

Universität Stuttgart
Institut für Sozialwissenschaften
Seminar „Soziologie der Algorithmen“
Dr. Yana Boeva
Sommersemester 2021

Die soziale Konstruktion der Corona-Warn-App

Eine Analyse der soziotechnischen Assemblage

vorgelegt von:
Claire Elisabeth Kutterer
BA Sozialwissenschaften, 4. Fachsemester
Abgabe: 31.09.2021

Inhaltsverzeichnis

1. Einleitung	3
2. Literaturdiskussion.....	4
3. Entstehungskontext der CWA.....	5
3.1 Regulatorische Anforderungen.....	6
3.2 Debatte dezentrale vs. zentrale Datenspeicherung	7
3.3 Exposure Notification Framework	7
3.4 Beauftragung	9
3.5 Selbstverpflichtungen.....	9
4. Algorithmische Risikoberechnung.....	10
4.1 Input	10
4.2 Risikoberechnung	11
4.3 Anpassungen der Risikoberechnung und der CWA	11
5. Fazit	16
6. Literaturverzeichnis.....	18

1. Einleitung

Im Zuge der globalen Covid-19-Pandemie wurde schon früh Kontaktverfolgungs-Applikationen eine zentrale Bedeutung zugemessen. Verschiedene Staaten verfolgten dabei ganz unterschiedliche Konzepte der Datenspeicherung, rechtlichen Ausgestaltung und Risikoberechnung. Mancherorts wurden dabei GPS-Daten und Zwangs-Selfies zur Überprüfung der Quarantäneerhaltung genutzt, anderswo nur dezentral Begegnungen mittels Bluetooth registriert. Teils galt eine Warnmeldung als gleichbedeutend mit einer amtlich verordneten Quarantäne, teils nur als Empfehlung einen Corona-Test durchzuführen (*Süddeutsche Zeitung* 2020). In Deutschland erschien am 16. April 2020 mit der Corona-Warn-App (im Folgenden kurz: CWA) eine von der Bundesregierung in Auftrag gegebene und finanzierte App zur digitalen Kontaktnachverfolgung (Greef 2021, S. 4). Diese war trotz ihres datensparsamen, dezentralen und quelloffenen Ansatzes häufig in der Kritik und ihre Entwicklung wurde medial intensiv verfolgt.

Die Risikoberechnung erfolgt bei der CWA mittels eines algorithmischen Systems, das auf Basis einiger Parameter einen individuellen Risikoscore ermittelt. Sie ist ein Beispiel dafür wie zunehmend Entscheidungen in verschiedensten Lebensbereichen mithilfe komplexer algorithmischer Systeme getroffen werden (Tufekci 2015, S. 217). Die Entscheidungen können dabei nicht als objektiv und rational betrachtet werden, sondern sind Ergebnis eines kaum verständlichen Zusammenspiels von Datensätzen und Code. Betrachtet man algorithmische Systeme aus einer soziologischen Perspektive, so werden auch oft Institutionen, menschliche sowie nicht-menschliche Akteure oder Diskurse als zentrale Einflussfaktoren oder gar Bestandteile von Algorithmen betrachtet (Seaver 2019, 414ff). Die vorliegende Arbeit möchte aus eben diesem Blickwinkel die soziale Situiertheit der CWA verdeutlichen und diese als soziotechnische Assemblage untersuchen. Um das Zusammenspiel von Akteur*innen aus Politik, Zivilgesellschaft, Wissenschaft, Wirtschaft und der Internet-Community mit dem entstehenden Code zu analysieren, soll insbesondere ein Blick auf Diskurse geworfen werden. Dabei stellt sich die Frage, inwiefern diese sich in das algorithmische System der CWA eingeschrieben haben und wie mächtig der Einfluss welcher Akteure war.

In einem ersten Schritt sollen hierfür einige theoretische Ansätze zu algorithmischen Systemen kurz diskutiert und die dieser Untersuchung zugrundeliegende Methodik begründet werden. Zweitens soll der regulatorische, politische, wirtschaftliche und gesellschaftliche Entstehungskontext der CWA erläutert werden. Daran anschlie-

Bend wird ein Blick auf die algorithmische Risikoberechnung und Anpassungen der App geworfen und ihre jeweilige soziale Einbettung untersucht. Die Arbeit endet mit einer Zusammenfassung der zentralen Ergebnisse und deren Grenzen.

2. Literaturdiskussion

Ein Algorithmus kann als definierte Abfolge rechnerischer Schritte verstanden werden, die einen Input an Werten in einen Output in Form von Werten transformiert (Seaver 2019, S. 412). Dazu muss die zu lösende Frage als mathematisches Problem formuliert werden und die nach spezifischen Eingaben gelieferte Lösung anschließend auf die anfängliche Fragestellung hin interpretiert werden (Algorithm-Watch 2016). Solch eine enge, technische Definition darf nicht darüber hinweg täuschen, dass algorithmische Systeme Ergebnis der Zusammenarbeit vieler Personen sind und meist so komplex, dass auch Insider ihre Outputs oft nicht erklären können (Seaver 2019, 417ff). Darüber hinaus werden sie immer aufbauend auf bestimmten Sichtweisen der sozialen Welt und auf bereits antizipierten Outcomes entwickelt. Sie entstehen folglich aus der sozialen Welt heraus und werden ebenso Teil von ihr, sind in Handlungen und Folgen verwoben. Nicht nur Schaffung und Design algorithmischer Systeme, sondern auch ihre Implementation und laufende Anpassung beziehungsweise Nachjustierung können also als Folge sozialer Kräfte verstanden werden (Beer 2017, 4). Dementsprechend betrachtet Seaver algorithmische Systeme als soziale Konstruktionen, an denen wir auch als Outsider teilhaben. Sie bestehen nicht lediglich aus Code, sondern sind dynamische Arrangements, von denen Code nur ein kleiner Teil ist neben Personen, Hardware, Institutionen oder diskursiven Konstruktionen (Seaver 2019, 413, 419f). In diesem Sinne bietet sich zu ihrer Untersuchung methodisch die Situationsanalyse nach Adele Clarke an. Mithilfe der Mapping-Prozesse, die sie darlegt, lassen sich die Beziehungen zwischen verschiedensten, in einer Situation befindlichen und bedeutsamen Elemente untersuchen (Clarke 2012, 123ff).

Beer betont die Relevanz der sozialen Macht von Algorithmen, wofür verbreitete Vorstellungen über den Algorithmus analysiert werden sollen und wie diese in Diskursen entworfen werden (Beer 2017, 9f). Auch hierfür bietet Clarke, die eine Einbeziehung der Diskursanalyse in die Situationsanalyse verfolgt, hilfreiche methodische Ansätze (Clarke 2012, 183ff). Diskurse sind deshalb in den Blick zu nehmen, weil sie nicht nur eine Form sozialen Handelns darstellen, sondern auch auf soziale Ordnung zurückwirken. Mit Foucault und Prior wird deshalb der Fokus der qualitativen Forschung vom wissenden Subjekt hin zu diskursiver Praxis verschoben (Clar-

ke 2012, S. 185). Die für dieses Thema relevante Form der Diskursanalyse ist aushandlungszentriert und untersucht wie Diskurse in soziales Handeln, also beispielsweise die Entwicklung der CWA, eingehen, wobei auch der Machtaspekt nicht zu vernachlässigen ist (Clarke 2012, 192f, 212f).

Ziel der Hausarbeit soll sein den sozialen, ökonomischen, politischen, regulatorischen und institutionellen Kontext zu untersuchen, in dem die CWA entwickelt wurde und bis heute laufend weiterentwickelt und angepasst wird. Hierbei muss herausgestellt werden, dass der Kontext aktiv an der Schaffung algorithmischer Systeme beteiligt ist und diese nicht nur umgibt: „cultural“ details *are* technical details“ (Seaver 2019, S. 419). Neben einer Betrachtung des Quellcodes, soll also die Methode in einer Analyse der soziotechnischen Assemblage der CWA bestehen, um das algorithmische System nicht von derselben zu dekontextualisieren (Kitchen 2017, 22f, 25). Hierzu sollen als Forschungsmaterial neben den GitHub Repositorien und Updates der CWA, Veröffentlichungen beteiligter Akteure sowie Medienberichte dienen, die sodann mit Literatur aus dem Bereich der *Critical Algorithm Studies* verknüpft werden.

Während gemessen an ihrem jungen Alter schon sehr viele wissenschaftliche Publikationen zur CWA existieren, scheint die Frage der Genese und sozialen Situiertheit des Entstehungsprozesses noch kaum gestellt zu werden (Greef 2021). Neben datenschutzrechtlichen Beurteilungen (Dix 2020) oder Effektivitätsabwägungen (Braun et al. 2020) finden sich vor allem zahlreiche Untersuchungen zu Nutzung beziehungsweise Nicht-Nutzung der App, Wahrnehmung, Bedenken oder Popularität dieser (Horstmann et al. 2021; Becker et al. 2020; Meyer et al. 2020; Urban 2021; Munzert et al. 2021). Eine Forschungslücke liegt also insofern vor, dass keine Arbeit bislang den Fokus auf das algorithmische System legt oder die soziale Konstruktion der CWA nachzuverfolgen versucht.

3. Entstehungskontext der CWA

Bevor die Funktionsweise des algorithmischen Systems der Risikoberechnung sowie dessen schrittweise Anpassung dargestellt werden kann, soll zuerst der Kontext der Entstehung der Applikation erläutert werden und die zentralen Akteure und nicht-menschlichen Aktanten vorgestellt werden. Dieser Teil führt von den rechtlichen Vorbedingungen bis hin zu Selbstverpflichtungen des Entwickler*innenteams und bietet somit auch eine abrisshafte chronologische Nachzeichnung der Entwicklungsgeschichte.

3.1 Regulatorische Anforderungen

Zunächst soll das algorithmische System der CWA als regulatorisches Objekt betrachtet werden, wobei hervorgehoben werden muss, dass Regulierungen Algorithmen nicht nur beschränken, sondern formen und als diskursive Konstruktionen zusammen mit anderen Akteuren koproduzieren (Seyfert 2021, 1f; Clarke 2012, S. 128). Die Bundesregierung verweist darauf, dass die Nutzung der CWA freiwillig erfolgt, da ein Nutzungszwang der Datenschutz-Grundverordnung (im Folgenden kurz: DSGVO) widerspreche (Bundesregierung 2021). Ein explizites Gesetz zur App-Nutzung wurde vom Sachverständigenrat für Verbraucherfragen und Politiker*innen der Grünen und der Linken zwar gefordert, von Bundesjustizministerin Lambrecht jedoch für überflüssig gehalten (tagesschau 2020). Die CWA soll den Standards der DSGVO entsprechen (GitHub 2020b), ist also auch europäischem Recht unterworfen, was dem Individuum weitgehende Rechte und Autorität über Aspekte der Datensammlung, -speicherung und -verarbeitung garantiert. Laut Seyfert können verschiedene Definitionen des Objekts Algorithmus zu verschiedenen Regulierungen führen, welche wiederum auf die Produktion algorithmischer Objekte einwirken (Seyfert 2021, 10ff). Ihm zufolge verfolgt die DSGVO einen essentialistischen Ansatz, sie fokussiert sich auf präzise Äußerungen im Code und betrachtet diesen als den Kern eines Algorithmus. Damit ist der Zugang durch Veröffentlichung des Quellcodes, welcher idealiter verständlich und erklärbar sein sollte, also nicht grundsätzlich als opak verstanden wird (Seyfert 2021, 2ff). Somit könnte argumentiert werden, dass die DSGVO an der Ko-Produktion von im Sinne der *digital literacy* verständlichen Algorithmen beteiligt ist, wie im Falle der CWA.

Darüber hinaus wurde die CWA noch durch eine EntschlieÙung des EU-Parlaments im April 2020 mitgeformt. Diese forderte, dass eine Nutzung entwickelter Anwendungen nicht verpflichtend sein dürfe, die gesamte Datenspeicherung dezentral erfolgen solle und eine Identifikation des Smartphones durch eine Verschlüsselung der Tagesschlüssel verhindert werde. Außerdem wird explizit uneingeschränkte Transparenz in Bezug auf die Funktionsweise der Apps verlangt, bis hin zur Offenlegung des Quellcodes (Europäisches Parlament 2020). In diesem Lichte erscheint die vielfach gelobte Entscheidung, der durch die Bundesregierung mit der Entwicklung der CWA beauftragten Institutionen, den gesamten Quellcode sowie die Softwarearchitektur auf GitHub offenzulegen wenig überraschend. Dabei kann davon ausgegangen werden, dass sich auch diese regulatorische EntschlieÙung in das algorithmische System einschrieb, beispielsweise in dem sich die Entwickler*innen

aufgrund der Quelloffenheit mit höheren Erwartungen an Verständlichkeit des Codes, Strukturiertheit der Repositorien und Erklärbarkeit konfrontiert sahen.

3.2 Debatte dezentrale vs. zentrale Datenspeicherung

Ausgangspunkt für eine öffentliche Debatte um das Modell der Datenspeicherung lieferte die multinationale Initiative PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing), die mit der Methode des Server-Side-Matchings auf einen zentralen Ansatz setzte und anfangs von deutschen Politiker*innen unterstützt wurde. Ein projektinterner Konflikt über die mangelnde Datenschutzfreundlichkeit dieser Lösung gipfelte am 19. April 2020 in einem offenen Brief 300 renommierter Expert*innen zugunsten eines dezentralen Ansatzes, dem Verlassen der Initiative durch einige Mitglieder und der Gründung des DP-3T-Konsortiums (Greef 2021, 8ff; Fraunhofer AISEC 2020). Ebenfalls im April veröffentlichten zivilgesellschaftliche Akteure ein gemeinsames Statement in dem sie eine Reihe von Forderungen an Kontaktverfolgungsapplikationen im Sinne der Menschenrechte aufstellten (Amnesty International 2020). Zum Ende des Monats hin verfassten deutsche Organisationen wie D64, LOAD oder der Chaos Computer Club (im Folgenden kurz: CCC) einen offenen Brief an die Bundesregierung und forderten eine quelloffen programmierte App mit transparentem Konzept und dezentraler Datenspeicherung (Greef 2021, S. 9).

3.3 Exposure Notification Framework

Für die anschließende Entscheidung der Bundesregierung zugunsten eines dezentralen Ansatzes wird das Engagement dieser zahlreichen Akteure aus Zivilgesellschaft, Wissenschaft und Politik jedoch weniger ausschlaggebend gewesen sein. Entscheidend war vielmehr die Entwicklung des Exposure Notification Frameworks (im Folgenden kurz: ENF) durch Google und Apple, das in seinem dezentralen Ansatz dem Protokoll des DP-3T-Konsortiums ähnelt und im Mai 2020 direkt in die jeweiligen Betriebssysteme implementiert wurde (Dix 2020, 780f). Hier wird deutlich weshalb es in soziologischen Analysen gilt, den technologischen Determinismus zu überwinden. Hinter Technologien wie der CWA stecken menschliche, institutionelle, politische oder wirtschaftliche Entscheidungen und nicht allein die Abwägung nach abstrakten technischen Gesichtspunkten (Gillespie 2014, S. 169). Da nur zum ENF passende Apps im Hintergrund laufen und auf die Bluetooth-Schnittstelle zugreifen können, waren Alternativen schwer umsetzbar und höchst impraktikabel, sie hätten immer im Vordergrund ausgeführt werden müssen. Mit einem gemeinsamen Marktanteil von 99% in Deutschland bestimmten Google und Apple so den Gestaltungs-

spielraum und wiesen die Politik in ihre Schranken. Deutlich greift hier Lessigs Gesetzmäßigkeit „Code is law“ (Greef 2021, 10f; Apple und Google 2020, 5ff). Dass durch die Nutzung des ENF zusätzliche personenbezogene Daten, wie beispielsweise die IP-Adresse der Nutzenden, an Google fließen und sich die Firma dazu nicht äußert, verstößt gegen die DSGVO, hatte aber bislang keine Folgen (Dix 2020, 781ff). Nutzenden wird lediglich die Wahl geboten auf ihre Rechte zu verzichten oder Services wie das ENF gar nicht zu nutzen, was bei der Marktmacht von Google und Apple und in Ermangelung gleichwertiger Alternativen einer Erpressung nahe kommt (Seyfert 2021, S. 13). Die Software-Beschränkung durch die beiden Tech-Konzerne ist praktisch unumkehrbar, denn Algorithmen sind hoch dependente Objekte, die nur in entsprechenden bereitgestellten Umwelten aus Hard- und Software, Servern, Stromnetzen etc. existieren können (Seyfert 2021, 4f). Google legte zwar einzelne Teile des Quellcodes des ENF frei, jedoch kann in solchen Fällen auch Transparenz kaum helfen, denn aktuelle Machtasymmetrien bleiben bestehen mangelt es derart an Alternativen (Crawford und Joler 2018, XVII). Nach Burrell liegt hier Opazität im Sinne eines beabsichtigten Unternehmensgeheimnisses vor, oder nach Pasquale im Sinne einer intendierten, grundsätzlich behebbaren Unverständlichkeit des Codes. Dabei könnte gar vermutet werden, dass der Code absichtlich opak gehalten wird um Regulierungen zu umgehen (Burrell 2016, 3f; Pasquale 2015b, S. 2). Das algorithmische System der CWA selbst ist jedoch höchstens opak aufgrund der *technical illiteracy* des Großteils der Bevölkerung (Burrell 2016, 5), wobei dem durch Erläuterungen des Codes und dessen Funktionsweise entgegen gearbeitet wird (GitHub 2021d). Dem nicht technikversierten Teil der Öffentlichkeit ist der Zugang zu Diskursen rund um die CWA trotzdem deutlich erschwert oder gar verwehrt, er kann nach Clarke als stummer Akteur betrachtet werden (Clarke 2012, 126ff).

In einer Situationsmap nach Clarke zeigt sich deutlich welche Machtkonstellationen in der Situation der CWA-Entwicklung zwischen den Akteuren vorliegen. Clarke zufolge sollten möglichst alle vorhandenen, auch die weniger mächtigen und laustarken Diskurse in einer Situationsanalyse abgebildet werden, anders als bei Foucault, dessen Aufmerksamkeit dem Diskurs der Mächtigen gilt (Clarke 2012, 212ff). Dies kann im Rahmen dieser Arbeit natürlich nicht ausreichend geschehen, doch es wurde deutlich, dass weniger mächtige Diskurse aus Zivilgesellschaft oder Wissenschaft hinter dem Einfluss der Festlegung Google und Apples ihre Betriebssysteme einem dezentralen Ansatz anzupassen zurücktraten. Von offizieller Seite her jedoch wird die „wissenschaftliche Debatte [...] unter dem Schlagwort „zentrale

vs. dezentrale Speicherung““ als ausschlaggebend genannt und nicht das Quasimonopol der Betriebssysteme IOS und Android (CWA 2020).

3.4 Auftragsvergabe

Für den Entstehungskontext außerdem wichtig ist die Beauftragung der Telekom und SAP mit der Entwicklung, dem Betrieb und der Wartung der CWA durch das RKI als Vertretung der Bundesregierung. Dies erfolgte laut Bundesgesundheitsministerium ohne öffentliche Ausschreibung „nach Feststellung der Dringlichkeit der Beschaffung [...] im Wege einer Verhandlungsvergabe ohne Teilnahmewettbewerb“, was „aufgrund der Unvorhersehbarkeit der Corona-Pandemie sowie zwingender epidemiologischer Erwägungen im Hinblick auf die Pandemiebekämpfung geboten“ war (BMG 2020). Passend hierzu bemerkt Beer, dass die Diskurse, die algorithmische Systeme umgeben oft etwas über die größeren politischen Dynamiken von denen diese Teil sind verraten. Nehmen wir Algorithmen in den Blick sollten wir laut ihm fragen, welche Versprechen und Ideale auf sie projiziert werden (Beer 2017, 9ff). Hier könnte man beispielsweise vermuten, dass die Vorstellung eines algorithmischen Systems als präziser und objektiver Entscheider, gepaart mit dem Krisenmodus in dem sich die Bundesregierung im Frühjahr 2020 befand, die eilige Beauftragung beeinflussten. Darüber hinaus könnte man auch von einer Beauftragung des algorithmischen Systems selbst mit der Beurteilung von Infektionsrisiken bei Begegnungen sprechen. Algorithmen können aufbauend auf der Prinzipal-Agent-Theorie als Agenten konzeptualisiert werden, die in der Welt ausgestattet mit *agency* handeln. Delegationsketten gestalten sich auch deshalb bei Algorithmen schwieriger, weil deren Arbeit unsichtbar und durch das Zusammenspiel des Codes mit riesigen Datensätzen veränderlich ist (Tufekci 2015, 207ff).

3.5 Selbstverpflichtungen

Schließlich muss bei einer Analyse der soziotechnischen Assemblage auch ein Blick auf diskursive Konstruktionen geworfen werden, die sich ebenso in das algorithmische System einschreiben können. Hier wären zum einen die Prüfsteine für die Beurteilung von „Contact Tracing“-Apps des CCC zu nennen, deren technischen Anforderungen sich das Entwickler*innenteam der CWA im Juli verpflichtete und eigens darlegte inwiefern diese erfüllt werden (GitHub 2020c). Ein zentraler Prüfstein und ebenso Vorschrift der DSGVO ist die Datensparsamkeit, beziehungsweise das Konzept der *Privacy by Design*, was sich bei Betrachtung des Quellcodes deutlich zeigt. Der Input besteht nur aus wenigen, unbedingt notwendigen Parametern, welche im Folgenden noch erläutert werden (GitHub 2021c). Des Weiteren verpflichtete sich das Entwickler*innenteam der CWA dem von Coraline Ada Ehmke

entwickelten Verhaltenskodex *Contributor Covenant*, der eine diskriminierungsfreie Zusammenarbeit an Open-Source-Projekten ermöglichen soll (GitHub 2020a). Auch solch banal erscheinenden nicht-technischen Details, kann eine Ko-Produktion des algorithmischen Systems nachgewiesen werden. So kann zu Beispiel das Umbenennen des *master branch* in *main branch* (GitHub 2020d), zum Zwecke einer Befreiung der Sprache von rassistisch aufgeladenen Begriffen, mitunter als Konsequenz der Verpflichtung zum *Contributor Covenant* interpretiert werden. Dies wirkt sich zwar nicht auf den Code an sich aus, zumindest aber auf alle Pfade zu Codestücken und erschwert damit die Zurückverfolgung der Entwicklung des Risikoberechnungsalgorithmus.

Nach diesem Blick auf die CWA konstruierende Diskurse und menschliche, sowie nicht-menschliche Akteure, wird deutlich, dass sogenannte Kontextfaktoren viel eher Teil des algorithmischen Systems sind als bloße Umwelt. Was sich im Umfeld eines Algorithmus befindet, Teil der Situation ist, wird sich in ihn einschreiben (Seaver 2019, S. 419). All jene obig genannten Elemente der Situation - und neben ihnen noch viele weitere, die hier den Rahmen sprengen würden - sind Teil der soziotechnischen Assemblage des algorithmischen Systems, schreiben sich in dasselbe ein und koproduzieren es demnach entsprechend ihrer Vorstellung der sozialen Welt (Beer 2017, 3ff).

4. Algorithmische Risikoberechnung

Der algorithmische Teil der CWA besteht in der Risikoberechnung, welche dezentral auf dem jeweiligen Smartphone stattfindet. Dafür wird ein Input mittels einer definierten Abfolge rechnerischer Schritte in einen Output transformiert (Seaver 2019, S. 412), welcher in Form eines einzelnen Wertes vorliegt, der schließlich entscheidet ob und welche Warnmeldung den Nutzenden erscheint. Im Folgenden soll ein Blick auf eben diesen Input, die Berechnungsmethode und schließlich auf Updates an der Risikoermittlung und der CWA als Ganzem geworfen werden.

4.1 Input

Die CWA generiert auf dem Smartphone des Nutzenden zwei Zufallscodes: einen Geräteschlüssel, der alle 24h neu erzeugt wird und eine Bluetooth-ID, die der Begegnungsaufzeichnung dient und alle 10-15min wechselt (Dix 2020, S. 779). Wird eine Person positiv auf SARS-CoV-2 getestet und entscheidet sich zum Teilen dieses Ergebnisses mittels der CWA, so werden bis zu 15 Positivkennungen (also ma-

ximal für 2 vergangene Wochen) auf den CWA-Server hochgeladen. Jedes andere Smartphone mit CWA lädt täglich alle Positivkennungen von diesem Server herunter. Der Input für die Risikoberechnung besteht bei dieser Methode zum ersten aus einem Übertragungsrisikowert, der jeder Positivkennung angehängt ist und den Abstand des jeweiligen Tages zum Datum des Upload des Tests angibt. Zweitens aus dem Verzugsrisikowert, der die Tage seit der letzten Begegnung mit der positiv getesteten Person zählt. Drittens aus der Entfernung der Smartphones zueinander, die mittels der ausgetauschten Bluetooth-IDs aus der Dämpfung des Bluetooth-Signals errechnet wird. Viertens aus einer Schätzung der Begegnungsdauer, die ebenfalls auf den ausgetauschten Bluetooth-IDs beruht (GitHub 2021d). Und fünftens fließt seit Update 1.5 die Art der Symptome und der Beginn dieser in die genauere Erfassung des Infektionsrisikos einer Begegnung ein, wobei diese Angaben freiwillig sind und so nicht Teil jeder algorithmischen Risikoberechnung (Hoerdt 2020).

4.2 Risikoberechnung

Passen die von einem Smartphone in den letzten 14 Tagen empfangenen und aufgezeichneten Zufallscodes zu einer vom CWA-Server heruntergeladenen Positivkennung, so findet auf dem Gerät eine Schätzung der Dauer und Entfernung der jeweiligen Risikobegegnungen statt. Unbedenkliche Begegnungen werden daraufhin verworfen, während bei nicht unbedenklichen für jede Begegnungsmenge ein Begegnungsrisiko aus obig erwähntem Übertragungsrisikowert und Verzugsrisikowert errechnet wird. Alle Begegnungen die dabei einen Grenzwert (*Minimum Risk Score*) unterschreiten werden wiederum verworfen, die verbliebenen werden als Risikobegegnungen angesehen. Für sie wird die jeweilige Zeit in min mit einem Faktor verrechnet, der je nach Dämpfung des Bluetooth-Signals, also Abstand der Smartphones anders ausfällt. Die so errechnete Gesamtzeit aller Risikobegegnungen wird schließlich mit dem Begegnungsrisiko der Begegnung mit dem höchsten Risiko in den letzten 14 Tagen verrechnet, wodurch sich die Gesamtzeit in min noch einmal deutlich verlängern oder verkürzen kann. Die so errechneten normalisierten Begegnungszeiten werden sodann aufsummiert. Die Summe dieser Kontaktzeiten stellt den Output des algorithmischen Systems dar, anhand dessen der endgültige Risikostatus bestimmt wird. Dies geschieht mittels definierter Schwellenwerte, die in unterschiedlichen Warnmeldungen an die Nutzenden resultieren (GitHub 2021d).

4.3 Anpassungen der Risikoberechnung und der CWA

Abschließend sollen nun relevante Updates an der CWA sowie Anpassungen der algorithmischen Risikoberechnung vorgestellt werden und mit einschlägiger Literatur

zu algorithmischen Systemen verknüpft werden. Zur besseren Nachvollziehbarkeit wird diese Darstellung chronologisch erfolgen. Dabei soll jeweils die soziale Situiertheit der Anpassungen verdeutlicht werden, wobei sich wiederum die Frage der Machtasymmetrien stellt.

Mit Update 1.5 wurde im September 2020 die Symptomerfassung in die CWA implementiert und etwaige Angaben wurden als Parameter Teil der algorithmischen Risikoberechnung (Hoerd 2020). Dies kann als Folge des steigenden Kenntnisstandes zu Symptomen und dem mit ihnen verbundenen Übertragungsrisiko verstanden werden, der unter anderem auch durch die Datenspende-App des RKI zunahm (RKI 2020). Die Symptomerfassung kann als Beispiel dafür gelten wie menschliche Körper zunehmend als Datenbanken betrachtet werden, deren Untersuchung oder Überwachung Nutzen bringen kann. Digitale Technologien erlauben es uns Details über unseren Körper zu dokumentieren, wobei das *data sense-making* in diesem Falle durch das algorithmische System der CWA und nicht durch Menschen geschieht (Lupton 2018, 2f). Außerdem unterstützte die Version 1.5 das europäische Corona-App-Gateway, wodurch nun länderübergreifend Zufallscodes ausgetauscht werden konnten, was den Input in das algorithmische System, zumindest quantitativ veränderte. Der Entwicklung dieses Gateways lag vermutlich die Empfehlung der EU-Kommission „ein gemeinsames Konzept der EU für die Nutzung solcher Anwendungen zu entwickeln“ zugrunde (Europäisches Parlament 2020). Doch auch ein gewisser Einfluss der Open-Source-Community auf GitHub kann attestiert werden, da deren Feedback bezüglich der Verständlichkeit der App-Texte in eine Verbesserung dieser einfluss (Hoerd 2020).

Eine weitere quantitative Erhöhung des Inputs konnte durch den Einbau von Erinnerungen das Testergebnis zu teilen mit Update 1.7 erreicht werden, in Folge dessen sich die Meldequote positiver Tests erhöhte. Hier zeigt sich inwiefern Algorithmen, die unser Verhalten tracken es durch *nudging* (hier in Form von Pop-up-Erinnerungen) auch in eine bestimmte, gewollte Richtung lenken können (Benjamin 2019, S. 71). Außerdem ermöglichte dieses Update, dass der Abruf der Positivkennungen vom CWA-Server und damit auch die Risikoermittlung nun sechsmal täglich statt einmal täglich möglich waren (Heine 2020b). Man könnte vermuten, dass dies unter anderem eine Reaktion auf die aktive Nutzung der App darstellte. Die Mehrheit der Nutzenden öffneten diese mehrmals täglich oder wöchentlich, insbesondere um den eigenen Risikostatus zu checken oder um das Funktionieren sicherzustellen (Meyer et al. 2020, 8ff). Eine häufigere serverseitige Aktualisierung des Risikostatus könnte eben hierbei ein positives und beruhigendes Gefühl vermit-

teln. Hier zeigt sich, wie die Berechnungen des algorithmischen Systems in das Leben der Menschen einfließen und bestimmen was diese wann erfahren. Algorithmen üben dabei Macht aus indem sie ordnen und klassifizieren und indem sie entscheiden wann etwas sichtbar ist (Beer 2017, 6f). Technologien wie die CWA verhalten sich dabei nicht nur instrumentell sondern auch konstitutiv gegenüber unseren Zwecken und Zielen und formen was wir denken (Pasquale 2015a, 34f). Den Risikostatus mehrmals täglich zu checken ist ein Bedürfnis, das erst durch die Existenz der App konstruiert wird. Ebenso ist eine erhöhte Vorsicht und Einhaltung der Hygienemaßnahmen bei gewarnten Nutzer*innen zu erwarten. Pasquale spricht hier davon, dass Technologien nicht nur überwachen und voraussagen, sondern dadurch auch kontrollieren und unser zukünftiges Verhalten beeinflussen (Pasquale 2015a, 36ff). Nach Bowker und Leigh kommt es zu Kategorien wie den Risikostatus, wenn sich verschiedene Gruppen über die Beschaffenheit eines Klassifikationssystems streiten. Sie entstehen somit aus organisierter Tätigkeit und Konflikten um Bedeutung (Bowker und Star 2017, 1ff), wie diese sicherlich auch in der Zusammenarbeit von SAP, RKI, dem Fraunhofer-Institut, dem Bundesgesundheitsministerium und vielen weiteren Akteuren stattfanden. Die Entscheidung für drei Risikokategorien (erhöhtes, moderates oder kein Risiko) ist somit als Ergebnis eines Prozesses zu betrachten, der auch viele andere Klassifikationssysteme hätte hervorbringen können, was schon bei einem Blick über die deutschen Grenzen hinweg deutlich wird. Für die Akzeptanz der Klassifikationen von Warn-Apps sind laut Dehmel Transparenz bezüglich der Berechnung der Scores sowie Freiwilligkeit, also die Möglichkeit dem Score ausweichen zu können notwendig (DEHMEL et al. 2020, S. 10). Beides ist bei der CWA vollends erfüllt.

Mit Update 1.9 wurde erstmals die algorithmische Risikoberechnung angepasst. Mehrere Begegnungen niedrigen Risikos konnten nun zu einer Einstufung erhöhten Risikos führen. Für die Risikobewertung war fortan die Summe der Risikominuten eines Tages anstelle einer einzelnen Begegnung ausschlaggebend (Heine 2020c). Die Klassifizierung durch das algorithmische System wurde somit genauer. Positiv Getestete mit sehr kurzer Kontaktdauer wurden davor gezählt und als Begegnungen niedrigen Risikos angezeigt, wohingegen von nun an solche, aus epidemiologischer Sicht nicht relevante Begegnungen herausgefiltert wurden (CWA 2020). Während unter Version 1 des ENF die durchschnittlichen Werte der Bluetooth-Signaldämpfung für alle Begegnungen mit einem Gerät an einem Tag als Daten der Risikoberechnung zugrunde lagen, erfolgte nun eine Betrachtung von 30 minütigen Zeitfenstern. Um berücksichtigt zu werden musste ein Zeitfenster fortan folgende Kriterien erfüllen: mindestens 10 der 30min muss die Signaldämpfung unter 73dB liegen und

das Begegnungsrisiko muss mindestens III betragen (Heine 2020d; CWA 2020; GitHub 2021a, 2021c). Diese Verfeinerung des Algorithmus scheint aber nicht lediglich in neuen wissenschaftlichen Diskursen begründet zu liegen, sondern maßgeblich in der Einführung der Version 2 des ENF durch Google und Apple. Bei der Entwicklung und fortlaufenden Anpassung eines Algorithmus finden fortwährend komplexe Verhandlungen zwischen verschiedenen Gruppen, Strukturen, Institutionen und dem algorithmischen System selbst statt (Crawford 2016, 82ff). So kann auch hier von Aushandlungen zwischen den großen wirtschaftlichen Betreibern der Systeme IOS und Android und dem RKI und der SAP andererseits ausgegangen werden, wobei jeweils aufeinander reagiert werden muss. In diesem Fall war eine Reaktion des CWA-Entwickler*innenteams auf eine neue Version der zugrundeliegenden Schnittstelle erforderlich und bestand in einer Systemanpassung. Anders als bei der Entscheidung für den dezentralen Ansatz wurde dieses Mal jedoch das ENF von offizieller Seite aus als ausschlaggebend genannt und die Weiterentwicklung als Ergebnis einer produktiven Zusammenarbeit positiv geframet (Heine 2020c). Die Macht von Google zeigte sich außerdem im Januar 2021 als nach Bekanntwerden von Problemen der Risikoermittlung auf Android-Smartphones Google den Fehler innerhalb eines Tages behob und dafür alle betroffenen Geräte eigenmächtig ohne die Nutzenden aktualisierte (Heine 2021f).

Mit den darauffolgenden Updates wurden der CWA Statistiken und Kennzahlen zum Infektionsgeschehen, ein Kontakttagebuch für Personen- und Ortseinträge sowie eine Begegnungshistorie für das Tagebuch hinzugefügt (Heine 2021i, 2020a). Diese Anpassungen können zum einen als Reaktion auf das Feedback und Wünsche von Nutzenden verstanden werden (Heine 2021a), zum anderen als Maßnahme „um stärkere Anreize für die freiwillige Nutzung zu setzen und damit die Effektivität der App im Sinne des Ziels einer effizienten Kontaktnachverfolgung zu erhöhen“ (Greef 2021, S. 12). Dabei folgt die CWA Erkenntnissen der Technikakzeptanzforschung, die die Relevanz der Darstellung, Kommunikation und Gewährleistung einer hohen wahrgenommenen Nützlichkeit und Bedienungsfreundlichkeit herausstellt (DEHMEL et al. 2020, 21f).

Eine Weiterentwicklung der algorithmischen Risikoberechnung erfolgte im Februar 2021. Kurzkontakte wurden nun ab einer Dauer von mindestens 5, statt wie vorher 10min berücksichtigt und der Schwellenwert der Signaldämpfung erhöhte sich von 73dB auf 79dB. Außerdem wurde die Gewichtung der Kontaktzeiten abhängig von der Signaldämpfung angepasst und der Schwellenwert der erforderlichen Risikominutensumme für eine Risikomeldung von 15 auf 13min herabgesetzt (GitHub

2021c; CWA 2020). Diese Präzisierung scheint Folge eines wissenschaftliche Diskurses zu sein und auf Untersuchungen des Fraunhofer Instituts zu basieren, welches in Experimentalsituationen „die Details der Zeiterfassung und die Abstandsschätzung durch Bluetooth [...] Low Energy“ (Heine 2021h) testete. Auch wenn teils Uneinigkeiten bestehen, die Nutzenden sehen am Ende nur ein Ergebnis, dass das algorithmische System als eine Art *governing agent* auch aus teils uneindeutigen Daten, beispielsweise der Signaldämpfung, ermittelt (Crawford 2016, 85f).

Weitere Tests der Messgenauigkeit der CWA durch das Fraunhofer-Institut und das RKI resultierten in einer dritten Anpassung der Risikoberechnung im März 2021. Im Unterschied zu den vorangegangenen Versionen wurden nun kurze Begegnungen unter 5min „nicht mehr herausgefiltert, sondern individuell bewertet und über den Tag summiert (Heine 2021e). Außerdem fließen auch Begegnungen mit einem Abstand zwischen 1,5 und 2,5m – eine klare Umrechnungsanweisung in die Bluetooth-Signaldämpfung in dB gibt es nicht – nun als nicht nahe Begegnungen gewichtet in die Berechnung ein. Deutlich wird hier, dass algorithmische Systeme Inhalte verbergen und filtern (Seaver 2019, S. 414). Entscheidungen fallen nicht auf Basis der Daten an sich, sondern auf Basis algorithmisch analysierter, gewichteter und bewerteter Daten (Beer 2017, 2ff). Im Fall der CWA werden als nicht riskant bewertete Begegnungen herausgefiltert, wobei die Bewertung dieser nur eine temporäre, lokale und kontingente Wahrheit sein kann. Aus einem konstruktivistischen Blickwinkel wird klar, dass Transparenz in Bezug auf Algorithmen nicht ausreicht und wir immer nur kontingentes und unvollständiges Wissen über sie erlangen können. Wichtig ist deshalb die Prozesse der Wissensproduktion in den Blick zu nehmen (Seaver 2019, 414f).

Mitte April 2021 erfolgte das bislang letzte Update der Risikoberechnung in Reaktion auf die durch Virus-Mutationen veränderte Infektionslage. Dabei wurde die Dauer einer kritischen Begegnung, welche in einer Warnung eines erhöhten Risikos resultiert, von 13 auf 9min herabgesetzt, wodurch die Anzahl der Warnungen deutlich steigt (Heine 2021c). Ebenso im April wurde die CWA Version 2.0 veröffentlicht, die erstmals eine Check-In Funktion für Veranstaltungen bot. Die Möglichkeit zur Eventregistrierung kann als Zusatz zur Bluetooth-basierten Risikoermittlung betrachtet werden und funktioniert ähnlich wie diese über das Herunterladen von Check-Ins positiv Getesteter vom CWA-Server und der anschließenden Beurteilung dieser anhand der gemeinsamen Zeit auf einem Event (GitHub 2021b; Heine 2021d). Dieses Update folgte aus dem durch zunehmende Öffnungsschritte wachsenden Bedarf an Kontaktrückverfolgungen und der mangelhaften Erfüllung dieses Bedarfs

durch private Anbieter von Eventregistrierungs-Apps. Besonderes Aufsehen erregte die Luca-App, die einen zentralen Ansatz mit direkter Anbindung an die Gesundheitsämter verfolgte und unter anderem durch die Beteiligung des Rappers Smudo schnell hohe Nutzer*innenzahlen verzeichnen konnte. Eine gemeinsame Stellungnahme von Wissenschaftler*innen und IT-Expert*innen sowie ein Statement des CCC wiesen auf eklatante Datenschutzängel hin und sahen Entwicklungsprinzipien der CWA wie Zweckbindung, Transparenz, Freiwilligkeit und Risikoabwägung bei der Luca-App nicht erfüllt (Greef 2021, 12f; CCC 2021). In diesem Falle kann die Anpassung der CWA also als Folge von Diskursen der Wissenschaft und kritischen Öffentlichkeit und deren Abbildung in den Massenmedien verstanden werden. Weitere Updates ermöglichten die Integration von Schnelltest-Ergebnissen, womit unter anderem eine höhere Meldequote beabsichtigt wurde, und die Integration von Impfzertifikaten, die wiederum eine Attraktivitätssteigerung der App und damit auch eine stärkere Nutzung der eigentlichen Warn-Funktion zum Ziel hatte (Heine 2021b, 2021g).

An der Darstellung einiger wichtiger Anpassungen der CWA im Allgemeinen und der Risikoberechnung im Besonderen zeigt sich deutlich, inwiefern verschiedenste Akteure an der Konstruktion eines algorithmischen Systems beteiligt sind. Eine wichtige Rolle spielten durchgehend neue epidemiologische Erkenntnisse, die jedoch nicht als rein objektiv betrachtet werden dürfen, sondern auch konstruiertes Wissen sind. Bei Anpassungen der Parameter und deren Verrechnung mittels des algorithmischen Systems scheinen Untersuchungen des Fraunhofer- und des Robert-Koch-Instituts und Erkenntnisse aus der Wissenschaft allgemein die wichtigste Rolle gespielt zu haben. Eingebettet waren diese Weiterentwicklungen der Risikoberechnung jedoch auch immer in die von Google und Apple bereitgestellte Schnittstelle und die Optionen die diese boten oder neu entwickelten. Die Beteiligung der Internet-Community und von Nutzenden fiel offenbar geringer aus als oft herausgestellt und beschränkte sich auf kleinere Anpassungen, wie beispielsweise der Darstellung, und Zusatz-Features. Viele Updates die sich nicht unmittelbar auf das algorithmische System auswirkten dienten vorrangig der Attraktivitätssteigerung der App und können als Reaktionen auf politische und gesellschaftliche Entwicklungen in der Pandemie betrachtet werden, wie beispielsweise im Fall der Eventregistrierung.

5. Fazit

Die CWA ist ein anschauliches Beispiel dafür, dass Algorithmen aus weit mehr als nur Code bestehen. Sie kann als Ko-Produktion von wirtschaftlichen Akteuren wie

Google, Apple oder SAP, wissenschaftlichen Akteuren wie dem RKI oder externen Expert*innen, politischen Institutionen wie der Bundesregierung oder der Europäischen Kommission und gesellschaftlichen Akteuren wie Vereinen oder einer kritischen Öffentlichkeit verstanden werden. Darüber hinaus formten auch nicht-menschliche Akteure wie Diskurse, beispielsweise um das Modell der Datenspeicherung, Konzepte wie der *Contributor Covenant* oder rechtliche Anforderungen das algorithmische System mit. Diese Erkenntnis steht im Einklang mit der grundlegenden Annahme der Situationsanalyse nach Clarke. Sie geht davon aus, „dass alles, was sich in der Situation befindet, so ziemlich alles andere, was sich in der Situation befindet, auf irgendeine (oder auch mehrere) Weise(n) konstituiert und beeinflusst“ (Clarke 2012, S. 114). Handlungsmöglichkeiten des Entwickler*innenteams wurden demnach von einer Vielzahl von Elementen geformt, was sich bis in den Code und die Softwarearchitektur einschreibt. Die Aufgabe einer Analyse der soziotechnischen Assemblage, in die ein algorithmisches System eingebettet ist, ist die rückblickende Entzifferung ebendieser Konstruktion. Dabei geht es auch darum aufzuzeigen, dass Algorithmen weil sie konstruiert sind, auch anders konstruiert werden könnten, wie am Beispiel des Klassifikationssystems sichtbar wurde. Dies kann einer Fetischisierung von algorithmischen Systemen entgegenwirken und ihre kritische Betrachtung befördern (Kitchin 2017, 21f, 25).

Bei der Untersuchung der sozialen Situiertheit der Entwicklung der CWA erwiesen sich die von Clarke entwickelten Mapping-Prozesse als besonders geeignet um darzustellen was empirisch in der vorliegenden Situation vorhanden ist und welche Verbindungen, Machtgefälle und Einflussmöglichkeiten zwischen den einzelnen Elementen bestehen. Eine Positions-Map wäre für die Analyse des Diskurses um die Risikoberechnung aber nicht geeignet gewesen, da bei diesem kaum Spielraum für das Einnehmen unterschiedlicher Positionen besteht. Aus dem Feld der wissenschaftlichen Reflexion von algorithmischen Systemen boten insbesondere die Arbeiten von Kitchin, Beer und Seaver hilfreiche Ansätze für die Analyse. Fruchtbar wäre sicherlich ein internationaler Vergleich von Kontaktnachverfolgungs-Applikationen, um aufzuzeigen inwiefern öffentliche Diskurse, geltendes Recht, wirtschaftliche Interessen oder auch das politische System die Ausgestaltung dieser beeinflussten, was im Rahmen dieser Arbeit aber nicht möglich war. Ebenso kamen an dieser Stelle die Untersuchung der diskursiven Macht des algorithmischen Systems und die Betrachtung seiner Rückwirkungen auf seine soziale Umgebung zu kurz. Während dargestellt wurde auf welche Weise Machtverhältnisse bei der Entstehung und Anpassung der CWA von Bedeutung waren, gilt es die Frage wie durch algorithmische Kontaktverfolgungs-Apps Macht ausgeübt werden kann noch zu beantworten.

6. Literaturverzeichnis

- AlgorithmWatch. 2016. 1. Arbeitspapier: Was ist ein Algorithmus?
<https://algorithmwatch.org/de/arbeitspapier-was-ist-ein-algorithmus/>. Zugegriffen: 2. September 2021.
- Amnesty International. 2020. Joint statement: States use of digital surveillance technologies to fight pandemic must respect human rights.
<https://www.amnesty.org/en/documents/pol30/2081/2020/en/>. Zugegriffen: 2. September 2021.
- Apple und Google. 2020. Exposure Notification: Cryptography Specification.
https://blog.google/documents/69/Exposure_Notification_-_Cryptography_Specification_v1.2.1.pdf/. Zugegriffen: 2. September 2020.
- Becker, Steffen, Martin Degeling, Markus Dürmuth, Florian M. Farke, Leonie Schaewitz, Theodor Schnitzler und Christine Utz. 2020. *Akzeptanz von Corona-Apps in Deutschland vor der Einführung der Corona-Warn-App*.
- Beer, David. 2017. The social power of algorithms. *Information, Communication & Society* 20 (1): 1–13. doi: 10.1080/1369118X.2016.1216147.
- Benjamin, Ruha. 2019. *Race after Technology. Abolitionist Tools for the New Jim Code*: Polity.
- BMG. 2020. *Dokumente zum Entwicklungsauftrag der "Corona-Warn-App" durch SAP und Telekom. Anfrage an: Bundesministerium für Gesundheit*.
- Bowker, Geoffrey und Susan Leigh Star. 2017. Kategoriale Arbeit und Grenzinfrastrukturen. In *Grenzobjekte und Medienforschung*, hrsg. Susan Leigh, 167–204: transcript Verlag.
- Braun, Peter, Steffen Haffner und Barry G. Woodcock. 2020. COVID-19 pandemic predictions using the modified Bateman SIZ model and observational data for Heidelberg, Germany: Effect of vaccination with a SARS-CoV-2 vaccine, coronavirus testing and application of the Corona-Warn-App. *International Journal of Clinical Pharmacology and Therapeutics* 58 (8): 417–425.
- Bundesregierung. 2021. Corona-Warn-App: Fragen und Antworten.
<https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-faq-1758392>. Zugegriffen: 2. September 2021.
- Burrell, Jenna. 2016. How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society* 3 (1): 2053951715622512. doi: 10.1177/2053951715622512.
- CCC. 2021. Luca-App: CCC fordert Bundesnotbremse.
<https://www.ccc.de/de/updates/2021/luca-app-ccc-fordert-bundesnotbremse>. Zugegriffen: 9. September 2021.
- Clarke, Adele E. 2012. *Situationsanalyse. Grounded Theory nach dem Postmodern Turn*. Interdisziplinäre Diskursforschung. Wiesbaden: Springer VS.

- Crawford, Kate. 2016. Can an Algorithm be Agonistic?: Ten Scenes from Life in Calculated Publics. *Science, Technology, & Human Values* 41 (1): 77–92. doi: 10.1177/0162243915589635.
- Crawford, Kate und Vladan Joler. 2018. Anatomy of an AI System: The Amazon Echo as an anatomical map of human labor, data and planetary resources. <https://anatomyof.ai/>. Zugegriffen: 2. September 2020.
- CWA. 2020. Häufig gestellte Fragen zur Corona-Warn-App: Welche Gründe waren am Ende ausschlaggebend dafür, den dezentralen Ansatz zur Begegnungsnachverfolgung zu favorisieren? https://www.coronawarn.app/de/faq/#reasoning_decentralized. Zugegriffen: 3. September 2021.
- DEHMEL, SUSANNE, PETER KENNING, GERT G. WAGNER, CHRISTA LIEDTKE, HANS W. MICKLITZ und LOUISA SPECHT-RIEMENSCHNEIDER. 2020. *Die Wirksamkeit der Corona-Warn-App wird sich nur im Praxistest zeigen. Der Datenschutz ist nur eine von vielen Herausforderungen*. Berlin.
- Dix, Alexander. 2020. Die deutsche Corona Warn-App – ein gelungenes Beispiel für Privacy by Design? *Datenschutz und Datensicherheit - DuD* 44 (12): 779–785. doi: 10.1007/s11623-020-1366-1.
- Europäisches Parlament. 2020. *P9_TA(2020)0054 Abgestimmte Maßnahmen der EU zur Bekämpfung der COVID-19- Pandemie und ihrer Folgen. Entschließung des Europäischen Parlaments vom 17. April 2020 zu abgestimmten Maßnahmen der EU zur Bekämpfung der COVID-19-Pandemie und ihrer Folgen (2020/2616(RSP))*.
- Fraunhofer AISEC. 2020. *Privacy Protecting Proximity Tracing: Multinationale Initiative entwickelt digitale Lösung im Kampf gegen Corona. Pressemitteilung / 01. April 2020*.
- Gillespie, Tarleton. 2014. The Relevance of Algorithms. In *Media Technologies: Essays on Communication, Materiality, and Society*, hrsg. Tarleton Gillespie, Pablo J. Boczkowski und Kirsten A. Foot, 167–193: The MIT Press.
- GitHub. 2020a. Contributor Covenant Code of Conduct. https://github.com/coronawarn-app/cwa-documentation/blob/master/CODE_OF_CONDUCT.md. Zugegriffen: 3. September 2021.
- GitHub. 2020b. Corona-Warn-App: Dokumentation: README-Datei. <https://github.com/corona-warn-app/cwa-documentation/blob/master/translations/README.de.md>. Zugegriffen: 2. September 2021.
- GitHub. 2020c. Prüfsteine für die Beurteilung von „Contact Tracing“-Apps. <https://github.com/corona-warn-app/cwa-documentation/blob/master/translations/pruefsteine.de.md>. Zugegriffen: 3. September 2021.

- GitHub. 2020d. Rename 'master' to 'main' by sorin-iovita · Pull Request #1032. <https://github.com/corona-warn-app/cwa-server/pull/1032>. Zugegriffen: 3. September 2021.
- GitHub. 2021a. cwa-
documentation/images/risk_calculation/risk_calculation_enf_v2_overview.pdf. https://github.com/corona-warn-app/cwa-documentation/blob/master/images/risk_calculation/risk_calculation_enf_v2_overview.pdf. Zugegriffen: 9. September 2020.
- GitHub. 2021b. Event Registration - Summary. https://github.com/corona-warn-app/cwa-documentation/blob/master/event_registration.md. Zugegriffen: 9. September 2021.
- GitHub. 2021c. merge Update parameters for risk calculation #1260 into main (#1262). <https://github.com/corona-warn-app/cwa-server/commit/e88332397d4010c3854bd91de5b1a60b52658c58#>. Zugegriffen: 3. September 2021.
- GitHub. 2021d. Wie ermittelt die Corona-Warn-App ein erhöhtes Risiko? <https://github.com/corona-warn-app/cwa-documentation/blob/master/translations/cwa-risk-assessment.de.md>. Zugegriffen: 4. September 2021.
- Greef, Samuel. 2021. Ein Jahr Corona-Warn-App: Die CWA aus der Perspektive staatlicher Steuerung. *i3 - Kasseler Diskussionspapiere* (14).
- Heine, Hanna. 2020a. Corona-Warn-App Version 1.10 mit Kontakt-Tagebuch ist da. <https://www.coronawarn.app/de/blog/2020-12-28-corona-warn-app-version-1-10/>. Zugegriffen: 9. September 2021.
- Heine, Hanna. 2020b. Corona-Warn-App Version 1.7 kann die Risikoermittlung mehrmals täglich durchführen. <https://www.coronawarn.app/de/blog/2020-11-25-corona-warn-app-version-1-7/>. Zugegriffen: 5. September 2021.
- Heine, Hanna. 2020c. Corona-Warn-App Version 1.9 greift auf Version 2 des Exposure Notification Framework zurück. <https://www.coronawarn.app/de/blog/2020-12-16-corona-warn-app-version-1-9/>. Zugegriffen: 7. September 2021.
- Heine, Hanna. 2020d. Risikoberechnung unter Version 2 des Exposure Notification Frameworks. <https://www.coronawarn.app/de/blog/2020-12-17-risk-calculation-exposure-notification-framework-2-0/>. Zugegriffen: 9. September 2021.
- Heine, Hanna. 2021a. Corona-Warn-App Version 1.12 mit zwei Neuerungen. <https://www.coronawarn.app/de/blog/2021-02-10-corona-warn-app-version-1-12/>. Zugegriffen: 9. September 2021.
- Heine, Hanna. 2021b. Corona-Warn-App Version 2.3 integriert den digitalen Impfnachweis. <https://www.coronawarn.app/de/blog/2021-06-10-cwa-version-2-3/>. Zugegriffen: 9. September 2021.

- Heine, Hanna. 2021c. Das Projektteam verbessert die Risikoberechnung der Corona-Warn-App in Reaktion auf die Infektionslage. <https://www.coronawarn.app/de/blog/2021-04-16-corona-warn-app-risk-calculation-further-improved/>. Zugegriffen: 9. September 2021.
- Heine, Hanna. 2021d. Das Projektteam veröffentlicht Corona-Warn-App 2.0 mit Eventregistrierung. <https://www.coronawarn.app/de/blog/2021-04-21-corona-warn-app-version-2-0/>. Zugegriffen: 9. September 2021.
- Heine, Hanna. 2021e. Die Risikoberechnung der Corona-Warn-App wird weiter verbessert. <https://www.coronawarn.app/de/blog/2021-03-19-risk-calculation-improvement/>. Zugegriffen: 9. September 2021.
- Heine, Hanna. 2021f. Problem mit Schlüsselabgleich unter Android behoben. <https://www.coronawarn.app/de/blog/2021-01-14-android-key-matching-issue-fixed/>. Zugegriffen: 9. September 2021.
- Heine, Hanna. 2021g. Projektteam integriert Schnelltests in Corona-Warn-App Version 2.1. <https://www.coronawarn.app/de/blog/2021-05-02-corona-warn-app-version-2-1/>. Zugegriffen: 9. September 2021.
- Heine, Hanna. 2021h. Risikoberechnung der Corona-Warn-App nach detaillierten Tests weiter angepasst. <https://www.coronawarn.app/de/blog/2021-02-23-corona-warn-app-risk-calculation-optimization/>. Zugegriffen: 9. September 2021.
- Heine, Hanna. 2021i. Version 1.11: Corona-Warn-App nun mit Kennzahlen zum Infektionsgeschehen. <https://www.coronawarn.app/de/blog/2021-01-28-corona-warn-app-version-1-11/>. Zugegriffen: 9. September 2021.
- Hoerdt, Janina. 2020. Neue Funktionen: Corona-Warn-App Version 1.5 ist ab sofort zum Download verfügbar. <https://www.coronawarn.app/de/blog/2020-10-19-version-1-5/>. Zugegriffen: 4. September 2021.
- Horstmann, Kai T., Susanne Buecker, Julia Krasko, Sarah Kritzler und Sophia Terwiel. 2021. Who does or does not use the 'Corona-Warn-App' and why? *European Journal of Public Health* 31 (1): 49–51.
- Kitchin, Rob. 2017. Thinking critically about and researching algorithms. *Information, Communication & Society* 20 (1): 14–29. doi: 10.1080/1369118X.2016.1154087.
- Lupton, Deborah. 2018. How do data come to matter? Living and becoming with personal data. *Big Data & Society* 5 (2): 2053951718786314. doi: 10.1177/2053951718786314.
- Meyer, Jochen, Thomas Fröhlich und Kai von Holdt. 2020. *Corona-Warn-App: Erste Ergebnisse einer Onlineumfrage zur (Nicht-)Nutzung und Gebrauch*. <http://arxiv.org/pdf/2011.11317v2>.
- Munzert, Simon, Myrto Papoutsis und Holger Nowak. 2021. *Ein Jahr digitale Kontaktpersonennachverfolgung mit der Corona-Warn-App*.
- Pasquale, Frank. 2015a. The Algorithmic Self. In *The Hedgehog Review*, Bd. 17.

- Pasquale, Frank. 2015b. *The Black Box Society. The secret algorithms that control money and information*. Cambridge: Harvard University Press.
- RKI. 2020. *Mit Daten von Fitnessarmbändern und Smartwatches mehr über die Verbreitung des Coronavirus erfahren. Pressemitteilung des Robert Koch-Instituts*.
- Seaver, Nick. 2019. Knowing Algorithms. In *digitalSTS: A fieldguide for Science & Technology Studies*, hrsg. Janet Vertesi und David Ribes, 412–422: Princeton University Press.
- Seyfert, Robert. 2021. Algorithms as regulatory objects. *Information, Communication & Society*: 1–17. doi: 10.1080/1369118X.2021.1874035.
- tagesschau. 2020. Kampf gegen Coronavirus: Die Warn-App kommt - ein App-Gesetz nicht. *tagesschau.de*. 15 Juni 2020.
<https://www.tagesschau.de/inland/corona-warn-app-101.html>. Zugegriffen: 2. September 2021.
- Tufekci, Zeynep. 2015. Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. *Colo. Tech. LJ* (13): 203–218.
- Urban, Monika. 2021. „Die Hoffnung, informiert zu sein“. *Effekte der Corona-Warn-App. Prävention und Gesundheitsförderung*: 1–6.
- Süddeutsche Zeitung*. 2020. Welche Tracing-Apps weltweit zum Einsatz kommen: Drei-Stufen-System in China, Selfies an die Behörden in Moskau, Lob für das Rote Kreuz in Österreich: Viele Staaten setzen auf Smartphone-Technik, um die Pandemie einzudämmen. 30 April 2020.
<https://www.sueddeutsche.de/digital/corona-tracing-apps-1.4889793>. Zugegriffen: 10. September 2021.