“Berliner Positionspapier": Freiwillige Corona-App

Positionspapier zu datenbasierten Ansätzen zur Eindämmung der Corona-Pandemie
LAG Digitales und Netzpolitik, Bündnis 90/Die Grünen Berlin
Beschluss im Umlaufverfahren (8. Mai 2020)

Deutschland streitet um Corona-App-Lösungen als Maßnahme zur Eindämmung der COVID-19-Pandemie. Entscheidungsträger*innen und Expert*innen sind sich nicht nur uneinig darüber, welchen Beitrag eine App bei der Pandemiebekämpfung leisten kann, sondern haben auch unvereinbare Vorstellungen darüber, wie die App funktionieren soll und welchen technischen Anforderungen sie genügen muss, um den datenschutzrechtlichen Vorgaben zu entsprechen.

Unsere Forderungen in Kürze:

Wir, die LAG Digitales und Netzpolitik von Bündnis 90/Die Grünen Berlin, setzen uns für eine **freiwillige Corona-App** ein. Bürger*innen sollen über diese App erfahren können, ob sie mit einer Person, die (möglicherweise) mit Sars-CoV-2 infiziert ist, in Kontakt standen und sich dadurch angesteckt haben könnten. Eine solche App kann ein wichtiger Baustein im Informationskonzept zur Eindäummung der Pandemie sein. Sie kann nur helfen, wenn sie von der Bevölkerung als Zusatzmaßnahme angesehen wird und zusammen mit anderen Eindämmungsmaßnahmen verwendet wird – beispielsweise “Abstandhalten” und Händewaschen. Wir fordern, dass die App schnell entwickelt wird, um bereits vor Beginn einer möglichen zweiten Welle verwendet werden zu können. Die derzeit einzig datenschutzfreundliche und rechtsstaatliche Lösung zur Erkennung von möglichen Kontakten ist die Verwendung der **Bluetooth**-Technik der Smartphones. Andere Ansätze – wie die Verwendung von Standort- und Bewegungsdaten auf Grundlage von GPS – sind ohnehin nicht erfolgversprechend, weil die Daten aus technischen Gründen zu ungenau sind. Die Lösung muss open source programmiert und frei überprüfbar sein. Der Bundesdatenschutzbeauftragte muss bei der Entwicklung der App von miteinbezogen werden. Staatliche Zertifizierungen würden das Vertrauen in die App stärken. Wir setzen uns für einen dezentralen Ansatz ein (sog. Peer-to-Peer-Modell). Das heißt: Die App speichert sämtliche persönlichen Daten **auf den Geräten der Verwender*innen**. Das DP3T-Konzept, das von Expert*innen entwickelt und unterstützt wurde, halten wir für einen möglichen Weg, um dies zu erreichen. Aufgezeichnete anonymisierte Kontaktdaten sollen auf einem sicheren Server liegen, und einer strikten Zweckbindung und klarer Löschfristen unterliegen. Auch muss die nötige Staatsferne sichergestellt werden.
Ein solcher dezentraler Ansatz verhindert, dass sensible Gesundheitsdaten unnötig an einer zentralen Stelle gespeichert werden. Das stärkt den Datenschutz der Bürger*innen, ohne dass das System deshalb schlechter funktionieren würde. Das dezentrale System bietet weniger Risiken eines missbräuchlichen Zugriffs auf die sensiblen Daten der Nutzer*innen. Sofern die Verwender*innen nach der App möglicherweise in Kontakt mit einer infizierten Person standen, müssen sie sich einer Untersuchung unterziehen können. Derzeit ist es nach unserer Überzeugung nicht möglich, tiefgreifende

Freiheitsbeschränkungen – wie beispielsweise Ausgangssperren – damit zu begründen, dass sich eine Person nach der App infiziert haben könnte. Für die Nutzer*innen der App darf auch kein Vorteil in dem Sinne entstehen, dass nur bei Verwendung der App der Zugang zu bestimmten Einrichtungen gestattet wird.

Zu dieser Position kommen wir aus den folgenden Gründen:

A. Hilft eine App gegen Corona?

Die Corona-Pandemie bedroht weltweit Menschenleben und Gesellschaften. Bund und Länder haben Maßnahmen beschlossen, um die Pandemie einzudämmen. Diese Maßnahmen waren und sind erforderlich, um Bürger*innen vor einer Erkrankung zu schützen. Zugleich beschränken sie Grundrechte in einer Form, die es so noch nie gab und die auch Expert*innen noch vor Kurzem nicht für möglich gehalten hätten. Die Maßnahmen der letzten Wochen scheinen erste Erfolge zu zeigen . Die Infektionsraten bewegen sich noch im Vergleich auf einem relativ niedrigen Niveau. Da die Grundrechtseinschränkungen wesentlich sind, müssen Entscheidungsträger*innen dynamisch beurteilen, ob weiterhin an den Maßnahmen festgehalten werden kann und in welchem Maße. Staatliche Akteure nehmen die vorläufigen Erfolge zum Anlass, Freiheitsbeschränkungen nach und nach zurückzudrehen. Warum diskutieren wir jetzt darüber, was für eine App wir brauchen?

Die Pandemie ist noch nicht vorbei. Ganz im Gegenteil: Expert*innen befürchten, dass eine zweite Welle droht und die Zahl der Erkrankten erheblich ansteigen könnte. Deutschland braucht jetzt ein Gesamtkonzept, wie dem entgegengewirkt werden kann. Eine App kann ein Bestandteil dieses Konzepts sein. Um die App sinnvoll einsetzen zu kennen, ist es wichtig zu verstehen, was Nutzer*innen von einer App erwarten können, wer möglicherweise Interesse an welchen Daten haben könnte und was eine App nicht leisten kann.

Was kann eine App nicht leisten? Eine Corona-App kann die Bedrohung der Pandemie *erstens* nicht im Alleingang lösen. Sie rettet für sich genommen kein Menschenleben, sondern kann nur ein Puzzlestück in einem Gesamtkonzept zur Eindämmung sein. Der Nutzen ist beispielsweise gering, wenn Verdachtsfälle aufgedeckt werden können, aber keine Testkapazitäten bestehen. Eine App verhindert keine Infektion. Nur das sorgsame Verhalten der Bürger*innen kann die Pandemie eindämmen. Wichtig ist, dass die Bevölkerung durch ihr Verhalten verhindert, dass sich ihre Mitmenschen infizieren – beispielsweise, indem sie ausreichend Abstand halten. *Zweitens* kann eine App keine absolute Sicherheit schaffen: Schon weil ein erheblicher Teil der Bürger*innen kein Smartphone verwendet, ist ein System lückenhaft. Vor allem Menschen, die wegen ihres Alters der Risikogruppe angehören, haben oftmals kein Gerät , auf dem sie die

App verwenden könnten. Hilfsmittel wie Bluetooth-Armbänder können das Problm lindern, aber ändern die Diagnose nicht grundlegend: Wenn eine Gesellschaft darauf vertraut, über ein solches System völlige Sicherheit über Infektionen zu erlangen, liegt sie einem Fehlglauben auf. Diese “falsche Sicherheit” wäre nicht nur töricht, sondern sie ist gefährlich.

Was eine App kann: Sie kann *erstens* helfen, Infektionsketten nachzuvollziehen. Das verbessert die Datenlage und ermöglicht das eigene Infektionsrisiko besser einzuschätzen. Damit kann sie **zu einem rücksichtsvollen Umgang** miteinander **beitragen**. Sie hilft der Zivilgesellschaft und ermöglicht es ihr, einen Beitrag zur Eindämmung der Pandemie zu leisten. Kurz: Eine App schützt nicht, sondern sie informiert. *Zweitens*: Eine freiwillige **Corona-App gewährleistet Freiheit** und beschränkt sie nicht; wenn sie richtig konzipiert ist. Wenn das Infektionsrisiko in der Gesellschaft sinkt und die Mehrheit der Bürger*innen sich verantwortungsvoll verhält, muss der Staat Freiheitsbeschränkungen zurückdrehen. Eine freiwillige App ermöglicht es Bürger*innen, verantwortungsbewusster zu handeln. Ergreifen sie diese Chance, nimmt damit die Gefährdung der Epidemie für die Allgemeinheit ab. Dann kann und muss der Staat andere Freiheiten weniger stark beschränken, als er das gerade tut. Eine freiwillige App ermöglicht es dem Staat, die Freiheit der Bürger*innen wieder aufleben zu lassen . Wenn Bürger*innen einen Beitrag dazu leisten können, die Pandemie einzudämmen, hilft das dem Staat im Gegenzug, das öffentliche Leben schrittweise wiederherzustellen. Das setzt voraus, dass viele die App verwenden wollen und sich den Maßnahme nicht verschließen. Einen Zwang zur App kann praktisch nicht kontrolliert werden. Die Erfahrung der letzten Wochen zeigt außerdem: Die Mehrheit will helfen, die Epidemie einzudämmen. Eine Pflicht zur App würde deren Erfolg nicht nur unterwandern, sondern wäre auch nicht angemessen.

B. Welche Lösungsansätze stehen zur Debatte?
Entscheidungsträger diskutieren gerade vor allem darüber, wie eine App programmiert und eingesetzt werden kann, um zur Eindämmung der Pandemie beizutragen. Der hier vorgestellte Ansatz für eine App ist jedoch nicht der einzige **technische Lösungsansatz**, um zu zu bestimmen, welche Personen in Kontakt zueinander standen. In den letzten Wochen wurden bereits mehrere Vorschläge unterbreitet wie z.B. eine Nachverfolgung der Bewegungsdaten von Bürger*innen im Wege einer nicht-freiwilligen Funkzellenabfrage

Die Entfernungsbestimmung über Bluetooth ist der einzige Ansatz, der einen Kontakt zwischen Personen sinnvoll nachvollziehen kann. Positionsbasierte Verfahren sind für diesen Zweck nicht geeignet.

I. Positionsbasierte Verfahren

Bei **positionsbasierten Verfahren** werden die Bewegungsprofile mehrerer Personen miteinander abgeglichen. Standort und Zeitpunkt werden benutzt, um einen Kontakt von Personen mit einer gewissen Wahrscheinlichkeit zu diagnostizieren. Es gibt derzeit **zwei Ansätze**: Erstens die Auswertung der **Daten, die Telekommunikationsunternehmen** bereits heute erheben, und zweitens die Verwendung von **GPS-Informationen** der Smartphones.

1. Telekommunikationsdaten (Funkzellendaten)

Bei den reinen Telekommunikationsdaten wird eine Handynummer von einem Server erfasst, sobald sich das Handy mit einer von vielen Mobilfunkbasisstationen verbindet. Das heißt, die auf dem Server gespeicherten Daten beinhalten Handynummer, Basisstation und Zeitstempel. Den Bereich, den eine Mobilfunkbasisstation abdeckt, bezeichnet man als **Funkzelle**. Somit lässt sich ermitteln, über welchen Zeitraum sich zwei Personen gemeinsam in derselben Funkzelle aufgehalten haben. Die **Durchmesser** der Zellen reichen **von unter 100 Metern bis zu mehreren Kilometern**. Dies ist für die flächendeckende Ermittlung von Kontaktpersonen **absolut ungeeignet**. Selbst wenn sich in einzelnen Gebieten die Position auf technischem Wege (z.B. über Triangulierung mehrerer Mobilfunkantennen) noch präzisieren lässt, ändert das nichts an der Bewertung: Der Ansatz ist zu ungenau.

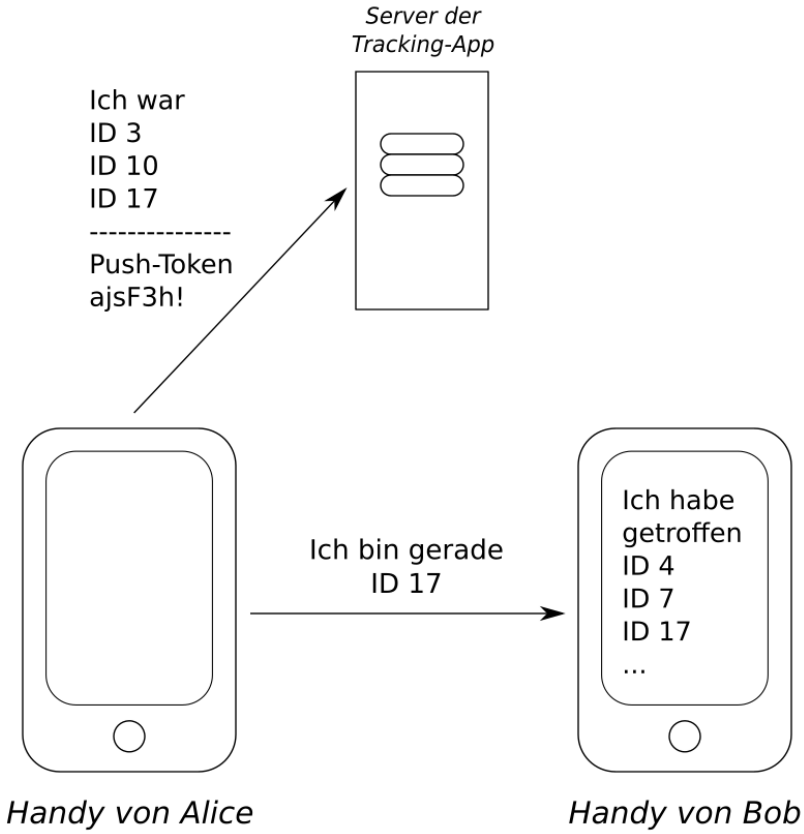
2. Standortdaten

Mittels der von einem Handy ermittelten **GPS-Position** ist eine bessere Standortbestimmung möglich. Der aktuelle Standort des Handys würde von einer App in kurzen Zeitabständen an einen Server geschickt werden. Unter freien Himmel hat GPS eine Genauigkeit von 2-13 Metern. Probleme gibt es innerhalb von Gebäuden (kein GPS-Empfang) und in der Nähe von hohen Wänden (GPS-Reflexionen). Die Position kann zusätzlich noch mit den Positionen bekannter mobiler Netzwerke (z.B. WLAN) in Reichweite abgeglichen werden.
Trotzdem bleibt die berechnete Position **oft ungenau**. Wer als Fußgänger*in in der Innenstadt häufiger mobile Apps zur Orientierung verwendet, weiß, dass die angezeigte Position nicht selten viele Meter von der tatsächlichen Position abweicht. Eine technische Lösung zur Erfassung von Kontaktpersonen ist nur dann hilfreich, wenn eine räumliche Nähe von unter zwei Metern zu einer infizierten Person mit einer hohen Zuverlässigkeit festgestellt werden kann. Dies kann eine GPS-basierte Lösung nicht leisten, weil sie zu ungenau ist. Damit eine solche Lösung wirkungsvoll wäre, darf sie echte Kontakte nicht übersehen ("false negatives"). Sie müsste folglich einen Kontakt selbst dann noch in Betracht ziehen, wenn die berechnete räumliche Distanz zwischen zwei Personen sehr hoch ist. Dies führt jedoch dazu, dass viele Nutzer fälschlicher Weise über einen Kontakt informiert werden, der tatsächlich nicht stattgefunden hat (“false positives”). Das würde das Vertrauen in die App wesentlich schmälern.

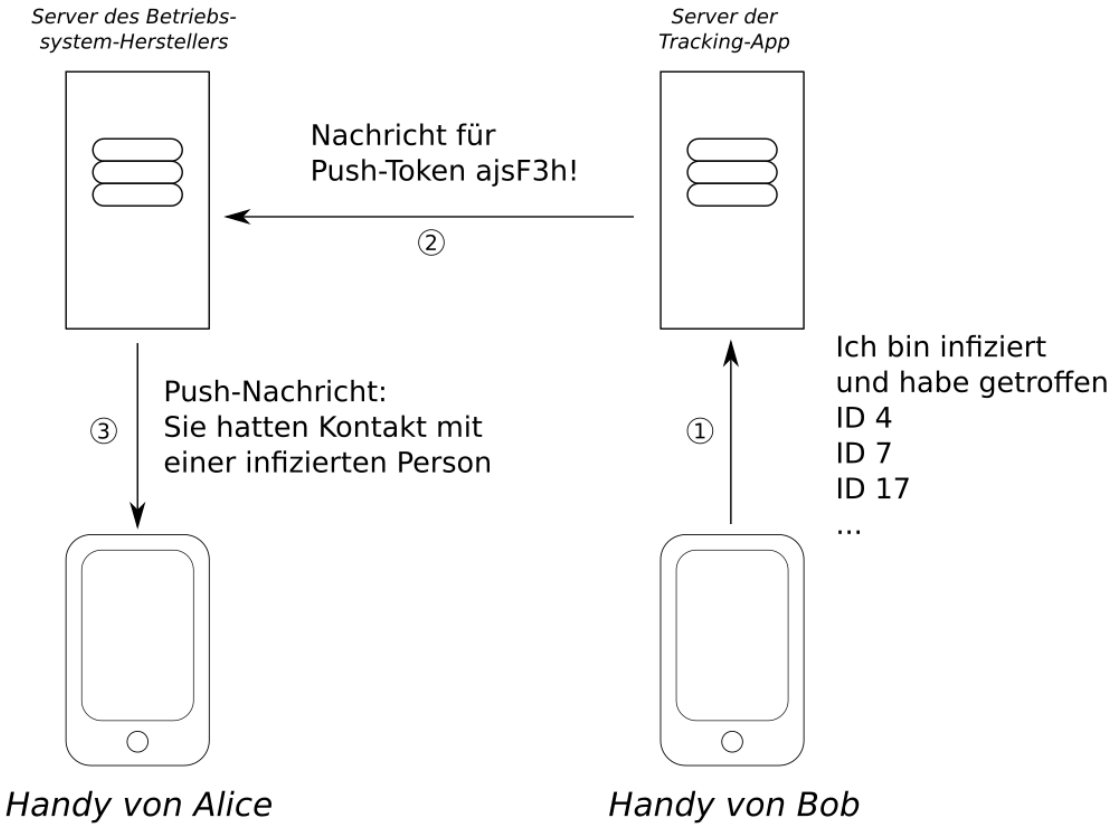
II. Entfernungsbestimmung über eine Bluetooth-App

Die Entfernungsbestimmung über eine Bluetooth-App ist **momentan die vielversprechendste Lösung**. Der Ansatz kommt **ohne Aufzeichnung von Standortdaten** aus. Zur Ermittlung von Kontaktpersonen wird die **Bluetooth-Schnittstelle** des Handys benutzt. Bluetooth ist ein Funktechnik-Standard zur **Übertragung von Daten über kurze Distanz** und genau das macht die Lösung technisch interessant: Weiter entfernte Personen werden bei Bluetooth einfach nicht mehr erfasst.

Statt auf einem Server zu errechnen, welche Personen ggf. miteinander Kontakt hatten, zeichnet jedes Smartphone mithilfe einer App unter Verwendung von Bluetooth auf, welche Teilnehmer*innen, die auch diese App benutzen, sich für einen gewissen Zeitraum in der Nähe aufgehalten haben. Erst wenn bei einer Person eine Infektion diagnostiziert wird, kann die Aufzeichnung an einen Server übertragen werden. Der Server schickt daraufhin über die App eine Nachricht an diejenigen Personen, für die eine Infektion in Betracht kommt.
Die Identität aller Benutzer*innen der App kann dabei **weitestgehend anonym** bleiben. Für die Benutzung der App muss kein Account angelegt werden. Im Konzept, wie es kürzlich durch **Initiative PEPP-PT** vorgestellt wurde, funktioniert das folgendermaßen: Die App überträgt an andere App-Benutzer*innen in Reichweite **zufällige generierte eindeutige Codes**. Der persönliche Code wird z.B. alle 30 Minuten neu erzeugt. Auf dem Server gespeichert werden nur zwei Dinge: die generierten Codes eines Handys der letzten zwei Wochen und ein sogenanntes **Push-Token,** das von diesem Handy erzeugt wurde. Mithilfe des Tokens sind die Hersteller der Betriebssysteme für Smartphones wie Apple oder Google in der Lage einem*einer Smartphone-Besitzer*in eine **Push-Nachricht** zuzustellen. Genau so eine Nachricht wird erstellt, wenn ein*e App-Benutzer*in darüber informiert werden soll, dass sie Kontakt mit einer infizierten Person hatte. Da die Nachricht verschlüsselt ist, haben die Betriebssystemhersteller keine Kenntnis des Inhalts. Und der Server, mit der die App kommuniziert, weiß nicht, zu welcher Person der Push-Token gehört.



Wenn nun bei einer Person eine Infektion diagnostiziert wurde, kann die infizierte Person über die App ihre aufgezeichneten Codes an den Server der Tracing-App schicken. Wichtig ist, dass die **App Codes löscht, die älter als zwei Wochen und damit epidemiologisch nicht mehr relevant sind**. Damit erhält auch der Server nie mehr Daten wie er braucht. Um Falschmeldungen vorzubeugen, muss die infizierte Person bevor sie die Nachricht mit den Codes an den Server senden kann, einen TAN-Code eingeben, den sie von einer berechtigten Person oder Behörde erhalten hat.
Nachdem der Server die Codes der Kontaktpersonen erhalten hat, sucht er die zugehörigen Push-Tokens in seiner Datenbank und schickt für jedes Token die erwähnte Push-Nachricht. Eine Person, die eine solche Nachricht empfangen hat, würde sich dann zum Beispiel mit dem Gesundheitsamt in Verbindung setzen, um einen Test zu vereinbaren.



Von der hier skizzierten Lösung gibt es noch einige Varianten, die derzeit diskutiert werden. Möglich wäre auch, dass alle Anwender die zufällig generierten oder die aufgezeichneten Codes aller infizierten Personen herunterladen. Dann würde der Abgleich, ob man Kontakt zu einer infizierten Person hatte, auf dem Endgerät stattfinden und es wäre nicht nötig, das Push-Token zusammen mit den zufälligen Codes jeder Person auf dem Server zu speichern.

Diskussion der Bluetooth-App

Die große Frage wird sein, ob die App schnell genug die notwendige Verbreitung in der Bevölkerung findet, damit sie bei der Eindämmung der Ausbreitung des Virus unterstützen kann. Das hängt nicht nicht zuletzt von der Verantwortung jeder einzelnen Person ab. Die Nachteile, die von der App ausgehen sind verhältnismäßig gering. Sie stehen in einem sinnvollen Verhältnis zu dem Nutzen, der sich aus der App ergibt.
Ein Nachteil der Bluetooth-Lösung ist, dass dafür Bluetooth permanent aktiv sein muss. Die Bluetooth-Schnittstelle ist nicht für ihre Sicherheit bekannt und bietet daher eine weitere Angriffsfläche für Hacker. Irritieren wird einige Anwender mit Android-Smartphones, dass die App die Berechtigung für die Standortdaten verlangt, obwohl diese ja nicht verwendet werden. Da mit der eingesetzten Bluetooth-Technik eben Entfernungen gemessen werde können, ist sie aus Sicht von Android im weiterem Sinne ein Mittel zum Erfassen von Standorten.

Auch bei dieser Lösung sind die Kriterien für einen Kontakt Dauer und Entfernung. Daten können bei Idealbedingungen mittels Bluetooth über eine Distanz von mehr wie 10 Metern übertragen werden. Das Verhalten von Bluetooth ist von Handy zu Handy oft verschieden. Eine individuelle Konfiguration ist nach Aussage von Experten jedoch möglich, sodass die Erkennung von Kontaktpersonen für verschiedene Handymodelle auf geringere Distanzen beschränkt werden kann.

Apple und Google wollen nach eigenen Angaben zusammenarbeiten, um Tracing zu erleichtern. Damit ist auch technisch der Weg frei für einen dezentralen Lösungsansatz. Die Lösung ist sinnvoll und kann schnell und effektiv eingeführt werden. Dabei kann auf die Erkenntnisse des interdisziplinären wissenschaftlichen Teams des DP3T-Projekts zurückgreifen. Das Team, das sich von dem europäischen Projekt PEPP-PT abgespaltet hat, arbeitet transparent und teilt seine Erkenntnisse mit der Allgemeinheit. Ein Rückgriff auf die Arbeitsergebnisse könnte dabei helfen, eine App zeitnah umzusetzen.

C. Ist eine Tracing App in Deutschland rechtlich möglich?

Bei der Auswertung von Daten mobiler Endgeräte zum Zwecke einer Nachverfolgung von Infektionsketten bewegen wir uns in einem rechtlichen Spannungsverhältnis: Auf der einen Seite bedeutet eine Datenverarbeitung von z.B. GPS Daten eines Smartphones durch eine Behörde einen schwerwiegenden Eingriff in das **Recht auf informationelle Selbstbestimmung** (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und das **Recht auf Datenschutz** (Art. 8 Abs. 1 Charta der Grundrechte der Europäischen Union); auf der anderen Seite muss der Staat seiner Schutzfunktion nachkommen – insbesondere in Zeiten einer pandemischen Krise. Die Schutzpflicht verlangt es, notwendige Maßnahmen zu treffen, um die Bevölkerung vor dem Corona-Virus zu schützen. Das bedeutet, dass der Staat das **Recht auf Leben und körperliche Unversehrtheit** nach Art. 2 Abs. 2 S. 1 GG gewährleisten muss. Diese Schutzpflicht steht für den Ansatz nach dem Standortdaten ausgewertet werden sollen, in starkem Widerspruch zur Pflicht des Staates, den Datenschutz der Handynutzer zu wahren. Eine flächendeckende Auswertung von Daten mobiler Endgeräte würde daher eventuell dazu beitragen, Infektionsketten detailliert nachvollzuziehen. Gleichzeitig schwächt dies den Datenschutz des einzelnen erheblich. Auch zu Zeiten von Corona kann der Gesundheitsschutz aber nicht über allem stehen. Das Spannungsverhältnis muss aufgelöst werden und die gegenüberstehenden Interessen müssen ausbalanciert werden.

I. Anwendung des Datenschutzrechts

Sobald ein Tracing die Verarbeitung personenbezogener Daten voraussetzt, findet die **europäische Datenschutz-Grundverordnung** (DSGVO) Anwendung. Dies gilt sowohl für die Datenverarbeitung durch Behörden, Gerichte oder andere öffentliche Stellen als auch für privatrechtliche Gesellschaften oder natürliche Personen. Folglich muss sich ein Staat genauso an die DSGVO halten wie ein privatwirtschaftliches Unternehmen.

Personenbezug liegt vor, wenn das Datum sich auf eine identifizierte oder identifizierbare natürliche Person bezieht; „als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung [...], zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann“. Folglich ist für die Anwendung des Datenschutzrechts nicht erforderlich, dass der Name der Person bekannt ist. Es ist bereits ausreichend, wenn die Information einer bestimmten Person zugeordnet werden kann. Falls Standortdaten über die Verwendung des GPS Signals einem mobilen Endgerät zugeordnet werden können, ist Personenbezug und die Anwendung der DSGVO zu bejahen. Gleiches kann auch bei der Verarbeitung von Funkzellendaten gelten, wenn man ihnen den Informationsgehalt entnehmen kann , dass sich ein Handynutzer in einer bestimmten Funkzelle befindet. Ebenfalls kann nach unserer Auffassung nicht gänzlich ausgeschlossen werden, dass eine Bluetooth-Lösung völlig ohne die Verarbeitung von personenbezogene Daten auskommen wird (*weitere Details unter VII.1.).*

II. Datenschutzkonforme Rechtsgrundlagen für die Datenverarbeitung

Die DSGVO unterscheidet bei der Prüfung, ob eine Datenverarbeitung zulässig ist, zwischen „gewöhnlichen“ und sensiblen Daten. Sensibel sind vor allem Informationen über die körperliche oder geistige Gesundheit. Wenn Daten mobiler Endgeräte genutzt werden, um nachzuvollziehen, ob sich eine infizierte Person in der Nähe einer anderer Person befunden hat , lässt dies Rückschlüsse auf die Gesundheit beider Personen zu: Die eine Person ist infiziert und die andere Person könnte sich angesteckt haben. Daher gelten für die Verarbeitung dieser Daten besonders strengeren Anforderungen.

Im Datenschutzrecht gilt das Prinzip des Verbots mit Erlaubnisvorbehalt (Regel-Ausnahme-Prinzip): Jede Verarbeitung von personenbezogenen Daten ist verboten (Regel), wenn nicht ein Gesetz dies erlaubt oder die betroffene Person einwilligt(Ausnahme).

III. Einwilligung der Betroffenen

Können Daten verwendet werden, wenn ein*e Nutzer*in in diese Verarbeitung einwilligt? Im Rahmen der Verarbeitung von Gesundheitsdaten ist eine **ausdrückliche Einwilligung** (Art. 9 Abs. 2 lit. a DSGVO) der betroffenen Handynutzer möglich, um eine Verarbeitung von Daten mobiler Endgeräte zum Zwecke der Infektionskettennachverfolgung zu rechtfertigen. I

Allerdings ist in diesem Zusammenhang die Tatsache problematisch, dass eine Einwilligung freiwillig erfolgen muss. **Freiwilligkeit** bedeutet im Datenschutzrecht, dass der*die Bürger*in eine echte und freie Wahl hat . Ausgeschlossen wäre eine solche Freiwilligkeit, wenn der Gesetzgeber eine Pflicht zur Installtation und Nutzung der Tracing-App schaffen würde. Aber auch wenn rechtliche Vorteile an die Nutzung der App gekoppelt werden, wie z.B. Nutzung gegen Lockerung der Ausgangsbeschränkung, ist die Einwilligung nach der DSVO nicht freiwillig und damit nicht zulässig.

Wir halten es für möglich, dass Bürger*innen eine freiwillige Einwilligung in die Nutzung der App erteilen. Auch ein sozialer Druck zur Verwendung der App schließt eine Freiwilligkeit nach unserem Dafürhalten nicht von vornherein aus. Wir erkennen jedoch an, dass mit guten Gründen eine andere Auffassung vertreten wird, nach der die Einwilligung nicht als Grundlage für die Verwendung der App taugt, weil die Nutzer*innen sich in Krisenzeiten moralisch zur Nutzung verpflichtet sehen und daher nicht unvoreingenommen darüber entscheiden können, ob sie wollen, dass Dritte ihre Daten verarbeiten. Welche Auffassung die Gerichte teilen werden, die sich erst in ferner Zukunft mit der Frage befassen werden, ist nicht abzusehen. Wir halten es daher für den besseren Ansatz, die Nutzung der App durch ein Gesetz datenschutzrechtlich zu ermöglichen. Das bedeutet, dass die gesetzliche Bestimmung die Datenverarbeitung legitimiert, sodass eine freiwillige Einwilligung nach der DSGVO für die Nutzung nicht zwingend ist. Klarstellend weisen wir darauf hin, dass wir uns deutlich gegen einen Zwang zur App durch Gesetz aussprechen.

IV. Gesetzliche Vorschrift

Die DSGVO lässt jedoch eine Verarbeitung von personenbezogenen Gesundheitsdaten auch **ohne Einwilligung** zu: Wenn die Verarbeitung erstens „aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren“, erforderlich ist und zweitens „auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person“ vorsieht (Art. 9 Abs. 2 lit. i DSGVO).

Der Begriff der öffentlichen Gesundheit ist weit zu verstehen. Daher sind alle Maßnahmen erfasst, die erforderlich sind, um Gefahren für die öffentliche Gesundheit oder Gesundheitsrisiken abzuwehren. Hierunter kann auch ein Tracing von Infektionsketten fallen, das der weltweiten Verbreitung des Corona-Virus entgegenwirken soll (m.w.N. Sebastian Bretthauer, „Datenschutz versus Katastrophenschutz“, https://verfassungsblog.de/datenschutz-versus-katastrophenschutz/).

Darüber hinaus verlangt die DSGVO, dass Datenverarbeitung entweder auf europäischem oder nationalem Recht beruht, das Maßnahmen regelt, um die Rechte und Freiheiten der betroffenen Personen zu schützen. Ein solches Gesetz besteht momentan weder auf europäischer noch auf deutscher Ebene.

Der Gesetzgeber müsste zunächst ein Gesetz schaffen , das die Anforderungen des Datenschutzrechts erfüllt. In diesem Zusammenhang hat das Bundesverfassungsgericht im **Volkszählungsurteil** aus dem Jahr 1983 klare Anforderungen definiert: Das Recht auf informationelle Selbstbestimmung kann erstens nur auf einer verfassungsgemäßen gesetzlichen Grundlage beschränkt werden. Zweitens muss das Gesetz den Umfang der Beschränkungen transparent und verständlich darstellen. Drittens muss der Gesetzgeber bei Schaffung des Gesetzes den Grundsatz der Verhältnismäßigkeit beachten.

Daher muss er vor allem organisatorische und verfahrensrechtliche Vorkehrungen treffen, die der Gefahr für die Rechte und Freiheiten der Betroffenen entgegenwirken. Diese Anforderungen sind strenger, wenn das Gesetz in die Privatsphäre der Bürger*innen eingreifen soll und Daten über zwischenmenschliche Kontakte oder Standortdaten verarbeitet werden. Der **Grundsatz der Verhältnismäßigkeit** verlangt, dass ein Gesetz, das in Grundrechte eingreift, einen legitimen Zweck verfolgen muss und überdies geeignet, erforderlich und angemessen ist. Dass der Staat einen verhältnismäßigen Ausgleich schafft, ist in Krisenzeiten wichtig. Entscheidungsträger müssen besonders akribisch darauf achten, die rechtsstaatlichen Regeln einzuhalten. Gerade in Ausnahmesituationen sollten sie keine übermäßigen Maßnahmen einführen, weil das das Risiko mit sich bringt, dass diese Vorgaben nach der Krise nicht zurückgedreht werden. Die Gefahr für das Recht der informationellen Selbstbestimmung ist besonders groß: Weil die Eingriffe oft nicht unmittelbar wahrgenommen werden, ist der Anreiz gering, die Maßnahmen zurückzudrehen.

V. Bewertung von Tracing auf Basis von Funkzellendaten

Das Gesetzesvorhaben des Bundesgesundheitsministeriums sah ursprünglich vor, eine Ermächtigung der Gesundheitsbehörden zu schaffen, „technische Mittel“ einzusetzen, die die Nachverfolgung von Kontaktpersonen ermöglichen. Hierzu sollte ein Herausgabeanspruch von Verkehrs- und Standortdaten der Mobilfunknutzer gegenüber den Anbietern von Telekommunikationsdiensten geschaffen werden. Glücklicherweise wurde dieses Vorhaben bisher nicht umgesetzt, denn es erfüllt die dargestellten Anforderungen des Verhältnismäßigkeitsgrundsatzes eindeutig nicht. Der Vorschlag ist nicht nicht geeignet, um der Verbreitung des Corona-Viruses entgegenzuwirken. Die Geeignetheit verlangt, dass die im Gesetz vorgesehen Maßnahmen den verfolgten Zweck erreichen oder zumindest fördern. Beides ist im Falle der Verarbeitung von Telekommunikationsdaten, die den Anbietern zur Verfügung stehen, nicht gegeben: Die Standortbestimmung über die Funkzellenabfrage ist so ungenau, dass lediglich im einem Durchmesser von etwa 100 Metern bis zu über einem Kilometer – je nach Größe der Funkzelle – bestimmt werden kann, ob sich in diesem Bereich Handynutzer aufgehalten haben. Der Nachweis, ob es tatsächlich zu einem Kontakt von Handynutzern gekommen ist, der infektionsrelevant wäre, ist durch diese Maßnahme nicht möglich. Dies würde eine deutlich höhere Granularität erfordern.

VI. Bewertung von Tracing auf Basis von GPS und WLAN-Abgleich

Auch eine Standortbestimmung über das GPS-Signal ist ungeeignet. Unter freiem Himmel hat GPS eine Genauigkeit von 2-13 Metern. Ungenauigkeiten können in Räumen, mehrgeschossigen Gebäuden oder bei hohen Wänden entstehen. Dieser Ungenauigkeit kann zumindest teilweise begegnet werden, indem zusätzliche WLAN-Daten verwendet werden. Dennoch bleibt die Position oftmals ungenau.

Vor allem ist die Verwendung von GPS und WLAN Daten nicht erforderlich. Erforderlich im Sinne der rechtsstaatlichen Verhältnismäßigkeitsprüfung ist eine Maßnahme, wenn kein milderes Mittel in Betracht kommt oder mildere Mittel nicht gleich geeignet sind. Es sellt sich die als in Frage, ob es Maßnahmen gibt, die genauso geeignet sind, aber weniger stark in die Rechte der Bürger*innen eingreifen. Eine durchgehende Standortbestimmung der betroffenen Handynutzer würde weitgehende Rückschlüsse über die Person zulassen: Zu welcher Zeit ist die Person an einem bestimmten Ort, wie lange verweilt die Person dort, mit wem trifft sie sich, was für Verkehrswege und Verkehrsmittel nutzt sie, usw. An dieser Stelle muss das Tracing über das Bluetooth-Signal ins Spiel kommen. Der Einsatz erfordert keine Standortbestimmung. Überdies ist die Genauigkeit über das Bluetooth-Signal für die Bestimmung eines menschlichen Kontakts vergleichbar oder sogar besser. Daher kann für den Gesetzgeber kein Weg an der „Bluetooth-Lösung“ vorbeiführen, weil dieser Ansatz weniger stark in die Rechte der Bürger*innen eingreift und gleichzeitig besser dabei helfen kann, die Pandemie einzuschränken.

VII. Bewertung von Tracing mittels Bluetooth-Signal

Ausschließlich ein Tracing über das Bluetooth-Signal genügt der Erforderlichkeit in der rechtsstaatlich erforderlichen Verhältnismäßigkeitsprüfung. Die Entfernungsbestimmung über eine Bluetooth-App stellt die datensparsamste und zugleich verlässlichste Methode dar, Infektionsketten zu verfolgen. Diese Lösung muss aufgrund des Verhältnismäßigkeitsgrundsatzes allen anderen dargestellten Lösungen vorgehen.

Aber auch in Rahmen einer Bluetooth-App verbleiben viele **Fragen und Gestaltungsspielräume:**

1. Kommt die Lösung tatsächlich allein mit anonymen Daten aus?

Eine der umstrittensten Fragen im Datenschutzrecht ist, ob ein Datum anonym ist oder Personenbezug hat. Diese Frage war in den letzten Jahren immer wieder Gegenstand gerichtlicher Entscheidungen. Entscheidend ist letztlich, ob die Information einer natürlichen Person zugeordnet werden kann. Die DSGVO setzt dabei nicht voraus, dass das Datum ausschließlich über den Namen zugeordnet werden kann. Es ist ausreichend, wenn ein*e App-Nutzer*in anhand eines Kennzeichens identifizieren kann. Dies wäre beispielsweise bereits der Fall, wenn der Push-Token verwendet wird. Der Push-Token soll gerade genutzt werden, um einem Nutzer bestimmte Bluetooth-IDs zuzuordnen oder Nachrichten zu übermitteln. Er dient dem App-Anbieter als Merkmal für eine eindeutige Zuordnung und kann somit Personenbezug herstellen.

Darüber hinaus ist ebenfalls denkbar, dass die Nutzer*innen trotz der Verwendung von IDs im Nachhinein feststellen können, von wem sie angesteckt worden sein könnten. Vor allem in ländlichen Regionen, ist es denkbar, dass ein*e Nutzer*in der App über einen Zeitraum von zwei Wochen lediglich auf eine Handvoll von Personen trifft. Falls dieser Nutzer dann eine Mitteilung über eine potentielle Ansteckung erhält, wird es dem Nutzer sehr wahrscheinlich möglich sein, diese Information mit einer bestimmten Person in Verbindung zu bringen.

Die Verwendung der App ist im Ergebnis nicht nicht völlig anonym. Das ist allerdings eher auf eine juristische Haarspalterei zurückzuführen, als dass für die Nutzer*innen eine echte Gefahr bestehen würde, dass ein App-Anbieter tatsächlich ihre Identität erfährt. Letztlich wäre die App trotzdem nicht verboten, sondern sie müsste sich nur an dem „strengen“ Datenschutzrecht messen lassen. Dies hat vor allem für die Nutzer*innen Vorteile, da die DSGVO legt die Rechte und Pflichten aller Teilnehmer*innen und insbesondere des App-Anbieters klar regelt. Das schafft eine Klarheit und Rechtssicherheit, die für die Nutzer*innen Vorteile bringt.

2. Sollten mehrere Daten kombiniert werden?
Teilweise fordern politische Akteure, eine Tracing App solle nach dem Vorbild des südkoreanischen Modells auf einer Verknüpfung von mehreren Datenquellen aufbauen. Zuletzt forderte der CDU-Wirtschaftsrat neben dem Zugriff auf Bewegungsprofile auch die Verwendung von Kreditkarten-Informationen (FAZ, aktualisiert am 31.3.2020, https://www.faz.net/aktuell/wirtschaft/cdu-wirtschaftsrat-findet-freiwillige-corona-app-unzureichend-16705496.html, zuletzt abgerufen am 23.4.2020). Stets zu Fragen ist bei solchen Forderungen nach dem „Warum?. Warum sollen weitere Daten kombiniert werden? Bringen Bewegungsprofile und Kreditkarteninformationen genauere Auswertungen? Die einfache Antwort: Nein. Bewegungsprofile sind nicht notwendig, um den Abstand zwischen zwei Nutzer*innen zu messen. Hierfür ist das Bluetooth-Signal bereits ausreichend. Es ist nicht erforderlich, weitere Daten zu erheben. Denn, wenn die Verwendung von weiteren Daten die Maßnahme nicht erheblich verbessert, aber gleichzeitig einen tieferen Eingriff in die Rechte der Bürger*inner bedeutet, sind solche Forderungen unverhältnismäßig.

3. Wie erfolgt die Benachrichtigung?
Was passiert, wenn Nutzer*innen eine Meldung erhalten , wonach sie sich in der Nähe eines infizierten Menschen aufgehalten haben. Eine App, die ohne die Namen und Personalien der Nutzer auskommt, kann keine direkten Meldungen über die Betroffenen an die Gesundheitsämter oder die Polizei übermitteln. Das ist auch gut so. Denn eine namentliche Meldung würde den Nutzer in seinen Rechten und Freiheiten beschränken. Corona ist eine meldepflichtige Krankheit. Daran soll auch eine App nichts ändern. Allerdings muss die Meldung durch die Nutzer*innen und nicht durch die App erfolgen.

Wird eine Infizierung nachgewiesen, erhält der Betreiber der App diese Information. Um Missbrauch zu vermeiden, kann die infizierte Person nicht selbst ihre Infektion melden, sondern dies bleibt bestimmten verifizierten Personen (etwa Ärzten) vorbehalten.

Eine Benachrichtigung wird bei vielen Menschen zu Angst und Ungewissheit führen: Werde ich auch krank? Habe ich andere bereits angesteckt? Wer kümmert sich um den Einkauf oder meinen Hund, wenn ich die nächsten Tage in Quarantäne bin? Um die Betroffenen aufzufangen, halten wir es für zwingend erforderlich, die Benachrichtigung mit der Option zu verbinden, telefonisch oder

per Chatfunktion Hilfe und Beratung zu erhalten. Niemand sollte mit einer solchen Benachrichtigung allein gelassen werden. Gleichzeitig muss den betroffenen Personen die Möglichkeit eingeräumt werden, sich umgehend testen zu lassen, um eine abschließende Klarheit zu erhalten. Andernfalls kann die Pandemie nicht wirksam eingedämmt werden.

4. Gesetzliche Pflicht zur Nutzung?
Verfassungsrechtlich stellt es eine schwierige Frage dar , ob der Gesetzgeber eine Pflicht zur Nutzung der App einführen kann. Befürworter argumentieren, eine wirksame Eindämmung und Nachverfolgung des Virus über eine Tracing-App sei nur möglich, wenn alle Smartphone-Nutzer*innen sie einsetzen. Das halten wir für falsch: Eine App mit wenigen Nutzer*innen ist hilfreicher als keine App. Auch eine App mit wenigen Nutzer*innen kann zur Eindämmung der Pandemie beitragen. Selbst wenn eine Pflicht die Wirksamkeit der App erhöhen könnte, käme in dem Ansatz ein Misstrauen gegenüber der Bevölkerung zum Ausdruck, den wir für schädlich halten.

Wir haben erhebliche Zweifel daran, ob eine gesetzliche Pflicht zum Tracing per App angemessen sein kann: Von einem solchen Gesetz wären über 65 Millionen Mobilfunknutzer in Deutschland betroffen – ein großer Teil davon ist noch minderjährig. Gleichzeitig bringt eine Pflicht-App ein hohes Überwachungspotential mit sich. Denn die App könnte als Einfallstor für weitere Maßnahmen dienen oder missbräuchlich genutzt werden, um weitere auf dem Endgerät befindliche Daten auszuspionieren. Vor allem besteht durch den verpflichtenden Einsatz einer App die Gefahr, dass den Handynutzer*innen ein ständiges Gefühl des Überwachtseins und der (staatlichen) Kontrolle vermittelt wird. Die Verwendung der App würde ihre Bereitschaft schmälern, die Pandemie zu bekämpfen. Die Bereitschaft von breiten Teilen de Bevölkerung, sich so zu verhalten, dass Infektionen verhindert werden, ist wichtig. Eine App muss hierzu beitragen. Sie darf die Büger*innen nicht abschrecken.

Es ist auch überhaupt nicht klar, wie diese Nutzungspflicht der App durchgesetzt werden soll: Sollen Polizisten die Nutzung der App kontrollieren, indem sie auf die Endgeräte zugreifen? Sollen Apple (iOS) oder Google (Android) verpflichtet werden, eine solche App als festen Standard über die Betriebssysteme einzuspielen? Das sind in unserer Gesellschaft derzeit keine realistischen Szenarien!

Wenn Bürger*innen darüber entscheiden können, ob sie die App verwenden, folgt daraus, dass ihnen aus der Verwendung der App keine unmittelbaren Nachteile erwachen dürfen. Das heißt einerseits: Eine Meldung führt für sich genommen nicht dazu, dass die Freiheiten der Verwender*innen verkürzt werden. Anderseits dürfen auch Mitmenschen andere nicht dazu zwingen - weder direkt noch indirekt infolge sozialen Drucks -, die App zu verwenden. Insbesondere darf die Teilnahme am öffentlichen Leben wie der Einkauf in Ladengeschäften von der Nutzung der App abhängen. Es muss technisch sichergestellt werden, dass dies nicht möglich ist.

Wir, die LAG Digitales und Netzpolitik von Bündnis 90/Die Grünen Berlin, lehnen eine gesetzliche Pflicht zur Nutzung einer Tracing-App ab. Stattdessen fordern wir, eine freiwillige App auf Basis von Bluetooth. Wir appellieren an den solidarischen Zusammenhalt der Bürger*innen und halten autoritäre staatliche Überwachungsmaßnahmen für nicht erforderlich und nicht zulässig. Auch in Krisenzeiten müssen wir einen Weg eingeschlagen, der die Grundrechte und die Freiheiten der Bürger*innen gewährleistet. Diese Freiheiten dürfen nur einschränkt werden, soweit dies absolut notwendig ist, um der Pandemie zu begegnen. Nur gemeinsam werden wir uns als freiheitliche Gesellschaft weiterentwickeln und dabei das Virus dabei besiegen.

D. Forderungen

Nach alledem unterstützen wir eine Tracing App, die die folgenden Anforderungen erfüllt:

1. **Keine gesetzliche Pflicht zur Nutzung:** Den Bürger*innen muss die Freiheit verbleiben, sich zu entschieden, ob sie die App installieren und nutzen wollen. Ein automatisches Aufspielen der App, selbst in Kombination mit einer Widerspruchslösung (Opt-out), lehnen wir ab. Jeglicher gesetzgeberischer Zwang im Zusammenhang mit der Nutzung führt zu Skepsis und Ablehnung einer solchen App. Wir halten aber eine gesetzliche Regelung für sinnvoll, die die Grundlagen für die Nutzung der App regelt, um klare Verhältnisse zu schaffen und dem Datenschutz gerecht zu werden. Darüber hinaus darf die gesellschaftliche Teilhabe nicht von der Verwendung der App abhängig gemacht werden. Das heißt, dass Freiheitsbeschränkungen nicht nur unter der Bedingung aufgehoben werden dürfen, dass Nutzer*innen die App installieren. Auch der Zugang zum öffentlichen Leben darf nicht davon abhängen, dass Personen die App installiert haben.

2. **Ausschließliche Verwendung der Bluetooth-Technik**: Die Verhältnismäßigkeit und die Grundsätze des Datenschutzrechts verlangen die Lösung zu wählen, die am sparsamten mit den Daten der Büger*innen umgeht. Daher kommt für uns ausschließlich die dargestellte Entfernungsbestimmung über eine Bluetooth-App in Betracht. Die App muss auf die Verwendung von weiteren Datenquellen (Standortdaten, Kreditkarteninformationen, Funkzellendaten, usw.) verzichten.

3. **App-Anbieter dürfen Nutzer*innen nicht identifizieren können:** Die App muss ausschließen , dass der Anbieter die Nutzer*innen durch weitere Informationen identifizieren kann. Nur so werden die Bürger*innen der App vertrauen. Das muss gesetzlich garantiert werden.

4. **Zweckbindung und Löschfristen:** Datenerhebung und Verarbeitung müssen einer strengen Zweckbindung unterliegen. Das muss sich eindeutig aus den gesetzlichen Vorgaben ergeben und darf nicht erweitert werden, indem weitere Zwecke für zulässig erklärt werden. Es müssen

kurze und klare Löschfristen festgelegt und normiert werden, die deutlich kommuniziert werden und deren Einhaltung überprüft wird.

5. **Dezentrale Speicherung und Verarbeitung**: Um IT-Sicherheitsrisiken und der Gefahr von Missbrauch vorzubeugen, muss die App zwingend dezentral und datensparsam gestaltet werden. Den DP-3T-Ansatz halten wir insofern für vorzugswürdig. Darüb er hinaus müssen sehr hohe Anforderungen an die Datensicherheit gestellt werden.

6. **Vollständige Transparenz und Datenhoheit für die Nutzer*innen:** Eine App muss die Einhaltung höchster Transparenzstandards erfüllen und auch der Softwarecode muss überprüfbar sein (Open Source). Die Nutzer*innen müssen vor der Verwendung der App verständlich über die Verwendung der Daten und ihre rechtliche Stellung informiert werden. Die „eigenen“ Daten müssen stets einsehbar und auslesbar sein. Ein Ausstieg aus der Nutzung der App muss jederzeit möglich sein.

7. **Klare gesetzliche Regelung zum Exit:** Wir fordern eindeutig zu regeln, dass die App nur so lange bestehen darf, wie die Corona-Krise anhält und die App bei der Bekämpfung einen Beitrag leisten kann. Wenn die App nicht mehr notwendig ist oder sich als ungeeignet erweist die Infektionen nachzuvollziehen, muss eine vollständige und endgültige Auflösung des Systems erfolgen.

8. **Tracing App nur Teil eines gesamtheitlichen Ansatzes:** Eine App kann nur Teil eines Gesamtkonzepts sein, das es uns ermöglicht, die Ausgangsbeschränkungen zu lockern, indem wir eine nachhaltige Eindämmung des Virus durch Tests, Nachverfolgung und einzelfallbezogener Quarantäne erreichen.