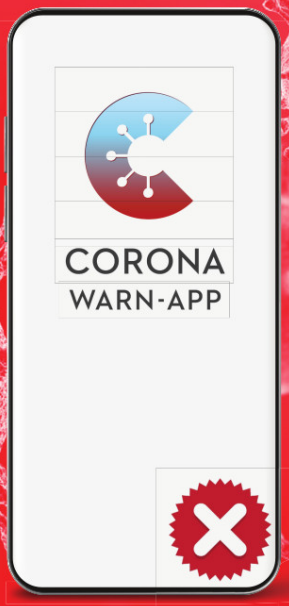
YES

NO

Die nachträgliche Rekonstruktion von Infektionsketten ist ein weiterer Baustein in der Ausweitung von Überwachung: Wer trifft wann wen für wie lange. Behörden und privaten Konzernen versprechen diese Daten detaillierte Einblicke in die Gesellschaft zur Kontrolle und Inwertsetzung der Individuen. Die berechtigte Angst vor dem Virus und das Bedürfnis, sich trotzdem solidarisch zu verhalten, wird genutzt, um einem Großteil der Bevölkerung ein autoritär hochwirksames Kontrollinstrument zu verabreichen. Einmal in der Welt wird diese Technologie bleiben und in weiteren Feldern zur Anwendung gebracht werden.

Deshalb: Nein zur Corona-Warn-App!



V.i.S.d.P. Gianfranco Kohler, Bahnhofstr. 17, Berlin 12305

In eurem Infoladen und bei https://black-mosquito.org/ gibt es seit dieser Woche das Plakat zum Aufruf gegen die Corona-Arn-App. Im Anhang auch als hochaufgelöste Druckvorrlage. Wir tragen in diesem Zusammenhang unseren neu zusammengestellten Verriss dieses umfassenden Kontrollinstruments erneut vor.

Die „freiwillige“ Corona-App und der digitale Immunitätsnachweis

Unter dem Label „Zusammen gegen Corona“ propagiert das Bundesministerium für Gesundheit die allgemeine Nutzung der sogenannten Corona-Warn-App zur nachträglichen Kontaktrekonstruktion Infizierter. Die berechtigte Angst vor dem Virus wird benutzt, um einem Großteil der Bevölkerung „freiwillig“ ein autoritär hochwirksames Werkzeug zu verabreichen.

Obwohl sich die deutsche Bundesregierung für die dezentrale Variante entschieden hat, kritisieren wir in diesem Artikel sowohl die technische Konstruktion und Infrastruktur der Apps, als auch ihre sozial-technokratischen Konsequenzen. Selbst wenn das Protokollieren von Kontakten vollständig pseudonym erfolgen würde, müssen wir dringend vor dieser App warnen. In dem Moment, wo (sogar anonyme) Verhaltensdaten flächendeckend anfallen, sind die prädiktiven Modelle, die damit trainiert werden, dazu in der Lage, ganze Populationen in Risikogruppen einzuteilen und algorithmisch zu verwalten. Es ist eine Überwachungsinfrastruktur, die da ausgerollt wird. Deshalb halten wir den Applaus einiger kritischer Datenschützer*innen für unangemessen – ja sogar fahrlässig.

Die Apps

Im März 2020 wurde bekannt, dass ein internationales Team, bestehend aus rund 130 Wissenschaftler*innen, IT-Entwickler*innen, Datenschutzbeauftragten und Soldat*innen, derzeit in einem Projekt mit dem Namen Pan-European Privacy-Protecting Proximity Tracing (PEPP-PT) an einer Software arbeitete, welche die SARS-CoV-2-Virusverbreitung einschränken sollte.

Um die Ausbreitung einzudämmen, sollen Kontaktpersonen von Infizierten frühzeitig gewarnt werden. Wenn Menschen Symptome zeigen, dann haben sie das Virus bereits weitergegeben. Deshalb sollen nach einer positiven Diagnose alle Smartphonebesitzer*innen benachrichtigt werden, deren Geräte in der Nähe der Erkrankten waren. Um Infektionsketten wirksam zu unterbrechen, streben die Forscher*innen eine Nutzer*innenbasis von etwa 60 Prozent der Bevölkerung an. In Deutschland wären das 50 Millionen Menschen. Bislang gibt es in Deutschland keine App, die nicht auf Smartphones vorinstalliert ist und bewusst heruntergeladen werden muss, die so viele Nutzer*innen hat. Allerdings könnte auch ein geringerer Anteil helfen, die Ausbreitung zumindest zu verlangsamen. Laut Bitkom besitzen 81 Prozent aller Menschen in Deutschland über 14 Jahren ein Smartphone.

21,3 Millionen mal ist die App laut Robert Koch-Institut (RKI) (Stand 6.11.2020) heruntergeladen worden. Wenn idealisierter Weise davon ausgegangen wird, dass jedem Download auch eine Installation und eine durchgängige Aktivierung der App entspricht, dann entspricht das bei einer geschätzten Bevölkerungszahl der BRD von 80 Millionen einem Durchdringungsgrad von ca. 27%. Die Wahrscheinlichkeit, dass in diesem Szenario 2 Personen aufeinandertreffen, die beide die App aktiviert haben, beträgt gerade mal etwas über 7%, und das trotz der sehr optimistischen Schätzung bezüglich der Aktivierung der App.

Um überhaupt dahin zu kommen, nur die Hälfte aller „Kontakte“ zu registrieren, müssten ca. 70% der Bevölkerung die App laufen haben. Das heißt, zu jeder Zeit müssten 70% der Menschen die App runter geladen, installiert und gestartet haben, Bluetooth müsste aktiviert sein und überhaupt geht das Ganze auch nur mit einem halbwegs aktuellen Smartphone, welches natürlich auch nicht zu Hause vergessen werden darf. Ein durchaus anspruchsvolles Szenario für nur die Hälfte des „Lagebildes“.

Technische Details der Apps

Die Apps weisen jedem Gerät eine vorübergehend gültige, authentifizierte und zufällig generierte Identifikationsnummer (ID) zu. Die temporäre ID funktioniert als Pseudonym, welches die Identität zuverlässig schützen soll. Sie wird in regelmäßigen Abständen geändert und soll nicht mit dem jeweiligen Telefon oder der Person in Verbindung gebracht werden können. Jedes PEPP-PT-Telefon (gemeint ist ein Smartphone, auf dem die App installiert ist) sendet über eine kurze Entfernung mit Bluetooth-Funktechnik (Bluetooth Low Energy) seine aktuelle ID und scannt gleichzeitig die Umgebung und erfasst, welche anderen Smartphones mit installierter PEPP-PT-Software sich in Reichweite befinden und lauscht parallel auf IDs benachbarter Geräte. Wenn sich zwei Geräte näher kommen, speichern die Apps die temporäre ID des jeweils anderen Smartphones. Die Annäherung von Telefonen anderer PEPP-PT-Benutzer*innen wird durch die Messung von Funksignalen (Bluetooth usw.) realisiert. Die Daten bleiben zunächst verschlüsselt auf dem Smartphone, niemand könne darauf zugreifen, heißt es. Nicht jede Annäherung wird gespeichert. Nur, wenn sich Smartphone A über einen epidemiologisch ausreichenden Zeitraum in der Nähe von Smartphone B befindet (die Rede ist von 15 Minuten in 1,5 Metern Entfernung), dann wird die aktuelle temporäre ID von Telefon B in der verschlüsselten, lokal auf dem Telefon gespeicherten Annäherungsgeschichte (Proximity-Historie) von A gespeichert (und umgekehrt). Offen bleibt, ob die Wahl von 15 Minuten eine sinnvolle Zeitdauer ist, denn Anhusten im Bus oder im Geschäft dauert nur wenige Sekunden, Kurzgespräche 1-2 Minuten. Das reicht auch schon für die Ansteckung. Offen bleibt auch, was konkret gespeichert wird. Laut PEPP-PT-Website werden keine Geolokalisierung,

persönlichen Informationen, einzigartige Gerätekennungen wie die IMEI-Nummer des Smartphones oder andere Daten protokolliert, die eine Identifizierung der Benutzer*in ermöglichen würden. Weiter heißt es: Die pseudonyme Annäherungsgeschichte kann von niemandem eingesehen werden, auch nicht von Benutzer*in von Telefon A. Ältere Ereignisse in der Annäherungsgeschichte werden gelöscht, wenn sie epidemiologisch unbedeutend werden.

„Wir messen nur, wie lange und wie nahe sich zwei Personen begegnet sind“, sagt Thomas Wiegand (Leiter des Heinrich-Herz-Instituts). Wo das Treffen stattgefunden habe, sei dem Virus egal. „Das sind die einzigen Informationen, die epidemiologisch von Bedeutung sind.“ Statt auf Tracking setzt PEPP-PT auf Tracing – es sollen nicht die Bewegungen von Menschen verfolgt, sondern nur ihre Kontakte nachverfolgbar werden.

Um Fehlalarme zu reduzieren, haben die Forscher*innen alle weit verbreiteten Smartphonemodelle untersucht und die Signalstärke der Funktechnik gemessen, da sie sich teils unterscheidet.

An der Genauigkeit und Aussagekraft der Maßnahme sind Zweifel angebracht angesichts der technischen Probleme mit Bluetooth (genauer BLE). Dieser Kurzstreckenfunk ist nicht dafür entwickelt worden, Abstandsmessungen vorzunehmen, dementsprechend schwankend sind auch die Ergebnisse. Hersteller verbauen unterschiedlichste Bluetooth-Chipsätze und Antennen, was die Vergleichbarkeit von Messergebnissen zusätzlich erschwert. Das RKI spricht auch folgerichtig von „Schätzungen“, wenn es um die Interpretation der gemessenen Sendeleitung benachbarter Bluetooth-Sender geht. Diese Schätzungen und damit die Kalibrierung der App werden laufend angepasst – schließlich hat die App das Potential, bei zu empfindlicher Kalibrierung weite Teile der Bevölkerung in die Isolation zu schicken mit all den Kollateralschäden, die damit verbunden sind. Andersrum könnte zur Wiederbelebung der Wirtschaft die Kalibrierung desensibilisiert werden. Angesichts der Hardwaresituation ist der Korridor für solche Nachkalibrierungen breit, auch ohne sich dem Verdacht auszusetzen, andere als epidemiologische Ziele zu verfolgen.

In dem Fall, dass ein*e Benutzer*in nicht getestet wird oder negativ getestet wurde, bleibt die Annäherungsgeschichte auf dem Telefon der Benutzer*in verschlüsselt und kann von niemandem eingesehen oder übertragen werden. Wenn allerdings bestätigt wurde, dass die Benutzer*in von Telefon A SARS-CoV-2-positiv ist (also in der Regel bereits an Covid-19 erkrankt ist), dann soll diese Person ihre aktuelle bis dato lokal gespeicherte ID-Liste in der Annäherungsgeschichte auf einen nationalen zentralen Server übermitteln. Das ist nicht ohne weiteres möglich. Ärzt*innen, Labore und Gesundheitsbehörden müssen die Meldung bestätigen. Es braucht also zwingend eine positive Diagnose. Dann setzen sich die Gesundheitsbehörden mit Benutzer*in A in Verbindung und stellen ihr eine TAN zur Verfügung, die sicherstellt, dass potenzielle Malware keine falschen Infektionsinformationen in das PEPP-PT-System einschleusen kann. Die Schnittstelle soll verschlüsselt und geheim funktionieren, sodass die Identität der Erkrankten geschützt bleibt. Die Benutzer*in verwendet diese TAN, um Informationen an den Server des nationalen Dienstleisters zu übermitteln, in Deutschland also ein Server des RKI.

Das Konsortium schreibt, da die Annäherungsgeschichte in der zentralisierten Variante pseudonyme Identifikatoren enthält, kann der Server aus diesen IDs nicht auflösen, welche Menschen sich dahinter verbergen, er kann aber alle betroffenen Kontaktpersonen über die App benachrichtigen und auffordern, sich testen zu lassen.
Allerdings muss dem Server Vertrauen entgegengebracht werden, dass er nach 21 Tagen epidemiologisch irrelevante Daten löscht – und nicht für Big-Data-Zwecke weiterhin speichert. Sobald man die Push-Token, die die App bei der Installation generiert, mit Daten des Providers verknüpfen würde (Push-Token-Zuordnung zu Geräte-ID, IMEI oder Rufnummer), wäre eine Zuordnung möglich.

Die dezentrale Variante: DP3T

Zwischen den Wissenschaftler*innen, die an der Entwicklung einer Technologie für die Covid-19-Kontaktrückverfolgung beteiligt sind, wurde öffentlich ein Konflikt ausgetragen. Im Wesentlichen ging es um die Frage, ob die verschlüsselten IDs der einzelnen App-Nutzer*innen zentral auf einem Server gespeichert werden sollen oder auf dem jeweiligen Gerät verbleiben. Die Forscher*innen teilen unsere am 05. April 2020 veröffentlichte Kritik [1], dass das zentrale Verfahren das Risiko einer (schleichenden) Ausweitung der Zweckbestimmung birgt. Dass sich das dezentrale Modell durchgesetzt hat, hat unterschiedliche Gründe. Nicht zuletzt auch, weil sich während der Debatte zentral/dezentral offenbarte, dass das RKI und Konsorten durchaus zwei Ziele verfolgten: Das öffentlich Bekanntgegebene als auch die Big-Data-Analyse der (epidemiologischen) Daten – angeblich nur, um die Infektionsausbreitung zu erfassen.

Im aktuellen dezentralen Modell verbleibt die Liste der IDs von Kontaktpersonen auf dem jeweiligen Endgerät. Infizierte schicken nach wie vor die Liste der IDs, die sie getroffen haben, an einen zentralen Server. Aber anstatt, dass der Server betroffene Personen benachrichtigt, erfragen die Apps in regelmäßigen Abständen, ob eine ID publiziert wurde, die sie in letzter Zeit getroffen haben. Die beiden Modelle zur digitalen Kontaktverfolgung unterscheiden sich also sehr grundsätzlich im Hinblick auf die Kontrolle über die anfallenden Daten, den Datenschutz und nicht zuletzt hinsichtlich der Missbrauchsmöglichkeiten. Aber auch der dezentrale Ansatz bietet keine absolute Sicherheit. Auch er funktioniert in den meisten Ausprägungen nicht „anonym“, selbst wenn das manche behaupten. Auch hier gibt es kryptographische Probleme, die gelöst werden müssen: DP3T hat mittlerweile die Linkability zwischen einzelnen Pseudonymen als Problem erkannt und in ihrem aktualisierten Whitepaper einen Non-linkable-Ansatz eingebaut. Aber er kommt ohne die Voraussetzung aus, einer zentralen (staatlichen) Instanz vertrauen zu müssen, dass sie die Daten exakt so verwendet, wie versprochen und das morgen auch noch so tun wird. Zwar wissen die zentralen Stellen, welche Pseudonyme die Infizierten in der Vergangenheit verwendet haben und können beim Upload der IDs auch dem Pseudonym eine IP-Adresse zuordnen [2], sie können jedoch die individuellen Kontaktnetzwerke nicht rekonstruieren. Es entstehen also keine zentral gespeicherten Informationen über das soziale Umfeld der App-Nutzenden. Der Server der Gesundheitsbehörden kann keine Abbildung des sozialen Umfelds ableiten und lernt von Verdachtsfällen nur, wenn die Nutzenden sich nach einer Aufforderung der App beim Gesundheitsamt beziehungsweise einer Ärzt*in melden. Verglichen mit dem zentralen Ansatz bewahren die Nutzenden der App ein größeres Maß an Privatsphäre und Autonomie gegenüber staatlichen Stellen und deren Infrastruktur.

Derzeit ist oft zu lesen, Datenschützer*innen sollten pragmatischer sein und sich endlich bewegen. Doch Vertrauen lässt sich nicht verordnen. Vertrauen erwirbt man durch Transparenz, zuverlässige Kommunikation und durch Institutionen, denen viele Menschen vertrauen. Hunderte Wissenschaftler*innen und diverse zivilgesellschaftliche Organisationen warnen inzwischen vor der zentralen Variante.

Was verbirgt sich hinter „Proximity Tracing“?

Das, was bei der App „Proximity Tracing“ genannt wird, ist ein Ausforschen des „Social Graphs“, das soziale Geflecht also, in dem sich eine Person bewegt: Wer/welche trifft sich mit wem, wann, wie lange und häufig. Es geht darum, alle „Kontakte“ der letzten 21 Tage der gesamten Bevölkerung digital zu erfassen und zu speichern. So zumindest ist das Design der Maßnahme angelegt. Eine derart ambitionierte Überwachungsinfrastruktur stellt selbst die vielen Projekte der NSA in den Schatten. Zugestanden, Proximity Tracing erfasst auch die „Kontakte“ z.B. im Supermarkt, also mehr als die eigentlich relevanten sozialen Kontakte. Die Social Graphs sind aber als Untermenge vollständig enthalten und rekonstruierbar. Dass die Repressionsbehörden an solchen Social Graphs

brennend interessiert sind, ist vielfach belegt. Aber auch „nicht-kriminelle“ Verhaltensweisen (wie etwa Affären oder Nebenjobs) lassen sich damit erkennen. Im Grunde handelt es sich hierbei um das Metadaten-Problem, welches schon lange Thema der netzpolitischen Debatte ist. Jetzt werden die Daten aber nicht aus anderen Daten (Telefonate, E-Mails, etc.) extrahiert, sondern direkt erfasst – und das auch, wenn ansonsten keine digitale Kommunikation stattfindet. Diese Überwachungsinfrastruktur ist wesensgleich mit der Vorratsdatenspeicherung. Daten werden erhoben und gespeichert, mit der Argumentation einer zukünftigen „sinnvollen“ Verwendung. Es wird erstmal der Heuhaufen aufgehäuft, bevor die Nadel gesucht wird (frei nach K. Alexander, Ex-Chef der NSA [3]).

Welche Auswirkungen diese Überwachungstechnologie haben kann, zeigt ein Beispiel aus Südkorea.[4] Mittels aggressivem Tracking von Infektionssträngen mithilfe von Überwachungsdaten sowie einer radikalen Transparenz über Neuansteckungen hatte Südkorea das Virus bisher eindämmen können. Dann machte es Schlagzeilen, dass ein Mann fünf Klubs und Bars der queeren Szene besuchte, potenziell mit 2.000 Menschen Kontakt hatte und vermeintlich mehrere Menschen mit Corona infiziert habe. Da Südkorea nach wie vor eine homophobe Gesellschaft ohne Antidiskriminierungsgesetz ist, schreckt dies potenziell betroffene Menschen jener Nacht vor Tests zurück. Denn jede*r Neuinfizierte wird von den Behörden zwar anonymisiert, jedoch mit Alter, Nationalität, Wohnbezirk und Bewegungsabläufen während jener Nacht veröffentlicht. Wer sich meldet, riskiert also ein Zwangs-Outing.

Wo ein Trog ist, kommen die Schweine[5]

„Zusammen gegen Corona“ ist der Name der Kampagne, in deren Zuge die App ideologisch flankiert wird. Was hinter dieser App steht, ist der Versuch, die Einzelfallverfolgung von Infektionen zur Aufdeckung der Infektionsketten und weiteren Infizierten auf die gesamte Gesellschaft zu skalieren. Einzelfallverfolgung ist erfolgreich bei früheren Ausbrüchen praktiziert worden, allerdings waren die betroffenen Personenzahlen bei SARS, Mers und auch Ebola viel kleiner.

Das Paradigma der vollständigen Überwachung der Bevölkerung ist übrigens unhinterfragt vom Gesundheitsministerium gesetzt worden. Debattiert wurden in der Öffentlichkeit nur Fragen des Datenschutzes und technische Details der Umsetzung.
„Eine zentrale Datenspeicherung findet selbstverständlich nicht statt“, versichert das Bundesministerium für Gesundheit – überprüfen lässt sich das nicht. Und es entspricht auch nicht der ursprünglichen Intention des Ministeriums, welches eine zentrale Datenspeicherung inklusive Auswertung implementieren wollte. Der Satz lässt außerdem offen, welche Daten gemeint sind: die aufgezeichneten Kontakte oder die Daten, die aus der Kommunikation der Apps mit der zentralen Infrastruktur rausfallen. Auch ist nicht klar, was das Ministerium unter „Speicherung“ versteht und was nicht mehr.

Dass Daten insbesondere bei größeren Mengen dezentral gespeichert werden, ist außerdem kein Alleinstellungsmerkmal, sondern Industriestandard. Unternehmen, Institutionen und Behörden wollen dadurch dem Ausfall einzelner Server die Brisanz nehmen und gleichzeitig sicherstellen, dass der Speicherpool auch zukünftig nicht an Kapazitätsgrenzen stößt, sondern mitwächst. Insofern ist die Aussage des Gesundheitsministerium bzgl. der nicht stattfindenden zentralen Datenspeicherung zumindest, wenn es um die Kontaktdaten geht, eine Nebelkerze.

Dass selbst Datenstaubsauger wie Google keine Millionen Endgeräte in ihrem Speicherpool haben, sondern nur ein paar Tausend, macht nur einen quantitativen Unterschied aus. Entscheidend ist die Frage, wer unter welchen Bedingungen auf die Daten zugreifen kann. Ein zentraler Zugriff auf die Kontaktdaten scheint zur Zeit. durch das Design der App unmöglich zu sein. Ein dezentraler Zugriff zum Beispiel nach der Beschlagnahmung eines Smartphones ist in der öffentlichen Debatte kaum

diskutiert. Bei derzeitigem Stand hat die App keinen verschlüsselten Container, in dem die Kontaktdaten und die verwendeten Schlüssel hinterlegt sind. Da Repressionsorgane grundsätzlich alle auffindbaren Smartphones beschlagnahmen, wäre es möglich, soziale Netze zumindest partiell zu rekonstruieren. Die Welle von neuen verschärften Polizeigesetzgebungen erlaubt diversen Behörden, „Staatstrojaner" einzusetzen, also Software unter der Kontrolle der jeweiligen Behörde auf dem trojanisierten Smartphone zu installieren und auszuführen. Das könnte die Behörde in die Lage versetzen, kontinuierlich Tagesschlüssel auszulesen zu können und damit einen Großteil der Kryptographie der App, die den Datenschutz sicherstellen soll, unwirksam zu machen. Aktuell gibt es wieder einen Vorstoß, auch Geheimdiensten den Einsatz von Staatstrojanern zu erlauben. Grundsätzliche Annahmen bezüglich der Integrität der Plattform, auf der die Corona-App läuft, stehen damit zusätzlich in Frage und damit auch alle Bemühungen, den Datenschutz auf diesen Plattformen zu gewährleisten.

Die Probleme, die sich aus der ungeeigneten Bluetooth Hardware und der notwendigen hohen Akzeptanz ergeben, waren bekannt, trotzdem wird ein „Besser als nichts"-Ansatz gefahren.

Sicherlich findet hier auch staatliche Industrieförderung von T-Systems und SAP statt, bislang hat die Maßnahme etwas über 60 Millionen Euro in die Kassen gespült. „Zusammen gegen Corona" aber darauf zu reduzieren, blendet den größeren Rahmen aus.
Die digitale Branche will die Gelegenheit nicht verpassen, sich als Problemlöser zu präsentieren. Nur Videokonferenzen und Home-Office zu ermöglichen, ist zu wenig, um zu glänzen. Für Solutionist*innen liefert die Pandemie die Chance, einen unübersehbaren Beleg zu erbringen, dass sich jedes Problem technisch lösen lasse. Hier wird über eine profane App hinaus gedacht. Leute wie Eric Schmidt (Ex-Google-Chef und u.a. frischer Berater der Stadt New York in Pandemiefragen) propagiert die pandemie-resistente Stadt, in der praktisch jede zwischenmenschliche Interaktion über eine digitale Plattform abgewickelt wird – „tele-everything". Los gehen soll es mit (Aus-)Bildung und Gesundheitsversorgung (Telemedizin). In diesem Entwurf erscheinen Menschen als biologische Bedrohung, während Maschinen steril und risikolos seien.

„Zusammen gegen Corona" zeichnet ein Bild, bei der die gesamte Gesellschaft wie eine Volksgemeinschaft zusammensteht, um sich gegen eine von außen kommenden Bedrohung zur Wehr zu setzen. In diesem Bild ziehen alle wie selbstverständlich an einem Strang – gesellschaftliche Widersprüche und divergierende Interessen werden verleugnet. Da passt eine App, die ein Angebot an die Bevölkerung darstellt, ein einfaches und nicht behinderndes Tool an die Hand zu bekommen, um so bei dem gesamtgesellschaftlichen Projekt der Bekämpfung der Pandemie teilnehmen zu können. Die Teilnahme am hoch ideologischen Szenario wird einfach gemacht. Dass Menschen das Bedürfnis haben, in einer Gefahrensituation solidarisch zu sein und bereit sind, sich zu engagieren, wird hier aber missbraucht, um ganz andere Projekte durchzudrücken.

Es zeigt sich ein bemerkenswerter Anlauf eines größenwahnsinnigen totalitären Überwachungsprojekts, welches aller Voraussicht nach an der unzulänglichen Teilnahme und der gegen ihr Design genutzten Hardware scheitern wird. Gleichzeitig aber den Boden legt für zukünftige, womöglich gezielterer Kontaktverfolgung.

Die Rolle von Google und Apple

Es ist wichtig, die grundlegenden Unterschiede zwischen den Tracing-Apps zu verstehen und ernst zu nehmen. Anstatt die technischen Details als Lappalie abzutun, sollten wir die Möglichkeit bedenken, dass Tracing-Apps womöglich keine temporäre Erscheinung sind, die wieder verschwinden, sobald die Pandemie unter Kontrolle gebracht ist. Tracing-Apps könnten sich als Instrument der Gesundheitspolitik oder in anderen Bereichen verstetigen. Wenn einmal ein großer Teil der Smartphone-Nutzenden eine solche App installiert hat und ihr Betrieb zum Normalfall

geworden ist, ergeben sich womöglich weitere Anwendungsmöglichkeiten, die jetzt noch jenseits des Vorstellbaren liegen. Das Verfolgen der jährlichen Influenza-Welle wäre nur ein erster Schritt. Wenn diese Funktionalität zur Verfügung steht, dann gibt es in Zukunft wahrscheinlich noch mehr Apps, die das nutzen. Des Weiteren haben Google und Apple auch Interesse an Social Graphs.

Dass diese Entwicklung wahrscheinlich ist, ist daran festzumachen, dass Google und Apple gemeinsam an Contact-Tracing-Software arbeiten[6]. Außerdem haben Google und Apple angekündigt, das dezentrale Modell der Kontaktverfolgung zu unterstützen, indem sie entsprechende Funktionen in ihre Smartphone-Betriebssysteme einbauen. Auf diese Weise kann die ständige Suche nach neuen Kontakten kontinuierlich im Hintergrund der Smartphones ablaufen, ohne den Akku zu sehr zu strapazieren. Die Kooperation könnte bald auf den meisten Smartphones auf der Welt Apps verfügbar machen, die ihre Nutzer*innen informieren, ob sie sich in der Nähe von möglichen Corona-Infizierten aufgehalten haben. Die außergewöhnliche Zusammenarbeit der zwei Technologiekonzerne schafft einen globalen Standard für Contact-Tracing. Denn anders als vielfach öffentlich kommuniziert, sind beide Ansätze auf eine Unterstützung durch die Betriebssysteme von Google und Apple angewiesen. Beide Unternehmen haben im Übrigen angekündigt, dass sie keine eigene Infrastruktur betreiben wollen, sondern diese Aufgabe den Gesundheitsbehörden überlassen werden, die an der digitalen Kontaktverfolgung mitwirken möchten. Die Schnittstelle im Betriebssystem der Smartphones soll dazu dienen, die notwendigen Daten lokal zu erheben und diese dann mit dem Server der Gesundheitsbehörden auszutauschen.

Apple und Google haben mittlerweile den Funktionsumfang erweitert: Statt einer App nur zu erlauben, kontinuierlich im Hintergrund zu laufen und die Bluetoothhardware in Anspruch zu nehmen, soll in zukünftigen Versionen von iOS und Android bereits eine komplette Tracing-App mit ausgeliefert werden. Alles, was dieser App dann noch fehlt, ist eine Art Konfigurationsdatei, die die Daten der angebundenen Infrastruktur der Gesundheitsbehörden enthält.

Offen bleibt die Frage, wie die geplanten Erweiterungen der Smartphone-Betriebssysteme genau umgesetzt werden; insbesondere, ob diese nicht vielleicht doch Informationen an die Konzerne zurücksenden könnten. Es ist daher essenziell, dass Google und Apple den Quellcode für ihre Erweiterungen offenlegen und damit unabhängigen Sicherheitsforscher*innen die Möglichkeit einräumen, zu überprüfen, dass keine zusätzlichen Funktionen eingebaut wurden.

Nachdem Apple und Google erkannt haben, dass „Gesundheit fast überall auf der Welt der größte oder zweitgrößte Sektor der Wirtschaft [ist]“ (Apple-Chef Tim Cook in einem Interview mit dem Magazin „Fortune“ im Herbst 2017 [7]), investieren die IT-Konzerne Milliarden in eigene Gesundheitsdatenbanken und versuchen mit Hochdruck, erweiterte Gesundheitsdienste in ihre Softwareumgebungen zu integrieren. Deshalb sind sowohl Apple als auch Google eigenständige relevante Akteure auf dem Gesundheitssektor. Aus diesem Grund war die Unterstützung der dezentralen Variante eine wichtige strategische Entscheidung. Die öffentliche Entscheidung für das dezentrale Modell aus Privacy-Aspekten dient aber auch durchaus der Imagepflege. Es macht sie aber vor allem zur unausweichlichen Instanz. Sie sind die einzigen, die den Zugriff auf den gesamten Datensatz haben. Staatliche Akteure müssen mit ihnen verhandeln, wenn sie doch Zugriff auf den gesamten Datensatz erlangen wollen.

Wie weit die faktische Macht der beiden dominanten Smartphone-Betriebssystem-Anbieter geht, lässt sich am Rückzieher der australischen Regierung mit ihrer zentralen Corona-App ablesen[8]: Die bereits gut fünf Millionen Mal heruntergeladene Corona-App „Covidsafe“ läuft auf iPhones nicht, da Bluetooth im Hintergrund nur eingeschränkt funktioniert. Daher musste die australische Regierung im Mai auf die Vorgabe von Apples und Googles geplanter Schnittstelle für Corona-Warn-Apps umsatteln.

Sicherheitslücke Bluetooth

Heutzutage ist Bluetooth ein integraler Bestandteil von mobilen Geräten. Laptops und Smartphones lassen sich mit Smartwatches und drahtlosen Kopfhörern verbinden. Standardmäßig sind die meisten Geräte so konfiguriert, dass sie Bluetooth-Verbindungen von jedem nicht authentifizierten Gerät in der Nähe zulassen. Bluetooth-Pakete werden durch den Bluetooth-Chip (auch Controller genannt) verarbeitet und dann an den Host (Android, Linux usw.) weitergeleitet. Sowohl die Firmware auf dem Chip als auch das Bluetooth-Subsystem des Hosts sind ein Ziel für Remote-Code-Execution-Angriffe (RCE).

Bluetooth hat eine 20 Jahre alte Geschichte der Unsicherheit. Alle paar Jahre gibt es einen neuen Angriff auf Bluetooths Pairing-Protokoll oder die verwendete Verschlüsselung. Auch aktuell gibt es eine Sicherheitslücke (CVE-2020-0022[9]) und einen Exploit, der diese ausnutzt (Bluetooth zero-click short-distance RCE exploit against Android 8/9 (bei Android 10 keine RCE, aber DoS)). Mit dieser Lücke und dem Exploit lässt sich ein Wurm schreiben, der sich ohne User*innen-Interaktion über Bluetooth weiterverbreitet und auf den Geräten Schadcode in einem privilegierten Prozess ausführen kann[10].

Wer jemandem zu nahe kommt, kann sich nicht nur selbst mit Covid-19 infizieren, sondern mit einem CVE-2020-0022-Wurm – dank der Corona-App – auch sein Smartphone, welches den Wurm dann munter weitergibt.

Die Schwachstelle ist in dem Security-Patch von Android Open Source Project (AOSP) vom Februar 2020 behoben. Aber welche Android-Smartphones werden den jemals erhalten?

Auch anonym trainieren wir Künstliche Intelligenz

Die für Deutschland geplante Corona-App soll nicht auf personenbezogene Daten des einzelnen Individuums zugreifen. Doch die Gefahren entstehen nicht nur bei der digitalen Ausleuchtung einzelner, sondern dadurch, dass eine entstehende Datensammlung in Verknüpfung mit anderen Datenbanken algorithmische Verfahren zur Bevölkerungsverwaltung ermöglicht.

Im konkreten Fall der dezentralen Corona-App, die aktuell verwendet wird, gibt ein Zusatz zu denken: Es solle die Möglichkeit integriert werden, freiwillig in pseudonymisierter Form die Daten zur epidemiologischen Forschung und Qualitätssicherung an das RKI zu übermitteln.[11] Ein unbedeutend klingender „Zusatz“, der die Dezentralität der Corona-App freiwillig aushebelt. Sollten Hunderttausende diese Option wählen (bzw. nicht abwählen), ließen sich aus den Zeitangaben der pseudonymen Tracing-Daten in der Verknüpfung z. B. mit einer Datenbank, wann, wo, welche Events stattgefunden haben, erahnen, wo sich vermeintlich unverantwortlich verhalten wurde. So lassen sich über zeitlich korrelierte Häufungen Regionen ausmachen, die eine etwaige Sonderbehandlung „rechtfertigen“. Spätestens, wenn sich die Meldungen vermeintlich Infizierter bei Gesundheitsämtern zeitlich in Verbindung bringen lassen, könnte (mit Einschränkungen) eine „Gefährder*innen“-Karte erstellt werden.

Pseudonymisierte Massendaten dienen zum Training künstlicher Intelligenzen (KI) z. B. im Kontext vorhersagender Analysen. In dem Moment, wo Verhaltensdaten fast flächendeckend anfallen und (sei es auch anonymisiert) erhoben werden, sind die prädiktiven Modelle, die damit trainiert werden, dazu in der Lage, ganze Populationen in Risikogruppen einzuteilen und algorithmisch zu verwalten. Datenbasierte Algorithmen können die Gesellschaft dann in unsichtbare soziale Klassen einteilen, zum Beispiel in Bezug darauf, wer aufgrund seiner Bewegungsmuster vermeintlich ein besonderes Sicherheits- oder Gesundheitsrisiko darstellt, weil das Bewegungsprofil erkennen lässt, dass jemand das Virus in besonderem Maße verbreitet hat oder wer prioritären Zugang zu knappen

medizinischen Ressourcen wie Beatmungsplätzen verdient. Dies ist möglich, ohne die Ortsdaten einzelner Individuen aufgezeichnet zu haben.

Algorithmische Scoring- und Entscheidungsverfahren beruhen auf einem anonymen Abgleich mit den Daten vieler anderer Individuen.

Daher kann mensch durch Weitergabe der eigenen (auch anonymisierten oder pseudonymisierten) Daten potenziell anderen Individuen und Gruppen schaden und umgekehrt durch die Datenweitergabe anderer potenziell selbst betroffen sein. Diese Gefahr wird in der verkürzten Debatte um die Corona-App und auch schon bei der Weitergabe anonymisierter Telekom-Daten oder anonymisierter Google-Positionsdaten ausgeblendet. Sie ist auch nicht Gegenstand wirksamer datenschutzrechtlicher Bemühungen. So schützt auch die Datenschutzgrundverordnung (DSGVO) nicht vor der Verwendung anonymisierter Daten für prädiktive algorithmische Entscheidungen, Risikoklassifizierung (Scoring) und verhaltensbasierte Ungleichbehandlung von Individuen oder Gruppen. In diesem Sinne trägt jede*r, der die Corona-App nutzt, zu solch einer Ungleichbehandlung bei.

Hier ist die Unterscheidung von anonymen und personenbezogenen Daten überholt, weil irrelevant!

Freiwilligkeit und Immunitätsnachweis

„Bitte haben Sie Verständnis dafür, dass wir zu ihrer eigenen Sicherheit und zur Sicherheit unserer Mitarbeiter*innen nur nachweislich nicht-infizierte Personen befördern können."

So könnte die Erklärung der Deutschen Bahn an allen Automaten und Ticket-Schaltern lauten, die ihre Dienstleistung „bis zum Ende der Corona-Krise" nur Fahrgästen mit einer ungefährlichen Kontakt-Tracing-Historie, wahlweise in Verbindung mit einem kürzlich durchgeführten Corona-Test (PCR oder Antikörper) oder einem „Immunitätsnachweis" anbietet.

Eine „freiwillige" Corona-App (egal ob zentral oder dezentral), die binnen der letzten zwei Wochen keinen Alarm geschlagen hat, ist eine Möglichkeit, diesen „Nachweis" zu erbringen. Das entspräche dem Status „grün" der (zentralen) chinesischen App wahlweise bei der Fahrkartenkontrolle oder beim Betreten des Bahnhofs. Eine zweite Möglichkeit des Nachweises ist der geplante, ebenso „freiwillige" „digitale Immunitätsausweis". Die Notwendigkeit, einen der beiden Nachweise erbringen zu müssen, stellt die soziale Unfreiwilligkeit der Konstruktion dar.

Die technischen Pläne für einen digitalen Immunitätsausweis wurden veröffentlicht[12]: Die Bundesregierung plant als Imitation der Idee von Bill Gates (siehe dazu den Text „Weniger Arzt im künstlich intelligenten Gesundheitssystem" in unserer Broschuere „diverge!") die Möglichkeit, Menschen bescheinigen zu lassen, dass sie eine Infektion mit dem Coronavirus überstanden haben – für den Fall, dass es gesicherte Erkenntnisse darüber gibt, dass eine überstandene Infektion für eine gewisse Zeit Immunität bedeutet. Derzeit gehen einige Wissenschaftler*innen (mit einer hohen Fehlerquote) von drei Monaten aus. Deutliche Kritik an diesem Vorhaben hat Gesundheitsminister Spahn Anfang Mai zum Rückzug eines Gesetzentwurfes gezwungen.

Es gibt einen historischen Vorläufer: Als das gefährliche Gelbfieber im 19. Jahrhundert in New Orleans grassierte, wurde ein „Immunitätsbonus" erprobt[13]. Die Folgen waren gravierend. Zusätzlich zur rassistischen Trennung zwischen Weißen und Schwarzen bildete sich nun auf beiden Seiten noch eine weitere unsichtbare Grenze aus: zwischen den bereits Immunen und den weiterhin vom Gelbfieber bedrohten. An der Immunität gegen Gelbfieber entschied sich die berufliche Anstellung, der Wohnort und der Lohn, Kreditwürdigkeit und wen man heiraten konnte. Der „Immunitätsbonus" verstärkte Rassismus, und Angestellte und Arbeiter*innen wurden dadurch

unter Existenzdruck gehalten. Der Druck war so stark, dass Menschen bewusst eine Ansteckung mit der durchaus auch tödlich verlaufenden Krankheit suchten, um nach Genesung in den Genuss des Bonus zu kommen. Damals war allerdings noch unbekannt, wie die Übertragung der Krankheit funktioniert, was vermutlich einigen das Leben rettete.

Im Mai 2020 sollte ein solcher Ausweis in Nordrhein-Westfalen zunächst nur erprobt werden. An diesem Projekt arbeiteten die Bundesdruckerei, die Lufthansa, die Unternehmen Digital-Health Germany, m.Doc und GovDigital sowie die Uniklinik und das Gesundheitsamt der Stadt Köln. Testpatient*innen sollten mithilfe einer App ihr Corona-Testergebnis verschlüsselt in einer Datenbank abspeichern. Flughäfen, Infrastrukturunternehmen und Behörden sollten so auf das Coronavirus-Testergebnis zugreifen können! In Erweiterung der seit Mai geltenden Praxis an den Flughäfen Frankfurt und Wien, per selbst zu zahlendem Corona-Schnelltest vor Ort die zweiwöchige Einreise-Quarantäne umgehen zu können, würde dann die „fälschungssicher" nachgewiesene Immunität ebenfalls Bewegungsfreiheit garantieren. Eine Regelung mit der fatalen Nebenwirkung vieler sich bereitwillig Ansteckender, die zur Wahrung ihrer Beweglichkeit das Gesundheitssystem an einem kritischen Punkt zusätzlich belasten könnten.

Die Konsequenz wäre eine gesellschaftlich spaltende Endsolidarisierung, die durch Corona bedingte Einschränkung der Bewegungsfreiheit nur für diejenigen zu lockern, die sich zumindest einem der beiden Programme unterwerfen. Als am 10. April der CSU-Politiker Hansjörg Durz vorschlug, nach dem Lockdown Druck auf potenzielle App-Verweigerer auszuüben, haben die meisten diese Option als unrealistisch abgewunken. Tatsächlich schlug er vor, was Spahn zwei Wochen später mit seinem Immunitätsausweis probierte: „So könnten Grundrechte wie die Bewegungsfreiheit denen wieder gewährt werden, die die App installiert haben", sagte der Vize-Vorsitzende des Digitalausschusses im Bundestag dem Handelsblatt. „Wer sich gegen die Nutzung der Corona-App entscheidet, müsste im Gegenzug größere Einschränkungen anderer Grundrechte in Kauf nehmen." Es ist keineswegs zynisch, das Vorhaben mit einer elektronischen Fußfessel zu vergleichen – Freigänger*innen müssen sie tragen oder zurück in den geschlossenen Vollzug.

Die „freiwillige" Corona-App und der „freiwillige" Immunitätsnachweis sollen damit zu Unterscheidungs-Werkzeugen für individuelle soziale Teilhabe werden. Wer Bahn fahren oder fliegen will, bräuchte dann entweder die App oder den Immunitätsnachweis. Der Staat „verordnet" diese App nicht, er stellt sie lediglich zur Verfügung. Wirtschaftliche Akteure – in unserem Beispiel die Deutsche Bahn – würden ihre Dienstleistung nur denen anbieten, die in diese algorithmischen Filter einwilligen. Regierung und Dienstleistungsunternehmen würden dabei ganz im Sinne einer übergeordneten Verantwortung für das Gemeinwohl handeln. Wer will da noch meckern – wo doch nun alles so „datensparsam" dezentral gelöst ist. Der Applaus einiger verengt blickender Datenschützer*innen ist ihnen leider gewiss.

Auf dieser Form von „Freiwilligkeit" basieren viele der derzeit erprobten Social-Scoring-Modelle in China. Wer nicht mitmacht oder die erforderliche Eigenschaft nicht erfüllt, kann ohne Verbotsverfügung „freiwillig" vom öffentlichen Leben ausgeschlossen werden: Die Corona-App und der Immunitätspass als Einübung individueller Einschluss- / Ausschluss-Mechanismen zukünftiger Soziale-Punkte-Systeme auch in Deutschland – ganz, ohne Zwang auszuüben.

Soziale Auswirkungen

Die App könnte wie ein Dammbruch fungieren. Deshalb ist es notwendig, Kritik am CCC und anderen zivilgesellschaftlichen Akteuren zu üben. Zwar üben sie Kritik[14], aber ihre Forderungen und Warnungen gehen nicht weit genug. Sie haben ein Klima der Akzeptanz für diese Apps geschaffen. Es ist gesellschaftlich egal, ob das PEPP-PT-Framework, die dezentralisierte DP3T-Implementation, oder eine andere technische Umsetzung gewählt wird. Denn entscheidend ist doch

die Schaffung der Akzeptanz, sich eine App für das vermeintliche gesellschaftliche Wohl zu installieren. Betont wird sowohl im zentralen als auch im dezentralen Modell die Freiwilligkeit. Nur wer will, installiert sich diese App und nur auf Initiative der Nutzer*innen erfährt der zentrale Server, mit welchen anderen temporären IDs dieses Smartphone in Kontakt war. Der soziale Druck wird ausgeblendet.

Treffend formulieren Aktivist*innen eines Brandanschlags auf eine Datenleitung zum HHI am 14. April 2020, dass die Debatte nicht um das Gesundheitssystem geht, sondern um das Individuum.

(…) Doch die Urängste der Menschen vor dem Tod werden mit dieser Pandemie instrumentalisiert. Mit diesen Ängsten wird „gespielt". Nicht die Privatisierungspolitik in den Gesundheitssystemen wird in Frage gestellt, sondern ob DU genug Abstand zum Nächsten hältst. Ob DU die Regeln einhältst. Diese Regeln werden überwacht (und teilweise auch bestraft). Und sie fördern allerorten eine der deutschesten Tugenden: den Hang zur Denunziation. Ihm gesellt sich in intellektuellen Kreisen der Vorwurf hinzu, man sei unsolidarisch, wenn man nicht den Verordnungen folge. Wenn DU diese Regeln nicht einhältst, bist DU schuld daran, wenn Menschen sterben. Mit dem Verweis auf die „Risikogruppen" werden andere Widersprüche abgewürgt. Die „Risikogruppen" werden ungeachtet ihrer individuellen Haltung zu einem Faktor der moralischen Erpressung, um unter Freund_innen die staatlichen und politischen Regeln unhinterfragt durchzusetzen. Mit der medizinischen Hygiene geht eine soziale Hygiene einher, die kaum schmutziges, widerständiges Denken und Debattieren zulässt." [15]

Wir sehen in einer breiten gesellschaftlichen Akzeptanz für eine App, die auf Kontaktdaten basiert – unabhängig davon, ob dies pseudonym geschieht oder nicht – die Gefahr, dass die Bereitschaft, sich für einen als individuell oder gesellschaftlich sinnvoll erachteten Zweck überwachen zu lassen, steigt. Dieser Zweck lässt sich theoretisch und mit Blick auf die Geschichte beliebig auf verschiedene Bereiche erweitern. Angefangen beim aktuellen Beispiel einer konkreten Bedrohungssituation durch die Verbreitung eines Virus über Krankheitsbekämpfung im Allgemeinen bis hin zum Aufdecken und Verfolgen anderer gesellschaftlich problematisierter Phänomene. So hat der Polizeichef von Minneapolis nach den Black Lives Matter-Riots laut darüber nachgedacht, die Daten der Tracing App zu benutzen, um Protestierende zu identifizieren.

Die grundlegende Bereitschaft, demographische und Bewegungsdaten von sich selbst preis zu geben, wächst zur Zeit auch in der analogen Welt: Ohne Angabe von persönlichen Daten lässt sich kaum mehr am gesellschaftlichen Leben teilnehmen, Angaben in Kneipen, Museen, Restaurants, Freibädern usw. sind Pflicht. Spätestens, nachdem bekannt wurde, dass sich die Polizei sehr freizügig dieser Daten bedient und sie damit zweckentfremdet, stieg die Kreativität in den abgegebenen Daten – endlich mal mit Darth Vader am Tresen plauschen können! Dass dies zu Problemen bei der Kontaktverfolgung führt, ist naheliegend und deshalb mittlerweile strafbewährt – Darth Vader trinkt jetzt wieder unter seinem bürgerlichen Namen und die Polizei, die diese Entwicklung provoziert hat, bedient sich weiterhin schamlos an den gesammelten Daten.

Kritik an der Kritik

Wie mit Kritik an unserer hin und wieder als verschwörungstheoretisch oder menschenfeindlich abqualifizierten Technologiekritik umgehen?

Immer wieder begegnen uns Argumente von Befürworter*innen der Corona-Warn-App, die entweder die scheinbare Wirksamkeit der App über alle ihre Nachteile und Einschränkungen stellen oder in naiver Weise dem Glauben schenken, was die Regierung verspricht, wenn sie sagt, die App sei sicher in Bezug auf Datenschutz und Angreifbarkeit. Wo kommt das Vertrauen in Aussagen und regierungsinitiierte, von SAP und Telekom entwickelte und von Apple und Google aktiv unterstützte

Software so unskeptisch daher?

Da fallen Aussagen wie „Wenn die App nur ein einziges Menschenleben rettet, dann sollte man sie benutzen“. Mit diesem Totschlagargument wären der Phantasie keine Grenzen gesetzt, was man alles im Sinne des Wohlbefindens der Menschen einsetzen könnte – grenzenlose und lückenlose Überwachung in allen öffentlichen, privaten und intimen Lebensbereichen, wie es sich beispielsweise Google mit seinem Selfish Ledger erträumt. Eine durchaus ernst gemeinte Zukunftsvision, in der ein für die Ewigkeit angelegtes „Buch des Lebens“ jegliche menschlichen Regungen festhält. Eine Vision, die mit Hilfe einer KI per Smartphones Menschen fern steuert und im gesellschaftlichen Interesse lenkt.

Wir hätten da einen Gegenvorschlag: Warum nicht einfach mal dafür einsetzen, dass die gewaltsamen und ausbeuterischen Umstände, die dem kapitalistischen System zu Grunde liegen, überwunden werden zugunsten einer herrschaftsfreien Gesellschaft, die nicht darauf aufbaut, dass große Teile der Bevölkerung unterdrückt werden, um der Herrschaftselite Macht und Wohlstand zu sichern?

Wir halten es für absolut widersprüchlich und scheinheilig, mit viel Geschrei eine App zu propagieren und gleichzeitig Kritiker*innen den Vorwurf zu machen, würde man sich nicht beteiligen, so würde man unnötig Menschenleben riskieren. Zum Einen ist die Wirksamkeit der App äußerst fragwürdig und birgt zudem die Gefahr, sich in einer Scheinsicherheit zu wägen, zum anderen sind das meist genau die Menschen, die sich ansonsten schön in ihrer heilen Welt eingerichtet haben und mit all den gewaltsamen Widersprüchlichkeiten, die an der Tagesordnung sind, wie, um nur ein paar wenige Bespiele zu nennen, Ausbeutung ganzer Bevölkerungen, Klimakatastrophe, Kriege, Flüchtlingsströme, Atomkraft, Unfalltote durch Autofahren, bestens klarzukommen scheinen.

Die Pandemie wird zu einer Krise instrumentalisiert, die im Gegensatz zu anderen Beispielen wie Terrorismus zunächst keinen offensichtlichen Gegner kennt, den es zu bekämpfen gilt. Es wird ein großes, schwierig zu kritisierendes „Wir“ ausgerufen, das zusammen halten und jegliche zur Verfügung stehenden Mittel zur Bekämpfung des Virus nutzen soll. Es findet ein Versuch der Manipulation statt, im Sinne der „Gesellschaft“ und vordergründig des Wohles aller zu handeln, in der alle partizipieren sollen. Es geht bei der App und allen anderen Maßnahmen nicht darum geht, dass es möglichst viele Menschen gesund bleiben, sondern dass die negativen Folgen für die Funktions- und Wettbewerbsfähigkeit des kapitalistischen Staates möglichst klein gehalten werden und gleichzeitig Überwachungstechnologien etabliert werden sollen, die, sind sie einmal in der Welt, nur schwer wieder wegzudenken sind.
Die gemeinsame App ist ein neues, von der Regierung initiiertes gesellschaftliches Projekt – alle können sich einbringen und so Reputation erlangen. Die, die sich verweigern, könnten als diejenigen angesehen werden, die eine Schuld an einer Verschlimmerung der Pandemie tragen, was im Endeffekt zu einer neuen Spaltung führt.

Ein Beispiel dafür gibt ein unternehmensfinanziertes Experiment an einer Schule in Mecklenburg-Vorpommern, in der die Schüler*innen sich „freiwillig“ regelmäßig testen lassen können, um mit einem negativen Testergebnis Vergünstigungen zu erlangen. Umgekehrt bedeutet dies ein „Disziplinierungsverfahren, wie dies Michel Foucault genannt hätte, das im Grunde alle Schüler zwingt, sich der angeblich freiwilligen Maßnahme zu unterwerfen, um nicht als Außenseiter oder Gefährder kenntlich zu werden.“ [16]

Gleiches gälte für einen Immunitätsausweis, der (abgesehen von seiner nicht hinreichenden Aussagekraft) ebenso ein neu konstruiertes „Wir“ und „Die“ aufmachen würde zwischen denen, die dadurch Teilhabe am öffentlichen Leben erlangen könnten und anderen, die entweder aufgrund

ihrer Verweigerung oder ihres negativen Immunstatus davon ausgeschlossen werden könnten. Wir halten es für wichtig, dass die Linke an diesem staatlich initiierten neuen gesellschaftlichen Projekt nicht teilnimmt, sondern auch die über die scheinbar nutzenbringenden und vordergründig harmlos erscheinenden Intentionen hinaus schaut.

Capulcu, November 2020

DIE CORONA-LEHRE

Quarantänehäuser sprießen,
Ärzte, Betten überall,
Forscher forschen, Gelder fließen –
Politik mit Überschall.
Also hat sie klargestellt:
Wenn sie will, dann kann die Welt.
Also will sie nicht beenden
Das Krepieren in den Kriegen,
Das Verrecken an den Stränden
Und dass Kinder schreiend liegen
In den Zelten, zitternd, nass.
Also will sie. Alles das.

Thomas Gsella

Fußnoten:
[1] https://capulcu.blackblogs.org/wp-content/uploads/sites/54/2020/04/Corona-App-final.pdf
[2] Allerdings kann das durch Verwendung von Proxies, VPNs oder Tor verhindert werden.
[3] Der ehemalige NSA-Direktor General Keith Alexander rechtfertigte die Massenüberwachung: „Du brauchst den ganzen Heuhaufen, um die Nadel zu finden." vgl. Ellen Nakashima und Joby Warrick. For NSA chief, terrorist threat drives passion to ‚collect it all'. Washingtonpost. 14.07.2013 https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html
[4] Fabian Kretschmer. Angst vor Zwangs-Outing per Tracking-App. 8.5.2020. Taz. https://taz.de/Angst-vor-Zwangs-Outing-per-Tracking-App/!5681439/
[5] Wir wollen uns an dieser Stelle bei allen Leser*innen der Gattung Sus scrofa domesticus für die Verwendung diese geflügelten Wortes entschuldigen – ihr seid im Folgenden nicht gemeint.
[6] Siehe dazu: Apple and Google partner on COVID-19 contact tracing technology https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology und https://netzpolitik.org/2020/apple-und-google-schaffen-globalen-standard/
[7] http://fortune.com/2017/09/11/apple-tim-cook-education-health-care/
[8] https://www.heise.de/mac-and-i/meldung/Australien-Corona-App-funktioniert-ohne-Apple-API-nicht-richtig-auf-iPhones-4716013.html
[9] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0022
[10] Für Angriffe auf BLE siehe Beispielsweise https://www.andreafortuna.org/2020/02/18/sweyntooth-bluetooth-vulnerabil… oder https://asset-group.github.io/disclosures/sweyntooth/
[11] Taz 26.4.20: https://taz.de/Debatte-um-die-Corona-App/!5681031
[12] https://ubirch.de/fileadmin/user_upload/2020-04-16_digital_corona_health_certificate.pdf
[13] Johannes Saltzwedel. Corona-Vorgänger Gelbfieber: Immunität als Gottesgeschenk. 01.05.2020, https://www.spiegel.de/geschichte/corona-vorgaenger-gelbfieber-immunitaet-als-gottesgeschenk-a-2f639c0c-14d0-4aa3-9bf1-edfb868debff

[14] Zu nennen sind hier Beispielsweise eine gemeinsame Erklärung zivilgesellschaftlicher Organisationen, in der es heißt: „Staaten müssen beim Einsatz digitaler Überwachungstechnologien zur Bekämpfung von Pandemien die Menschenrechte achten“. Dort fordern sie „Regierungen nachdrücklich auf, bei der Bekämpfung der Pandemie sicherzustellen, dass der Einsatz digitaler Technologien zur Verfolgung und Überwachung von Einzelpersonen und Bevölkerungsgruppen streng im Einklang mit den Menschenrechten erfolgt.“ Weiter sind die 10 Prüfsteine für die Beurteilung von „Contact Tracing“-Apps des CCC zu nennen. In der es heißt: „Sämtliche Konzepte [sind] strikt abzulehnen, die die Privatsphäre verletzen oder auch nur gefährden. Die auch bei konzeptionell und technisch sinnvollen Konzepten verbleibenden Restrisiken müssen fortlaufend beobachtet, offen debattiert und so weit wie möglich minimiert werden.“ Das Forum InformatikerInnen für Frieden und Gesellschaftliche Verantwortung (FIfF) veröffentlichte eine Datenschutz-Folgenabschätzung (DSFA) für die Corona-App. Dort heißt es: „Wirksamkeit und Folgen entsprechender Apps sind noch nicht absehbar und es ist davon auszugehen, dass innerhalb der EU verschiedene Varianten erprobt und evaluiert werden. Die datenschutz- und somit grundrechtsrelevanten Folgen dieses Unterfangens betreffen potenziell nicht nur Einzelpersonen, sondern die Gesellschaft als Ganze.“
[15] „Vulkangruppe shut down the power / Digitale Zurichtung sabotieren“, [B] Dokumentation: Shut down the power! Digitale Zurichtung sabotiert.“ veröffentlicht am: 2020-04-14 http://raxuatgmxdvnp4no.onion/?node=77193
[16] https://www.heise.de/tp/features/Coronavirusepidemie-Kontroll-und-Ueberwachungstechniken-fuer-Schulen-4779309.html