrund von vernachlässigten technischen Mängeln ein Schaden für Personen und die Gesellschaft entstehen, der nicht gerechtfertigt oder schädlich ist. Z.B. hat, wie in Kapitel 1.1.3 dargestellt, die Entfernungsmessung durch BLE Schwächen in der praktischen Anwendung.

Die Wirksamkeit der Corona-Warn-App und anderer dezentral aufgebauter Kontaktnachverfolgungs-Apps ist allein durch die Architektur dieser Apps schwer zu belegen. Da die Daten auf den Geräten verbleiben und auch die Funktionalität dort ausgeführt wird, ist schwer nachzuvollziehen, wie viele Personen bisher gewarnt wurden und wie viele der Gewarnten tatsächlich infiziert waren.[122]

Durch eine freiwillige Datenfreigabe von Benutzer:innen und eine Onlinebefragung erstellte das RKI eine Datenbasis, um die Wirkung der CWA zu schätzen: Laut dieser Hochrechnung wurden bis Juni 2021 ca. 230.000 Personen, die tatsächlich anschließend positiv getestet wurden, über die CWA gewarnt.[123]

Diese Zahlen können allerdings so nicht von den Gesundheitsämtern bestätigt werden. Grundsätzlich meldet die CWA nicht von sich aus Daten an die Gesundheitsämter. Bei einer Warnung über die App ist der/die Nutzer:in berechtigt, einen PCR-Test beim zuständigen Gesundheitsamt machen zu lassen. Im Fall eines positiven Tests meldet das Gesundheitsamt die Daten an das RKI, die Angabe darüber wie der Fall bekannt geworden ist, ist aber nur optional. Bei den meisten gemeldeten Fällen, in denen überhaupt eine Angabe gemacht wurde, wurden nicht die CWA sondern Reihenuntersuchungen und Tests als Auslöser genannt.[124]

Einige Daten können sicher genannt werden: Im Zeitraum vom 01. September 2020 bis 23. Juni 2021 wurden insgesamt 773.462 potenziell teilbare positive Testergebnisse erfasst. Davon haben sich 61% der Nutzer:innen der CWA dazu entschieden, ihr positives Testergebnis über die App mit möglichen Kontakten zu teilen. Warum fast 40% der Nutzer ihr Testergebniss verifizieren, dieses dann aber nicht in der Gemeinschaft der App-Nutzer:innen teilen, ist unklar.[125]

[121] Vgl. Reh20, S. 15ff.
[122] Vgl. Ant21
[123] Vgl. Köv21c
[124] Vgl. Köv21c
[125] Vgl. RKI21e

Ein aktuelles Beispiel lässt allerdings hoffen, dass die Wirksamkeit der dezentral organisierten Apps trotzdem gegeben sein könnte. In England wurde in den letzten Wochen 1,5 Millionen Menschen über die dort genutzte App[126] nahegelegt, sich sofort zu isolieren. Dies geschah anonym und ohne Umwege über die Gesundheitsämter. Auch wenn einzelne Parameter in der Risikobewertung dieser App nun nachgebessert werden sollen, ist es nicht unwahrscheinlich, dass die Infektionszahlen trotz der Delta-Variante durch den Einfluss der App weiter sinken werden.[127]

Für die luca-App bzw. sonstige zentral organisierte Apps müssen andere Aspekte hinsichtlich ihrer Wirksamkeit betrachtet werden. Argument für die umfassendere Datenerhebung und deren zentrale Speicherung ist die Möglichkeit der zentral organisierten und daher vermutlich wirksameren Kontaktnachverfolgung. Doch auch hier steht die luca-App in der Kritik.

Die tatsächliche Kontaktnachverfolgung in den Gesundheitsämtern erfolgt häufig per Hand, ist recht aufwändig und wird daher nur nach vorheriger Analyse und ausreichender Relevanz des Clusters durchgeführt.[128] Brisanz erhält dieser Punkt, wenn die Infektionszahlen steigen und dieses Szenario häufiger auftritt. Nach Aussage von Mitarbeiter:innen des Gesundheitsamts Berlin liefert luca eine Masse an Daten in unaufbereiteter Form und ohne sinnvolle Filtermöglichkeiten, so dass oftmals kein Nutzen aus den gesammelten Informationen gezogen werden kann.[129] Eine technische Unterstützung könnte die in den Gesundheitsämtern verwendete Software Sormas (Surveillance Outbreak Response Management and Analysis System) sein. Allerdings bietet diese keine Schnittstelle zum Import der luca-Daten, der Hersteller von Sormas meldete hier Sicherheitsbedenken. Zusammenfassend lässt sich feststellen: Es wurden und werden täglich etliche Daten gesammelt, welche nun ihrem Zweck nicht dienlich sein können.

Es ist offensichtlich, dass die gefragte Schnelligkeit, Qualität und Wirksamkeit unter diesen Umständen maßgeblich leiden dürften. Es ist sogar nicht unwahrscheinlich, dass deshalb wichtiges Personal gebunden wird, ohne einen sinnvollen Effekt auf die Pandemie zu bewirken. Somit könnte die luca-App sogar eher schaden als nützen.

# 3 Ausblick

## 3.1 Entwicklungsperspektiven bestehender Lösungen

Beide Lösungsansätze und konkrete Implementierungen in Deutschland, die CWA und die luca-App, bieten Vor- und Nachteile. Es ist fraglich, welche Lösung den größeren Effekt in der Pandemiebekämpfung haben kann.

Einige Mängel der luca-App ließen sich mit einer besseren Umsetzung beheben und auch eine vertrauensvollere Umgebung ließe sich für die Systemarchitektur schaffen. Es wirkt so, als habe Culture4life einen geringen Fokus in die konzeptuelle Ausarbeitung der App gesteckt. Offensichtlich setzt man darauf, die App im Live-Betrieb zu entwickeln.

[126] Die App wurde bisher über 27 Millionen Mal heruntergeladen. Siehe https://stats.app.covid19.nhs.uk/#app-downloads.
[127] Vgl. Sch21b
[128] Vgl. Bun21b
[129] Vgl. Bei21, Sch21b

Voraussetzung für die Wirksamkeit der CWA ist, dass möglichst viele Menschen die App installieren und nutzen. Um die Nutzerzahl zu vergrößern, sollte das Vertrauen in die App und in ihre Wirksamkeit gestärkt werden. Die verantwortliche Handhabung der App durch die Nutzer:innen bleibt ein Risiko für die Wirksamkeit.

Die Dringlichkeit der Pandemiebekämpfung zwingt die Gesellschaft dazu, die beste Lösung für manche Szenarien über die Zeit zu ermitteln. Wichtig ist dabei, in der Retrospektive Fehler zu erkennen und Irrwege zu beenden, sollten sie sich als solche herausstellen.

## 3.2 Digitalisierung und digitaler Impfnachweis

Die Corona-Pandemie und die zu ihrer Bekämpfung ergriffenen Maßnahmen haben in allen Lebensbereichen für einen Digitalisierungsschub gesorgt. Viele Schulen stellten ihren Unterricht im Lockdown auf digitale Plattformen um und behalten diese auch weiterhin bei. Kurse für verschiedenste Hobbys fanden zuhause via Online-Schulung statt und sogar Arztgespräche oder Therapiesitzungen wurden auf Entfernung digital durchgeführt.

Es ist offensichtlich, dass Datenschutz, Datensicherheit und Privatsphäre im Zuge dieser Entwicklungen zu immer größerer Relevanz gelangen. Häufig genug ist es jedoch der Fall, dass Lösungen schnell und pragmatisch gefunden werden und erst im Nachhinein über die Themen Datenschutz und Sicherheit diskutiert und diesbezüglich nachgebessert wird. Der Ansatz der CWA diese Aspekte von Anfang an mitbedacht zu haben, ist daher vorbildlich.

In den Gesundheitsämtern wurden viele der bisher papierbasierten Prozesse im Verlauf des letzten Jahres auf digitale Lösungen umgestellt. Die Zusammenarbeit zwischen den Städten und Ländern wird dadurch vereinfacht. Auch innerhalb Europas finden Projekte zusammen: Etliche der dezentral organisierten europäischen Corona-Warn-Apps sind mittlerweile miteinander kompatibel und vernetzt.[130]

Das prominenteste Beispiel für Digitalisierung ist der im Rahmen der Impfkampagnen im Juni 2021 eingeführte, europaweit gültige digitale Impfnachweis. Dieser wird in allen EU-Mitgliedstaaten und einigen weiteren Ländern anerkannt. Er ist durch einen QR-Code mit elektronischer Signatur identifizierbar, für die valide und EU-weite Prüfung wird allerdings eine App benötigt. Als Institutionen des Vertrauens können Krankenhäuser, Testzentren oder Gesundheitsbehörden mit eigenen digitalen Signaturschlüsseln die Zertifikate ausstellen und signieren. Sämtliche Schlüssel sind EU-weit in einer sicheren Datenbank gespeichert.

Das digitale Zertifikat enthält wichtige Informationen wie Name der/des Geimpften, Geburts- und Ausstellungsdatum sowie Angaben zum Impfstoff und ein individuelles Erkennungsmerkmal. Wenn ein Zertifikat überprüft wird, dürfen diese Daten nicht gespeichert oder einbehalten werden. Zu Authentifizierungszwecken wird nur die Gültigkeit des Zertifikats kontrolliert, indem überprüft wird, wer es ausgestellt und unterzeichnet hat.[131]

Auch im Falle des digitalen Impfnachweises konnten Sicherheitslücken und niedrige Hürden für Missbrauch identifiziert werden. So wurde beispielsweise die Signatur des QR-Codes während des Einlesens des Zertifikats in die CWA nicht geprüft. Der G DATA CyberDefense AG war es möglich, einen gefälschten Impfnachweis mit ausgedachter

[130] Vgl. Kom21a
[131] Vgl. Kom21b

Signatur aus dem Jahr 1890 erfolgreich in der App zu hinterlegen. Diese Lücke weist die alternative App CovPass nicht auf, dennoch wird der Impfnachweis im Alltag oft genug durch eine einfache Sichtprüfung validiert. Gefälschte Webseiten oder Dokumente, die das Aussehen auf dem Handy simulieren, sind schnell und einfach nachgebaut.

Analog zu den Kontaktnachverfolgungs-Apps veröffentlichte der CCC für das Konzept der digitalen Impfausweise gesellschaftliche und technische Mindestanforderungen, stellt aber gleichzeitig in Frage, ob das Projekt an sich überhaupt sinnvoll ist. Freiwilligkeit und Zweckgebundenheit der Daten werden als wesentlich genannt. Als ebenso wichtig wird herausgestellt, das Erstellen von Bewegungsprofilen zu verhindern, z.B. beim Abgreifen von Daten zum Zeitpunkt der Validierung.[132]

[132] Vgl. erd21

# 4 Fazit

Kontaktnachverfolgungs-Apps können ein wirksames Instrument zu Bekämpfung der Pandemie sein, gleichzeitig steht ihr möglicher Missbrauch immer im Raum. Insbesondere bei zentral organisierten Implementationen ist das integre Handeln des/der Betreiber:in wesentliche Voraussetzung. Zweckgebundenheit der technischen Hilfsmittel und eine Tradition diese, wenn ihre Einsatzgrundlage nicht mehr besteht, wieder zu entfernen, sollten durch regelmäßige Evaluierungszyklen im politischen Geschehen fest implementiert werden. Der Einschätzung des CCC, dass technische Lösungen per Design einem Missbrauch vorbeugen sollten, ist beizupflichten.

Zusammenfassend wird deutlich, dass die Konzepte hinsichtlich Datenschutz und Privatsphäre für Kontaktnachverfolgungs-Apps bereits vom Ansatz her grundverschieden sein können. In der Pandemiebekämpfung wird unterschiedlich eingeschätzt, wie schützenswert diese Werte sind. Besonders überrascht hat mich in meiner Ausarbeitung die Einschätzung der Vorsitzenden des Ethikrats, die nicht etwa dafür eintritt, Grundwerte der Gesellschaft in der Pandemie zu schützen, sondern im Gegenteil darauf drängt, diese auch im Rahmen der Kontaktnachverfolgung über Bord zu werfen.

Ein weiterer nicht zu vernachlässigender Aspekt ist aus meiner Sicht, dass die flächendeckende Einführung der luca-App und ihre dadurch resultierende Popularität, am Ende auch Einfluss auf die Wirksamkeit der Corona-Warn-App haben wird. Menschen die die luca-App verwenden (müssen), laden womöglich keine zweite App auf ihr Mobilgerät. Entweder in dem Glauben, die bessere Wahl getroffen zu haben oder um keine weiteren Kontaktnachverfolgungs-Apps auf ihrem Gerät zu haben. Ihre volle Effektivität entfalten zu können, indem möglichst viele Menschen die App verwenden, wird der CWA damit paradoxerweise aus der Politik heraus besonders schwer gemacht. Also von denjenigen, die ihre größten Unterstützer sein müssten.

Schließlich wird deutlich, dass technologische Lösungen zum Teil überschätzt werden. Eine Applikation oder ein System muss konzeptuell sorgfältig ausgearbeitet sein und auch hinsichtlich der zu erreichenden Ziele wohlüberlegt, damit das Gesamtsystem dagegen geprüft werden und entsprechend der Erwartung funktionieren kann. Zwei Beispiele, in denen dies teilweise nicht der Fall ist, wurden in dieser Arbeit genannt: Erstens die überschätze Funktionalität von BLE, welche die Erwartungen vermutlich per Design nicht zuverlässig erfüllen kann. Zweitens die große Masse gesammelter Daten des luca-Systems, welche nun als sinnlose „Datenwurst“[133] ihrem Zweck nicht dienlich ist. Insofern stellt sich die Frage, ob die Eingriffe in die Privatsphäre der Menschen im Rahmen der Kontaktnachverfolgung überhaupt gerechtfertigt sind, wenn sie ihren Zweck nicht erfüllen.

[133] Bei21

# Eidesstattliche Erklärung

Ich versichere an Eides statt, dass ich die vorliegende Arbeit selbstständig angefertigt habe. Ich habe mich keiner fremden Hilfe bedient und keine anderen, als die angegebenen Quellen und Hilfsmittel benutzt. Alle Stellen, die wörtlich oder sinngemäß veröffentlichten oder nicht veröffentlichten Schriften und anderen Quellen entnommen sind, habe ich als solche kenntlich gemacht. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

| Ort, Datum | Vorname Name / Matrikelnummer |
|---|---|
| Gevelsberg, 29.8.2021 | Henschen-Bolte, Meike / 108119200602 |

# Literaturverzeichnis

**[al20] Baumgärtner et al.** *Mind the GAP: Security & Privacy Risks ofContact Tracing Apps.* Forschungsarbeit. Technische Universität Darmstadt et al, 6. Nov. 2020. url: https: //arxiv.org/pdf/2006.05914.pdf.

**[al21a] Prof. Dr. Florian Alt et al.** *Gemeinsame Stellungnahme zur digitalen Kontaktnachverfolgung*. 15. Juni 2021. url: https://digikoletter.github.io/.

**[al21b] Stadler et al.** *Preliminary Analysis of Potential Harms in the Luca Tracing System.* Radboud University, 23. März 2021. url: https://arxiv.org/pdf/2103.11958. pdf.

**[Ant21] Katerini Tagmatarchi Storeng, Antoine de Bengy Puyvallée**. *The Big Digital Contact Tracing Experiment*. 19. Juni 2021. url: https://onlinelibrary.wiley.com/doi/full/10.1111/1758-5899.12964.

**[Bei21] Sabine Beikler.** *Krisentreffen wegen Luca-App in Berlin.* 16. Aug. 2021. url: https://www.tagesspiegel.de/berlin/problem-bei-der-kontaktnachverfolgung-krisentreffen-wegen-luca-app-in-berlin/27519876.html.

**[Bid20] Sam Biddle.** *The inventors of Bluetooth say there could be problems using their tech for Coronavirus contact tracing.* 5. Mai 2020. url: https://theintercept.com/2020/05/05/coronavirus-bluetooth-contact-tracing/.

**[Böh20] Prof. Dr. Rainer Böhme.** *Skript Modul IT-Sicherheitsmanagement im Fernstudiengang Applied IT-Security msc.* Feb. 2020.

**[Bun21a] Deutsche Bundesregierung.** *Eventregistrierung in der Corona-Warn-App.* 13. Mai 2021. url: https://www.bundesregierung.de/breg-de/themen/coronavirus/corona-warn-app-version-2-0-1889868.

**[Bun21b] Deutscher Bundestag.** *Ausschuss Digitale Agenda/Anhörung*. 6. Mai 2021. url: https://www. bundestag.de/ada#url=L3ByZXNzZS9oaWlvODM5OTc0LTgzOTk3NA==&mod=mod540578.

**[Chr20] NDR Christian Drosten.** *Auch die Atemluft spielt eine Rolle.* 6. Apr. 2020. url: https://www.ndr.de/nachrichten/info/28-Auch-die-Atemluft-spielt-eine-Rolle,audio664160.html.

**[Cul21a] Culture4Life GmbH.** *luca App: Begrüßungstext bei der Installation.* 6. Juli 2021.

**[Cul21b] Culture4Life GmbH.** *luca App: Datenschutzerklärung.* 6. Juli 2021.

**[Cul21c] Culture4Life GmbH.** *luca App: Nutzungsbedingungen.* 6. Juli 2021.

**[Cul21d] Culture4Life GmbH.** *luca App: Secrets and Identifiers.* 6. Juli 2021. url: https://luca-app.de/securityoverview/.

**[Cul21e] culture4life GmbH**. *luca App.* Juni 2021. url: https://www.luca-app.de/.

**[cul21f] Culture4Life GmbH.** *Nachts im Zoo von Osnabrück und danach im Modehaus in Bohmte.* 7. Apr. 2021. url: https://www.luca-app.de/nachts-im-zoo-von-osnabruck-und-danach-im-modehaus-in-bohmte/.

**[cul21g] Culture4Life GmbH.** *Stellungnahme: Hinweis auf einen potentiellen Missbrauch des luca Systems im Zusammenhang Microsoft Excel Code Injection.* 26. Mai 2021. url: https://cdn.netzpolitik.org/wp-upload/2021/05/200526-PM-Luca-Injection.pdf.

**[Dom20] ZDF Dominik Rzepka.** *Chaos Computer Club lobt deutsche Corona-App.* 17. Juni 2020. url: https://www.zdf.de/nachrichten/politik/corona- app- launch- 100. html.

**[Dou20] Stephen Farrell, Douglas J. Leith.** *Contact Tracing App Privacy: What Data Is Shared By Europe's GAEN Contact Tracing Apps.* 18. Juli 2020. url: https://www.scss. tcd.ie/Doug.Leith/pubs/contact_tracing_app_traffic.pdf.

**[dpa20a] dpa.** *Apple und Google veröffentlichen Schnittstellen für Corona-Warn-Apps.* 21. Mai 2020. url: https://www.heise.de/news/Apple-und-Google-veroeffentlichen-Schnittstellen-fuer-Corona-Warn-Apps-4726167.html.

**[dpa20b] © dpa/aerzteblatt.de.** *Drosten: Explosive Übertragungsereignisse sind Treiber der Epidemie.* 27. Mai 2020. url: https://www.aerzteblatt.de/nachrichten/113249/ Drosten-Explosive-Uebertragungsereignisse-sind-Treiber-der-Epidemie.

**[dpa21] Friedhelm Greis/ dpa.** *Laschet empfiehlt App für digitale Gästelisten.* 23. Feb. 2021. url: https://www.golem.de/news/kontaktnachverfolgung- laschet- empfiehlt-app-fuer-digitale-gaestelisten-2102-154443.html.

**[erd21] erdgeist.** *Impfausweise beenden keine Pandemien.* 17. Mai 2021. url: https://www. ccc.de/de/updates/2021/impfausweise-beenden-keine-pandemien.

**[EU-20a] EU-Kommision.** *Coronavirus: Kommission gibt Empfehlung zur Unterstützung von Ausstiegsstrategien durch Daten von mobilen Geräten und Mobil-Apps an.* 8. Apr. 2020. url: https://ec.europa.eu/commission/presscorner/detail/de/ip_20_626.

**[EU-20b] EU-Kommision.** *Coronavirus: Leitlinien zur Gewährleistung der uneingeschränkten Einhaltung der Datenschutzstandards durch Mobil-Apps zur Bekämpfung der Pandemie.* 16. Apr. 2020. url: https://ec.europa.eu/commission/ presscorner/detail/ de/IP_20_669.

**[Fak21] Tagesschau Faktenfinder.** *Mit "Lucaäus dem Lockdown?* 1. März 2021. url: https: //www.tagesschau.de/faktenfinder/hintergrund/luca- app- hintergrund-101.html.

**[Git20a] DP-3T Project auf GitHub.** *DP3T - Decentralized Privacy-Preserving Proximity Tracing.* 30. Sep. 2020. url: https://github.com/DP-3T/documents.

**[Git20b] DP-3T Project auf GitHub.** *FAQ: Decentralized Proximity Tracing.* 2020. url: https: //github.com/DP-3T/documents/blob/master/FAQ.md.

**[Goo20a] Google.** *Exposure Notifications API.* 2020. url: https://developers.google.com/ android/exposure-notifications/exposure-notifications-api.

**[Goo20b] Apple, Google.** *COVID-19-Benachrichtigungen: Wie wir die Gesundheitsbehörden durch Technologie bei der Eindämmung von COVID-19 unterstützen.* Aug. 2020. url: https: //www.google.com/covid19/exposurenotifications/.

**[Goo20c] Apple, Google.** *Exposure Notification, Cryptography Specification.* Apr. 2020. url: https://blog.google/documents/69/Exposure_Notification_-_Cryptography_Specification_ v1.2.1.pdf/.

**[Goo21] Google.** *Exposure Notifications API. Ihre Standortdaten.* Abgerufen am 14.7.2021. 2021. url: https://policies.google.com/privacy?hl=de.

**[Hol21] Martin Holland.** *England:Google und Apple blockieren Update der Corona-App mit Check-In-Funktion.* 14. Apr. 2021. url: https://www.heise.de/news/England-Google - und - Apple - blockieren - Update - der - Corona - App - mit - Check - In - Funktion-6012630.html.

**[Ins20] Robert Koch Institut.** *Grundsätzliche Funktionsweise der Corona-Warn-App.* 19. Aug. 2020. url: https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Funktion_Detail.pdf?__blob=publicationFile.

**[Int18] Institut für Integrierte Produktion Hannover.** *Whitepaper: Indoor-Navigation ermöglicht den Einsatz neuer Technik für Mensch und Maschine.* 2018. url: https://www.iph-hannover.de/_media/files/downloads/Whitepaper_IndoorNavigation.pdf

**[Kau14] Tim Kaufmann.** *iBeacon ist mehr als ein Leuchtfeuer.* 27. März 2014. url: https: //www.golem.de/news/bluetooth-low-energy-ibeacon-ist-mehr-als-ein-leuchtfeuer-1403-105331.html.

**[Köh21] Kristian Köhntopp.** 14. Apr. 2021. url: https://twitter.com/isotopp/status/1382234793140752385.

**[Kom21a] Europäische Kommission.** *Kontaktnachverfolgung – welche App in welchem Land?* 19. Aug. 2021. url: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracingapps-eu-member-states_de.

**[Kom21b] Europäische Kommission.** Kontaktnachverfolgung – welche App in welchem Land? 19. Aug. 2021. url: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_de.

**[Kon21] Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder.** *Chancen der Corona-Warn-App 2.0 nutzen.* 29. Apr. 2021. url: https://www.datenschutzkonferenz-online.de/media/en/20210429_DSK_Entschlie%C3%9Fung_Chancen_der_CWA_2.0_nutzen.pdf.

**[Köv21a] Chris Köver.** *Das zentrale Problem von Luca.* 23. März 2021. url: https://netzpolitik. org/2021/digitale-gaestelisten-das-zentrale-problem-von-luca/.

**[Köv21b] Chris Köver.** *Sicherheitslücke bei Luca: Schlüsselanhänger mit Folgen.* 14. Apr. 2021. url: https://netzpolitik.org/2021/sicherheitsluecke-bei-luca-schluesselanhaenger-mit-folgen/.

**[Köv21c] Chris Köver.** *Widersprüche zur Wirkung der Corona-Warn-App.* 18. Juni 2021. url: https://netzpolitik.org/2021/robert-koch-institut-widersprueche-zur-wirkung-der-corona-warn-app/.

**[Kre20] Stefan Krempl.** *Corona-App: Apple und Google wollen Regierungswünschen nachkommen.* 24. Apr. 2020. url: https://www.heise.de/newsticker/meldung/Corona-App-Apple-und-Google-wollen-Regierungswuenschen-nachkommen-4709428.html.

**[Kri20] Christian Feld, Kristin Becker.** *Bundesregierung denkt bei App um.* 26. Apr. 2020. url: https://www.tagesschau.de/inland/coronavirus-app-107.html.

**[Kut21] Nicolas Kutschera.** *Die Corona-Warn-App – Eine Zwischenbewertung*. Universität Würzburg, Feb. 2021. url: https://www.uni-wuerzburg.de/fileadmin/02000015/2021/Die_Corona-Warn-App_-_eine_Zwischenbewertung.pdf.

**[Lau20] Dominik Lauck.** *iPhone-Lücke war seit Wochen bekannt.* 27. Juli 2020. url: https: //www.tagesschau.de/investigativ/corona-warn-app-121.html.

**[Lau21] Daniel Laufer.** *Polizei nutzt Corona-Kontaktlisten für Drogenermittlungen.* 31. Juli 2021. url: https://netzpolitik.org/2020/bayern-polizei-nutzt-corona-kontaktlisten-fuer-drogenermittlungen/.

**[Len21] Maximilian Lenkeit.** *CWA Documentation - Event Registration - Summary.* 1. Mai 2021. url: https://github.com/corona-warn-app/cwa-documentation/blob/master/event_registration.md.

**[Mec21] Infrastruktur und Digitalisierung Mecklenburg-Vorpommern - Ministerium für Energie.** *Luca-App für M-V trägt zu Lockerungen im öffentlichen Leben bei - FAQ.* 2021. url: https://www.regierung-mv.de/Landesregierung/em/Service/Luca-App/.

**[Mer19] Bettinger Merry.** *Smartphone GPS accuracy study in an urban environment.* 18. Juli 2019. url: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0219890.

**[Mik13] iSEC Partners Mike Ryan.** *Bluetooth: With Low Energy Comes Low Security.* 13. Aug. 2013. url: https://www.usenix.org/conference/woot13/workshop-program/presentation/ryan.

**[MS19] Praxistipps MS.** *Bluetooth LE (Low Energy): Das ist der Unterschied zu normalem Bluetooth.* 30. Sep. 2019. url: https://praxistipps.chip.de/bluetooth-lelow-energy-das-ist-der-unterschied-zu-normalem-bluetooth_114239.

**[Mül20] Juergen Müller.** *Corona-Warn-App Entwicklung: "Architektur der App muss sich kontinuierlich anpassen".* 20. Mai 2020. url: https://news.sap.com/germany/2020/05/covid19-technische-grundlage-corona-warn-app/.

**[Mut20] Max Muth.** *Wie eine obskure Drahtlos-Technologie zur Hoffnung der Menschheit wurde.* 20. Apr. 2020. url: https://www.sueddeutsche.de/digital/bluetooth-lowenergy-corona-apps-pepp-pt-dp3t-tracing-1.4880839.

**[NDR21] NDR.** *Moderator Böhmermann führt Luca-App in Osnabrück in die Irre.* 8. April 2021. url: https://www.ndr.de/nachrichten/niedersachsen/osnabrueck_emsland/Moderator-Boehmermann-fuehrt-Luca-App-in-Osnabrueck-in-die-Irre,luca128.html.

**[Neu20] Linus Neumann.** *10 Prüfsteine für die Beurteilung von „Contact Tracing"-Apps.* 6. Apr. 2020. url: https://www.ccc.de/de/updates/2020/contact-tracing-requirements.

**[Neu21] Linus Neumann.** *Luca-App: CCC forder Bundesnotbremse.* 13. Apr. 2021. url: https: //www.ccc.de/de/updates/2021/luca-app-ccc-fordert-bundesnotbremse.

**[New20] SAP News.** *In knapp 50 Tagen programmiert: Telekom und SAP veröffentlichen Corona-Warn-App.* 17. Juni 2020. url: https://news.sap.com/germany /2020/06/veroeffentlichung-corona-warn-app/.

**[Rat16] Europäisches Parlament und Rat.** *Datenschutz Grundverordnung.* 27. Apr. 2016. url: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:02016R0679-20160504.

**[Reh20] Bock et. al.** *Datenschutz-Folgenabschätzung für die Corona-Warn-App.* 29. Apr. 2020. url: https://www.fiff.de/dsfa-corona.

**[Reu21] Markus Reuter.** *Schon wieder desaströse Sicherheitslücke in Luca App.* 26. Mai 2021. url: https://netzpolitik.org/2021/it-sicherheit-schon-wieder-desastroese-sicherheitsluecke-in-luca-app/.

**[RKI21a] RKI.** *Ansteckung mit COVID-19 - So wird das Coronavirus übertragen.* 1. Juli 2021. url: https://www.zusammengegencorona.de/informieren/basiswissen-zum-coronavirus/ansteckung-mit-corona-so-wird-das-coronavirus-uebertragen/.

**[RKI21b] RKI.** *Corona Warn App. Apple AppStore*, Juni 2021.

**[RKI21c] RKI.** *FAQ: Datenschutz und Sicherheit.* Juli 2021. url: https://www.coronawarn. app/de/faq/#privacy_security.

**[RKI21d] RKI.** *FAQ: Event Check-In.* Juli 2021. url: https://www.coronawarn.app/de/faq/ #check_in.

**[RKI21e] RKI.** *Kennzahlen zur Corona-Warn-App.* 24. Juni 2021. url: https://www.rki.de/ DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Archiv_Kennzahlen/ Kennzahlen_25062021.pdf?__blob=publicationFile.

**[Sch20a] Fabian A. Scherschel.** *Corona-Tracking: Wie Contact-Tracing-Apps funktionieren, was davon zu halten ist.* 26. Apr. 2020. url: https://www.heise.de/hinter grund/Corona-Tracking-Wie-Contact-Tracing-Apps-funktionieren-was-davon-zu-halten-ist-4709903.html.

**[Sch20b] Fabian A. Scherschel.** *TÜV-Prüfung der Corona-App: App soll stabil und sicher laufen.* 14. Juni 2020. url: https://www.heise.de/news/TUeV-Pruefung-der-Corona-App-App-soll-stabil-und-sicher-laufen-4782882.html.

**[Sch20c] Christiane Schulzki-Haddouti.** *PEPP-PT-Projekt: Forscher fordern besseren Datenschutz bei Corona-Warn-Apps.* 20. Apr. 2020. url: https://www.heise.de/newsticker /meldung/PEPP-PT-Projekt-Forscher-fordern-besseren-Datenschutz-bei-Corona-Warn-Apps-4705948.html.

**[Sch21a] Manfred Schermer.** *Corona: Viele Ansteckungen in Innenräumen - Aerosol-Papst verrät, wie man sich schützen kann.* 26. Mai 2021. url: https://www.fuldaerzeitung. de/fulda/corona-aerosole-innenraeume-plexiglas-scheiben-supermarkt-gerhard-scheuch-interview-fulda-90658380.html.

**[Sch21b] Christian Schiffer.** *Warum die Luca-App nicht im Kampf gegen die Pandemie hilft.* 11. Aug. 2021. url: https://www.br.de/nachrichten/netzwelt/warum-die-luca-app-nicht-im-kampf-gegen-die-pandemie-hilft,Sffqfh9.

**[Sch21c] Gregor Schmalzried.** *Was kann die Luca-App, was die Corona-Warn-App nicht kann?* 24. Feb. 2021. url: https://www.br.de/nachrichten/netzwelt/luca-app-was-sie-kann-was-die-corona-warn-app-nicht-bietet,SPvxQ5P.

**[Tod21] Feliks Todtmann.** *Luca-App: Sicherheitslücke gefährdet Gesundheitsämter.* 26. Mai 2021. url: https://www.rnd.de/digital/luca-app-sicherheitsluecke-gefaehrdet-gesundheitsaemter-OAUQAQ62FBA4HMW5MT5ERAEBOQ.html.

**[ZDF20] ZDF.** *Buyx zur Corona-Warn-App - Ethikrat: Weniger Datenschutz wäre vertretbar.* 29. Okt. 2020. url: https://www.zdf.de/nachrichten/digitales/coronavirus-warnapp-datenschutz--kritik-100.html.