

Kasseler Diskussionspapiere

i3

Ideen,
Interessen und
Institutionen im Wandel

Ein Jahr Corona-Warn-App

Die CWA aus der Perspektive staatlicher Steuerung

Samuel Greef



Nr.

14

07 / 2021

U N I K A S S E L
V E R S I T Ä T

Fachgebiet
Politisches System der BRD –
Staatlichkeit im Wandel



Editorial

Liebe Leser:innen,

wir freuen uns, dass Sie auf diese Ausgabe der *i3* aufmerksam geworden sind. Bei *i3* handelt es sich um eine Reihe politikwissenschaftlicher Diskussionspapiere. Sie werden herausgegeben von Prof. Dr. Wolfgang Schroeder und dem Fachgebiet „Politisches System der BRD – Staatlichkeit im Wandel“ an der Universität Kassel. In unregelmäßigen Abständen finden Sie in den Diskussionspapieren neue Forschungsergebnisse und Beiträge zu aktuellen politikwissenschaftlichen Debatten. Thematisch erwartet Sie ein breites Spektrum an Schwerpunkten mit besonderem Fokus auf die Parteien-, Verbände- und Wohlfahrtsstaatsforschung. Jede Ausgabe behandelt ein für den Lehrstuhl relevantes Thema, das sich perspektivisch etwa mit Wandlungsprozessen in Politikfeldern, Veränderungen von Akteuren und Akteursstrukturen oder dem Wandel von Regieren und Staatlichkeit befasst. Ein gemeinsamer Bezugspunkt, der auch den Titel der Diskussionspapier-Reihe inspiriert, ist der von Max Weber über Rainer M. Lepsius aufgenommene Spannungsbogen, welcher den Wandel von Ideen, Interessen und Institutionen thematisiert. Neben Artikeln von dem Lehrstuhl nahestehenden Wissenschaftlerinnen und Wissenschaftlern sind auch Gastbeiträge gerne gesehen.

Wir wünschen Ihnen nun eine anregende Lektüre und würden uns freuen, Sie auch bei den nächsten Ausgaben der *i3* wieder als Leser begrüßen zu dürfen. Hinweise, Anregungen und Kommentare nehmen wir gerne über die Redaktionsadresse entgegen.

Das Herausgeber- und Redaktionsteam

redaktion-i3@uni-kassel.de

Herausgeber

Prof. Dr. Wolfgang Schroeder

Universität Kassel, FB05 Gesellschaftswissenschaften

Fachgebiet Politisches System der BRD - Staatlichkeit im Wandel

Nora-Platiel-Str. 1

34127 Kassel

Erscheinungsweise

Die *i3 - Kasseler Diskussionspapiere – Ideen, Interessen und Institutionen im Wandel* erscheinen in unregelmäßigen Abständen und sind nur als PDF-Version zum Download unter der Adresse

<http://www.uni-kassel.de/fb05/index.php?id=i3> erhältlich.

ISSN 2363 – 7250

DOI: [10.17170/kobra-202106274171](https://doi.org/10.17170/kobra-202106274171)

Logo der Corona Warn-App: Copyright © 2020 SAP SE or an SAP affiliate company. Lizenziert gemäß Apache Licence Version 2.0

<https://www.apache.org/licenses/LICENSE-2.0>



Autor

Dr. Samuel Greef ist promovierter Politologe und Informatiker. Er arbeitet als wissenschaftlicher Assistent an der Universität Kassel zu den Forschungsschwerpunkten Digital- und Netzpolitik, Digitalisierung, Industrie 4.0 sowie in der Verbände- und Gewerkschaftsforschung. Kontakt: greef@uni-kassel.de

Inhalt

1	Einleitung	4
2	Digitale Kontaktnachverfolgung mit der Corona-Warn-App	5
3	Vertrauen durch Freiwilligkeit	7
4	Die Rolle von Apple und Google: Code is Law.....	10
5	Vertrauen und Responsivität durch Open Source	11
6	Fazit	13
7	Literatur	14

Ein Jahr Corona-Warn-App

Die CWA aus der Perspektive staatlicher Steuerung

Samuel Greef

1 Einleitung

Am 27. Januar 2020 wurde der erste Corona-Fall in Deutschland im Landkreis Starnberg in Bayern bekannt. Knapp fünf Monate später, am 16. Juni 2020, erschien unter dem Namen *Corona-Warn-App* (CWA) die offizielle deutsche App zur digitalen Kontaktnachverfolgung [*Digital Contact Tracing* (DCT)] mithilfe von Mobiltelefonen in den App-Stores von Apple und Google. In diesem Zeitraum hatte sich das Coronavirus SARS-CoV-2 von einer „weiterhin gering[en]“ „Gefahr für die Gesundheit der Menschen in Deutschland“, so Bundesgesundheitsminister Jens Spahn im Januar 2020, zu einer weltweiten Pandemie ausgeweitet (vgl. BMG 2021). Bis zum 16. Juni 2020 wurden in Deutschland 188.382 Infektionen und 8.910 Todesfälle im Zusammenhang mit COVID-19 gemeldet. Zu diesem Zeitpunkt war die erste Welle gebrochen und die Zahl der täglich gemeldeten Fälle schwankte nur noch zwischen 200 und 1.000 im Gegensatz zu 6.551 Meldungen in der Spitze am 4. April 2020. Zugleich sollten die kommenden Höchstwerte in der zweiten (33.987 am 23.12.2020) und dritten Welle (29.487 am 21.04.2021) noch deutlich darüber liegen (vgl. RKI 2021b).

Mit Beginn der zweiten Welle im Oktober 2020 mehrten sich Berichte von „überlasteten“ und „überforderten“ Gesundheitsämtern, die für die analoge Nachverfolgung¹ von Kontakten mit Infizierten zuständig sind. Sie standen trotz der Unterstützung von Bundeswehr und Freiwilligen „am Limit“ oder „vor dem Kollaps“ und konnten die Kontaktnachverfolgung nur noch „lückenhaft“ und in „heiklen Fällen“ aufrechterhalten (siehe beispielhaft Schmidt/ Schneider 2020; Pfadenhauer 2020, 2021; Sartor 2020). Die CWA soll daher unter anderem die Gesundheitsämter entlasten, indem sie automatisiert Kontaktpersonen von Infizierten erkennt und informiert, um so Infektionsketten frühzeitig zu unterbrechen. Sie ist damit ein Baustein in der Strategie der Bundesregierung zum Umgang mit den multiplen Herausforderungen in der Corona-Pandemie. Dieser Baustein soll im Folgenden vertiefend in den Blick genommen und insbesondere aus der Perspektive auf staatliche Steuerung(sbemühungen) betrachtet werden.

Aus Steuerungsperspektive lag der Fokus bisher eher auf dem starken, durchsetzungsfähigen Staat in der Krise. So fiel etwa ein zwiespältiger Blick insbesondere auf China, das die Krise durch autoritäre Eingriffe, mit der Isolation und Überwachung von Millionen von Menschen, einerseits schnell in den Griff bekam. Andererseits wurde dem autoritären Regime der kommunistischen Partei vorgeworfen, den Ausbruch der Krankheit zu lange verheimlicht und Informationen unterdrückt zu haben (vgl. Ther 2020: 40). Gleichwohl kam vor diesem Hintergrund die Diskussion auf, ob autoritäre und totalitäre Regime über eine bessere Ausgangslage bei der Pandemiebekämpfung verfügen würden als (westliche) Demokratien,² weil diese Staaten von oben durchregieren könnten, ohne dabei auf demokratische und rechtsstaatliche Prinzipien Rücksicht nehmen zu müssen. Außerachtgelassen wurden bei diesem

¹ Wobei auf der organisatorischen Ebene der Gesundheitsämter mit dem *Surveillance Outbreak Response Management and Analysis System* (SORMAS), entwickelt im Zuge der Ebola-Epidemie 2014, bereits ein digitales Unterstützungssystem vorlag. Im Januar 2021 nutzen dieses aber nur ein Drittel der 375 Gesundheitsämter, während zwei Drittel noch auf Fax und Papier setzten. Erst Ende März 2021 hatte sich der Anteil auf 84 Prozent erhöht (vgl. Krempf 2021a; b).

² Für die Debatte um die Demokratie in Deutschland in der Corona-Pandemie siehe bspw. Decker (2020).

verkürzten Blickwinkel auf einen globalen Systemwettbewerb die wichtigeren Aspekte wie die Stabilität von Staatlichkeit und politischem Entscheidungssystem, die Qualität und Finanzierung des Gesundheitssystems und die gesellschaftliche Akzeptanz für das politische Handeln und die konkreten Maßnahmen (vgl. Merkel 2020; Ther 2020).

In Europa setzen fast alle Staaten beim Schutz der Gesundheit ihrer Bevölkerung und bei der Bekämpfung der Pandemie auf direkte Steuerung durch *Ge- und Verbote*. Diese schränken auch grundrechtlichen Freiheiten ein (vgl. bspw. Knieps 2020). Der Interventionsstaat zeigt mit Ausgangsbeschränkungen, Kontaktverboten, Abstandsregeln sowie Betriebs- und Geschäftsschließungen seine Funktionsfähigkeit sowohl gegenüber Bürger:innen als auch Organisationen und Unternehmen. Diese Beschränkungen setzt die Bundesregierung, auch in Absprache mit den Ministerpräsident:innen der Länder, durch Verordnungen im Rahmen des Infektionsschutzgesetzes (IfSG) um.³ Mit Blick auf digitale Technologien spielen aber auch andere Steuerungsinstrumente in der Pandemie eine Rolle. Denn diese wirkte als „eine Art Digitalisierungsbeschleuniger in ganz unterschiedlichen Gesellschaftsfeldern“ (Bieber 2020: 3). Decker (2020: 130) bezeichnet die Auswirkungen auf die Digitalisierung als eine der sich jetzt schon abzeichnenden „wichtigsten Langzeitwirkungen der Pandemie“. Eines dieser digitalen Instrumente in der Pandemie ist die Corona-Warn-App. Sie unterscheidet sich auf mehreren Ebenen als Steuerungsinstrument von direkter Steuerung durch Ge- und Verbote, was im Folgenden anhand der Entstehungsgeschichte der App herausgearbeitet wird.

2 Digitale Kontaktnachverfolgung mit der Corona-Warn-App

Deutschland setzt, wie auch viele andere Staaten,⁴ auf eine digitale Kontaktnachverfolgung, die aufgrund der großen Verbreitung von Mobiltelefonen⁵ auf eine App zurückgreift. Diese nutzen den Nahfunk-Datenübertragungsstandard Bluetooth LE [Low Energy], um die räumliche Nähe von Mobiltelefonen – und damit Kontakte zwischen Personen – zu protokollieren.⁶ Dafür tauscht die App anonyme Schlüssel aus, die dann mit den von einem zentralen Server zur Verfügung gestellten Schlüssel von nachweislich infizierten Personen abgeglichen werden können. In Deutschland wurden die SAP und die Telekom mit der Entwicklung, Wartung und dem Betrieb⁷ der Corona-Warn-App durch das Robert Koch-Institut (RKI) (als zentrale Einrichtung der Bundesregierung beziehungsweise für das

³ Dieses Vorgehen führte unter anderem zu einer Debatte über das Verhältnis zwischen Regierung und Parlament, da diese weitreichenden Eingriffe in die Grundrechte am Bundestag vorbei stattfanden. Die Forderungen der Parlamentarier:innen nach mehr Mitsprache führte zur Diskussion und Verabschiedung des „Dritten Gesetzes zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite“ (Deutscher Bundestag 2020). Mit dieser Reform des Infektionsschutzgesetzes wurden insbesondere die möglichen, von Regierungsseite zu treffenden Maßnahmen konkretisiert und damit die Verordnungen von Bund und Ländern auf eine neue Rechtsgrundlage gestellt.

⁴ Für eine Übersicht siehe bspw. den MIT Technology Review Covid Tracing Tracker, der bereits im Mai 2020 weltweit 25 Tracing Apps auswies (O’Neil et al. 2020). Für die Verteilung von (de-)zentralen Umsetzungen siehe etwa Kaya (2020: 5f.).

⁵ Etwa 60 Millionen Menschen in Deutschland besitzen ein Mobiltelefon mit Internetfunktionalität (auch als Smartphone bezeichnet) (vgl. Deloitte 2020; statista 2019).

⁶ Aus Datenschutzperspektive hat die Bluetooth-Nutzung den Vorteil, dass damit, im Gegensatz zur Nutzung von GPS-Positionsdaten, die einige asiatische Länder (ebenfalls) nutzen, keine Geolokalisierung verbunden ist und somit keine Bewegungsprofile angelegt werden können. Ohnehin besteht das höchste Infektionsrisiko aber in geschlossenen Räumen, wo GPS aufgrund fehlender freier Sichtverbindung zu den Satelliten nicht funktioniert.

⁷ Zum Betrieb gehören insbesondere die Back-End-Serverinfrastruktur zum Informationsaustausch (Schlüssel der positiv getesteten Kontakte) mit der App und eine Verifikations-Hotline, die durch ein TAN-Verfahren vor falschen Test-Meldungen schützen soll. Zusätzlich gibt es eine mehrsprachige Telefonhotline (Callcenter) für Anfragen zur Nutzung und Funktionalität der App.

Bundesministerium für Gesundheit) beauftragt.⁸ Insgesamt betrug das Budget für die CWA rund 68 Millionen Euro (bis Ende 2021). Davon entfielen etwa 20 Millionen auf die Entwicklung der App und ihrer Server-Komponente, 2 Millionen auf die Wartung und Pflege derselben, 43 Millionen auf den Betrieb sowie 3,5 Millionen auf Werbung (vgl. Voss 2020).

Die Corona-Warn-App lässt sich aus zwei Perspektiven als ein Steuerungsinstrument klassifizieren, das auf die Steuerungsform der *Information, Aufklärung und Überzeugung* setzt. Zum einen betrifft dies den Steuerungsimpuls für die zentral intendierte Steuerungswirkung. Die App informiert Nutzer:innen anonym über Kontakte mit anderen Nutzer:innen, von denen möglicherweise ein persönliches Ansteckungsrisiko für SARS-CoV-2 ausgeht.⁹ Sie klärt über das in diesen Fällen sinnvolle weitere Vorgehen auf und ermöglicht die anonyme Bekanntgabe eines eigenen positiven oder negativen Testergebnisses.¹⁰ So sollen wiederum die eigenen Kontakte über ein mögliches Risiko informiert und damit frühzeitig Infektionsketten unterbrochen werden.¹¹ Die intendierte Steuerungswirkung auf das Steuerungsobjekt besteht dabei darin, bei einem ausgewiesenen niedrigen Risiko ohne oder trotz Risiko-Begegnung ein umsichtiges Verhalten (Einhalten der Abstands- und Hygieneregeln) an den Tag zu legen. Bei einem ausgewiesenen erhöhten Risiko sollen persönliche Kontakte reduziert, verstärkt auf Symptome geachtet und bei Symptomen eine mögliche Testung mit der Hausarztpraxis, dem kassenärztlichen Bereitschaftsdienst oder dem Gesundheitsamt abgeklärt werden (vgl. RKI 2020b).

Der zweite auf die Steuerungsform der Information bezogene Aspekt der Corona-Warn-App liegt in der Implementation des Instruments. Es gab die bewusste politische Entscheidung, kein (Begleit-)Gesetz zu verabschieden und keine Verordnung zu erlassen, die eine Nutzung der App (in bestimmten Kontexten) verpflichtend gemacht hätte.¹² Aufgrund der *Freiwilligkeit des Instruments* konnte seine

⁸ Für die CWA gab es keine öffentliche Ausschreibung. „Die Vergabe der Verträge über die Erstellung und den Betrieb der Corona-Warn-App erfolgte nach Feststellung der Dringlichkeit der Beschaffung durch den Krisenstab (...) im Wege einer Verhandlungsvergabe ohne Teilnahmewettbewerb“ (BMG 2020a).

⁹ Zum Zeitpunkt dieser Untersuchung basierte die Formel für die Risikoeinschätzung auf vier Indikatoren: dem Übertragungsrisiko des positiv getesteten Kontakts, der Dauer der Begegnung, der Zeit, die seit der Begegnung vergangen ist sowie der Unmittelbarkeit des Kontakts (vgl. RKI 2020b). Letzterer meint den Dämpfungswert beziehungsweise die Signalstärke der Bluetooth-Verbindung zwischen den Mobiltelefonen. Eine höhere Dämpfung oder eine geringere Signalstärke sind Anzeichen für einen größeren Abstand zwischen den Personen (wenngleich auch physische Gegenstände und Bauten zwischen den Mobiltelefonen das Signal schwächen können, weshalb die Entfernungsbestimmung mit Unsicherheit behaftet ist).

¹⁰ Eine reibungslose Meldung von Testergebnissen wird dadurch erschwert, dass noch nicht alle Labore an die App-Infrastruktur angeschlossen sind. Um Falschmeldungen zu vermeiden, können nur verifizierte Ergebnisse gemeldet werden. Bei nicht angeschlossenen Laboren ist daher eine telefonische Verifikation notwendig. Im November 2020 waren von 169 niedergelassenen Laboren, die ihre Tests an das RKI melden, 152 an die CWA-Infrastruktur angebunden (vgl. ÄrzteZeitung 2020).

¹¹ Für eine schnellere Kontaktnachverfolgung und -information wurde auch technisch nachgesteuert. Beispielsweise ließen sich zum Ausrollen der App nur einmal in 24 Stunden die Daten der positiv Getesteten abrufen und auf Risikobegegnungen hin überprüfen. Dieser Rhythmus wurde mit dem Update der App auf Version 1.7 (25.11.2020) auf sechsmal täglich erhöht (vgl. BMG 2020b: 1; Heine 2020a).

¹² Ein Begleitgesetz hätte aber auch die Freiwilligkeit der App festschreiben können. Aus dem fehlenden Gesetz folgte daher auf der anderen Seite die prinzipielle Möglichkeit für Privatakteure, in Hausordnungen oder AGBs eine verpflichtende Nutzung der Corona-Warn-App in bestimmten Kontexten festzuschreiben (auch wenn damit datenschutzrechtlich aufgrund des Einwilligungserfordernisses große Probleme einhergehen, weil damit die dem RKI ausgestellte Erlaubnis zur Auftragsdatenverarbeitung erlischt). So forderte etwa auch der DGB (2020) „klare rechtliche Regelungen“, unter anderem bezogen auf die Anordnungsmöglichkeiten von Arbeitgeber:innen, damit für Arbeitnehmer:innen „[w]eder die Nutzung, noch die Nichtnutzung (...) negative Konsequenzen (...) nach sich ziehen.“

Nach demselben Muster erfolgte später die Debatte um die Notwendigkeit einer gesetzlichen Grundlage für den Umgang mit (nicht) geimpften Menschen. Hierbei ging es um ein Verbot von Sonderrechten für Geimpfte

Anwendung, und damit mittelfristig auch seine Wirksamkeit,¹³ nur durch Information, Aufklärung und Bewerbung unterstützt werden – zumal erschwerend die Freiwilligkeit auf opt-in (die App muss aktiv heruntergeladen und genutzt werden) statt opt-out basiert.¹⁴ Dennoch startete die CWA relativ erfolgreich. Mit 24,2 Millionen Downloads (Stand 17.12.2020) war sie zu diesem Zeitpunkt die erfolgreichste europäische Warn-App (vgl. RKI 2020c: 1).¹⁵ Bezogen auf die Verbreitung von Smartphones (Mobiltelefone mit Internetzugang), die etwa 60 Millionen Menschen in Deutschland besitzen, fallen die Downloadzahlen gleichwohl niedrig aus (vgl. Deloitte 2020; statista 2019). Zugleich ist ein Download nicht gleichbedeutend mit der kontinuierlichen Nutzung der App.¹⁶ Im August 2020 lag die Nutzungsquote¹⁷ bei etwa 80 Prozent (vgl. Greis 2020). Bei einer bundesweiten Umfrage Ende November 2020 gaben 36 Prozent der Befragten an, die App zu nutzen (vgl. Kantar 2020).¹⁸ Die primären Argumente, die einen Anreiz zur Nutzung darstellen sollen, sind der gesamtgesellschaftliche Beitrag zur Eindämmung der Pandemie (durch Unterstützung der Kontaktnachverfolgung) und der individuelle Nutzen durch die zeitnahe Aufklärung über eine mögliche Gefahr für die eigene Gesundheit und damit möglicherweise auch für nahe Angehörige und Freunde. Dieser Erwartung entsprechen auch die in einer Umfrage im November 2020 am häufigsten genannten Gründe für die Nutzung der App: für 72 Prozent der Nutzer:innen war der Grund ausschlaggebend, sich selbst und seine Gesundheit zu schützen. Auf dem zweiten Platz folgte mit 55 Prozent die Begründung, sein Umfeld (Familie, Freunde, Bekannte) zu schützen (vgl. ebd.).

3 Vertrauen durch Freiwilligkeit

Die Entscheidung, auf Freiwilligkeit und Information zu setzen, wirkte wiederum auf die konkrete Ausgestaltung des Instruments zurück. Eine zentrale Frage ist dabei, wie sich ein größtmögliches *Vertrauen* in das Instrument herstellen lässt, damit es auch tatsächlich genutzt wird. Dies betrifft bei der Corona-Warn-App mindestens zwei Dimensionen: erstens das Vertrauen in die *Nützlichkeit* der App als einem geeigneten (wirksamen) und effektiven Instrument zur Pandemiebekämpfung.¹⁹ Hierbei kommt der

beziehungsweise der Verhinderung von Diskriminierung von nicht geimpften Menschen (vgl. bspw. FAZ 2020b). Zugleich entwickelten international unterschiedliche Akteure (technische) Lösungen für einen Impfausweis bzw. -nachweis (vgl. bspw. Muscato/ Ferguson 2020).

¹³ An dieser Stelle bleiben die Debatten um den tatsächlichen Nutzen und die Wirksamkeit der App zur Eindämmung der Pandemie unberücksichtigt.

¹⁴ Für einen Opt-out-Mechanismus hätten die Mobiltelefonhersteller oder Apple und Google als Verantwortliche für die maßgeblichen Betriebssysteme die App automatische installieren und ausliefern müssen.

¹⁵ Die Zahl der Downloads stieg mit Stand 02.06.2021 auf 28,1 Millionen (vgl. RKI 2021a: 1).

¹⁶ Testdownloads werden genauso gezählt, wie der wiederholte Download der App beim Wechsel oder Neuaufrichten des Mobiltelefons.

¹⁷ Berechnet wurde das Verhältnis der Downloadzahl zur Anzahl der Apps, die täglich die aktuellen Schlüssel vom Server abfragten.

¹⁸ Eine frühere Umfrage im September ergab eine Nutzungsquote von 38,4 Prozent (vgl. Brüesch et al. 2020: 15).

¹⁹ Bezogen auf die Effektivität und Wirksamkeit von DCT existiert ein gewisses Dilemma („Henne-Ei-Problem“): der Grad der Wirksamkeit hängt direkt mit dem Verbreitungsgrad der App zusammen, für deren Verbreitung damit nicht bereits mit einer nachgewiesenen Wirksamkeit geworben werden kann (siehe auch Blasimme/ Vayena 2020: 760).

Bezogen auf die deutsche CWA wurde in einer Umfrage Ende November 2020 dann auch von 33 Prozent (und damit am häufigsten) der Nicht-Nutzer:innen der App als ausschlaggebender Grund genannt, dass „die App bei der Pandemie-Bekämpfung nicht hilft/ weil die App nichts bringt“. Auf Platz 2 folgte mit 19 Prozent ein Mangel an Datenschutz, Privatsphäre und ein Überwachungsgefühl (vgl. Kantar 2020: 6). Ähnliche Zahlen ergab die frühere Umfrage im September, bei der 35 Prozent angaben, „Die App schützt mich nicht“ und 31 Prozent Datenschutzgründe nannten (vgl. Brüesch et al. 2020: 17).

wissenschaftlich und medial unterstützten Kommunikation und Bewerbung eine wichtige Aufgabe zu.²⁰ In einer Umfrage im September 2020 gaben 59,2 Prozent derjenigen Befragten, welche die CWA installiert hatten, an, von der Kampagne der Regierung beeinflusst worden zu sein sowie 55,9 Prozent von der Medienberichterstattung – das persönliche Umfeld folgt erst mit 33,2 Prozent (vgl. Brüesch et al. 2020: 20).

Zweitens²¹ spielte das Vertrauen in die *beschränkte* Funktionalität²² der App und den sachgemäßen Umgang mit den Daten und dem Wissen, das staatliche Akteure bei Nutzung der App gewinnen, eine zentrale Rolle.²³ Dieser Punkt führte in der Phase der Entscheidungsfindung über die Architektur der App zu insbesondere zwei Debatten, von denen eine stark kontrovers geführt wurde. Hofmann (2020: 33) spricht von „Zielkonflikten, die im Zuge von Digitalisierungsprozessen beigelegt werden müssen.“ Im Gegensatz zu vielen anderen Konflikten um infrastrukturelle und technische Designentscheidungen wurde der Diskurs um den „richtigen“ Ansatz des Contract Tracing in Deutschland öffentlich geführt (vgl. ebd.: 34). Umstritten war das Modell der Datenspeicherung, bei dem sich zwei gegensätzliche Konzepte gegenüberstanden. Brack et al. (2020) charakterisieren die Debatte auch als Streit zwischen „zwei verschiedenen Vertrauensmodellen“, bei denen das eine auf „ein hierarchisches, obrigkeitsstaatliches Überwachungssystem setzt“ und das andere „auf das verantwortungsvolle Handeln der Beteiligten“.

Den Ausgangspunkt bildet das PEPP-PT Projekt [Pan-European Privacy-Preserving Proximity Tracking]. Beteiligt waren unterschiedliche Akteure wie Hans-Christian Boos (Mitglied des Digitalrats der Bundesregierung und Gründer der Arago GmbH), Fraunhofer AISEC und HHI, die Helmholtz-Gemeinschaft oder das RKI.²⁴ Die Gruppe war maßgeblich für die Idee der Nutzung von Bluetooth verantwortlich und zeigte im ersten *Proof-of-Concept* die grundsätzliche Funktionsfähigkeit dieses Ansatzes. Das Projekt setzte dabei auf eine zentrale Lösung, das sogenannte *Server-side-Matching*. Hierbei wären die von den Mobiltelefonen ausgesandten Schlüssel zentral auf einem Server gesammelt worden. Die Schlüssel von (Nicht-)Infizierten wären *auf dem Server* auf Kontakte abgeglichen worden und ausschließlich diejenigen Apps benachrichtigt worden, für die tatsächlich ein Kontakt festgestellt wurde. Da Kontaktdaten und Kontaktbewertung zentral erfolgt wäre, hätte das Modell zur Berechnung der Infektionsgefahr einfach serverseitig an neue wissenschaftliche Erkenntnisse angepasst werden können. Ebenso wären weitere Informationen über Ansteckungen verfügbar – und damit epidemiologische Erkenntnisse gewinnbar²⁵ – sowie eine zentrale Cluster-Erkennung möglich gewesen (vgl. etwa Bieber

²⁰ Von einigen Akteur:innen wird kritisiert, dass der mediale und politische Umgang mit dem Thema DCT an Technikgläubigkeit grenzte. Es wäre teilweise insbesondere zu Beginn der Eindruck vermittelt worden, mit der App würde sich die Pandemie, zumindest aber die Einschränkungen des täglichen Lebens, schnell(er) beenden lassen (vgl. Krempf 2020).

²¹ Blasimme und Vayena (2020: 760) nennen vier Aspekte, die zu einer geringen Verbreitung von DCT beigetragen haben könnten: „general awareness of DCT Apps, privacy risks, and the actual effectiveness of DCT, as well as public attitudes toward a potentially pervasive form of digital surveillance.“

²² Beschränkte Funktionalität meint hier, dass die App auch nur das tut, was sie zu tun vorgibt und nicht anderweitige, undokumentierte Funktionen (wie etwa zur Überwachung) enthält oder unnötige Daten sammelt.

²³ In einer Befragung im September 2020 lag das Vertrauen sowohl in die Hersteller als auch den Betreiber der CWA bei denjenigen, welche die App installiert hatten, signifikant höher als bei denjenigen, welche die App nicht installiert hatten. Wobei dem Betreiber (RKI) mehr Vertrauen entgegengebracht wurde als den Herstellern (SAP, Telekom). Noch deutlich größer war die Diskrepanz zwischen Nutzer:innen und Nicht-Nutzer:innen in der Frage des Vertrauens in Datenschutz und Datensicherheit (vgl. Brüesch et al. 2020: 27ff.).

²⁴ Am 1. April 2020 gehörten dem PEPP-PT Projekt 130 Mitglieder in sieben EU-Ländern an.

²⁵ Unabhängig von der CWA setzt das RKI ohnehin zusätzlich die Corona-Datenspende-App ein, um weitreichende medizinisch-wissenschaftliche pseudonymisierte Daten zu erhalten (vgl. RKI 2020a).

2020: 5).²⁶ Unter Datenschutzgesichtspunkten hätte jedoch das Problem bestanden, dass Personen-, Gesundheits- und Kontaktdaten eines großen Teils der Bevölkerung an einer zentralen (staatlichen) Stelle gespeichert worden wären. Hierüber entspann sich im April 2020 ein grundsätzlicher Konflikt innerhalb des Projektes. Dieser eskalierte am 19. April in einem offenen Brief von 300 renommierten Expert:innen, die sich für eine datenschutzfreundliche, dezentrale Alternative einsetzten, um „trust in and acceptance of such an application“ nicht zu gefährden und die Gefahr einer staatlichen oder privaten Überwachungsinfrastruktur (insbesondere in nicht-demokratischen Staaten) abzuwenden (vgl. o. A. 2020).²⁷ Zugleich verließen wichtige Akteure, wie etwa das Helmholtz Center for Information Security (CISPA),²⁸ das PEPP-PT Projekt und begannen stattdessen das DP-3T-Konsortium [Decentralized Privacy-Preserving Proximity Tracing] zu unterstützen. Das Konsortium verfolgte den datensparsamen²⁹ und dezentralen Ansatz des sogenannten *Client-side-Matching*. Bei diesem Ansatz verbleiben alle Kontaktinformationen *auf den Mobiltelefonen* der Nutzer:innen und auch die Berechnung der Infektionsgefahr erfolgt auf dem jeweiligen Gerät. Bei einer bestätigten Infektion können Nutzer:innen freiwillig ihre Schlüssel an den zentralen Server schicken, der diese dann an alle Nutzer:innen der App weiter verteilt, damit diese jeweils lokal einen möglichen Kontakt abgleichen können. Der Ansatz folgt damit dem Gedanken von *Privacy by Design*.³⁰

Die Kontroverse zwischen PEPP-PT und DP-3T reiht sich in die Debatten um eine zunehmende Gefahr staatlicher Überwachung und gläserner Bürger:innen im digitalen Zeitalter ein, die sich in der Corona-Krise mit mahnenden Stimmen vereinte, die generell vor dem Aus- und Aufbau eines totalitären Staates warnten, dessen Abbau nach durchgestandener Krise alles andere als sicher sei. Gemäßigte Stimmen brachten insbesondere Datenschutzaspekte in die Debatte ein.³¹ Von anderer Seite wurde dagegen gerade der Datenschutz zu einem der Probleme in der Bearbeitung der Krise stilisiert (siehe etwa Nida-Rümelin/ Hilgendorf 2021), weil in Deutschland zu viele Menschen gleich die „Anfänge des Überwachungsstaats“ wittern würden (vgl. Pieper 2020). In einer Umfrage Ende November 2020 nannten die

²⁶ Auch im dezentralen Modell sind Cluster-Erkennung und Änderungen an der Berechnung möglich, sie müssen aber über ein Update der App auf allen Endgeräten ausgerollt werden. So können etwa seit Version 1.9 (16.12.2020) aufsummierte Kontaktzeiten mit niedrigem Risiko zur Bewertung eines erhöhten Risikos führen. Dafür greift die App auf die erweiterten Daten der zweiten Version des ENF zurück (vgl. Heine 2020b).

²⁷ Zusätzlich wandten sich deutsche Organisationen wie D64, LOAD, Chaos Computer Club (CCC) oder die Gesellschaft für Informatik am 24.4.2020 in einem offenen Brief an die Bundesregierung. Sie solle von der Idee einer App auf Basis der PEPP-PT Initiative Abstand nehmen, denn „[e]ine App, die zumindest eine Aussicht auf Erfolg haben soll, muss ein transparentes Konzept verfolgen, quelloffen programmiert werden, auf zentrale Datenspeicherung verzichten und die Anonymität der Nutzerinnen und Nutzer so weitgehend wie möglich schützen“ (D64 et al. 2020).

²⁸ Seine Gründe verdeutlichte CISPA (2020) in einer längeren Pressemitteilung: „Any contact tracing app can only make a meaningful contribution if it is widely adopted by the population, if it is absolutely trustworthy and transparent in its governance, functionalities, and risk, and if it meets accepted security standards. (...) CISPA together with other leading security and privacy scientists worldwide is confident that only a state-of-the-art decentralised, privacy-by-design technology with strong security guarantees can offer adequate safeguards and gain the necessary trust of the public.“

²⁹ Im Konzept der Datensparsamkeit unterscheidet sich die digitale Kontaktnachverfolgung mittels der CWA in Deutschland grundsätzlich von der Herangehensweise beispielsweise Chinas und Südkoreas, wo umfassende Daten und unterschiedlichen Quellen zusammengeführt und genutzt werden.

³⁰ In einer Analyse des PEPP-PT-Ansatzes sah das DP-3T-Konsortium dagegen nicht nur theoretische „privacy and security issues“, sondern die reale Gefahr, dass „adopting this system would open up significant avenues for systemic misuse“ (The DP-3T Project 2020: 5).

³¹ Auch im internationalen Kontext gab es Beiträge zur Notwendigkeit von „regulatory frameworks for data privacy and protection“ für Contact-Tracing-Apps (Owusu 2020: 3). Unterschiedliche zivilgesellschaftliche Akteure veröffentlichten ein gemeinsames Statement, in dem sie dazu aufforderten, dass „States use of digital surveillance technologies to fight pandemic must respect human rights“ (Amnesty International 2020).

Nichtnutzer:innen der App einen Mangel an Datenschutz, Privatsphäre und Überwachung als zweithäufigsten Grund für die Nichtnutzung (19 %) (vgl. Kantar 2020: 6)³² – und das, obwohl sich die Bundesregierung letztlich am 25. April 2020 für den datenschutzfreundlichen dezentralen Ansatz entschieden hatte, bei dem die Kontaktdaten auf dem jeweils eigenen Mobiltelefon verbleiben.

4 Die Rolle von Apple und Google: Code is Law

Die politische Entscheidung zugunsten des dezentralen Ansatzes lässt sich nicht zwingend damit begründen, dass sich die DP-3T-Seite mit den besseren Argumenten in der Debatte durchgesetzt hätte. Vielmehr wurde der Handlungsspielraum für die Ausgestaltung des Steuerungsinstruments der Corona-Warn-App durch Google und Apple begrenzt. Beide Konzerne besitzen die technische Hoheit über ihr jeweiliges Mobilbetriebssysteme (Android und iOS) und kommen in Deutschland auf einen gemeinsamen Marktanteil von 99 Prozent (Stand Mai 2021) (vgl. StatCounter 2021). Google und Apple entschieden sich dafür, die grundlegende Funktionalität von Tracing-Apps in der dezentralen Variante direkt in ihre Betriebssysteme über das sogenannten *Exposure Notification Framework* (ENF) zu implementieren.³³ Damit konnten nur dazu passende Apps mit der notwendigen Berechtigung dauerhaft im Hintergrund laufen und dabei auf die Bluetooth-Schnittstelle zugreifen.³⁴ Folglich bot technisch nur noch die Umsetzung des DP-3T-Ansatzes eine funktionsfähige Lösung.

Das Beispiel der Corona-Warn-App zeigt damit deutlich die Wirkmächtigkeit der von Laurence Lessig bereits in den 1990er-Jahren beschriebenen Gesetzmäßigkeit: *Code is Law*.³⁵ Die Debatte um eine zentrale Datenhaltung als Lackmustest der Wirksamkeit war von vornherein zum Scheitern verurteilt. Den Möglichkeitsraum der Ausgestaltung für dieses Steuerungsinstruments bestimmten Google und Apple durch ihre Hoheit über die Implementation auf Software- und Hardwareebene (in den Mobiltelefon-Betriebssystemen). Überlegungen zur Anwendung alternativer Konzepte waren zwar nicht nur theoretischer Art, sondern wären auch praktisch umsetzbar gewesen – allerdings nicht praktikabel. Die Wirksamkeit einer solchen App war wegen der notwendigen technischen Implementierung aufgrund der Software-Beschränkungen auf der verbreiteten Hardware zum Scheitern verurteilt. Hieraus lässt sich nicht automatisch eine geschwächte staatliche Steuerungsfähigkeit ableiten, aber die Ausgestaltung des Steuerungsinstruments war beschränkt. Zugleich wird aber auch deutlich, dass die digitale

³² Lasarov (2020: 13) untersuchte beispielhaft die Leser:innen-Debatte unter einem Artikel der Zeit zur Veröffentlichung der CWA, in der in 37 Prozent der 667 relevanten Beiträge die Frage des Nutzens der App aufgegriffen wurde, gefolgt von 26 Prozent mit Bezug zum Thema Datenschutz, Privatsphäre, Transparenz und Vertrauen.

³³ Hieran entzündete sich ein weiterer Konflikt. Einige EU-Regierungen (insbesondere Deutschland und Frankreich) wollten Apple und Google nicht die Entscheidung über einige grundsätzlichen Annahmen über Covid-19, Infektionswege und -risiken überlassen, welche die Basis für die Implementation des ENF bildeten. Frankreich entschied sich für den nationalen Alleingang und entwickelte eine zentrale App, die nicht auf dem ENF aufbaut.

³⁴ Zwar hätte dennoch weiterhin eine App programmiert und ausgerollt werden können, welche die Daten zur Kontaktnachverfolgung auf zentralen Servern speichert. Allerdings hätte diese App immer im Vordergrund auf dem Mobiltelefon geöffnet sein müssen, damit sichergestellt gewesen wäre, dass sie dauerhaft ihre Funktionalität ausführt (und nicht etwa durch Stromsparmaßnahmen des Betriebssystems beendet wird). Sie wäre damit zwar theoretisch möglich gewesen, aber deutlich weniger praktisch nutzbar. Das zeigt auch der verhältnismäßig geringe Erfolg der französischen App mit zentralistischem Ansatz, die im Oktober 2020 auf weniger als fünf Millionen aktive Installationen kam (vgl. Moulinet 2020).

³⁵ Lessig bezog sich auf das Internet bzw. das entstehende World Wide Web. Der Gesetzescharakter von Code (unter dem Lessig sowohl Hard- als auch Software versteht) hat dabei eine doppelte Bedeutung: Code „make cyberspace what it is [and] also regulate cyberspace as it is“ (Lessig 2006: 5).

Fortentwicklung keinem technologischen Determinismus unterliegt, sondern ein „mit Unsicherheiten behafteter, ergebnisoffener und umstrittener Prozess“ ist (Hofmann 2020: 33).

5 Vertrauen und Responsivität durch Open Source

Die zweite Entscheidung, die – nicht nur, aber auch – als vertrauensbildende Maßnahme verstanden werden kann, betraf die Art der Erstellung der App, mit der SAP und Telekom beauftragt wurden. Die CWA ist nicht proprietär, also nicht Eigentum der beiden Unternehmen. Ihre Entwicklung erfolgte Open Source unter der Apache Freie-Software-Lizenz. Sie folgt damit auch der Forderung der Free Software Foundation Europe (fsfe),³⁶ dass steuerfinanzierte Software ein öffentliches Gut sein sollte: „*public money – public code*“ (vgl. auch Bieber 2020: 4). Der Quellcode der App liegt auf einem für alle zugänglich Repository auf GitHub (o. J.). Sie ist damit nicht nur kostenlos nutz- und kopierbar, sondern kann auch verändert und weiterentwickelt werden (vgl. hierzu etwa die Open-Source-Definition der Open Source Initiative 2007).³⁷

Tabelle 1: Ausgewählte Versionen der Corona-Warn-App mit Funktionalitätserweiterung

Version	Datum	Funktionalität
1.5	19.10.2020	Symptomerfassung Unterstützung des europäischen Corona-App-Gateways
1.7	25.11.2020	Risikoermittlung mehrmals statt einmal täglich möglich
1.9	16.12.2020	Anzeige des Tages der letzten Begegnung mit erhöhtem Risiko Mehrere Begegnungen mit niedrigem Risiko können zu einer Bewertung mit erhöhtem Risiko führen
1.10	24.12.2020	Kontakttagbuch
1.11	28.01.2021	Statistiken und Kennzahlen zum Infektionsgeschehen
1.12	04.02.2021	Begegnungshistorie für Kontakttagbuch
2.0	21.04.2021	Check-In-Funktion/ Eventregistrierung
2.1	02.05.2021	Ergebnisse von PCR-Schnelltests integrierbar

Quellen: Heine (2020a; b; c, 2021a; b; c; d); Hoerdt (2020a; b); eigene Zusammenstellung.

Dies geschieht auch mit der offiziellen Version der App, die aktiv weiterentwickelt wird und für die immer wieder Ergänzung um weitere Funktionen debattiert werden. Die Open-Source-Umsetzung ist damit auch Basis für Responsivität gegenüber neuen wissenschaftlichen Erkenntnissen genauso wie gegenüber Interessen von Bürger:innen. So können Nutzer:innen seit dem Update auf Version 1.5 ihre Symptome erfassen. Mit Version 1.9 zeigt die App den genauen Tag an, an dem der letzte Kontakt mit einer positiv getesteten Person stattfand, aus dem eine erhöhte Risikobewertung resultiert. Und seit Version 1.10 können Nutzer:innen ein Kontakttagbuch führen und dieses bei einer Infektion freiwillig dem Gesundheitsamt zur einfacheren Kontaktnachverfolgung zusenden (s. Tabelle 1). Außerdem wurden Benachrichtigungen als Nudging-Element eingeführt. Sie sollen in der App an die Meldung von positiven Testergebnissen erinnern, um „alle Nutzenden zu motivieren, ihren positiven Befund zu teilen“

³⁶ Die Kampagne der fsfe ist unter <https://publiccode.eu/de/> erreichbar (abgerufen am 06.06.2021).

³⁷ Der Open Source-Ansatz ermöglicht es so etwa auch, dass Sicherheitslücken schneller gefunden und behoben werden können – wie etwa im Fall der Server-Komponente der CWA im November 2020 geschehen. Dies zeigt, „dass der Open-Source- sowie Community-Prozess einwandfrei funktioniert und zur Sicherheit des Betriebs der Corona-Warn-App entscheidend beiträgt“ (Hoerdt 2020b).

Bock et al. (2020: 337) heben die aus der quelloffenen Entwicklung folgende Transparenz für die Öffentlichkeit hervor, geben jedoch gleichzeitig zu bedenken, dass eine „technische Fokussierung“ auf diesen Aspekt auch „durchaus größere gesellschaftliche Implikationen des gesamten Verfahrens verschleiern kann“, wenn nicht zugleich auch eine „qualitativ hochwertige Datenschutz-Folgeabschätzung[]“ erfolgt.

(BMG 2020b: 1), denn auch die Meldung erfolgt, wie die Nutzung der App, freiwillig. Tatsächlich erhöhte sich die Meldequote nach Einführung der Benachrichtigungen und weiterer Funktionalitätsupdates.³⁸ So können erweiterte (regionale) statistische Informationen über den Infektionsverlauf (wie etwa Neuinfektionen oder Inzidenzwerte) abgerufen werden (vgl. Bundesregierung 2020: 9). „[Z]usätzliche Funktionalitäten [sollen] die Motivation[,] die Corona-Warn-App zu nutzen, erhöhen“ (BMG 2020b: 2). Darüber hinaus unterstützt die App seit Version 2.0 (21.04.2021) eine Eventregistrierung, die in der Gastronomie, im Einzelhandel und bei Veranstaltungen genutzt werden kann, um über einen QR-Code einzuchecken und so die Kontaktnachverfolgung über die App und eine Cluster-Erkennung (Situationen, in denen viele Personen nah beieinander sind) zu ermöglichen. Diese Funktionalität setzt weiterhin auf Freiwilligkeit und Dezentralität (lokale Speicherung auf dem Mobiltelefon).³⁹ Daher bleibt ohne Gesetzesänderung ein händisches Ausfüllen von Papier-Kontaktbögen oder die Nutzung digitaler Lösungen von Drittanbietern notwendig (vgl. Lindern 2021; Heine 2021c; Köver 2021). Seit Version 2.1 (02.05.2021) können negative Ergebnisse der PCR-Schnelltests einiger Testzentren für 48 Stunden in der App gespeichert werden, um diese beim Friseurbesuch oder Einkauf vorzuzeigen oder positive Ergebnisse gemeldet werden, um Kontakte über die App zu warnen (vgl. Heine 2021d; Wilkens 2021).

Dieser Überblick zeigt, dass die regelmäßige Aktualisierung und Funktionserweiterung der CWA nicht nur der Anpassung an neue Erkenntnisse im Verlauf der Pandemie und Wünsche der Nutzer:innen dient. Es geht auch immer wieder darum, die Nützlichkeit der App zu verbessern, um stärkere Anreize für die freiwillige Nutzung zu setzen und damit die Effektivität der App im Sinne des Ziels einer effizienten Kontaktnachverfolgung zu erhöhen. Unter Bezugnahme auf das Steuerungsmodell der „adaptive governance“ stellen Blasimme und Vayene (2020: 761) fest, dass die Akzeptanz und Verbreitung von DCT dadurch gestärkt werden kann, dass soziale Lernprozesse ermöglicht werden, indem eine breite Basis aus Stakeholdern (Entwickler:innen, Gesundheitsministerium, Datenschützer:innen, Expert:innen und Öffentlichkeit) eingebunden und gleichzeitig schnell auf neues Wissen reagiert wird. Dies scheint zumindest mit Blick auf die Open-Source-Implementierung und breite Debatte um die (Weiter-)Entwicklung der CWA in Deutschland der Fall zu sein. Zwar existiert keine institutionalisierte demokratische Beteiligung für die Weiterentwicklung der App. Durch die Entscheidung für Open Source und das

³⁸ Vor der Vorstellung und Einführung der Erinnerungsfunktion (vgl. FAZ 2020a) hatten nur 54,6 Prozent der Nutzer:innen im Zeitraum 1.9. bis 16.12.2020 (Stand: 17.12.2020) ihr positives Testergebnis auch über die App gemeldet (vgl. RKI 2020c: 2). Zusammen mit der begrenzten Verbreitung der CWA lag daher bis Mitte November 2020 der Anteil der positiv getesteten Personen, die ihr Ergebnis über die App teilten, an allen gemeldeten Neuinfektionen im 7-Tage-Mittelwert bei maximal knapp 14 Prozent (vgl. Böhme 2020).

Mit Stand 02.06.2021 stieg der Anteil der geteilten Testergebnisse auf 61,5 Prozent an. Berücksichtigt man nur die zwischen 17.12.2020 und 02.06.2021 neu hinzugekommenen potenziell teilbaren Testergebnisse liegt die Quote sogar bei 64,6 Prozent (vgl. RKI 2021a: 2).

³⁹ Die CWA unterscheidet sich dabei insbesondere von der zeitweise – auch wegen der Beteiligung des Rappers Smudo von den Fantastischen Vier – medial stark gehypten App luca des Berliner Unternehmens culture4life und der Startup-Ausgründung neXenio des Hasso-Plattner-Instituts (HPI). Diese setzt auf zentrale Datenspeicherung und eine direkte Anbindung an die Gesundheitsämter (vgl. Bunte 2021; Brühl/ Hurtz 2021). Innerhalb von nur zwei Monaten erwarben 13 Bundesländer für etwa 20 Millionen Euro ohne Ausschreibungsverfahren eine Jahreslizenz der Software (vgl. Bleich 2021).

Luca machte im Folgenden vor allem mit Designfehlern und Sicherheitslücken auf sich aufmerksam, über die u. a. auch die Gesundheitsämter hätten angegriffen werden können (Schmidt/ Weiß 2021; s. auch Reuter 2021). Der CCC (2021) forderte am 13.04.2021 „das sofortige Ende der staatlichen Alimentierung von Smudos Steuer-Millionengrab ‚Luca-App‘.“ Zwei Wochen später verwiesen 77 Wissenschaftler:innen und IT-Expert:innen in einer gemeinsamen Stellungnahme auf die vier Entwicklungsprinzipien der CWA: Zweckbindung, Offenheit und Transparenz, Freiwilligkeit, Risikoabwägung und konzidierten, das „bereits in vielen Bundesländern eingesetzte LUCA-System erfüllt keine dieser Prinzipien“ (o. A. 2021).

Hosting auf GitHub gibt es über diese Plattform jedoch zumindest für die dort aktive Community die Möglichkeit, neue Funktionen vorzuschlagen und zu debattieren.⁴⁰

Auch wenn die Weiterentwicklung der CWA einigen Akteuren immer wieder zu langsam erfolgte, zeigen die Berichte von BMG (2020b) und Bundesregierung (2020), dass ein Monitoring der App und eine adaptive Nachsteuerung durch die Anpassung des Instrumentes stattfindet. Dabei fokussieren sie sich auf zwei für die Wirksamkeit der Corona-Warn-App zentrale Aspekte: neue Anreize sollen erstens die Anzahl derjenigen erhöhen, die sich die App auf ihr Mobiltelefon herunterladen und installieren, und zweitens die freiwillige Bekanntgabe von positiven Testergebnissen steigern.

6 Fazit

Seit einem Jahr wird die Corona-Warn-App als digitales Steuerungsinstrument in der Corona-Pandemie eingesetzt. Sie wirkt als indirekte Steuerungsform durch Information, Aufklärung und Überzeugung. Die Wirksamkeit der CWA hängt dabei maßgeblich von Nützlichkeit und Vertrauen ab, weil ihre Nutzung freiwillig erfolgt. Das hinter der App stehende Steuerungskonzept steht damit den Ge- und Verboten im Rahmen des Infektionsschutzgesetzes diametral gegenüber. Zugleich bringt diese Steuerungsform ihre eigenen Herausforderungen mit sich. Erfolgreiche Steuerung über Information und Aufklärung ist voraussetzungsvoll. Sie funktioniert nur, wenn 1. die Steuerungsadressat:innen erreicht werden, sie 2. technisch dazu in der Lage sind, die CWA zu nutzen, sie 3. die Informationen verstehen – sowohl sprachlich als auch im Sinne von digital literacy, also der Digital- sowie digitalen Gesundheitskompetenz – und sie sich 4. auch von diesen überzeugen lassen, also ihr Verhalten anpassen.

Die politische Entscheidung für eine dezentrale Implementierung der digitalen Kontaktnachverfolgung erscheint als vertrauenssteigernde Maßnahme schlüssig, lässt sich aber vor allem durch die von Apple und Google gesetzten technischen Restriktionen im Sinne des Code of Law erklären. Ganz anders bei der bewussten Entscheidung, die CWA in der für die öffentliche Hand immer noch ungewöhnlichen Form des Open-Source-Projektes umzusetzen. Diese solle insbesondere das Vertrauen in die App und damit die Wahrscheinlichkeit für eine breite Nutzung erhöhen. Sie ermöglicht aber auch eine responsive Anpassung des Instruments und eröffnet Beteiligungsmöglichkeiten. Im Gegensatz zu anderen (digitalen) (Infrastruktur-)Großprojekten erfolgte die Umsetzung sehr schnell. Zu beiden Aspekten trug sicherlich auch die Bedingung einer existentiellen gesellschaftlichen Krise – der Konfrontation mit einer unmittelbar lebensbedrohlichen und zugleich unkontrollierbaren Gefahr – bei. Sie führt zu „experimentalistische[r] Kreativität“ nicht nur im Handeln der Bürger:innen, sondern auch von institutionellen Akteuren (Beck 2020: 466).

Zugleich dient der Krisenkontext zwar der Begründung und Legitimation von (Digitalisierungs-)Entscheidungen, deren „langfristige, unumkehrbare Auswirkungen“ weisen jedoch weit über diesen hinaus (Hofmann 2020: 33). Für das hinter der CWA stehende Konzept sieht Hofmann (ebd.) die Möglichkeit, dass sich dieses infrastrukturell verstetigt. Im Sinne von Streeck und Thelens (2005: 31) Kategorisierung von Institutionenwandel könnte dies etwa durch *Conversion*, also den Wechsel auf neue Anwendungsfälle oder Aufgabenfelder,⁴¹ oder durch *Layering*, etwa durch Übertragung des Konzeptes auf bestehende Infrastrukturen, ohne diese grundsätzlich in Frage zu stellen, erfolgen. Dafür müssen sich experimentelle Konzepte zunächst bewähren, eine Standardisierung erfahren und sich dann als

⁴⁰ Diese Möglichkeit (unter <https://github.com/corona-warn-app/cwa-wishlist/issues>; abgerufen am 21.06.2021) wurde auch genutzt. Am 21.06.2021 gab es 273 offene und 175 (ab)geschlossene „feature request“ oder „enhancement“-Vorschläge.

⁴¹ Noch sehr nah am Ausgangsfall bleibt dabei die CovPass-App für den digitalen Impfnachweis. Auch dieser soll als Open-Source-Lösung implementiert werden und die Daten nicht zentral ablegen, sondern auf dem Mobiltelefon vorhalten (vgl. Ballweber 2021).

(vom ursprünglichen Kern in gewissem Maße abstrahierte) funktionale Infrastrukturen normalisieren (vgl. Hofmann 2020: 34f.). In diesem Sinne könnte die Corona-Warn-App nicht nur „im Rückblick als jenes Beispiel wahrgenommen [werden], das dem Geschäftsbereich ‚Digitalisierung‘ im politischen Raum zu der Bedeutung verholfen hat, den er seit mehreren Jahren längst schon verdient“ (Bieber 2020: 6). Vielmehr besitzt sie das Potenzial, beispielhaft auf die möglichen positiven Effekte in Bezug auf die Steuerungsfähigkeit hinzuweisen, die entstehen, wenn weiche Steuerungsinstrumente mit frühzeitiger Beteiligung konkurrierender oder konfligierender Interessen und transparenter Umsetzung kombiniert werden.

Die CWA ist ein Beispiel für staatliche Handlungsfähigkeit in Krisenzeiten jenseits von hierarchischer Steuerung durch Ge- und Verbote und damit für erfolgreiche Governance. Zwar lässt sich ihre konkrete Wirkung im Sinne der Pandemiebekämpfung nicht einfach beziffern. Bei ihrer Nutzungsrate (13,4 %) lag sie allerdings bereits im Juli 2020, einen Monat nach ihrem Erscheinen, auf Platz 3 von 20 Ländern mit mehr als 20 Millionen Einwohner:innen – hinter Australien (21,6 %) und der Türkei (17,3 %), deren Apps bereits im April gestartet waren und deren Nutzung im Fall der Türkei nicht grundsätzlich freiwillig ist (vgl. Chan 2020; Norton Rose Fulbright 2021). Insofern kann hier zumindest von vergleichsweise erfolgreichem politischem Steuerungsbemühen in Bezug auf das Steuerungsziel der Nutzung der CWA gesprochen werden. Nicht zuletzt zeigt sich an der Rolle von Apple und Google im Entscheidungssetting jedoch die grundlegende Gefahr, dass im Zuge der Digitalisierung (staatliche) Handlungs- und Entscheidungsspielräume durch Anbieter:innen zentraler Infrastrukturen und Plattformen eingeschränkt werden.

7 Literatur

- Amnesty International (2020): Joint civil society statement: States use of digital surveillance technologies to fight pandemic must respect human rights, URL: <https://www.amnestyusa.org/wp-content/uploads/2020/04/FULL-STATEMENT.pdf> (abgerufen am 12.5.2020).
- ÄrzteZeitung (2020): SARS-CoV-2-Testergebnisse. 90 Prozent der Labore melden an Corona-Warn-App, ÄrzteZeitung, URL: <https://www.aerztezeitung.de/Wirtschaft/Wie-viele-Testlabore-melden-an-Corona-Warn-App-414435.html> (abgerufen am 29.12.2020).
- Ballweber, Jana (2021): Corona-Warn-App. Digitaler Impfnachweis wird dezentral und Open Source, netzpolitik.org, URL: <https://netzpolitik.org/2021/corona-warn-app-digitaler-impfnachweis-wird-dezentral-und-open-source/> (abgerufen am 24.5.2021).
- Beck, Teresa Koloma (2020): Alltag im Reallabor. Pandemie und Bürgerkrieg als existentielle gesellschaftliche Krisen, in: Leviathan, 48 (3), S. 451–469, DOI: <https://dx.doi.org/10.5771/0340-0425-2020-3-451>.
- Bieber, Christoph (2020): Eine neue Netzpolitik ist verfügbar? Die Corona-Warn-App als politisches Software-Projekt, regierungsforschung.de, Duisburg: NRW School of Governance, URL: https://regierungsforschung.de/wp-content/uploads/2020/06/17062020_regierungsforschung.de_Bieber_Coronaapp.pdf (abgerufen am 23.6.2021).
- Blasimme, Alessandro/ Vayena, Effy (2020): What’s next for COVID-19 Apps? Governance and Oversight, in: Science, 370 (6518), S. 760–762, DOI: <https://dx.doi.org/10.1126/science.abd9006>.
- Bleich, Holger (2021): Luca first, Bedenken second: Pandemiebekämpfung mit lückenhafter Software, heise online, URL: <https://www.heise.de/news/Luca-first-Bedenken-second-Pandemiebekämpfung-mit-lueckenhafter-Software-6020201.html> (abgerufen am 19.5.2021).
- BMG (2020a): Dokumente zum Entwicklungsauftrag der „Corona-Warn-App“ durch SAP und Telekom, FragDenStaat, URL: <https://fragdenstaat.de/anfrage/dokumente-zum-entwicklungsauftrag-der-corona-warn-app-durch-sap-und-telekom/> (abgerufen am 25.11.2020).

- BMG (2020b): Corona-Warn-App: Bericht zur Weiterentwicklung, Bundesministerium für Gesundheit.
- BMG (2021): Coronavirus-Pandemie (SARS-CoV-2): Chronik bisheriger Maßnahmen und Ereignisse, Bundesgesundheitsministerium, URL: https://www.bundesgesundheitsministerium.de/coronavirus/chronik-coronavirus.html?fbclid=IwAR2hRYwFAn1GtFA9-kxaxvly77bzK4_hBgyj0PME-Vyn2LpqDneMFc1w5XxU (abgerufen am 23.6.2021).
- Bock, Kirsten/ Kühne, Christian Ricardo/ Mühlhoff, Rainer/ Ost, Měto R./ Pohle, Jörg/ Rehak, Rainer (2020): Das Verfahren geht weit über „die App“ hinaus – Datenschutzfragen von Corona-Tracing-Apps: Einführung in Datenschutz-Folgenabschätzungen als Mittel, gesellschaftliche Implikationen zu diskutieren, in: Informatik Spektrum, 43 (5), S. 334–338, DOI: <https://dx.doi.org/10.1007/s00287-020-01313-z>.
- Böhme, Michael (2020): micb25.github.io/dka, URL: <https://micb25.github.io/dka/> (abgerufen am 19.11.2020).
- Brack, Samuel/ Hofmann, Jeanette/ Reichert, Leonie/ Scheuermann, Björn (2020): Tracing-Technologien. Die Corona-App Ihres Vertrauens, netzpolitik.org, URL: <https://netzpolitik.org/2020/die-corona-app-ihres-vertrauens/> (abgerufen am 29.4.2020).
- Brüesch, Caroline/ Fischer, Damaris/ Lang, Achim (2020): Bevölkerungsumfrage in der Schweiz, Deutschland und Österreich zur nationalen Contact Tracing-App. Eine Studie des Instituts für Verwaltungs-Management der ZHAW, Winterthur: ZHAW School of Management and Law.
- Brühl, Jannis/ Hurtz, Simon (2021): Corona-Warn-App: Version 2.0 bringt Event-Registrierung, Süddeutsche.de, URL: <https://www.sueddeutsche.de/politik/corona-warn-app-event-registrierung-luca-1.5271436> (abgerufen am 24.5.2021).
- Bundesregierung (2020): Videoschaltkonferenz der Bundeskanzlerin mit den Regierungschefinnen und Regierungschefs der Länder am 16. November 2020, Bundesregierung, URL: <https://www.bundesregierung.de/resource/blob/997532/1811822/964c5e7487b051beee105d4c7554fbd6/2020-11-16-beschluss-mpk-data.pdf?download=1> (abgerufen am 19.11.2020).
- Bünthe, Oliver (2021): Corona-Warn-App 2.0 unterstützt Check-In-Funktion für Eventregistrierung, heise online, URL: <https://www.heise.de/news/Corona-Warn-App-2-0-unterstuetzt-Check-In-Funktion-fuer-Eventregistrierung-6023056.html> (abgerufen am 24.5.2021).
- CCC (2021): Luca-App: CCC fordert Bundesnotbremse, URL: <https://www.ccc.de/de/updates/2021/luca-app-ccc-fordert-bundesnotbremse> (abgerufen am 6.6.2021).
- Chan, Stephanie (2020): COVID-19 Contact Tracing Apps Reach 9% Adoption In Most Populous Countries, SensorTower, URL: <https://sensortower.com/blog/contact-tracing-app-adoption> (abgerufen am 23.6.2021).
- CISPA (2020): Contact Tracing App for the SARS-CoV-2 Pandemic. CISPA's Withdrawal from PEPP-PT and Ongoing Contribution to DP-3T, CISPA, URL: <https://cispa.de/en/news-and-events/news-archive/articles/2020/contact-tracing-app-for-the-sars-cov-2-pandemic> (abgerufen am 28.12.2020).
- D64/ LOAD/ Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung/ Gesellschaft für Informatik/ Chaos Computer Club/ Stiftung Datenschutz (2020): Offener Brief: Geplante Corona-App ist höchst problematisch, URL: https://www.ccc.de/system/uploads/300/original/Offener_Brief_Corona_App_BMG.pdf (abgerufen am 25.4.2020).
- Decker, Frank (2020): Die Demokratie im Zeichen der Coronakrise. Chance oder Bedrohung?, in: Zeitschrift für Politik, 67 (2), S. 123–132, DOI: <https://dx.doi.org/10.5771/0044-3360-2020-2-123>.
- Deloitte (2020): Smartphone-Nutzung am Limit? Der deutsche Mobile Consumer im Profil, Deloitte.
- Deutscher Bundestag (2020): Drittes Gesetz zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite, Bundesgesetzblatt Jahrgang 2020 Teil I 52, Bonn: Bundesanzeiger.

- DGB (2020): Corona-Virus / Covid 19. Corona Tracing App – Bundesregierung muss Vertrauen und Akzeptanz schaffen, Pressemitteilung 039, Berlin: DGB, URL: <https://www.dgb.de/presse/++co++7ef5dc68-af05-11ea-9948-52540088cada> (abgerufen am 2.9.2020).
- FAZ (2020a): Erinnerungsfunktion geplant. Nutzer der Corona-App sollen Testergebnisse häufiger teilen, in: FAZ.NET, 16. November 2020, URL: <https://www.faz.net/1.7055151> (abgerufen am 16.11.2020).
- FAZ (2020b): Corona-Sonderrechte. Union und SPD prüfen Verbot von Privilegien für Geimpfte, in: FAZ.NET, 29. Dezember 2020, URL: <https://www.faz.net/1.7122421> (abgerufen am 29.12.2020).
- GitHub (o. J.): Corona-Warn-App. The Official COVID-19 Exposure Notification App for Germany, GitHub, URL: <https://github.com/corona-warn-app> (abgerufen am 13.11.2020).
- Greis, Friedhelm (2020): Deutsche Telekom. Täglich 14 Millionen Server-Abfragen bei der Corona-Warn-App - Golem.de, golem.de, URL: <https://www.golem.de/news/deutsche-telekom-taeglich-14-millionen-server-abfragen-bei-der-corona-warn-app-2008-150526.html> (abgerufen am 19.11.2020).
- Heine, Hanna (2020a): Corona-Warn-App Version 1.7 kann die Risikoermittlung mehrmals täglich durchführen, Corona Warn-App Open Source Project, URL: <https://www.corona-warn.app/de/blog/2020-11-25-corona-warn-app-version-1-7/> (abgerufen am 30.12.2020).
- Heine, Hanna (2020b): Corona-Warn-App Version 1.9 greift auf Version 2 des Exposure Notification Framework zurück, Corona Warn-App Open Source Project, URL: <https://www.corona-warn.app/de/blog/2020-12-16-corona-warn-app-version-1-9/> (abgerufen am 30.12.2020).
- Heine, Hanna (2020c): Corona-Warn-App Version 1.10 mit Kontakt-Tagebuch ist da, Corona Warn-App Open Source Project, URL: <https://www.coronawarn.app/de/blog/2020-12-28-corona-warn-app-version-1-10/> (abgerufen am 30.12.2020).
- Heine, Hanna (2021a): Version 1.11: Corona-Warn-App nun mit Kennzahlen zum Infektionsgeschehen, URL: <https://www.coronawarn.app/de/blog/2021-01-28-corona-warn-app-version-1-11/> (abgerufen am 3.5.2021).
- Heine, Hanna (2021b): Corona-Warn-App Version 1.12 mit zwei Neuerungen, URL: <https://www.coronawarn.app/de/blog/2021-02-10-corona-warn-app-version-1-12/> (abgerufen am 3.5.2021).
- Heine, Hanna (2021c): Das Projektteam veröffentlicht Corona-Warn-App 2.0 mit Eventregistrierung, URL: <https://www.coronawarn.app/de/blog/2021-04-21-corona-warn-app-version-2-0/> (abgerufen am 3.5.2021).
- Heine, Hanna (2021d): Projektteam integriert Schnelltests in Corona-Warn-App Version 2.1, URL: <https://www.coronawarn.app/de/blog/2021-05-02-corona-warn-app-version-2-1/> (abgerufen am 3.5.2021).
- Hoerdt, Janina (2020a): Neue Funktionen: Corona-Warn-App Version 1.5 ist ab sofort zum Download verfügbar, Corona Warn-App Open Source Project, URL: <https://www.corona-warn.app/de/blog/2020-10-19-version-1-5/> (abgerufen am 30.12.2020).
- Hoerdt, Janina (2020b): Sicherheitsupdate für Corona-Warn-App-Server, Corona Warn-App, URL: <https://www.coronawarn.app/de/blog/2020-11-19-security-update/> (abgerufen am 19.11.2020).
- Hofmann, Jeanette (2020): Was von Corona-Apps übrig bleibt. Eine Infrastruktur-Perspektive, in: WZB-Mitteilungen, o.Jg. (168), S. 33–35.
- Kantar (2020): Corona Warn-App - KW 48/2020, Kantar, URL: docs.dpaq.de/17221-kantar_umfrage_corona-app.pdf (abgerufen am 30.12.2020).

- Kaya, Emre Kursat (2020): Safety and Privacy in the Time of COVID-19: Contact Tracing Applications, Cyber Governance and Digital Democracy 2020/05/EN, Centre for Economics and Foreign Policy Studies.
- Knieps, Franz (2020): Die Corona-Pandemie und das Grundgesetz – Anmerkungen nicht nur zu Rechtsfragen, in: Gesundheits- und Sozialpolitik, 74 (3), S. 6–10, DOI: <https://dx.doi.org/10.5771/1611-5821-2020-3-6>.
- Köver, Chris (2021): Neue Version der Corona-Warn-App. Einchecken per QR-Code, netzpolitik.org, URL: <https://netzpolitik.org/2021/neue-version-der-corona-warn-app-einchecken-per-qr-code/> (abgerufen am 24.5.2021).
- Krempf, Stefan (2020): Informatiker: Die Corona-App „ist wie ein trojanisches Pferd“, heise online,.
- Krempf, Stefan (2021a): Kontaktverfolgung: Zwei Drittel der Gesundheitsämter setzen auf Fax & Co., heise online, URL: <https://www.heise.de/news/Kontaktverfolgung-Zwei-Drittel-der-Gesundheitsaemter-setzen-auf-Fax-Co-5028143.html> (abgerufen am 6.6.2021).
- Krempf, Stefan (2021b): Kontaktverfolgung: Sormas bei 84 Prozent der Gesundheitsämter einsetzbar, heise online, URL: <https://www.heise.de/news/Kontaktverfolgung-Sormas-bei-84-Prozent-der-Gesundheitsaemter-einsetzbar-6020119.html> (abgerufen am 24.5.2021).
- Lasarov, Wassili (2020): Im Spannungsfeld zwischen Sicherheit und Freiheit: Eine Analyse zur Akzeptanz der Corona-Warn-App, in: HMD Praxis der Wirtschaftsinformatik, DOI: 10.1365/s40702-020-00646-3, DOI: <https://dx.doi.org/10.1365/s40702-020-00646-3>.
- Lessig, Lawrence (2006): Code. Version 2.0, 2. Aufl., New York: Basic Books.
- Lindern, Jakob von (2021): Pandemiebekämpfung. Jetzt hat's die Corona-Warn-App auch gecheckt, in: Die Zeit, Hamburg, 21. April 2021, URL: https://www.zeit.de/digital/2021-04/corona-warn-app-update-check-in-luca-faq?utm_referrer=https%3A%2F%2Fwww.google.com (abgerufen am 6.6.2021).
- Merkel, Wolfgang (2020): Das Virus und der Wettlauf der Systeme, in: Neue Gesellschaft/Frankfurter Hefte, 67 (5), S. 16–20.
- Moulinet, Noah (2020): TousAntiCovid a mieux démarré que StopCovid, Capital.fr, URL: <https://www.capital.fr/economie-politique/tousanticovid-a-mieux-demarre-que-stopcovid-1384555> (abgerufen am 28.12.2020).
- Muscato, Lindsay/ Ferguson, Cat (2020): Will you have to carry a vaccine passport on your phone?, Technology Review, URL: <https://www.technologyreview.com/2020/12/21/1015353/covid-vaccine-passport-digital-immunity-record/> (abgerufen am 4.1.2021).
- Nida-Rümelin, Julian/ Hilgendorf, Eric (2021): Unser Datenschutz verhindert eine wirksame Corona-Warn-App, Die Welt, URL: <https://www.welt.de/debatte/kommentare/plus224695267/Grundrechte-Unser-Datenschutz-verhindert-eine-wirksame-Corona-Warn-App.html> (abgerufen am 25.6.2021).
- Norton Rose Fulbright (2021): Contact Tracing Apps: A New World for Data Privacy, <https://www.nortonrosefulbright.com/en-tr/knowledge/publications/d7a9a296/contact-tracing-apps-a-new-world-for-data-privacy> (abgerufen am 23.6.2021).
- O. A. (2020): Joint Statement on Contact Tracing: Date 19th April 2020, URL: <https://drive.google.com/file/d/1OQg2dxPu-x-RZzETlpV3lFa259Nrpk1J/view> (abgerufen am 28.12.2020).
- O. A. (2021): Gemeinsame Stellungnahme zur digitalen Kontaktnachverfolgung, URL: <https://digikoletter.github.io/> (abgerufen am 6.6.2021).

- O’Neil, Patrick Howell/ Ryan-Mosley, Tate/ Johnson, Bobbie (2020): A Flood of Coronavirus Apps Are Tracking Us. Now It’s Time to Keep Track of Them., MIT Technology Review, URL: <https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/> (abgerufen am 6.6.2021).
- Owusu, Priscilla N. (2020): Digital Technology Applications for Contact Tracing: The New Promise for COVID-19 and Beyond?, in: Global Health Research and Policy, 5 (36), S. 3, DOI: <https://dx.doi.org/10.1186/s41256-020-00164-1>.
- Pfadenhauer, Katharina (2020): Kontaktnachverfolger spricht von „katastrophalen“ Zuständen, BR24, URL: <https://www.br.de/nachrichten/bayern/kontaktnachverfolger-spricht-von-katastrophalen-zustaenden,SHwKDp0> (abgerufen am 23.6.2021).
- Pfadenhauer, Katharina (2021): Gesundheitsämter: Teils ohne Leitung - und weiter am Limit, BR24, URL: <https://www.br.de/nachrichten/bayern/gesundheitsaemter-in-bayern-teils-ohne-leitung-und-weiter-am-limit,SX6Lc6O> (abgerufen am 23.6.2021).
- Pieper, Dietmar (2020): Corona und die Folgen. Keine Angst vor dem starken Staat, Spiegel Online, URL: <https://www.spiegel.de/politik/ausland/corona-folgen-keine-angst-vor-dem-starken-staat-a-345260a4-8cac-4570-8ff9-eed065d2e49c> (abgerufen am 5.4.2020).
- Reuter, Markus (2021): IT-Sicherheit. Schon wieder desaströse Sicherheitslücke in Luca App, netzpolitik.org, URL: <https://netzpolitik.org/2021/it-sicherheit-schon-wieder-desastroese-sicherheits-luecke-in-luca-app/> (abgerufen am 26.5.2021).
- RKI (2020a): Corona-Datenspende-App, RKI - Coronavirus SARS-CoV-2, URL: https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Corona-Datenspende-allgemein.html (abgerufen am 29.12.2020).
- RKI (2020b): So funktioniert die Corona-Warn-App im Detail, Berlin: Robert Koch-Institut.
- RKI (2020c): Kennzahlen zur Corona-Warn-App, Robert Koch Institut, URL: https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Archiv_Kennzahlen/Kennzahlen_18122020.pdf;jsessionid=3953683FA083073A28BF75E55D3E4417.inter-net092?__blob=publicationFile (abgerufen am 30.12.2020).
- RKI (2021a): Kennzahlen zur Corona-Warn-App, Robert Koch Institut, URL: https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Archiv_Kennzahlen/Kennzahlen_03062021.pdf?__blob=publicationFile (abgerufen am 5.6.2021).
- RKI (2021b): Robert Koch-Institut: COVID-19-Dashboard, URL: <https://experience.arcgis.com/experience/478220a4c454480e823b17327b2bf1d4> (abgerufen am 23.6.2021).
- Sartor, Stephanie (2020): Gesundheitsämter vor Kollaps: Können Corona-Kontakte noch verfolgt werden?, Augsburger Allgemeine, URL: <https://www.augsburger-allgemeine.de/bayern/Corona-Krise-Gesundheitsaemter-vor-Kollaps-Koennen-Corona-Kontakte-noch-verfolgt-werden-id58499121.html> (abgerufen am 23.6.2021).
- Schmidt, Jürgen/ Weiß, Eva-Maria (2021): Gefahr für Gesundheitsämter: Luca-App ermöglicht Code Injection, heise online, URL: <https://www.heise.de/news/Gefahr-fuer-Gesundheitsaemter-Luca-App-ermoeglicht-Code-Injection-6054744.html> (abgerufen am 6.6.2021).
- Schmidt, Martin/ Schneider, Tom (2020): Überlastete Gesundheitsämter: Nur noch die heiklen Fälle, tagesschau.de, URL: <https://www.tagesschau.de/inland/coronavirus-gesundheitsaemter-103.html> (abgerufen am 23.6.2021).
- StatCounter (2021): Mobile Operating System Market Share Germany, StatCounter Global Stats, URL: <https://gs.statcounter.com/os-market-share/mobile/germany/> (abgerufen am 28.6.2021).

- statista (2019): Anteil der Smartphone-Nutzer in Deutschland nach Altersgruppe im Jahr 2019, statista, URL: <https://de.statista.com/statistik/daten/studie/459963/umfrage/anteil-der-smartphone-nutzer-in-deutschland-nach-altersgruppe/> (abgerufen am 19.11.2020).
- Streeck, Wolfgang/ Thelen, Kathleen (2005): Introduction: Institutional Change in Advanced Political Economies, in: Streeck, Wolfgang/ Thelen, Kathleen (Hrsg.): Beyond continuity: institutional change in advanced political economies, Oxford: Oxford University Press, S. 1–39.
- The DP-3T Project (2020): Security and privacy analysis of the document „PEPP-PT: Data Protection and Information Security Architecture“, o. A.: The DP-3T Project.
- Ther, Philipp (2020): Wettbewerb der Systeme. Die Corona-Pandemie als Herausforderung für Demokratie und europäische Integration, in: Aus Politik und Zeitgeschichte, 70 (35–37), S. 40–45.
- Voss, Oliver (2020): Warum die Corona-Warn-App so viel kostet, Der Tagesspiegel, URL: <https://www.tagesspiegel.de/wirtschaft/69-millionen-euro-warum-die-corona-warn-app-so-viel-kostet/25929302.html> (abgerufen am 25.11.2020).
- Wilkens, Andreas (2021): Corona-Warn-App: Schnelltest-Ergebnisse jetzt eintragbar, heise online, URL: <https://www.heise.de/hintergrund/Corona-Warn-App-Schnelltest-Ergebnisse-jetzt-eintragbar-6034627.html> (abgerufen am 3.5.2021).