

Zur Evaluation der digitalen Kontaktverfolgung: ein Debattenbeitrag

Henrik Graßhoff und Stefan Schiffner

Zusammenfassung

Dieser Artikel soll einen Beitrag zur Bewertung von digitaler Kontaktverfolgung in einer Pandemie leisten und damit die allgemeine Bewertung von Schutzmaßnahmen unterstützen. Dazu betrachten wir Kontaktverfolgungsapps und analysieren den dadurch entstehenden Datenmarkt. Ausgehend von den Marktteilnehmern beschreiben wir deren Teilnahmegründe und Rahmenbedingungen. In einer narrativen Literaturstudie leiten wir aus den Ergebnissen der Technologieakzeptanzforschung Best Practices für Kontaktverfolgungsapps ab und stellen offene Fragen und mögliche Hindernisse zur Disposition. Unser Beitrag versteht sich als vorläufig; weitere Untersuchungen, insbesondere quantitative Betrachtungen, fehlen. Unsere Analyse zeigt, dass viele der Einflussfaktoren untereinander stark abhängig sind, somit ist eine klarere Formalisierung dieser Abhängigkeiten nötig. Insbesondere technologische Einflüsse sind derzeit aber schwer erforschbar, da die meisten Apps und auch Google und Apples Kontaktverfolgungsframework nicht mehr zugänglich sind.

1. Einleitung

Am 22. März 2024 jährte sich der erste Corona-Lockdown in Deutschland zum vierten Mal. Diesen Jahrestag nahmen viele Politiker:innen und Medien zum Anlass, auf die deutsche Corona-Politik zurückzublicken und die Notwendigkeit ihrer umfassende Aufarbeitung zu betonen.¹ Diese soll, so der augenscheinliche Konsens, die Verhältnismäßigkeit und Effektivität vergangener Schutzmaßnahmen bewerten, um hieraus Handlungsempfehlungen für zukünftige Pandemien abzuleiten.

Das Ziel dieses Kommentars ist es, einen Debattenbeitrag zur Evaluation der digitalen Kontaktverfolgung zu leisten. Hierzu nehmen wir eine

1 *Deutschlandfunk*, Worum es bei der Aufarbeitung der Corona-Maßnahmen geht.

neue Perspektive ein und beschreiben digitale Kontaktverfolgung in ihrer Gesamtheit als Datenmarkt, auf dem verschiedene Akteure Kontaktdaten generieren, sammeln, wertschöpfend verarbeiten und handeln. Wir betten den gegenwärtigen Erkenntnisstand in diese Marktperspektive ein, identifizieren Leerstellen und geben Impulse für eine zukünftige Forschungsausrichtung. Abseits dessen ergeben sich aus der Tatsache, dass der Kontaktverfolgungsmarkt unfrei und durch undemokratische Entscheidungen geprägt war und ist, zweifelhafte politische Abhängigkeiten von digitalen Gatekeepern. Die deshalb auftretenden (potenziellen) Konflikte werden im Rahmen dieses Kommentars beschrieben und können als Anstoß für notwendige, umfassendere, politische Erwägungen dienen.

2. Kontaktverfolgung als Datenmarkt

In einer pandemischen Notlage ist der folgende Grundgedanke gleichermaßen simpel wie nachvollziehbar: Werden Bürger:innen rechtzeitig nach einer Begegnung mit einer infizierten Person benachrichtigt, verhalten sie sich vorsichtiger und unterbrechen so eine mögliche Infektionskette. Falls hierbei zur Begegnungsermittlung im weitesten Sinne digitale Technologien eingesetzt werden, spricht man von *digitaler Kontaktverfolgung*.

Während der Coronapandemie hat sich dieser Ausdruck zunehmend als Synonym für so genannte *Kontaktverfolgungsapps* (KVAs) etabliert.² Unter diesem Begriff sind Smartphoneanwendungen für Endanwender:innen zusammengefasst, die letztere bei der Identifikation von Begegnungen mit Infizierten unterstützen. In vielen Ländern wurde die Entwicklung einer KVA durch die nationale Regierung selbst initiiert. Im europäischen Kontext sind diese in der Regel diejenigen KVAs mit den höchsten Nutzungsraten, sodass die durch Regierungen angetriebenen Apps gelegentlich als *die* nationalen KVAs referenziert werden.³ In Deutschland stand zwischen Juni 2020 und Juni 2023 die *Corona-Warn-App* (CWA) in den App-Stores von Google und Apple zur Verfügung, ihre Weiterentwicklung wurde mittlerweile eingestellt.⁴

Vor diesem Hintergrund mag es zunächst einmal nicht naheliegend sein, digitale Kontaktverfolgung als Datenmarkt anzusehen. Vielmehr scheint

2 Martin u.a., Wireless Communications and Mobile Computing 2020.

3 Ebd.

4 Robert Koch Institut, Infektionsketten digital unterbrechen mit der Corona-Warn-App.

es so, dass Bürger:innen durch freiwillige Mitarbeit (Nutzung einer KVA) Gesundheitsämter bei der Erfüllung hoheitlicher Aufgaben (manuelle Kontaktverfolgung) unterstützen. In welchem Sinne lässt sich hier also von einem *Markt* sprechen?

Hierzu muss man lediglich feststellen, dass, sofern die KVA-Nutzung freiwillig erfolgt, alle beteiligten Akteur:innen nach einer rationalen Abwägung ihrer – wenn auch sehr unterschiedlich charakterisierten – Kosten und Nutzen handeln. Am offensichtlichsten gilt dies für Privatunternehmen, die während der Coronapandemie digitale Kontaktverfolgung in einer Vielzahl von Dienstleistungen und Produkte monetär verwerteten.^{5, 6} Daneben wägen auch nationale Regierungen die Entwicklungs- und Betriebskosten gegenüber einem, im Bezug auf das öffentliche Gesundheitssystem teilweise auch monetären, Nutzen ab. Insbesondere bei einer freiwilligen KVA gilt Gleiches aber auch letztlich für einzelne Endanwender:innen. Nichtmonetäre Kostenkomponenten (z. B. Nutzungskosten oder eine empfundene Überwachungsgefahr) und Gewinnerwartungen (z. B. Gesundheitsschutz oder soziale Anerkennung) treten hierbei an die Stelle direkter monetärer Interessen und entscheiden darüber, ob eine Einzelperson eine KVA verwendet – mit anderen Worten, ob sie Marktteilnehmer:in wird.

3. Marktkomponenten

Im Folgenden nehmen wir nacheinander die auftretenden Marktkomponenten – Endanwender:innen, die öffentliche Hand, digitale Gatekeeper und Privatanbieter:innen – in den Blick, fassen jeweils Forschungsfragen und den hierzu gegenwärtigen Erkenntnisstand zusammen und beschreiben potentielle zukünftige Fragen und offene, zur Diskussion stehende Aspekte.

5 *Petereit*, Corona-App wird Magenta: Telekom und SAP erhalten Auftrag der Bundesregierung.

6 *Besser/Welch*, Australia's coronavirus tracing app's data storage contract goes offshore to Amazon.

3.1 Endanwender:innen

Als Endanwender:innen betrachten wir die Zielgruppe, die letztlich die App auf ihren Mobilgeräten installiert. Da die Effektivität von KVAs stark von ihrer Prävalenz in der Gesellschaft abhängt,⁷ ist es nachvollziehbar, dass der überwiegende Anteil der Forschung im Bereich der Endanwender:innen auf Technikakzeptanzuntersuchungen entfällt.

Im März und April 2020 – als KVAs in nur einer Handvoll Ländern verfügbar waren – führten Altmann u.a.⁸ eine Akzeptanzumfrage unter 5995 Teilnehmenden aus fünf Ländern durch (davon 1013 aus Deutschland). In allen Ländern waren über zwei Drittel der Befragten prinzipiell bereit, eine KVA zu nutzen. Der Gesundheitsschutz nahestehender Personen und die Hoffnung auf ein Ende der Pandemie wirkten dabei als stärkste Treiber; die Sorge vor staatlicher Überwachung und eine befürchtete Angreifbarkeit durch Hacker hingegen wurden am häufigsten als Barrieren genannt. Diese ersten Ergebnisse wurden im Verlauf der Coronapandemie durch zahlreiche weitere Studien präzisiert. In einer Literaturanalyse von 13 Arbeiten extrahierten Oyibo u.a.⁹ insgesamt 56 Akzeptanzfaktoren, von denen als stärkste Treiber die empfundene Nützlichkeit für die eigene und die öffentliche Gesundheit wirkten, als stärkste Barrieren Privatsphärebedenken sowie ein empfundenes Misstrauen (insbesondere in die eigene Regierung). Zu einem ähnlichen Ergebnis kam Kuo¹⁰ in einem Vergleich von 76 Studien und einer Metaanalyse der Daten aus 25 dieser Studien. Demzufolge sind die einflussreichsten Akzeptanztreiber der empfundene persönliche und soziale Nutzen, das Vertrauen in KVAs, soziale Normen sowie begünstigende Bedingungen. Überraschenderweise konnte dabei kein signifikanter Zusammenhang zwischen Privatsphärebedenken und der Nutzungsabsicht nachgewiesen werden. Kuo selbst stellt heraus, dass die untersuchten Studien hinsichtlich der Signifikanz der Privatsphärebedenken variieren und der Zusammenhang zur KVA-Akzeptanz noch aufzuklären ist.¹¹

Insgesamt ist festzuhalten, dass die Einflussfaktoren auf die Nutzungsbereitschaft vergleichsweise gut verstanden sind. Aus ihren Ergebnissen leiten Oyibo u.a. sowie Kuo Empfehlungen für die Gestaltung von KVAs ab: (1) eine datensparsame App-Architektur, die Anwender:innen eine Wahl-

7 Ferretini u.a., Science 2020.

8 Altmann u.a., JMIR Mhealth Uhealth 2020.

9 Oyibo u.a., Front. Digit. Health 2022.

10 Kuo, BMC Medical Informatics and Decision Making 2023.

11 Kuo, BMC Medical Informatics and Decision Making 2023.

freiheit über das Teilen ihrer Daten lässt, (2) eine visuell ansprechende Erklärung der getroffenen Sicherheits- und Privatsphärenmechanismen, (3) ein niedrigschwelliges und anregendes App-Design, (4) das aktive Bewerben des Gesundheitsnutzens in konventionellen und sozialen Medien sowie (5) die Herstellung öffentlichen Vertrauens durch Delegation des App-Betriebs an vertrauenswürdige Institutionen und die Veröffentlichung des Quellcodes.

Eine Umsetzung dieser Empfehlungen garantiert jedoch nicht hohe Nutzungsraten. So ließen sich durchweg große Differenzen zwischen der Nutzungsbereitschaft und den faktischen Nutzungszahlen von KVAs beobachten,¹² was auf die Präsenz einer *Intentions-Verhaltens-Lücke* hinweist. Diese Lücke – also das Auseinanderklaffen zwischen den Absichten einer Person, eine bestimmte Technologie zu verwenden, und ihrem tatsächlichen Verhalten¹³ – ist Zetterholm u.a. zufolge „vermutlich eine der kritischsten Barrieren in Ländern mit freiwilligen KVAs“¹⁴ und einer der wichtigsten Punkte für weitere Forschung.

Es erscheint uns daher angemessen, zukünftige Akzeptanzforschung auf die praktische Steigerung der Nutzungszahlen auszurichten. Legt man hierfür als Theorie vorherrschende Modelle der Technikakzeptanz und der Verhaltenspsychologie zugrunde,¹⁵ gilt es, begünstigende Bedingungen sowie die empfundene Verhaltenskontrolle¹⁶ zu fördern: Welche konkreten Elemente im UX- und UI-Design erhöhen die Selbstwirksamkeit der Anwender:innen? Kann (monetäres) Nudging in diesem Bereich erfolgreich eingesetzt werden?¹⁷ Mit welchen Strategien kann die Funktionsweise der App effektiver kommuniziert werden? Wie muss eine KVA gestaltet werden, um den unterschiedlichen Anforderungen verschiedenster Bevölkerungsgruppen gerecht zu werden?

12 Garrett u.a., PLoS ONE 2021.

13 Siehe z. B. Sheeran/Webb, Social and Personality Psychology Compass 2016.

14 Zetterholm u.a., Informatics 2021.

15 Siehe Tabelle 3 in Kuo, BMC Medical Informatics and Decision Making 2023.

16 Im Modell der *Unified theory of acceptance and use of technology* wird die Intentions-Verhaltens-Lücke durch „begünstigende Bedingungen“ (bspw. ausreichende Ressourcen) beeinflusst, in der *Theorie des geplanten Verhaltens* durch die empfundene Kontrolle über das eigene Verhalten (Selbstwirksamkeit). Siehe hierzu: Venkatesh u.a., MIS Quarterly 2003; Ajzen, Organizational Behavior and Human Decision Processes 1991.

17 Munzert u.a., Nature Human Behaviour 2021.

Bei all diesen Überlegungen gilt es selbstverständlich auch, eine App zu entwickeln, welche faktisch sicher ist, um die Integrität der App und den Schutz der Privatsphäre ihrer Anwender:innen zu gewährleisten. An dieser Stelle müssen wir jedoch eine Erkenntnislücke diagnostizieren, denn nur wenige Arbeiten widmen sich der Analyse realer Privatsphäris Risiken der gängigsten KVAs. Baumgärtner u.a.¹⁸ demonstrierten 2020 die Durchführbarkeit eines bereits bekannten Angriffs auf das Protokoll der CWA, indem sie die Bewegungen infizierter Nutzer:innen mithilfe passiver Bluetooth-Sensoren verfolgten. Ergebnisse von Graßhoff u.a.¹⁹ deuten darauf hin, dass im Bereich eines solchen Sensors statistisch etwa 29 Smartphones mit aktivierter CWA durch Varianzen in ihrem Bluetooth-Sendeverhalten unterschieden werden können – was in einem gewissen Umfang auch das Tracking von Nichtinfizierten ermöglicht. Derartige technische Analysen bilden allerdings die Ausnahme in der KVA-Forschung; in der Regel werden gewünschte Sicherheitseigenschaften bei KVAs eher angenommen²⁰ oder aus formalen Protokollanalysen gefolgert.²¹ Ein notwendiger und beworbener Privatsphäreschutz muss allerdings stets anhand der konkreten Implementierung validiert werden können. Hier ist für zukünftige Anwendungen technisch tiefergehende Forschung notwendig, die derzeit jedoch durch die Abschaltung der Corona-Warn-App und des darunterliegenden Betriebssystemframeworks²² erschwert wird.

3.2 Öffentliche Hand und Gatekeeper

In unserem Modell des Kontaktverfolgungsdatenmarktes agiert die öffentliche Hand in einer Multirolle. Während die Legislative als Regulatorin des Marktes auftritt, ist die Exekutive zugleich Marktteilnehmerin durch die Entwicklung einer nationalen App (oder die Beauftragung hierzu),

18 Baumgärtner u.a., IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) 2020.

19 Graßhoff u.a., Proceedings of the 18th International Conference on Availability, Reliability and Security 2023.

20 Bei der CWA wurde beispielsweise verkürzt argumentiert, sie unterbinde Tracking, da sie lediglich Pseudonyme per Bluetooth aussende und diese aus kryptografisch sicheren Primitiven berechnet und regelmäßig geändert werden.

21 Morio u.a., 32nd USENIX Security Symposium (USENIX Security 23) 2023.

22 Siehe Fußnote 29.

von deren Nutzung wiederum das öffentliche Gesundheitssystem und die Gesellschaft als Ganzes profitieren.²³

In ihrer Rolle als Marktteilnehmerin obliegt es ihr, durch die Architektur und Gestaltung der App wesentlich deren Rezeption und Akzeptanz in der Bevölkerung zu beeinflussen. Vor dem Hintergrund der beschriebenen Akzeptanzfaktoren (siehe 3.1), ist hierbei die Bildung von Vertrauen – gerade in individualistischen Gesellschaften²⁴ wie Deutschland – besonders hervorzuheben. Unter diesen Gesichtspunkten wurde die Konzeption und Entwicklung der CWA vielfach gelobt. Unter anderem der Chaos Computer Club²⁵ hob den Privacy-by-Design-Ansatz und die Umsetzung des Open-Source-Grundsatzes mit Feedbackschleifen für Expert:innen und Öffentlichkeit positiv hervor. Die CWA ist hier zweifelsfrei ein Projekt mit Modellcharakter, das erörterungswürdige Fragen für zukünftige öffentliche Digitalprojekte aufwirft: Welche Bedingungen begünstigen oder behindern den Erfolg solcher Open-Source-Entwicklungsprojekte? Welche Best Practices lassen sich für die Entwicklung anderer E-Governance-Dienste (auch auf kleineren Maßstabsebenen) lernen? Können Synergieeffekte im Hinblick auf demokratische Partizipation und Kostensenkung²⁶ aktiv gefördert werden (etwa durch Einbindung in Schulprojekte)?

Unabhängig von der Bereitstellung einer eigenen nationalen App, kommt der Legislative die Aufgabe zu, digitale Kontaktverfolgung zum Wohl der Gesellschaft zu regulieren. Sharon²⁷ beschrieb 2021 die entstehenden Gefahren, wenn diese Regulierungsrolle nicht durch legitimierte Institutionen, sondern privatwirtschaftliche Technologiekonzerne übernommen wird. In der De-facto-Standardisierung der Kontaktverfolgung durch die GAEN-Schnittstelle²⁸ von Google und Apple sieht sie einen solchen illegitimen

23 Die Effektivität von KVAs zur Pandemieeindämmung ist nicht Gegenstand dieses Artikels. Hierfür verweisen wir etwa auf: *Anglemyer u.a.*, Cochrane Database of Systematic Reviews 2020.

24 Gemessen an der kulturellen Dimension *Individualismus–Kollektivismus* von Hofstede sind Privatsphärebedenken in individualistischen Gesellschaften (wie Deutschland und den USA) gewichtigere Nutzungsbarrieren als in kollektivistischen (wie Singapur). Siehe hierzu: *Kuo*, BMC Medical Informatics and Decision Making 2023; *Geber/Ho*, Information, Communication & Society 2023.

25 *RedaktionsNetzwerk Deutschland*, Erste Reaktionen auf die Corona-Warn-App: Ein großer Kritikpunkt bleibt.

26 *Der Spiegel*, Gesamtkosten für Corona-Warn-App steigen auf 220 Millionen Euro.

27 *Sharon*, Ethics and Information Technology 2021.

28 Bei *Google Apple Exposure Notification* (GAEN) handelt es sich um eine Betriebssystemsschnittstelle für KVAs, welche 2020 in Android und iOS implementiert wurde.

„sector creep“²⁹ und bezeichnet dies als Beispiel für das allgemeinere Phänomen der „Gesundheits-Googlisierung“.³⁰ Paradoxerweise erhielt die technische Spezifikation der Schnittstelle durch zwei Gatekeeper, die in der Regel eher für invasive Datenpraktiken bekannt sind, weitreichende³¹ – obgleich nicht einvernehmliche³² – Anerkennung in der Privacy-Fachwelt. Dies stärkte mutmaßlich die rigorose Durchsetzbarkeit von GAEN: Verschiedene Repräsentant:innen nationaler Regierungen berichteten davon, dass Google und Apple etwa das korrekte Funktionieren ihrer Apps unterbanden, sofern diese nicht die GAEN-Schnittstelle verwendeten,³³ und hinterfragten, mit welchem Ausmaß diese Konzerne „einer demokratisch gewählten Regierung oder ihren Gesundheitsbehörden vorschreiben könnten, was ihre App leisten darf und was nicht“?³⁴

Diese Probleme betten sich in eine wachsende, immer schärfer geführte Debatte um die Regulierung großer Technikkonzerne ein, die auf europäischer Ebene mittlerweile sehr präsent geführt wird. Digitale Kontaktverfolgung als Beispiel eines solchen „sector creeps“ muss in diesem größeren Zusammenhang politisch und juristisch diskutiert werden, sie ist eine konkrete Instanz eines sich ausprägenden Machtungleichgewichts. Die in diesem Bereich beobachtbare, deutliche Abhängigkeit demokratisch gewählter Regierungen von privatwirtschaftlichen Technologieriesen außerhalb Europas liefert somit ein weiteres Argument für die Notwendigkeit einer sorgfältig abgewogenen Regulierung.

Ist eine autorisierte App installiert und aktiviert, berechnet das Betriebssystem kryptografische Pseudonyme und sendet diese in kurzen Abständen per Bluetooth Low Energy aus, um hierdurch Begegnungen zu ermitteln. GAEN ist dezentralisiert, was bedeutet, dass Begegnungsdaten lediglich lokal auf dem Smartphone gespeichert werden. Seit dem 18. September 2023 ist GAEN nicht mehr verfügbar; ob eine Evaluation und Weiterentwicklung der Schnittstelle vorgesehen ist oder passiert, ist unklar.

29 Sharon, Ethics and Information Technology 2021.

30 Sharon, Personalized Medicine 2016.

31 Sharon, Ethics and Information Technology 2021.

32 Hoepman, A Critique of the Google Apple Exposure Notification (GAEN) Framework, 2021.

33 Scott u.a., How Google and Apple outflanked governments in the race to build coronavirus apps.

34 Ilves, Why are Google and Apple dictating how European democracies fight coronavirus?

3.3 Privatanbieter

Im Bereich allgemeiner digitaler Kontaktverfolgungslösungen³⁵ stellt sich grundlegend die Frage, wie viel privatwirtschaftlicher Wettbewerb zwischen verschiedenen Anbietern zuzulassen und wünschenswert ist. Es ließe sich erwarten, dass die Wahlfreiheit zwischen verschiedenen Anwendungen das Vertrauen in Kontaktverfolgung allgemein zu steigern vermag, indem sie die digitale Kontaktverfolgung dem Nimbus einer staatlichen Überwachung entzieht: Hat eine Anwenderin etwa Misstrauen in die nationale App, nutzt sie an deren Stelle möglicherweise ein anderes Produkt. Auf der anderen Seite sind negative Auswirkungen auf Effektivität, Sicherheit und Rezeption nicht auszuschließen; es gälte hierbei, eine allzu große Fragmentierung inkompatibler Ökosysteme zu vermeiden,³⁶ das Risiko auftretender Sicherheitslücken abzuwägen³⁷ sowie einzuschätzen, in welchem Maße derartige Lücken zu einer Kollektivbewertung von „digitaler Kontaktverfolgung allgemein“ beitragen (bspw. könnten Mängel einer einzelnen KVA pauschalisierend als Defekt aller KVAs wahrgenommen werden). Vor diesem Hintergrund kann es durchaus profitabel erscheinen, das Angebot digitaler Kontaktverfolgungslösungen, insbesondere KVAs, zu beschränken.

In Deutschland hatten sich auf diesem Markt eine Vielzahl von Anbietern wie SmartMeeting oder die Darfichrein GmbH etabliert. Für Irritationen sorgte hier die Zweigleisigkeit zwischen der Bundesregierung und einigen Landesregierungen. Während erstere weiterhin die aus Steuermitteln finanzierte CWA bewarb, kauften letztere Lizenzen im Umfang von über 20 Millionen Euro³⁸ für die Nutzung der Luca-App der culture4life GmbH. Investitionen in diese App wurden nicht nur von Datenschützer:innen äußert kritisch gesehen. Auch die Start-up-Initiative „WirFürDigitalisierung“ kritisierte eine exklusive Förderung der Luca-App und forderte stattdessen eine „kollaborative, offene und gemeinsame Schnittstelle“.³⁹

35 Dies umfasst neben KVAs beispielsweise auch Online-Check-in-Systeme umfasst.

36 Auf europäischer Ebene wurde zwischen Oktober 2020 und Februar 2023 unter dem Namen *European Federation Gateway Service* ein Dienst in Betrieb genommen, der eine grenzüberschreitende Interoperabilität der Apps aus 18 EU-Mitgliedsländern sowie Norwegen ermöglichte.

37 Die Sicherheit der Luca-App der culture4life GmbH wurde wegen ihrer zentralisierten Architektur und diverser Sicherheitsmängel vielfach kritisiert. Siehe: *Weiß*, Sicherheitsforscher: Risiken der Luca-App „völlig unverhältnismäßig“.

38 *Köber/Fanta*, Mehr als 20 Millionen Euro für Luca.

39 *ZEIT ONLINE*, Start-up-Initiative gegen Einführung der Luca-App.

Für KVAs speziell wurde die Entwicklung einer solchen Schnittstelle erfolgreich von Google und Apple zugunsten ihrer eigenen GAEN-Schnittstelle verhindert (vgl. Abschnitt 3.2). Der Submarkt der digitalen KVAs ist folglich hochgradig unfrei und unterliegt Bedingungen, die von zwei Gatekeepern dominiert wurden und werden. Wie argumentiert, kann dies im Hinblick auf KVAs durchaus als wünschenswert angesehen werden. Angesichts jüngerer europäischer Regulationen⁴⁰ und Klagen des US-Justizministeriums gegen Apple⁴¹ ergeben sich jedoch praktische Fragen, etwa ob eine Beschränkung der GAEN-Schnittstelle auf von Google und Apple autorisierte Apps überhaupt zulässig ist.

4. Schluss

Die meisten Kontaktverfolgungsapps sind aus den App-Stores verschwunden; die reale oder empfundene Bedrohung durch COVID ist stark gesunken. Untersuchungen zur Technikakzeptanz mit echten Nutzer:innen wird somit zunehmend schwieriger und sind allenfalls retrospektiv durchführbar. Mit dem zumindest nach außen kommunizierten Ende des Supports des GAEN-Frameworks ist eine quantitative Untersuchung wichtiger technischer Komponenten der Corona-Warn-App stark erschwert.

Das gesellschaftliche Wohl im Blick, ist es aber offensichtlich, dass es sich lohnt, sich frühzeitig um die Technik und deren Akzeptanz zu kümmern. Ansonsten werden wir bei der nächsten Pandemie wieder beobachten, dass auf „schnelle und einfache“ Lösungen zurückgegriffen wird, die im Zweifel weder demokratisch legitimiert noch ausgereift sind. Mit den Worten Ulrich Kelbers: „Die Software braucht also eine ständige Pflege und Weiterentwicklung, auch wenn gerade keine Krise ist. Der digitale Austausch muss gewährleistet sein. Die Rechtsgrundlagen müssen evaluiert und angepasst werden“.⁴²

40 Insbesondere Digital Markets Act, Data Act und Data Governance Act.

41 Ein Anklagepunkt ist des US-Justizministeriums ist exakt, Apple schränke den Zugriff auf Hardware- und Software-Schnittstellen für Dritte ein, siehe: U.S. Department of Justice Office of Public Affairs, 2024.

42 Kelber, in: Schmoeckel (Hrsg.), Herausforderung der Rechtsordnung durch die Pandemie, 2021, 195 (210).

Literatur

- Ajzen, Icek (1991): The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), S. 179–211. doi:10.1016/0749-5978(91)90020-T.
- Altmann, Samuel; Milsom, Luke; Zillessen, Hannah; Blasone, Raffaele; Gerdon, Fred-eric; Bach, Ruben; Kreuter, Frauke; Nosenzo, Daniele; Toussaert, Séverine und Abeler, Johannes (2020): Acceptability of App-Based Contact Tracing for COVID-19: Cross-Country Survey Study. *JMIR Mhealth Uhealth*, 8(8). doi:10.2196/19857.
- Anglemyer, Andrew; Moore, Theresa HM; Parker, Lisa; Chambers, Timothy; Grady, Alice; Chiu, Kellia; Parry, Matthew; Wilczynska, Magdalena; Flemyng, Ella und Bero, Lisa (2020): Digital contact tracing technologies in epidemics: a rapid review. *Cochrane Database of Systematic Reviews*, 2020(8). doi:10.1002/14651858.CD013699.
- Baumgärtner, Lars; Dmitrienko, Alexandra; Freisleben, Bernd; Gruler, Alexander; Höchst, Jonas; Kühlberg, Joshua; Mezini, Mira; Mitev, Richard; Miettinen, Markus; Muhamedagic, Anel; Nguyen, Thien Duc; Penning, Alvar; Pustelnik, Dermot; Roos, Philipp; Sadeghi, Ahmad-Reza; Schwarz, Michael und Uhl, Christian (2020): Mind the GAP: Security & Privacy Risks of Contact Tracing Apps. *IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. doi:10.1109/TrustCom50675.2020.00069.
- Besser, Linton und Welch, Dylan (26. Apr. 2020): Australia's coronavirus tracing app's data storage contract goes offshore to Amazon. URL: <https://www.abc.net.au/news/2020-04-24/amazon-to-provide-cloud-services-for-coronavirus-tracing-app/12176682> (besucht am 14. Mai 2024).
- Der Spiegel (03. Dez. 2022): Gesamtkosten für Corona-Warn-App steigen auf 220 Millionen Euro. URL: <https://spiegel.de/netzwelt/gesamtkosten-fuer-corona-warn-app-steigen-auf-220-millionen-euro-a-0202c5e9-f2f9-4586-a8f1-e469fd5437fb> (besucht am 14. Mai 2024).
- Deutschlandfunk (2024): Worum es bei der Aufarbeitung der Corona-Maßnahmen geht. URL: <https://www.deutschlandfunk.de/corona-massnahmen-aufarbeitung-pan-demie-lockdown-100.html> (besucht am 31. März 2024).
- Ferretini, Luca; Wymant, Chris; Kendall, Michelle; Zhao, Lele; Nurtay, Anel; Abeler-Dörner, Lucie; Parker, Michael; Bonsall, David und Fraser, Christophe (2020): Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science*, 368(6491). doi:10.1126/science.abb6936.
- Garrett, Paul M.; White, Joshua P.; Lewandowsky, Stephan; Kashima, Yoshihisa; Perfors, Andrew; Little, Daniel R.; Geard, Nic; Mitchell, Lewis; Tomko, Martin und Dennis, Simon (2021): The acceptability and uptake of smartphone tracking for COVID-19 in Australia. *PLoS ONE*, 16(1). doi:10.1371/journal.pone.0244827.
- Geber, Sarah und Ho, Shirley S. (2022): Examining the cultural dimension of contact-tracing app adoption during the COVID-19 pandemic: a cross-country study in Singapore and Switzerland. *Information, Communication & Society*, 26(11), S. 2229–2249. doi:10.1080/1369118X.2022.2082880.

- Graßhoff, Henrik; Adamsky, Florian und Schiffner, Stefan (2023): Smartphones in a Microwave: Formal and Experimental Feasibility Study on Fingerprinting the Corona-Warn-App. *Proceedings of the 18th International Conference on Availability, Reliability and Security*, doi:10.1145/3600160.3605011.
- Hoepman, Jaap-Henk (2021): *A Critique of the Google Apple Exposure Notification (GAEN) Framework*. doi:10.48550/arXiv.2012.05097.
- Ilves, Ieva (16. Juni 2020): Why are Google and Apple dictating how European democracies fight coronavirus? URL: <https://theguardian.com/commentisfree/2020/jun/16/google-apple-dictating-european-democracies-coronavirus> (besucht am 14. Mai 2024).
- Kelber, Ulrich (2021): Datenschutz und Datensicherheit in Corona-Zeiten. In: Schmoekel, Matthias (Hrsg.): *Herausforderung der Rechtsordnung durch die Pandemie* (58). Baden-Baden: Nomos, S. 195–210. doi:10.5771/9783748912767.
- Köver, Chris und Fanta, Alexander (12. April 2021): Mehr als 20 Millionen Euro für Luca. URL: <https://netzpolitik.org/2021/digitale-kontaktverfolgung-fast-20-millionen-euro-fuer-luca/> (besucht am 14. Mai 2024).
- Kuo, Kuang-Ming (2023): Antecedents predicting digital contact tracing acceptance: a systematic review and meta-analysis. *BMC Medical Informatics and Decision Making*, 23. doi:10.1186/s12911-023-02313-1.
- Martin, Tania; Karopoulos, Georgios; Hernández-Ramos, José L.; Kambourakis, Georgios und Nai Fovino, Igor (2020): Demystifying COVID-19 Digital Contact Tracing: A Survey on Frameworks and Mobile Apps. *Wireless Communications and Mobile Computing*, 2020, S. 1–29. doi:10.1155/2020/8851429.
- Morio, Kevin; Esiyok, Ilkan; Jackson, Dennis und Künnemann, Robert (2023): Automated Security Analysis of Exposure Notification Systems. *32nd USENIX Security Symposium (USENIX Security 23)*. S. 6593–6610.
- Munzert, Simon; Selb, Peter; Gohdes, Anita; Stoetzer, Lukas F. und Lowe, Will (2021): Tracking and promoting the usage of a COVID-19 contact tracing app. *Nature Human Behaviour*, 5, S. 247–255. doi:10.1038/s41562-020-01044-x.
- Oyibo, Kiemute; Sahu, Kirti Sundar; Oetomo, Arlene und Morita Plinio Pelegri-ni (2022): Factors Influencing the Adoption of Contact Tracing Applications: Systematic Review and Recommendations. *Front. Digit. Health*, 4. doi:10.3389/fdgh.2022.862466.
- Petereit, Dieter (01. Mai 2020): Corona-App wird Magenta: Telekom und SAP erhalten Auftrag der Bundesregierung. URL: <https://t3n.de/news/corona-app-magenta-telekom-sap-1274327/> (besucht am 14. Mai 2024).
- RedaktionsNetzwerk Deutschland (17. Juni 2020): Erste Reaktionen auf die Corona-Warn-App: Ein großer Kritikpunkt bleibt. URL: <https://rnd.de/digital/corona-warn-app-erste-reaktionen-zeigen-grossen-kritikpunkt-GJECMZBZAVF2JF545XI26OEZ ZY.html> (besucht am 14. Mai 2024).
- Robert Koch Institut (15. Feb. 2024): Infektionsketten digital unterbrechen mit der Corona-Warn-App. URL: <https://rki.de/cwa> (besucht am 14. Mai 2024).

- Scott, Mark; Braun, Elisa; Delcker, Janosch und Manancourt, Vincent (15. Mai 2020): How Google and Apple outflanked governments in the race to build coronavirus apps. URL: <https://politico.eu/article/google-apple-coronavirus-app-privacy-uk-france-germany/> (besucht am 14. Mai 2024).
- Sharon, Tamar (2016): The Googlization of Health Research: From Disruptive Innovation to Disruptive Ethics. *Personalized Ethics*, 13(6), S. 563–574. doi:10.2217/pme-2016-0057.
- Sharon, Tamar (2021): Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers. *Ethics and Information Technology*, 23, S. 45–57. doi:10.1007/s10676-020-09547-x.
- Sheeran, Paschal und Webb, Thomas L. (2016): The Intention-Behavior Gap. *Social and Personality Psychology Compass*, 10(9), S. 503–518. doi:10.1111/spc3.12265.
- U.S. Department of Justice Office of Public Affairs (2024): Justice Department Sues Apple for Monopolizing Smartphone Markets. URL: <https://www.justice.gov/opa/pr/justice-department-sues-apple-monopolizing-smartphone-markets> (besucht am 31. März 2024).
- Venkatesh, Viswanath; Morris, Michael G.; Davis, Gordon B. und Davis, Fred D. (2003): User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, 27(3), S. 425–478.
- Weiß, Eva-Maria (29. April 2021): Sicherheitsforscher: Risiken der Luca-App „völlig unverhältnismäßig“. URL: <https://heise.de/news/Sicherheitsforscher-Risiken-der-Luca-App-voellig-unverhaeltnismaessig-6031770.html> (besucht am 14. Mai 2024).
- ZEIT ONLINE (05. März 2021): Start-up-Initiative gegen Einführung der Luca-App. URL: <https://zeit.de/news/2021-03/05/start-up-initiative-gegen-einfuehrung-der-luca-app> (besucht am 14. Mai 2024).
- Zetterholm, My Villius; Lin, Yanqing und Jokela, Päivi (2021): Digital Contact Tracing Applications during COVID-19: A Scoping Review about Public Acceptance. *Informatics*, 8(3). doi:10.3390/informatics8030048.

