Contact Tracing in der COVID-19 Pandemie

Stellungnahme der Bioethikkommission

Contact Tracing in der COVID-19 Pandemie

Stellungnahme der Bioethikkommission

Wien, 2020

Impressum

Medieninhaber, Verleger und Herausgeber:
Geschäftsstelle der Bioethikkommission, Ballhausplatz 2, 1010 Wien
Autorinnen und Autoren: Bioethikkommission
Wien, 2020. Stand: 8. Juni 2020

Inhalt

1 Einführung

Die COVID-19-Pandemie ist für jeden Einzelnen, für unsere Gesellschaft und für unsere Wirtschaft mit massiven Einschränkungen und Umbrüchen verbunden. Global wird um Lösungen gerungen, Infektionsraten zu minimieren und uns zumindest mittelfristig ein Leben mit dem Virus zu ermöglichen, das der Normalität vor der Pandemie möglichst nahekommt. Während die Notwendigkeit, Impfstoffe und effektive Medikamente gegen COVID-19 zu entwickeln, so gut wie unbestritten ist, haben digitale Methoden zur Aufklärung von Infektionsketten – insbesondere als Applikationen auf Mobiltelefonen mit Bluetooth- und WLAN-Schnittstellen („Corona-Apps") – eine sehr kontroverse und emotional geführte Debatte ausgelöst. Während sie manchen als unumgängliches Werkzeug zur Eindämmung der Pandemie erscheinen, dessen Nutzung nach Ansicht mancher Befürworterinnen bzw. Befürworter verpflichtend sein sollte, weisen Kritikerinnen bzw. Kritiker vor allem auf die Gefahr unkontrollierter und von der Nutzerin bzw. dem Nutzer unbemerkter Überwachung und nicht autorisierter Verwendung personenbezogener Daten für politische, kommerzielle und andere Zwecke hin.

Derzeit wird in vielen Ländern die Verwendung unterschiedlicher „Corona-Apps" diskutiert, die sich darin unterscheiden, welchem Ziel bzw. welchen Zielen sie dienen.[1] Neben Apps zur Nachverfolgung von Infektionsketten, gibt es eine Reihe anderer mit COVID-19 in Zusammenhang stehender Apps:

- Informations-Apps informieren z. B. über die aktuellen, an einem bestimmten Ort bzw. für eine bestimmte Einrichtung geltenden Beschränkungen oder auch über die Personendichte an einem bestimmten Ort.
- Datenspende-Apps dienen der Preisgabe von Mobilitätsdaten und ähnlichen Daten für Zwecke der Pandemie-Forschung und zu öffentlichen Planungszwecken.
- Immunitäts-Apps (eigentlich treffender: Immunitätsausweise, oder Immunitäts-„Führerscheine"[2]) dienen der Erfassung des Immunitätsstatus von Personen für

---

1 Laufend aktualisierte Listen mit Apps u.a. auf https://www.gsa.europa.eu/GNSS4Crisis (s. News European Parliament 15 May 2020, COVID-19 tracking apps: ensuring privacy and data protection, https://www.europarl.europa.eu/news/en/headlines/society/20200429STO78174/covid-19-tracing-apps-ensuring-privacy-and-data-protection) (zugegriffen am 29. Mai 2020); Verweis auf COVID-19 Digital Rights Tracker via Morley et al., Ethical guidelines for COVID-19 tracing apps, Nature 28 May 2020, unter: https://www.nature.com/articles/d41586-020-01578-0 (zugegriffen am 29. Mai 2020); COVID Tracing Tracker (MIT Technology Review): https://www.technologyreview.com/2020/05/07/1001354/how-to-submit-a-change-to-the-covid-tracing-tracker-project/ (zugegriffen am 27. Mai 2020).

2 Persad, Govind, and Ezekiel J. Emanuel. "The Ethics of COVID-19 Immunity-Based Licenses ("Immunity Passports")." JAMA (online May 6, 2020), DOI: 10.1001/jama.2020.8102.; Natalie Kofler, Françoise Baylis, "Ten reasons why immunity passports are a bad idea", Nature 581 (28 May), 379-381, (2020).

Situationen, in denen die Bewegungsfreiheit oder der Zugang zu bestimmten Orten oder Leistungen von Immunität abhängig ist.
- Quarantäne-Apps überwachen die Einhaltung von Quarantänebestimmungen durch Personen, die zur Selbstisolation aufgefordert sind, oder gar allgemein die Einhaltung von Betretungsverboten, Abstandsvorschriften udgl. durch die Bevölkerung.
- Symptomcheck-Apps, die erfassen, an welchen Symptomen infizierte Personen leiden, um die Krankheit besser zu verstehen, und die es Menschen mit bestimmten Symptomkombinationen erleichtern, eine mögliche COVID-19-Infektion zu erkennen und sich frühzeitig zu isolieren und testen zu lassen.

Die vorliegende Stellungnahme ausschließlich mit Apps, die dem Contact Tracing dienen (auch Exposure Tracing Apps, Proximity Tracing Apps genannt). Die anderen Typen von Apps im Zusammenhang mit COVID-19 sind nicht Gegenstand der vorliegenden Stellungnahme.

Die derzeit gängigsten Modelle der Contact Tracing Apps verwenden Bluetooth-Signale, die angeben, welche mobilen Geräte (und damit welche Personen) sich in unmittelbarer Nähe eines anderen Gerätes aufgehalten haben. Ziel ihrer Anwendung ist die digitale Nachverfolgung von möglichen Infektionsketten mit dem Ziel der Benachrichtigung und Isolierung betroffener Personen. Daneben gibt es Ansätze, die auf der Verwendung von Standortdaten (wie etwa über Mobilfunk- oder WLAN-Netze ermittelten GPS-Koordinaten) beruhen oder diese mit Bluetooth-gestütztem Proximity Tracing kombinieren.

Sprachlich wird in der Literatur häufig zwischen „Tracking“ und „Tracing“ unterschieden. Wenngleich diese Begriffe in Zusammenhang mit digitalem Monitoring oft als Synonyme gebraucht werden, so bezieht sich typischerweise ersteres auf die Erfassung von Daten, die man eventuell in der Zukunft zur Rückverfolgung von Infektionsketten verwenden kann (also proaktives Datensammeln). Zweiteres hingegen, das „Tracing“ im engeren Sinne, bezeichnet die retrospektive Darstellung von möglichen Infektionswegen. In dieser Stellungnahme verwenden wir den Begriff „Tracing“ als Überbegriff, wenn beide Praktiken gemeint sind; wenn nur eine spezifische Funktion gemeint ist wird dies gesondert angemerkt.

Dass sich Contact Tracing technischer Hilfsmittel – wie Informations- und Kommunikationstechnologien – bedient, ist an sich nicht neu. Neu an den sog. „Corona-Apps“ ist dagegen zum einen die Möglichkeit, einige oder sogar alle der Schritte, die vormals von Menschen durchgeführt wurden, zu automatisieren. Dies ist dann von Vorteil, wenn das Volumen der bearbeiteten Fälle hoch ist und das Tracing schnell gehen muss, um betroffene Personen isolieren zu können und damit der Weiterverbreitung des Virus Einhalt zu gebieten. Neu ist zum anderen der proaktive Charakter, da gleichsam vorsorglich eine große Menge an Kontaktdaten erhoben und verarbeitet werden, von denen sich erst nachträglich ein sehr kleiner Teil als tatsächlich infektionsrelevant herausstellt. Die Datenerfassung und das theoretische Überwachungs- und Diskriminierungspotenzial, die mit einem derartigen proaktiven und automatisierten Contact Tracing einhergehen, bringen eine Reihe ethischer, rechtlicher und gesellschaftspolitischer Herausforderungen mit sich. Diese sind Gegenstand der vorliegenden Stellungnahme.

2 Eindämmung von Epidemien durch Contact Tracing

Contact Tracing – also die Zurückverfolgung physischer Kontakte, welche eine infizierte Person während der ansteckenden Krankheitsphase mit anderen Menschen hatte – ist ein etabliertes und anerkanntes Mittel der Epidemiebekämpfung. Diese Methode hat beispielsweise ganz wesentlich zur Eindämmung der Ebola-Epidemie beigetragen.[3] Vorrangig geht es meist darum, Kontaktpersonen so rasch als möglich zu testen bzw. zu isolieren, um eine Weiterverbreitung der Krankheit einzudämmen. Daneben nehmen Forschungsinteressen eine wichtige Rolle ein, da es nur durch die Nachverfolgung von Infektionsketten gelingt, eine Krankheit besser zu verstehen. Nur so können auch verantwortungsvolle politische Schritte gesetzt werden, einschränkende Maßnahmen auf solche Bereiche zu konzentrieren, bei denen diese Maßnahmen erforderlich und verhältnismäßig sind.

2.1 Klassisches („händisches“) Contact Tracing

Beim klassischen Contact Tracing, wie es auf der Grundlage von § 5 EpidemieG schon sehr lange erfolgt, werden anlässlich eines Infektionsfalles die infektionsrelevanten Kontakte individuell („händisch“) durch Mitarbeiterinnen und Mitarbeiter der Gesundheitsbehörden ermittelt. Dies geschieht i.d.R. durch Befragung sowohl der infizierten Person selbst als auch von Personen in deren Umfeld (Arbeitgeberinnen und Arbeitgeber, Familienangehörige usw.) und – in weiterer Folge – der auf diese Weise ermittelten Kontaktpersonen. Auch bei diesem „händischen“ Tracing können Informations- und Kommunikationstechnologien eine Rolle spielen, etwa wenn gemeinsam mit einer positiv getesteten Person anhand deren digitalem Terminkalender, Chat-Verläufen udgl. die Kontakte während der infektiösen Phase rekonstruiert werden.

Klassisches Contact Tracing ist überaus personal- und ressourcenintensiv. Die eingesetzten Mitarbeiterinnen und Mitarbeiter der Behörden bedürfen eingehender Schulung. Generell ist der Zeitfaktor essentiell, damit sich die Kontaktpersonen ermitteln und isolieren lassen, bevor infizierte Kontaktpersonen das Virus weiterverbreiten konnten. Idealerweise ist diese Form von Contact Tracing mit Vor-Ort-Testungen und – bei ent-

3 World Health Organization (WHO), Implementation and management of contact tracing for Ebola virus disease. Emergency Guideline (2015), https://apps.who.int/iris/bitstream/handle/10665/185258/WHO_EVD_Guidance_Contact_15.1_eng.pdf;jsessionid=6E13ABBDB48EC4E2D153FA7803CF45F9?sequence=1 (Zugriff am 23.5.2020).

sprechender Infektionswahrscheinlichkeit – mit Erlass eines Absonderungsbescheids, mindestens bis zur Abklärung der Befundsituation, verbunden.

Zu schwierigen ethischen Fragen kann es insbesondere kommen, wenn es um Vertraulichkeit geht. Beim Contact Tracing können überaus sensible Informationen preisgegeben werden (z. B. betreffend außereheliche Liebesverhältnisse, illegale Arbeitsverhältnisse, etc.). Diesbezüglich kann als Faustregel gelten, dass die Identität der positiv getesteten Person gegenüber einer aufgesuchten Kontaktperson offengelegt werden darf und muss, wenn dies für eine zielführende Befragung von Kontaktpersonen erforderlich ist, niemals jedoch der Weg, wie sich die positiv getestete Person infiziert haben könnte, und auch nicht die Identität anderer Kontaktpersonen.

Aufgesuchte Personen werden ferner nur dann bereit sein, Kontakte offenzulegen, wenn sie sich sicher sein können, dass zum Zweck des Contact Tracing offen gelegte Informationen nicht in einem allfälligen gerichtlichen oder behördlichen Verfahren gegen sie selbst verwendet werden können. Diesbezüglich sollte daher ein Beweisverwertungsverbot erwogen werden.

2.2 Contact Tracing durch Betreiberinnen bzw. Betreiber von Einrichtungen

Beim proaktivem Contact Tracing (also dem „Tracking“ im Wortsinne) durch Betreiberinnen bzw. Betreiber von Einrichtungen werden vorsorglich Daten erhoben (oder Vorbereitungen für die Offenlegung aus anderen Gründen erhobener Daten getroffen), aus denen sich physische Kontakte zwischen Personen in einer Einrichtung ergeben und die dann bei Auftreten eines Falles für Contact Tracing verwendet werden können. Klassisches Beispiel wäre die Erfassung der Anwesenheit von Arbeitnehmerinnen und Arbeitnehmern am Arbeitsplatz durch Arbeitgeberinnen und Arbeitgeber. Dies kann ganz analog mithilfe von Anwesenheitslisten und Belegungsplänen erfolgen (die die Arbeitnehmerinnen und Arbeitnehmer manchmal selbst ausfüllen), oder aber auch digital, etwa durch die Verpflichtung für Arbeitnehmerinnen und Arbeitnehmer, sich mit der eigenen Chip-Karte zu registrieren, wenn man einen Raum betritt oder einen Arbeitsplatz einnimmt.

Was in der Arbeitswelt und in wenigen anderen Kontexten bereits als Beitrag zur Eindämmung von COVID-19 üblich ist, ließe sich dem Prinzip nach auf viele Einrichtungen übertragen. So wäre es etwa denkbar, dass Identität und Sitzplatz von Theaterbesucherinnen und Theaterbesuchern oder Restaurantgästen erfasst werden, oder dass sich Hotelgäste mit ihrer Zimmerkarte und damit mit ihrer Identität registrieren, wenn sie eine bestimmte Abteilung des Wellnessbereichs benutzen.

Unterschiede bestehen nicht nur in Bezug auf die Art und Weise der Datenerhebung (gänzlich analog, digital, in einem standardisierten Datenformat), sondern auch in Bezug auf die weitere Verarbeitung der Daten. So können die Daten an eine zentrale Stelle weitergeleitet werden oder in der jeweiligen Einrichtung verbleiben und nur auf

anlassbezogene Anfrage seitens der Gesundheitsbehörde offenbart werden („enhanced manual tracing“).

Auch beim Contact Tracing auf Initiative der Betreiberinnen bzw. Betreiber von Einrichtungen können bestimmte Modelle von „Corona-Apps“ zum Einsatz kommen. Diese können etwa vorsehen, dass Nutzerinnen bzw. Nutzer der betreffenden Einrichtung einen von der Einrichtung ausgestellten QR-Code (Veranstaltungscode) scannen müssen, oder aber dass umgekehrt die Einrichtung einen Code auf dem Mobiltelefon der Nutzerin bzw. des Nutzers scannt. Dies wiederum erlaubt ganz ähnliche Funktionalitäten, wie wir sie vom derzeit gängigen Proximity Tracing (dazu sogleich unter 2.3) kennen, etwa das automatisierte Versenden von Warnmeldungen auf die Mobiltelefone betroffener Nutzerinnen und Nutzer. Die Methode adressiert gezielter das Phänomen von „Superspreader Events“, also Situationen, in denen oft nur eine einzige infizierte Person eine große Anzahl weiterer Personen „auf einen Schlag“ infiziert (vgl. Medienberichte über Après-Ski Bars, Chorproben, Cocktail-Partys, Familienfeiern). Sie hat Vorteile zudem etwa in Situationen, in denen das ständige Mit-sich-Führen eines Mobiltelefons untunlich, ein „Check-in“ und „Check-out“ am Eingang aber möglich ist (z. B. Sauna, Whirlpool). Je nachdem, wie granular die „Veranstaltungen“ definiert sind (z. B. kann auch ein Tisch in einem Restaurant oder eine Loge in einem Theater einen eigenen Code haben), bietet diese Methode gegebenenfalls ein höheres Maß an Verlässlichkeit als Proximity Tracing mittels automatisierten digitalen Handshakes.

2.3 Dezentrales digitales Contact Tracing

Beim vollkommen dezentralen Contact Tracing mittels „Corona-Apps“ geht es um eine breitflächige, nicht auf bestimmte Personengruppen oder Situationen beschränkte Rekonstruktion physischer Kontakte einer bestimmten Mindestdauer und räumlichen Mindestnähe.

Dabei ist die Kombination eines breiten Spektrums verschieden gestalteter Apps denkbar. Unterschiede bestehen zunächst in der Definition eines infektionsrelevanten Kontakts (Dauer des Kontakts, Abstand, erfasste Zeitspanne) und in der zu seiner Feststellung verwendeten Technologie (präzise GPS-Lokalisation aller App-Nutzerinnen und -Nutzer oder Kommunikation der Endgeräte untereinander durch „digitalen Handshake“). Unterschiede bestehen auch etwa in Bezug auf die Authentifizierung der Nutzerinnen und Nutzer bei der App-Installation (keine Authentifizierung, IP-Adresse, starke Authentifizierung), in Bezug auf die Voraussetzungen, unter denen eine COVID-19- Infektion über die App erfasst wird (zwingend oder freiwillig, bestätigt durch Gesundheitspersonal oder nicht), sowie allgemein in Bezug auf die Speicherung der relevanten Daten (zentral oder dezentral im jeweiligen Endgerät).

Ein weiterer Unterschied besteht zwischen Apps, die die über das App-Netzwerk erfassten Kontakte positiv getesteter Personen automatisch über ihr Infektionsrisiko und die Verpflichtung zur Selbstisolation bzw. Testung informieren (Track- and Trace-Apps),

und jenen, die dies nicht tun. Apps in der letzteren Gruppe führen zu „enhanced manual tracing“, indem sie den Gesundheitsbehörden zwar Zugang zu den Proximity-Protokollen der Apps positiv getesteter Personen geben, es aber den Gesundheitsbehörden überlassen, die Infektionsketten händisch nachzuverfolgen und mit möglichen weiteren Infizierten in Kontakt zu treten. Aus datenschutzrechtlicher Sicht sind die zuletzt genannten Modelle kritischer zu bewerten, da sie zu einer unmittelbaren Identifizierung von Kontaktpersonen durch die Behörden führen.

3 Ethische und rechtliche Anforderungen an Tracing-Apps

Ethische Überlegungen beruhen auf einem Wertekanon, der im Besonderen auch in den Grundrechten zum Ausdruck kommt.[4] Da in diesem Kontext der Wahrung der Menschenwürde, dem Schutz des Lebens und der Gesundheit sowie der Freiheit des Individuums ein hoher Stellenwert zukommt, müssen diese Werte und die damit verbundenen ethischen Prinzipien, wie Autonomie, Gerechtigkeit, sowie die informationelle Selbstbestimmung, auch bei der Anwendung von Apps im Rahmen der Eindämmung einer Pandemie vorrangig handlungsleitend sein. Dies kann nicht heißen, dass Bürgerinnen und Bürger unhinterfragt mit der Anwendung einer „Corona-App“ einverstanden sein sollen und sie, wenn schon nicht offensichtlich, so zumindest indirekt zur Anwendung gezwungen werden (dazu unten 4). Es kann jedoch auch nicht heißen, dass – sofern diverse Probleme bezüglich der Wahrung von Freiheitsrechten, Verhinderung von Missbrauch der gesammelten Daten (z. B. für Überwachungszwecke) oder der sinnvollen epidemiologischen Auswertung gelöst werden – derartige Apps nicht weiterentwickelt und möglichst vielen Menschen zugänglich gemacht werden sollten. Im Gegenteil kann der Einsatz einer bestimmten Technik zur Eindämmung einer Pandemie nach Lage des Falles sogar das „gelindere Mittel“ sein, das weitreichendere Eingriffe in Grundrechte, so beispielsweise in das Grundrecht auf Freizügigkeit oder in die Versammlungsfreiheit, vermeiden hilft. Dies setzt jedoch Vertrauen seitens der Bürgerinnen und Bürger in die Technologie sowie deren Anwendung und Datenauswertung im Rahmen staatlicher Strukturen voraus. Das heißt, es müssen rigoros Maßnahmen umgesetzt werden, die es

4 Siehe dazu auch: Cohen, I.G., Gostin, L.O. and Weitzner, D.J., Digital Smartphone Tracking for COVID-19: Public Health and Civil Liberties in Tension. JAMA.

ermöglichen, „Corona-Apps" epidemiologisch sinnvoll, nachvollziehbar, evidenzbasiert und für Bürgerinnen bzw. Bürger und ihre Privatsphäre sicher einzusetzen. Ein derzeit noch nicht geklärtes Thema beim Einsatz dieser Apps ist zudem ihre technische Reife und Verlässlichkeit, sodass eine laufende und kritische Evaluierung notwendig ist. Hinzu kommen eine klare zeitliche Begrenzung der Sammlung von Daten, sowie die Einbettung in eine Gesamtstrategie im Umgang mit der Pandemie. Im Folgenden werden einige dieser Punkte näher beleuchtet.[5]

3.1 Epidemiologische Geeignetheit der Maßnahme

Erste Voraussetzung ist die epidemiologische Geeignetheit der Maßnahme, die Pandemie einzudämmen, wobei die Treffsicherheit eine entscheidende Rolle spielt. Bisherige Erfahrungen mit einer Reihe von „Corona-Apps" verweisen auf das Problem von falsch-negativen Ergebnissen, in denen die App Corona-Fälle nicht entdecken kann.[6] Es gibt beispielsweise bei der vom österreichischen Roten Kreuz in Zusammenarbeit mit Accenture entwickelten „Stopp-Corona-App" eine ganze Reihe von Gründen für falsch-negative Ergebnisse, d. h. Corona-Fälle, die die App nicht entdecken kann. Dies könnte etwa in folgenden Fällen auftreten:

- Eine COVID-19-positive Person hat keine App, trägt zum Zeitpunkt des infektiösen Kontakts ihr Mobiltelefon nicht am Körper, hat Bluetooth deaktiviert, odgl.
- Der infektiöse Kontakt ist zu kurz, um von der App registriert zu werden (z. B. in einem öffentlichen Verkehrsmittel oder beim Vorbei-Joggen).
- Der infektiöse Kontakt hat früher als 54 Stunden vor der Krankmeldung stattgefunden (z. B. weil Symptome erst spät richtig gedeutet wurden).
- Eine COVID-19-positive Person ist asymptomatisch und lässt sich nie testen oder meldet (aus welchen Gründen auch immer) ihr Testergebnis nicht über die App.

---

5 Zur ethischen Bewertung von Tracing-Apps vgl auch bereits Contact Tracing als Instrument der Pandemiebekämpfung – Zentrale Gesichtspunkte aus der Perspektive der Ethik, Stellungnahme Nr. 33/2020 vom 6. April 2020 der Nationalen Ethikkommission in der Schweiz im Bereich der Humanmedizin (NEK), https://www.nek-cne.admin.ch/inhalte/Themen/Stellungnahmen/NEK-stellungnahme-Contact_Tracing.pdf; World Health Organisation (WHO), Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing, Interim Guidance vom 28. Mai 2020, https://www.who.int/publications-detail/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1; Jeffrey Kahn and Johns Hopkins Project on Ethics and Governance of Digital Contact Tracing Technologies (Hrsg), Digital Contact Tracing for Pandemic Response: Ethics and Governance Guidance (2020), https://muse.jhu.edu/book/75831.

6 So wird medial berichtet, dass die australische COVIDSafe-App trotz sechs Millionen Downloads in über vier Wochen nur zur Identifizierung eines einzigen Infizierten geführt habe und auch die Erfahrungen in Singapur scheinen ernüchternd zu sein, https://www.tagesschau.de/ausland/australien-coronavirus-app-103.html.

- COVID-19 wird anders als durch engen physischen Kontakt übertragen (z. B. Schmier- oder Aerosolinfektion).

Ebenfalls gibt es viele Gründe für falsch-positive Ergebnisse, d. h. den umgekehrten Fall, dass Fälle, die keine Corona-Fälle sind, von der App als solche gewertet werden. Das könnte aus folgenden Gründen der Fall sein:

- Eine Person hat vorschnell eine Warnung über die App abgegeben (z. B. Symptome falsch gedeutet, sonst überreagiert oder aus fremden Motiven heraus gehandelt).
- Ein registrierter Kontakt war objektiv nicht geeignet, zu einer Infektion zu führen (z. B. Zwischenwand, Rücken an Rücken in einem öffentlichen Verkehrsmittel).

Während falsch-positive Ergebnisse grundsätzlich zum Wesen von Contact Tracing gehören und als solches nicht bedenklich sind, führt eine zu hohe Anzahl von Fällen, die zu Unrecht als Corona-Fälle kategorisiert werden, zu Frustrationserlebnissen und allgemein zu einem Motivations- und Vertrauensverlust bei Nutzerinnen und Nutzern. Falsch-negative Ergebnisse sind dann besonders schädlich, wenn durch die App ein „umgekehrter Placebo-Effekt" eintritt, d. h. Menschen im falschen Vertrauen darauf, aufgrund der Verwendung der App geschützt zu sein bzw. ihren Beitrag zur Eindämmung des Virus zu leisten, auf präventive Schutzmaßnahmen gegen eine Ansteckung (Abstand, mechanische Schutzvorkehrungen) verzichten.

Sowohl falsch-negative als auch falsch-positive Ergebnisse sind daher durch ein entsprechendes Systemdesign möglichst zu minimieren. Beispielsweise müsste gewährleistet werden, dass Personen, die positiv auf COVID-19 getestet werden, unter behördlicher Überwachung eine Warnmeldung über die App abgeben. Darüber hinaus müssten Maßnahmen getroffen werden, dass jene, die eine Warnung erhalten, sich auch einem Test unterziehen (siehe auch 3.2).

3.2 Einbettung in eine Gesamtstrategie (Systemsicht)

Zur Bekämpfung von COVID-19 bedarf es eines umfassenden Konzepts zur Eindämmung der Pandemie, das aus vielen Komponenten besteht und nur in seiner Gesamtheit sinnvoll bewertet werden kann. Die Fokussierung der medialen Aufmerksamkeit auf „Corona-Apps" lenkt von der Erkenntnis ab, dass diese immer nur als Bausteine in einem größeren Konzept fungieren können. Zu den Komponenten eines solchen Konzepts gehören neben dem weiterhin unverzichtbaren „händischen" Tracing jedenfalls auch eine Teststrategie und eine Isolierungsstrategie sowie eine adäquate Kommunikationsstrategie.

Unmittelbarer Zweck der Applikation sollte die rasche Isolation möglicherweise infizierter Personen und die zielgerichtete Allokation von Test-Ressourcen sein, z. B. indem Handy-Besitzer, die eine Warnung erhalten, aufgefordert werden, sich unverzüglich selbst zu isolieren und sich testen zu lassen. Dazu müssen ausreichende, leicht erreichbare und

kostenfreie Testmöglichkeiten bereitstehen, die relativ rasch ein verlässliches Ergebnis produzieren. Je umständlicher es für gewarnte Personen ist, sich einem Test zu unterziehen, je länger sie auf Testergebnisse warten und berufliche Termine odgl. stornieren müssen, umso geringer ist die Bereitschaft, auf eine Warnmeldung zu reagieren. Auch wirkungsvolle Maßnahmen gegen eine Stigmatisierung positiv getesteter Personen können die Bereitschaft, auf Warnmeldungen zu reagieren, erhöhen.

Unabdingbar für einen erfolgreichen Einsatz der App ist eine entsprechende öffentliche Kommunikationsstrategie. Dies beginnt bei der klaren Kommunikation darüber, dass der Besitz der App nicht vor einer persönlichen Ansteckung schützt und keine Schutzmaßnahmen ersetzen kann, bis hin zu einer ausgewogenen Kommunikation über die Bedeutung einer Warnmeldung und die aufgrund einer solchen zu setzenden Schritte. Die Kommunikation sollte Vertrauen aufbauen und sowohl Panik vermeiden als auch Anreize setzen, sich unverzüglich in Isolation zu begeben und sich testen zu lassen. Mehrere Warnstufen – je nach der Intensität der Exposition – können empfehlenswert sein („exposure risk calculation", „exposure risk score"). Insgesamt sollte diese Kommunikationsstrategie nicht bloß als „Informationskampagne" verstanden werden, mit der die Öffentlichkeit von der Nützlichkeit der Apps überzeugt werden soll; vielmehr sollten auch Räume und Orte für Erfahrungen, Fragen, und Vorschläge seitens der Bevölkerung geschaffen werden.

3.3 Eignung im grenzüberschreitenden Kontext

Menschen sind mobil, und die Landesgrenzen – insbesondere innerhalb des Schengen-Raums bzw. innerhalb der Europäischen Union – werden seit Mai 2020 schrittweise wieder geöffnet. Es ist daher für ein zeitgemäßes Schutzkonzept essentiell, dass eine Applikation nicht nur innerhalb der Ländergrenzen funktioniert, sondern dass eine grenzüberschreitend entwickelte Lösung genutzt[7] oder aber zumindest die Interoperabilität verschiedener Systeme sichergestellt wird.[8]

---

7 GitHub, Decentralized Privacy-Preserving Proximity Tracing, https://github.com/DP-3T; Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT), https://www.pepp-pt.org/.

8 Mobile applications to support contact tracing in the EU's fight against COVID-19: Common EU Toolbox for Member States (15. April 2020), https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf; Interoperability guidelines for approved contact tracing mobile applications in the EU (13. Mai 2020), https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf.

3.4 Folgenabschätzung und Evaluierung

Die Implementierung einer Contact Tracing-Strategie, die die Verwendung von Apps miteinschließt, setzt eine sorgfältige Folgenabschätzung unter Berücksichtigung aller gesellschaftlichen Auswirkungen voraus. Sie muss ferner mit einem Plan zur Evaluierung der Effektivität der Strategie einhergehen. Zu einer solchen Evaluationsstrategie können u.a. folgende Punkte gehören:

- Entsprechen Architektur und Programmierung noch neuesten epidemiologischen Kenntnissen (z. B. betreffend Ansteckungswege)?
- Wie wirkt sich ein sich verändernder Anteil der Menschen, die die Apps verwenden, auf die Infektionsraten aus (u. U. regionenspezifische Auswertung unter Verwendung von Postleitzahlen etc.)? Wenn eine größere App-Nutzungsdichte zeitlich mit einer stagnierenden oder wachsenden Infektionsrate zusammenfällt, was sind die Gründe dafür?
- Wie wirkt sich ein wachsender Anteil von Menschen, die entsprechende Apps verwenden, auf das Vertrauen der Bevölkerung in das Gesundheitswesen und die Bundesregierung aus?
- Von welchen Bedenken bezüglich Datenschutz, Schutz der Privatsphäre, Autonomie, Erfahrungen im Gebrauch etc. berichten die Nutzerinnen und Nutzer der Apps?

Insgesamt muss sich digital gestütztes Contact Tracing ständig neuen epidemiologischen Erkenntnissen anpassen und sollte für verschiedene Situationen möglichst maßgeschneiderte Lösungen bereithalten, ohne die einzelnen Nutzerinnen bzw. Nutzer mit der hinter diesen Lösungen liegenden Komplexität zu konfrontieren. Dabei wäre etwa auch das „Superspreader"-Phänomen angemessen zu adressieren, z. B. indem für bestimmte Typen von Veranstaltungen, Orte und Einrichtungen, bei denen das derzeit gängige Bluetooth-gestützte Proximity Tracing nicht oder nicht gut funktioniert, spezielle technische Lösungen entwickelt werden.

3.5 Vertrauen durch Transparenz

Da die Wirksamkeit von automatisiertem Contact Tracing stark von der Verbreitung der App abhängt, und deren Verbreitung stark vom Vertrauen der Menschen, ist absolute Transparenz über die Funktionsweise und Leistungsfähigkeit einer App essentiell. Dabei dürfen Zusicherungen nicht nur von denjenigen Personen oder Organisationen kommen, welche eine konkrete App entwickelt haben. Vielmehr ist eine Publikation des Source Code und die Überprüfung durch unabhängige Einrichtungen (Datenschutzbehörden, NGOs u.a.) zu fordern. Auch die Etablierung eines Nutzergremiums und die Begleitung durch ein multidisziplinäres Expertengremium wäre von Vorteil (siehe auch 3.8).

3.6 Datenschutz und Datensicherheit

Bei der Bewertung von „Corona-Apps“ und in der öffentlichen Diskussion stehen regelmäßig datenschutzrechtliche Erwägungen im Vordergrund. Dabei sind zwei Typen von Datenverarbeitung zu unterscheiden: die Verarbeitung von Gesundheitsdaten einer COVID-19-positiv getesteten Person bei einer Krankmeldung und möglicherweise der gesundheitsrelevanten Daten entsprechender Kontaktpersonen beim Contact Tracing einerseits und die im Rahmen der vorsorglichen Speicherung von Daten für eine eventuelle spätere Rekonstruktion der Infektionskette anfallenden allgemeinen Daten andererseits.

Die Verarbeitung dieser Daten erfolgt unterschiedlich, je nachdem ob die App einem dezentralen oder einem zentralen Ansatz folgt. Aus dem Blickwinkel des Datenschutzes und hier im Besonderen des Grundsatzes der Datenminimierung ist Systemen mit einer dezentralen Architektur der Vorzug zu geben. Bei den derzeit am meisten propagierten Modellen dezentraler Architekturen werden ausschließlich pseudonymisierte[9] Daten ausgetauscht und lokal auf den jeweiligen Smartphones gespeichert. Dazu versendet jedes Smartphone, auf dem eine App installiert ist, einen periodisch (etwa alle 15 Minuten) wechselnden Code, der von anderen Smartphones mit App im räumlichen Nahebereich aufgenommen und lokal abgespeichert wird. Der Code alleine lässt keine Rückschlüsse auf dessen Versender zu. Erhält eine Person die Information, dass sie positiv auf COVID-19 getestet wurde oder mit einer positiv getesteten Person in Kontakt war, kann oder muss sie je nach Rechtslage die von ihrem Smartphone in einem bestimmten Zeitraum versendeten Codes auf einen zentralen Server (S1) hochladen. Dazu benötigt die Person in aller Regel einen eigenen Freischaltcode, der einmalig von einem anderen, staatlich betriebenen Server (S2) bei einem entsprechenden Eintrag im (nicht-öffentlichen) Register der anzeigepflichtigen Krankheiten gemäß § 4 EpidemieG generiert wird, um falsche Warnungen von nicht COVID-19-positiven Personen zu verhindern. Daten von Smartphones werden dazu jedoch an den S2 nicht übermittelt. Auf dem S1 sind lediglich pseudonymisierte Daten gespeichert und keine Kontaktdaten. Alle Smartphones mit App synchronisieren regelmäßig mit S1 und erhalten so alle Codes, die das Smartphone von einer positiv getesteten Person versendet hat. Dadurch ist lokal am Smartphone ein Abgleich mit den vom Smartphone gespeicherten Codes möglich. Stimmt ein vom S1 abgerufener mit einem lokal gespeicherten Code überein, hatte die Nutzerin bzw. der Nutzer des Smartphones im relevanten Zeitraum Kontakt mit einer

---

9 Pseudonymisierte Daten sind Daten, die für sich alleinstehend nicht auf eine konkrete Person zurückgeführt werden können, die jedoch durch einen Schlüssel mit Namen und/oder Kontaktdaten spezifischer Personen verbunden sind. Auch wenn der Schlüssel nur einer einzigen Person zugänglich ist spricht man in diesem Fall trotzdem bei pseudonymisierten Daten auch von personenbezogenen Daten, und die datenschutzrechtlichen Bestimmungen der DSGVO greifen weiterhin. Erst wenn der Schlüssel, der die beiden Datensätze mit einander verbindet, unwiederbringlich zerstört ist, und wenn es dadurch unmöglich geworden ist, zurückzuverfolgen, von welcher Person die Daten stammen, spricht man von anonymisierten Daten. Anonymisierte Daten liegen auch nicht im sachlichen Geltungsbereich der DSGVO.

positiv getesteten Person, die die von ihrem Smartphone gespeicherten Codes deshalb auf S1 hochgeladen hat, und erhält eine entsprechende Warnmeldung. Rückschlüsse auf die andere Person oder weitere Personen, die Kontakt mit dieser Person hatten, sind jedoch technisch nicht möglich. Eine Identifizierung der positiv getesteten Person ist weder aufgrund der auf S1 gespeicherten Codes noch aufgrund der auf den anderen Smartphones gespeicherten pseudonymisierten Kontaktdaten möglich. Die im Register gemäß § 4 EpidemieG gespeicherten Daten über positive Tests werden lediglich zur Generierung des Freischaltcodes benötigt und sind nicht mit dem System der App verbunden. Zu einer „Enttarnung" der Erkrankten kommt es nicht.

Die konsequente Anwendung der Pseudonymisierung und die Beschränkung der verarbeiteten Daten auf ein Minimum bei dezentralen Systemen kann nach Ansicht der Bioethikkommission die datenschutzrechtlichen Risiken erheblich senken.[10] Die Grundsätze des Datenschutzrechts sind gleichwohl auch bei derartigen Systemen anzuwenden und zu beachten.

Was die damit gebotene Rechtsgrundlage der Datenverarbeitung anbelangt, so ist diese betreffend Gesundheitsdaten in Art. 9 DSGVO, betreffend allgemeiner Daten (nicht gesundheitsbezogene Mobilitätsdaten usw.) dagegen in Art. 6 DSGVO zu suchen. Zusätzlich kann bei Zugriff auf im Endgerät bereits gespeicherte Daten Telekommunikationsrecht in Umsetzung der ePrivacy-Richtlinie anwendbar sein.

Relativ unproblematisch ist die Verarbeitung von Daten der erkanntermaßen infizierten Person selbst sowie ihrer Kontakte auf Art. 9 Abs. 2 lit. i oder lit. h DSGVO i.V.m. dem EpidemieG, § 10 Abs. 2 DSG sowie weiteren nationalen Rechtsvorschriften zu stützen.[11] Was die vorsorgliche Speicherung von Kontaktdaten anbelangt, ist dagegen danach zu differenzieren, auf wessen Initiative hin die Verwendung der App und damit die Erhebung und weitere Verarbeitung der Daten erfolgt. Ergreift die Initiative die betroffene Person selbst, indem sie – um einen Beitrag zur Eindämmung der Pandemie zu leisten – die App freiwillig nutzt, kann die Verarbeitung regelmäßig bereits auf die freie und informierte Einwilligung der betroffenen Person (Art. 6 Abs. 1 lit. a, Art. 9 Abs. 2 lit. a DSGVO) gestützt werden. Erfolgt die Verwendung dagegen primär auf staatliche Initiative oder auf Initiative der Betreiberin bzw. des Betreibers einer Einrichtung, ist die

---

10 Vgl. i.d.S. auch allgemein ErwGr 28 zur DSGVO sowie EDPB Guidelines (Fn. 11), Annex: Contact tracing applications analysis guide; Chaos Computer Club, 10 requirements for the evaluation of "Contact Tracing" apps, 6.4.2020, https://www.ccc.de/en/updates/2020/contact-tracing-requirements.

11 European Data Protection Board, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 21 April 2020, Rn. 33, abrufbar unter https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf; implizit kritisch gegenüber der „Enttarnung" von COVID-Kranken ohne deren Einwilligung Forgó, Einige Bmerkungen zu datenschutzrechtlichen Rahmenbedingungen des Einsatzes von Tracing Apps zur Bekämpfung der COVID-19-Krise, Version 1.0 (13.4.2020) 10, abrufbar unter https://id.univie.ac.at/fileadmin/user_upload/i_id/Website_Header_IDLaw/Gutachten13.pdf.

für eine Einwilligung erforderliche Freiwilligkeit nur schwierig herzustellen (insbesondere wäre es nach Art. 7 Abs. 4 DSGVO unzulässig, eine Leistung von der Einwilligung abhängig zu machen). Je nach konkreter Ausgestaltung des Systems wird es dann eine spezifische Rechtsgrundlage im Sinne des Art. 6 Abs. 1 lit. c oder e i.V.m. Abs. 3 DSGVO oder allenfalls auch des Art. 9 Abs. 2 lit. g DSGVO brauchen.

Eine solche ist dem EpidemieG in seiner derzeit geltenden Fassung bei grundrechtskonformer Lesart nicht zu entnehmen, insbesondere auch nicht dessen § 5 Abs. 3. Es bedürfte im Fall von Contact Tracing im Zusammenhang mit einem Theaterbesuch udgl. also entweder einer Anpassung des EpidemieG oder einer Grundlage in spezieller COVID-19-Gesetzgebung. Diese spezielle gesetzliche Grundlage muss u.a. geeignete Garantien für betroffen Personen, klare Zweckbegrenzungen für die Datenverarbeitung sowie eindeutige Bestimmung der Stellen, an welche Daten übermittelt werden dürfen, sowie die Bedingungen, unter welchen dies erfolgen darf, enthalten.[12] Auch die Festlegung weiterer Details, insbesondere betreffend Speicherfristen, die Bedingungen einer Weiternutzung für Forschungszwecke udgl. sollten in diesem Gesetz geregelt werden.

Bei allem hat die Datenverarbeitung den allgemeinen, in Art. 5 DSGVO zum Ausdruck kommenden Grundsätzen der Datenverarbeitung zu folgen, u.a. dem Gebot der Datenminimierung, der Zweckbindung, der Speicherbegrenzung und der Gewährleistung bestmöglicher Datensicherheit. Zur Zweckbindung gehört es dabei u.a., dass jede mit dem Zweck der Datenerhebung unvereinbare Sekundärnutzung – insbesondere etwa in gerichtlichen oder behördlichen Verfahren gegen die betreffende Nutzerin bzw. den betreffenden Nutzer – ausgeschlossen ist. Diese Grundsätze sind auch bereits durch das technische Design selbst zu verwirklichen (Privacy-by-Design, vgl. Art. 25 DSGVO).

3.7 Gerechtigkeit und Verhinderung von Diskriminierung

Die Verwendung von Apps zur Unterstützung des Contact Tracing kann nur dann empfohlen werden, wenn sichergestellt ist, dass jenen Menschen, die diese Apps nicht verwenden können oder aus zu respektierenden Gründen nicht nutzen wollen (oder jene, für die dies nur mit Schwierigkeiten möglich ist) keine Nachteile bezüglich ihrer Bewegungsfreiheit und Autonomie entstehen. Sollten Contact Tracing-Apps großflächig eingeführt werden, wird es in manchen Fällen unvermeidlich sein, dass die Identifikation von Menschen, die daran nicht teilnehmen, etwas länger dauert, und dass dadurch eventuell weitere Personen infiziert werden. Die Nichtverwendung von Apps darf dabei den Menschen nicht zu Lasten gelegt werden; auch darf in die Privatsphäre dieser Menschen nicht durch Ersatzmaßnahmen (z. B. Überwachung von elektronischen Zahlungsströmen, um nachzuvollziehen, wo sie sich wann aufgehalten haben) stärker eingegriffen werden als es bei App-Benutzerinnen bzw. -Benutzern der Fall ist.

---

12 EDPB Guidelines (Fn. 11) Rn. 31; noch weitergehend Forgó (Fn. 11) S. 34.

3.8 Gesamtgesellschaftliche Auswirkungen – auf dem Weg in eine Überwachungskultur?

Als „function creep" bezeichnet man in der Fachliteratur die Situation, Daten oder Technologien für immer weitere Zwecke heranzuziehen „weil sie nun mal schon da sind". Wie wir aus empirischen Studien wissen,[13] gehört dies zu den wichtigsten Sorgen der Menschen. Selbst wenn diese Apps so datenschutzfreundlich sind, dass das Risiko missbräuchlicher Nutzung ausgeschlossen ist, kann allein die Gewöhnung an die Nutzung von Apps einen fruchtbaren Boden für „function creep" bieten. Um diesen Prozess zu vermeiden, wäre es wichtig, die Mitentscheidung seitens der Nutzerinnen und Nutzer durch geeignete Strukturen sicherzustellen und die automatische Löschung von Daten oder deren Anonymisierung (zu Forschungszwecken) und die Deaktivierung der betreffenden Applikationen und Backend-Strukturen nach dem Ende der Pandemie sicherzustellen.

Zudem sind aus einer Perspektive auf gesamtgesellschaftliche Auswirkungen auch Aspekte der wirtschaftlichen Dominanz und der wirtschaftlichen und politischen Macht zu beachten. Auch wenn Technologiekonzerne wie Google, Apple, oder Amazon sich an Corona-Apps nicht direkt bereichern, so ist die Einbindung ihrer Technologie in Contact Tracing und Datenerfassungs- oder Archivierungsstrategien doch in der Hinsicht problematisch, dass damit mächtige Großunternehmen ihre marktdominierende Position noch weiter ausbauen können - und auch mehr politisches Gewicht erlangen.[14] Der amerikanische Rechtswissenschafter Frank Pasquale diagnostizierte bereits vor einigen Jahren, dass solche Firmen durch ihren wirtschaftlichen und politischen Einfluss von Marktteilnehmern zu Regulierungsinstanzen geworden waren.[15] Auch wenn es in Österreich kein Eigentumsrecht durch Dritte an persönlichen Daten der Menschen gibt, so spielt es doch eine wesentliche Rolle, wer die Kontrolle über Datensätze großer Teile der Bevölkerung hat: ein privates, multinationales Unternehmen oder eine Organisation, die demokratischer Kontrolle unterliegt und der Öffentlichkeit gegenüber rechenschaftspflichtig ist.

---

13 Z. B. Ipsos, M.O.R.I., 2016. The one-way mirror: public attitudes to commercial access to health data. London: Wellcome Trust.

14 Z.B Sharon, T., 2016. The Googlization of health research: from disruptive innovation to disruptive ethics. Personalized Medicine, 13(6), pp.563-574. Prainsack, B., 2020. The political economy of digital data: introduction to the special issue. Policy Studies [online first].

15 Pasquale F. (2017) From territorial to functional sovereignty: The case of Amazon. Law and Political Economy (6 December). Available at: https://lpeblog.org/2017/12/06/from-territorial-to-functional-sovereignty-the-case-of-amazon/ (accessed 1 June 2020).

4 Freiwilligkeit und Verpflichtung

Die wohl am kontroversesten diskutierte Frage rund um die ethische Bewertung von Contact Tracing Apps stellt diejenige dar, inwieweit die Verwendung vollkommen freiwillig bleiben muss oder der Staat oder private Einrichtungen die Verwendung vorschreiben oder zumindest zur Bedingung dafür machen können, bestimmte Orte betreten und bestimmte Leistungen in Anspruch nehmen zu können. Diese Frage ist zwar eng mit derjenigen nach der datenschutzrechtlichen Rechtsgrundlage verknüpft, aber keinesfalls identisch:[16] Auch dann, wenn die Datenverarbeitung auf eine gesetzliche Rechtsgrundlage, und nicht auf eine Einwilligung der betroffenen Person, gestützt wird, kann es dennoch geboten sein, die Verwendung einer App rein freiwillig auszugestalten.

4.1 Zulässigkeit staatlicher Vorgaben

Jede staatlicherseits angeordnete Verpflichtung zur Nutzung einer App stellt einen Eingriff in Grundrechte dar. Dies gilt selbst dann, wenn (noch) überhaupt keine personenbezogenen Daten das Endgerät der Nutzerin bzw. des Nutzers verlassen, da schon die Aktivität der App auf dem Endgerät selbst einen Eingriff darstellt (Bluetooth-Verbindung, Akkuverbrauch, Speicherplatz) und außerdem nicht nur die objektiv verarbeiteten Daten und sonstige objektive Einschränkungen zu berücksichtigen sind, sondern auch das subjektive Gefühl vieler Menschen, staatlich überwacht zu werden bzw. dass sich die Gesellschaft in die Richtung einer Überwachungsgesellschaft entwickelt, und damit verbundenes Unbehagen. Damit muss jede derartige Verpflichtung strikt dem Prinzip der Verhältnismäßigkeit genügen.

Ist das Verhältnismäßigkeitsprinzip gewahrt, ist es aber – sofern die oben (3). dargelegten ethische und rechtlichen Anforderungen erfüllt sind – prinzipiell in Epidemiezeiten denkbar, dass ein Staat eine – von vornherein befristete – Verpflichtung zur Nutzung derartiger Apps einführt. Dies kann insbesondere dann gerechtfertigt sein, wenn die Alternative nur die gänzliche Untersagung vieler Aktivitäten wäre, also ein in aller Regel drastischerer Eingriff in Grundrechte (z. B. Freizügigkeit, Versammlungsfreiheit, Erwerbsfreiheit, Freiheit der Religionsausübung, Freiheit der Kunst usw.), so dass sich die Verwendung einer App letztlich als das gelindere Mittel darstellt. In diesem Kontext sind die konkrete Architektur einer App und die mit dieser verbundenen datenschutzrechtlichen Implikationen sowie die alternativ möglichen Formen der Nachverfolgung

16 EDPB Guidelines (Fn. 11) Rn. 29.

und des Tracings ins Kalkül zu ziehen. Eine solche Maßnahme bedürfte in jedem Fall einer spezifischen, möglichst befristeten gesetzlichen Grundlage, also entweder der Aufnahme einer neuen Vorschrift im EpidemieG oder einer speziellen COVID-19-Regelung.

Eine allgemeine Verpflichtung zur Verwendung einer App (etwa: an allen öffentlichen Orten) wäre wohl in jedem Fall unverhältnismäßig, zumal auch ohne eine App keine Sperrung aller öffentlichen Orte droht bzw. grundrechtlich in Betracht kommt. Auch für diejenigen Orte und Einrichtungen, für die allseits akzeptierte und gangbare Benützungsregelungen (Abstand, Mund-Nasen-Schutz udgl.) gefunden werden konnten, dürfte die weitere Anwendung dieser Regelungen die geeignetere und verhältnismäßigere Maßnahme darstellen.

Eine verpflichtende Einführung der App könnte aber für Orte und Einrichtungen erwogen werden, die derzeit aus epidemiologischen Gründen noch geschlossen sind oder bei denen die Einhaltung derzeit geltender Benützungsregelungen für alle Beteiligten so gravierende Einschränkungen mit sich bringt, dass sich die Verwendung der App unter Abwägung aller Umstände als der mildere Grundrechtseingriff darstellt. Um mögliche Effekte einer Diskriminierung auszuschließen, müssten für Personen, die kein Smartphone besitzen oder deren Betriebssystem aus irgendwelchen Gründen mit einer App nicht kompatibel ist, Alternativen (z. B. Formen einer herkömmlichen Registrierung) gefunden werden.

Daher kann sich die Verpflichtung zu digitalem Contact Tracing als Bedingung für die Nutzung einer Einrichtung als verhältnismäßige Maßnahme darstellen, sofern neben den unter 3 beschriebenen ethischen und rechtlichen Anforderungen die folgenden Voraussetzungen kumulativ erfüllt sind:

- Die Einrichtung gehört nicht zur Grundversorgung (also etwa nicht bei Supermärkten, Apotheken, Spitälern, öffentlichen Massenverkehrsmitten odgl.)
- Aus epidemiologischer Sicht wäre die Alternative, dass die Einrichtung gar nicht betrieben werden kann (insbesondere, weil anderweitige Schutzmaßnahmen aus technischen oder wirtschaftlichen Gründen nicht durchführbar sind) oder dass für andere Personen unzumutbare Einschränkungen (z. B. infolge von Knappheit und Wartezeiten) entstehen, in Summe also ein noch stärkerer Grundrechtseingriff erfolgte als durch die App.
- Es werden Lösungen (z. B. Leihgeräte mit Registrierung) für Menschen gefunden, denen es (aufgrund von Alter, Gesundheitszustand, Einkommen odgl.) nicht zugemutet werden kann, ein Smartphone oder die App zu nutzen, und damit eine Diskriminierung zuverlässig vermieden.

Zusätzlich kann im Rahmen eines größeren Schutzkonzepts für Einrichtungen erwogen werden, unter Wahrung des Verhältnismäßigkeitsprinzips eine Verpflichtung zur Nutzung derartiger Apps für bestimmte Berufsträgerinnen und Berufsträger vorzusehen, die mit besonders vielen wechselnden Menschen in engem physischem Kontakt stehen und daher als besondere Ansteckungs-Multiplikatoren wirken könnten (z. B. Gesundheits-

berufe, Kindergärtnerinnen und Kindergärtner). Ergänzend dazu müssen Menschen, die einem besonders hohen Infektionsrisiko ausgesetzt sind, allerdings durch engmaschige Testung und händisches Nachverfolgen begleitet werden.

4.2 Zulässigkeit von Vorgaben privater Akteure

Wenn private Akteure (z. B. Supermärkte, Restaurants) den Abschluss eines Vertrags von der Erfüllung bestimmter Voraussetzungen abhängig machen, sind bei Massengeschäften zunächst die Vorschriften des III. Teils des Gleichbehandlungsgesetzes (GlBG) zu berücksichtigen. Allerdings dürfte sich eine mittelbare Diskriminierung aufgrund eines der dort genannten Merkmale kaum je konstruieren lassen (anders aufgrund einer abweichenden Rechtslage in Deutschland). Weitergehender Diskriminierungsschutz (z. B. aufgrund des Alters – hier möglicherweise relevant) besteht nach dem II. Teil in der Arbeitswelt. Sofern nicht weitere Spezialregelungen (z. B. NahversorgungsG) eingreifen, sind darüber hinaus die Grundsätze über den allgemeinen Kontrahierungszwang zu berücksichtigen. Das bedeutet, dass ein Unternehmer, der die Leistung bestimmter Sachen oder Dienste öffentlich in Aussicht stellt, einem zum angesprochenen Personenkreis gehörigen Interessenten, wenn diesem zumutbare Ausweichmöglichkeiten fehlen, die zur Befriedigung seines Bedarfs nötige einschlägige Leistung und den sie vorbereitenden Vertragsschluss ohne sachlich gerechtfertigte Gründe nicht verweigern darf, wenn es sich dabei um „Normalbedarf“ oder „Notbedarf“ handelt und er willens und in der Lage ist, sie zu den gewöhnlichen Bedingungen zu erwerben. Daran ändert im Prinzip auch das Hausrecht nichts, d.h. das Hausrecht erfährt insoweit eine Beschränkung. Auch außerhalb eines Kontrahierungszwanges ist aus dem Grundrecht auf Persönlichkeitsschutz jeder diskriminierende Ausschluss von der Inanspruchnahme einer Leistung zu vermeiden, wenn eine hinreichende sachliche Rechtfertigung nicht gegeben ist; maßgebend dabei ist, dass bei dem Zusammenprall der Interessen des Befugten, nach seiner Disposition Verträge zu schließen, und den Interessen anderer, nicht diskriminierend ungleich behandelt zu werden, die durch die guten Sitten gezogenen Grenzen nicht überschritten werden.[17] Damit konzentriert sich alles auf die Frage, ob die Verweigerung des Vertragsschlusses mit einem Kunden ohne App „sachlich gerechtfertigt“ wäre.

4.3 Gesetzliche Absicherung der Freiwilligkeit?

Wiederholt ist gefordert worden, nicht die Verpflichtung zur Teilnahme an digitalem Contact Tracing gesetzlich zu regeln, sondern vielmehr primär die absolute Freiwillig-

17 So z. B. OGH 3 Ob 548/91.

keit der Maßnahme gesetzlich festzuschreiben.[18] Dies mag zwar auf den ersten Blick erstaunen, ist doch Freiheit die Regel, und staatlicher Zwang die Ausnahme, die es gesetzlich festzuschreiben und zu begründen gilt. Bei näherem Hinsehen zeigt sich aber in der Tat, dass zwischen Freiwilligkeit und staatlichem Zwang ein fließender Übergang besteht, weil durch das Hinzutreten der Betreiberinnen bzw. Betreiber von Einrichtungen eine Situation eintreten kann, in der auch ohne jeglichen (direkten) staatlichen Zwang de facto die Verwendung der App verpflichtend wird. So ist etwa jede Betreiberin bzw. jeder Betreiber einer Einrichtung, jede Veranstalterin bzw. jeder Veranstalter usw. ohnehin verpflichtet oder zumindest gehalten, ein COVID-19-Schutzkonzept für die Einrichtung bzw. Veranstaltung zu erarbeiten, um allfällige Schadenersatzansprüche abzuwehren oder einen Reputationsverlust zu vermeiden. Dabei gehört es zu den naheliegendsten – weil für die Betreiberin und den Betreiber bzw. die Veranstalterin und den Veranstalter besonders einfach und kostengünstig zu implementierenden – Komponenten eines solchen Schutzkonzepts, digitales Contact Tracing vorzuschreiben. Auch Datenschutzgesichtspunkte können für Betreiberinnen bzw. Betreiber dafür sprechen, lieber die Verwendung einer App mit einer dezentralen Architektur vorzuschreiben anstatt weitaus eingriffsintensivere, „händische" Methoden (z. B. Erfassung von Kontaktdaten der Kundinnen und Kunden zur Weitergabe an Gesundheitsbehörden im Bedarfsfall) zu nutzen. Es ist daher nicht fernliegend, zu erwarten, dass sich auch ohne jeglichen staatlichen Zwang eine relativ flächendeckende Vorschreibung digitalen Contact Tracings durch private Akteure etablieren könnte.

Aus diesen Gründen – und auch um für alle Beteiligten Rechtssicherheit zu schaffen – kann es in der Tat empfehlenswert sein, die Voraussetzungen, unter denen auch seitens privater Akteure die Verwendung digitalen Contact Tracings zur Vorbedingung für die Nutzung einer Einrichtung oder die Teilnahme an einer Veranstaltung gemacht werden kann, gesetzlich abschließend festzuschreiben. Diesbezüglich werden letztlich die Überlegungen, welche zur Rechtfertigung einer staatlichen Verpflichtung oben unter 4.1 herausgearbeitet wurden, ebenfalls maßgeblich sein.

18 So dezidiert Forgó (Fn. 11) S. 34; angedeutet in EDPB Guidelines (Fn. 11) Rn. 31.

5 Schlussfolgerungen und Empfehlungen

1. Contact Tracing ist in einer Pandemie alternativlos. Dies gilt insbesondere für eine Phase, in welcher sich die Verbreitung der Infektion noch (oder bereits wieder) in einem Bereich bewegt, in dem die gezielte Isolierung von Infektionsclustern flächendeckende Einschränkungen für die gesamte Bevölkerung entbehrlich macht. Es kann daher nur um das Wie, und nicht um das Ob, von Contact Tracing gehen. Diesbezüglich werden neben klassischem („händischem") Tracing immer mehr auch verschiedene Formen des digital gestützten Contact Tracking und Tracing diskutiert, insbesondere unter Verwendung digitaler Applikationen auf Mobiltelefonen („Corona-Apps").
2. Mindestanforderungen an derartige Applikationen sind ihre epidemiologische Geeignetheit, die Einbettung in eine Gesamtstrategie, Eignung im grenzüberschreitenden Kontext, Folgeabschätzung und regelmäßige Evaluierung und ggf. Adaptierung, Transparenz, umfängliche Gewährleistung von Datenschutz und Datensicherheit einschließlich der zeitlichen Begrenzung der Maßnahme, die zuverlässige Verhinderung von Diskriminierung und eine sorgfältige Abwägung und Steuerung gesamtgesellschaftlicher Auswirkungen. Letzteres betrifft auch und gerade effektive Maßnahmen gegen „function creep", also die schleichende Etablierung von Überwachungstechnologien über den konkreten Anlassfall der COVID-19-Pandemie hinaus.
3. Eine detaillierte Regelung im EpidemieG oder in spezieller COVID-Gesetzgebung, welche neben den Voraussetzungen für die Anwendung der Maßnahme auch deren begrenzte Dauer, das Verbot der Datenverarbeitung zu anderen Zwecken als denen der Eindämmung von COVID-19 und weitere Punkte ausdrücklich klarstellt, ist im Interesse der Rechtssicherheit für alle Beteiligten zu fordern. Eine Begleitung der Maßnahme durch ein multidisziplinäres Expertengremium wäre wünschenswert. Zusätzlich könnte die zivilgesellschaftliche Kontrolle durch die Etablierung eines Nutzergremiums erhöht werden, das bei Entscheidungen über sich verändernde Funktionalitäten der App ein Mitspracherecht hat.

4. Die Verwendung solcher Applikationen muss grundsätzlich auf Freiwilligkeit beruhen, wobei bereits unterhalb der Schwelle gesetzlicher Verpflichtung und insbesondere durch das Hinzutreten privater Akteure (z. B. Betreiberinnen bzw. Betreiber von Einrichtungen oder Veranstalterinnen bzw. Veranstalter) echte Freiwilligkeit oft nicht gegeben ist. Es sollten daher für staatliche wie für private Akteure ähnliche Bedingungen formuliert werden, unter denen die Verwendung einer bestimmten Applikation zur Bedingung für die Nutzung einer Einrichtung oder die Inanspruchnahme einer Leistung gemacht werden kann. Menschen, die solche Applikationen nicht verwenden wollen oder können, darf dies zu keinen Nachteilen bezüglich ihrer Bewegungsfreiheit oder Autonomie gereichen.
5. Eine Verpflichtung zu digitalem Contact Tracing kann gerechtfertigt sein für die Nutzung von Einrichtungen, die nicht zur Grundversorgung zählen (also bspw. Konzerthäuser oder Restaurants, nicht dagegen Supermärkte, Spitäler oder öffentliche Verkehrsmittel). Dies gilt aber nur bei strikter Verhältnismäßigkeit der Maßnahme. Diese ist grundsätzlich nur dann gegeben, wenn anderenfalls die betreffende Einrichtung (z. B. Konzerthaus) geschlossen bliebe oder nur unter unzumutbaren Einschränkungen betrieben werden könnte und daher insgesamt ein noch schwererer Grundrechtseingriff erfolgen müsste, sich digitales Tracing also unter Grundrechtsgesichtspunkten als das mildere Mittel darstellt. Für Personen, die kein Smartphone besitzen oder zur Verwendung entsprechender Endgeräte nicht in der Lage sind, müssen zur Vermeidung einer Diskriminierung zumutbare Alternativen geschaffen werden.
6. Digital gestütztes Contact Tracing – auch unter Verwendung von Apps – muss sich ständig neuen epidemiologischen Erkenntnissen anpassen und sollte für verschiedene Situationen möglichst maßgeschneiderte Lösungen bereithalten, ohne die einzelnen Nutzerinnen und Nutzer mit der hinter diesen Lösungen liegenden Komplexität zu konfrontieren. Dabei wäre etwa auch das „Superspreader"-Phänomen angemessen zu adressieren. Digitale Tracing-Lösungen sollten daher für bestimmte Berufsträgerinnen und Berufsträger entwickelt werden, die in besonders gravierender Weise als Multiplikatoren des Virus fungieren können (z. B. Kindergärtnerinnen und Kindergärtner, Gesundheitspersonal). Auch wären für bestimmte Typen von Veranstaltungen, Orte und Einrichtungen, bei denen das derzeit gängige Bluetooth-gestützte Proximity Tracing nicht oder nicht gut funktioniert, spezielle technische Lösungen zu entwickeln.

Mitglieder der Bioethikkommission für das Mandat 2017 bis 2020

Vorsitzende
Dr. Christiane Druml

Stv. Vorsitzender
Univ.-Prof. Mag. Dr. Markus Hengstschläger

Stv. Vorsitzender
Univ.-Prof. Dr. h.c. Dr. Peter Kampits

Univ.-Prof. DDr. Matthias Beck
Univ.-Prof. Dr. Alois Birklbauer
Dr. Andrea Bronner
Univ.-Prof. Dr. Christian Egarter
Dr. Thomas Frühwald
Dr. Ludwig Kaspar
Univ.-Prof. Dr. Lukas Kenner
Dr. Maria Kletecka-Pulker
Univ.-Prof. Dr. Ursula Köller MPH
Univ.-Prof. Mag. Dr. Michael Mayrhofer
Univ.-Prof. Dr. Johannes Gobertus Meran MA
Dr. Stephanie Merckens
Univ.-Prof. Dr. Siegfried Meryn
Univ.-Prof. Dr. Christina Peters
Univ.-Prof. Mag. Dr. Barbara Prainsack
Univ.-Prof. DDr. Walter Schaupp
Univ.-Prof. Dr. Andreas Valentin MBA
Dr. Klaus Voget
Univ.-Prof. Dr. Ina Wagner
Priv.-Doz. Dr. Jürgen Wallner MBA
Univ.-Prof. Dr. Christiane Wendehorst LL.M
Univ.-Prof. Dr. Gabriele Werner-Felmayer