KONRAD ADENAUER STIFTUNG

23. September 2020

Mit dem Smartphone gegen Viren

Verfassungsrechtliche Betrachtung der Corona-Apps in fünf Regionen der Welt

Pavel Usvatov, Hartmut Rank, Stanislav Splavnic, Gisela Elsner, Aishwarya Natarajan, Marie-Christine Fuchs, Magdalena Schaffler, Malte Gaier, Anja Finke, Arne Wulff

Mithilfe der Corona-App sollen Covid-19-Infektionswege nachvollziehbar werden. Länder auf der ganzen Welt haben diese Apps eingeführt. Wir schauen nach Südosteuropa, Asien, Lateinamerika, Nahost sowie Nordafrika und nach Subsahara-Afrika. Wie steht es um die rechtlichen Rahmenbedingungen vor Ort? Wie steht es um die praktische Umsetzung? Welche Probleme sind aufgetreten?

Inhaltsverzeichnis

Einleitung

Pavel Usvatov

Seit dem 16. Juni 2020 kann in Deutschland die im Auftrag der Bundesregierung von SAP und T-Systems (Telekom) entwickelte „Corona-Warn-App" heruntergeladen und auf einem Smartphone installiert werden. Sie solle zum „Begleiter und Beschützer" werden und helfen, Infektionsketten zu unterbrechen.[1] Mittels einer Bluetooth-Verbindung können Smartphones, auf denen die App installiert ist, sich gegenseitig erkennen, und bei einem Aufenthalt von mehr als 15 Minuten in einem Abstand von unter zwei Metern werden die Daten (anonyme ID, Zeitpunkt, Dauer und Signalstärke) auf den Geräten lokal gespeichert. Im Falle einer Infektion entscheidet die Person selbst, ob sie über die App die Kontaktpersonen (und nur diese) warnen möchte; das setzt allerdings die Bestätigung der Infektion durch ein Corona-Test-Labor mittels eines QR-Codes oder einer TAN voraus. Bis Ende Juli verzeichnete die App bereits über 16 Millionen Downloads.[2]

Die Einführung der Tracing[3]-App wurde hierzulande von einer anhaltenden Debatte über die Rechtmäßigkeit ihres Einsatzes begleitet, die insbesondere von Datenschützern angezweifelt wurde.[4] Die Entwickler und die Bundesregierung betonen, dass die Daten durch den dezentralen Speicheransatz und den öffentlich zugänglichen Quellcode der App sicher vor Missbrauch geschützt seien. Die IT-Experten der TU Darmstadt und der Universitäten Marburg und Würzburg konnten indessen nachweisen, „dass externe Angreifer detaillierte Bewegungsprofile von Corona-Infizierten erstellen und gegebenenfalls die betroffenen Personen identifizieren können. Auch Kontaktinformationen könnten manipuliert […] werden."[5] Der FIfF e. V. seinerseits verweist auf die trotz großer Fortschritte noch vorhandenen Schwachstellen in der Datenschutzfolgenabwägung (DSFA, gefordert durch den – zwingend umzusetzenden – Art. 35 DSGVO) und bleibt bei seiner kritischen Haltung.[6]

Trotz der genannten Beanstandungen darf aber festgehalten werden, dass es sich um Kritik auf einem sehr hohen Niveau handelt: Es geht nicht etwa um die Befürchtung, die Regierung und staatliche Stellen könnten die Daten missbräuchlich nutzen, sondern vielmehr um den Umgang der Wirtschaft mit der App und den Daten. Allen voran werden Apple und Google genannt, die die IT-Schnittstellen einseitig gestalten und damit auch die Kontrolle über die Daten erhalten können (sog. Google-Apple-Protokoll, GAP, das anfällig für die Erstellung von Bewegungsprofilen sein soll);[7] auch besteht beispielsweise die Besorgnis, dass die App in der Privatwirtschaft zu einer Art „Eintrittskarte" umfunktioniert und damit mittelbar die Freiwilligkeit der Nutzung ausgehebelt werden könnte.[8]

In der verfassungsrechtlichen Diskussion in Deutschland und der EU ging und geht es nicht unmittelbar um die vielerorts angebotenen Tracing-Apps selbst, die in der Regel im Zusammenhang mit der DSGVO diskutiert werden, sondern um die Einschränkungen der Freiheitsrechte und „Notstandsregelungen" generell,[9] die insbesondere in Süd- und Südosteuropa, aber z. B. auch bei unserem westlichen Nachbar Frankreich mit intensiven Eingriffen in die Grundrechte der Bevölkerung einhergingen und zum Teil mit einer für die jüngere Generation der Europäer eher ungewohnten Kriegsrhetorik garniert wurden.[10]

In den folgenden fünf Abschnitten befassen sich die Autoren mit den technischen und rechtlichen Rahmenbedingungen für die in großen Teilen bereits erfolgte Einführung von Corona-Apps, neben Tracing- auch Tracking-Apps, in fünf Regionen der Welt:

In Südosteuropa, in Asien, in Lateinamerika, in der MENA-Region (Nahost und Nordafrika) und in Subsahara-Afrika. Der sechste Abschnitt fasst die Entwicklungen und rechtliche Herausforderungen zusammen.

I. Südosteuropa

Hartmut Rank, Stanislav Splavnic

Viele Länder im Südosten Europas waren zu Beginn der Pandemie im Frühjahr 2020 zunächst deutlich schwächer von ihr betroffen als süd-, mittel- oder westeuropäische Staaten wie Italien, Spanien, Frankreich und Großbritannien. Trotz geringer Infektionszahlen wurden auf dem Balkan jedoch sehr schnell und in größerem Umfang als in Deutschland Maßnahmen getroffen, welche die Freiheitsrechte der Bürger einschränkten.
Dies hatte vor allem zwei Gründe:

Zum einen arbeitet ein beträchtlicher Teil der Bevölkerung aller Staaten Südosteuropas, unabhängig davon, ob sie Mitglied in der EU sind und daher von der Arbeitnehmer-Freizügigkeit profitieren, in anderen EU-Staaten. Diese pendeln regelmäßig zwischen ihrer Heimat und ihrem Arbeitsort, vor allem in den Sommermonaten, aber auch zu religiösen Feiertagen im Frühjahr. Die Befürchtung dieser Staaten, sich aus dem damaligen Hotspot Norditalien viele Infektionsfälle zu „importieren", schien daher real. Schon die ersten bekannt gewordenen Corona-Fälle im März betrafen beispielsweise in Albanien und Rumänien aus Italien eingereiste Bürger.

Zum anderen sind die Gesundheitssysteme südosteuropäischer Staaten insgesamt deutlich weniger leistungsfähig. Dies ist nicht nur eine Frage der Finanzierung der Krankenhäuser (insbesondere bei der Ausstattung), in denen bei Ausbruch der Krise tatsächlich deutlich weniger Kapazitäten zur Behandlung hochansteckender, übertragbarer Atemwegserkrankungen bestanden. Es ist vor allem auch eine Frage des Mangels an medizinischem Fachpersonal: Die Abwanderung gut ausgebildeter Ärzte und Krankenschwestern vor allem nach Westeuropa in den letzten drei Jahrzehnten hat spürbare Lücken in staatlichen Krankenhäusern hinterlassen.

So erklären sich die rigiden Ausgangsbeschränkungen in der Region zu einem hohen Grad mit der Sorge der Behörden wie auch zahlreicher Bürger vor einer raschen Überlastung der desolaten Gesundheitssysteme. Viele Regierungen griffen schnell zu starken Einschnitten wie mehrwöchigen bis mehrmonatigen Ausgangssperren. Einige Länder führten die Pflicht ein, spezielle Passierscheine bei sich zu führen, in Rumänien zum Beispiel eine vom Arbeitgeber unterzeichnete Bescheinigung für den Arbeitsweg. Verstöße waren strafbewährt oder wurden mit hohen Bußgeldern geahndet, wovon u. a. in Rumänien auch intensiv Gebrauch gemacht wurde.

Rechtliche Rahmenbedingungen

Verfassungen der meisten Länder der Region verfügen über Notstandsklauseln, die zu unterschiedlichen Zeitpunkten nach Ausbruch der Pandemie ausgelöst wurden. Dabei sind verfassungsrechtlich nur solche Einschränkungen der Bürgerrechte erlaubt, die dem Verhältnismäßigkeitsgrundsatz entsprechen. Außerdem sind fast alle Staaten Südosteuropas (Ausnahme: **Kosovo**) auch Vertragsstaaten der Europäischen Menschenrechtskonvention, deren Notstandklausel, Art. 15 EMRK[11], auch die verhältnismäßige Einschränkung der in der Konvention geregelten Rechte und Freiheiten gestattet.

Einige Staaten haben in den letzten Monaten im Kontext der Corona-Pandemie die EMRK-Notstandklausel genutzt. Andere Länder, in denen es lange Zeit gar keine Infektionsfälle gab (z. B. Montenegro), haben von dieser Möglichkeit bisher keinen Gebrauch gemacht.

Obwohl die Beschlussfassung auch in südosteuropäischen Ländern zu einem bestimmten Grad durch Notstandsmittel gekennzeichnet war (Beispiel **Rumänien**: Verabschiedung „militärischer (Not-)Verordnungen" durch den Innenminister), blieben die Parlamente einsatzfähig und tätig. So hat sich die Krise der Gesundheits- und Wirtschaftssysteme nicht zu einer parlamentarischen Krise ausgeweitet.

Die rechtliche Ausgestaltung des Datenschutzes in Südosteuropa ist unterschiedlich. In vier südosteuropäischen Staaten, die Mitglieder der EU sind (**Bulgarien, Rumänien, Kroatien** und **Slowenien**), gilt seit Mai 2018 die DSGVO (Datenschutz-Grundverordnung). Die meisten anderen Staaten der Region, unabhängig davon, ob ihnen bereits ein EU-Beitrittskandidatenstatus gewährt wurde oder nicht, befinden sich in einem Prozess der schrittweisen Anpassung nationalen Rechts an den acquis communautaire der EU. Ihre nationalen Datenschutzgesetze sind daher mehrheitlich modern ausgestaltet und an die DSGVO angepasst, wie das im März 2019 in Kraft getretene *Data Protection Law* im **Kosovo**. Gleiches gilt in der **Republik Moldau**: Obwohl kein Beitrittskandidat oder auch nur Beitrittsanwärter, hat sie Ende 2018 die DSGVO in Teilen ins nationale Rechtssystem umgesetzt. Bezüglich des Schutzes der Daten der an COVID-19 erkrankten Menschen wird bisher weder in Moldau noch in Rumänien eine ernsthafte Debatte über systematische Fehlinterpretation bzw. Verletzungen der DSGVO geführt. Die Staaten dürfen dabei nach internem Recht Notmaßnahmen ergreifen, welche die Kommunikationsmittel weiter regeln (d.h. einschränken), wovon aber nach derzeitigem Kenntnisstand bisher kein Gebrauch gemacht wurde.

In **Rumänien** und der **Republik Moldau** hat der Gesetzgeber keine besonderen Regeln für die Verarbeitung von Gesundheitsdaten festgelegt, die speziell für die COVID-19-Pandemie gälten. Gleichzeitig wurde dort jedoch die Pflicht der Arbeitgeber eingeführt, Gesundheitskontrollen von Mitarbeitern (Temperaturmessung mit Thermometern) durchzuführen. Gleiches gilt beim Betreten eines Supermarkts, was im Lichte der DSGVO nicht problematisch zu sein scheint: Dabei handelt es sich nicht um solche Daten, die eine Person identifizierbar machen würden. Gleichzeitig ist es zu früh, um die systemische Wirkung aller neu eingeführten Sonderregeln einschätzen zu können.

Praktische Umsetzung

Verglichen mit einigen asiatischen Staaten (s.u. II.) kamen in Südosteuropa Corona-Tracing-Apps erst spät zum Einsatz. Den Datenschutzbedenken der Bevölkerung wurde teilweise Raum gegeben, wie wir es auch aus der Debatte um die Art der Datenspeicherung (zentral vs. dezentral) aus Deutschland kennen. Beispielsweise in Polen haben die Behörden vor dem Einsatz der Bluetooth-basierten App „ProteGO" deren Quellcode veröffentlicht, um Meinungen von IT-Experten einzuholen und Bedenken bei der Bevölkerung auszuräumen. Diese sind, begründet oder unbegründet, in Europa immer noch stark ausgeprägt. So hat beispielsweise eine Umfrage Mitte Juli in **Slowenien** ergeben, dass nur etwa ein Viertel der Bevölkerung eine Tracing-App freiwillig auf ihren Mobiltelefonen installieren würde. Das slowenische Parlament verabschiedete Anfang Juli ein Gesetz, welches den Einsatz einer App in **Slowenien** gestattet. Der Ministerpräsident Jansa forderte jedoch eine einheitliche EU-weite App, welche für alle Bürger verpflichtend sein solle.[12]

Eine europäische oder zumindest EU-weite einheitliche technische Lösung für den Einsatz von „Corona tracing apps" (CTA) ist jedoch noch immer nicht in Sicht. Dementsprechend haben neben Ungarn beispielsweise die südosteuropäischen EU-Mitgliedsstaaten **Kroatien**

und **Rumänien** inzwischen eigene Pläne, eine nationale App zu entwickeln und in Kürze zu starten, wobei solche Apps allerdings noch nicht im Einsatz sind (Stand: Ende Juli 2020).

Inzwischen gibt es allerdings in einigen anderen Staaten Südosteuropas nun erste Erfahrungen mit Tracing Apps. So ist etwa im EU-Mitgliedsstaat **Bulgarien** schon seit Anfang April 2020 die App „ViruSafe" im Einsatz. Der Nutzer muss bei Registrierung seine Ausweisdaten eintragen, die Daten werden in einem zentralen Register gespeichert.[13] Ersten Berichten zu Folge wird diese App aber nur von wenigen Bulgaren genutzt. Im EU-Anwärterstaat **Nordmazedonien** können Bürger seit dem 13. April 2020 die App „StopKorona!" nutzen.[14] Diese ist Bluetooth-basiert, bei der Programmierung haben sich die Entwickler an der in Singapur verwendeten „TraceTogether App" orientiert. Daten werden für maximal 14 Tage auf den mobilen Smartphons derer, die die App freiwillig heruntergeladen und installiert haben, gespeichert. Darüber haben mazedonische Anwender die Option, freiwillig Daten an das Gesundheitsministerium zu senden.

In **Kroatien** war der Weg zum Einsatz einer App etwas länger: Zunächst wurde eine Gesetzesänderung des Telekommunikationsgesetzes diskutiert, die den Behörden eine Geolokalisierung erlaubt hätte. Ende Juli wurde allerdings doch eine App durch die staatliche Regulierungsbehörde genehmigt, welche auf Bluetooth-Basis funktioniert: Die Tracing-App „Stop COVID 19" setzt auf dezentrale Datenspeicherung und überträgt keine Standortdaten.[15]

Es ist zu erwarten, dass auch weitere Staaten der Region in Kürze nachziehen und ähnliche, auf dezentraler Datenspeicherung beruhende Apps zum Einsatz bringen werden, darunter **Serbien**, welches sein Datenschutzrecht bereits weitgehend mit EU-Recht harmonisiert hat.[16]

Einige südosteuropäische Staaten haben andere – bedenklichere – Wege zur Eindämmung der weiteren Ausbreitung der Pandemie beschritten: **Montenegro** hatte kurzzeitig eine Liste mit Namen aller Bürger veröffentlicht, welche unter Quarantäne standen. Staatliche Stellen in Bosnien-Herzegowina veröffentlichten Ende März die Namen all derer, die die Selbst-Isolation nicht eingehalten hatten, und das obwohl die bosnischen Datenschutz-Agenturen diese Praxis für nicht rechtmäßig erklärt hatten.[17]

In der **Republik Moldau** wurde während der Pandemie bzw. des gesundheitlichen Notstands eine App nur für eine kleine Gruppe der an Tuberkulose erkrankten Menschen entwickelt, damit diese als Risikogruppe fernbehandelt werden können. Keine moldauische Regierungsbehörde hat jedoch bisher die Entwicklung einer CTA angekündigt. Auch IT-Experten aus der Privatwirtschaft beschäftigen sich dort bisher nicht damit, sondern eher mit Aspekten der Erleichterung der Behandlung von Corona-Patienten.

In **Rumänien** hat die Regierung erst vergleichsweise spät, nämlich im Juni 2020, mitgeteilt, dass ein militärisches Krankenhaus in Zusammenarbeit mit einem privaten Unternehmen derzeit eine solche App entwickele. Die rumänische CTA werde jedoch erst in einem Jahr einsatzfähig sein, so die zuständige Behörde. Es gibt derzeit keine große Debatte über die Architektur der App. Zum jetzigen Augenblick ist nur bekannt, dass, ähnlich wie in Ländern, die eine solche App schon einsetzen, die CTA die Nutzer benachrichtigen werde, sobald sie sich einem Corona-Hotspot nähern, was ebenfalls durch die Anwendung von Bluetooth erfolgen solle. Darüber hinaus solle diese Anwendung den Gesundheitsbehörden ermöglichen, die Hotspots schneller zu orten und zu handeln. Die Daten werden verschlüsselt an eine staatliche Behörde versandt. Wegen der Verschlüsselung werde die Regierung keinen Zugriff auf personalisierte Daten haben. Es bleibt jedoch fragwürdig, ob bei Einsatz erst in einem Jahr eine solche App ihren Zweck noch vernünftig erfüllen kann.

Rechtliche Probleme

Mit Blick auf den Datenschutz muss festgestellt werden, dass trotz der den Anforderungen der DSGVO formal entsprechenden nationalen Regelungen in Südosteuropa der Weg zu einem wirksamen, von allen Akteuren auch verinnerlichten und eingehaltenen Schutz personenbezogener Daten noch weit ist: Die Veröffentlichung von Namenslisten Infizierter in **Montenegro** (die im Internet veröffentlichten Daten wurden inzwischen gelöscht) und Quarantäne-Verstößen (**Bosnien-Herzegowina**) sind nur die schwerwiegendsten Verstöße. Einzelfälle solcher Veröffentlichungen gab es auch in anderen südosteuropäischen Staaten, z. B. als der moldauische Staatspräsident den vollen Namen des ersten infizierten moldauischen Bürgers öffentlich bekanntgegeben hatte, was offensichtlich gegen das moldauische Datenschutzrecht verstieß.

Schlussfolgerung und Perspektiven

Das aus dem in den Verfassungen aller Ländern Südosteuropas verankerten Gewaltenteilungsprinzip hergeleitete Gesetzgebungsmonopol der Parlamente wurde bisher stets beachtet. In einigen Ländern wurden spezielle auf die Pandemie bezogene Regelungen durch einfache Gesetze verabschiedet, wobei der jeweiligen (Notstands-)Behörde ein bestimmter Spielraum bezüglich dessen Konkretisierung überlassen wurde, dazu gehört z. B. die Festlegung einer Liste von „sicheren Herkunftsländern" bei Einreise in das Staatsgebiet.

Für eine abschließende Bewertung von technischen Anwendungen in Südosteuropa zur Nachverfolgung von Corona-Infektionen mittels Smartphones ist es noch zu früh. Viele Staaten der Region haben noch keine App im Einsatz. Datenschutzrechtliche Aspekte werden jedoch vorwiegend beachtet, weswegen in der Praxis Lösungen mit dezentraler Datenspeicherung überwiegen. Gerichtliche Untersuchungen dieser Apps sind noch nicht bekannt. Dass aber Grundrechtserwägungen durch die Gerichte selbst in Zeiten der Corona-Pandemie auch praktisch beachtet werden, haben die Prüfung und Verwerfung bspw. von Ausgangssperren durch Verfassungsgerichte der Region gezeigt.[18]

II. Asien

Gisela Elsner, Aishwarya Natarajan

In Asien werden nach derzeitigem Stand in insgesamt 10 bis 15 Ländern unterschiedliche Technologien zur Kontaktnachverfolgung zwecks Eindämmung und Bekämpfung der Pandemie eingesetzt oder befinden sich in der Entwicklung, größtenteils in Form von Apps, die über Smartphones funktionieren. Dieser Beitrag greift mit **Singapur**, **Südkorea** und **Indien** drei asiatische Länder heraus, um die breiten regionalen Trends bei der Verwendung von Apps zur Ermittlung von Kontaktpersonen zur Bekämpfung der COVID-19-Pandemie aufzuzeigen.

Rechtliche Rahmenbedingungen

Alle drei Länder sind ihren Verfassungstexten nach konstitutionelle Demokratien. Die Verfassungen enthalten jeweils Notstandsbestimmungen, die jedoch nicht zur Bekämpfung der COVID-19-Pandemie herangezogen wurden.

Singapur verabschiedete im April 2020 ein spezielles Gesetz, den *COVID-19 Temporary Measures Act 2020 (CTMA).* Zu Beginn des Ausbruchs stützte sich Singapurs Regierung auf das Gesetz über Infektionskrankheiten *(Infectious Diseases Act)* und das Einwanderungsgesetz

(Immigration Act), um auf die Gesundheitskrise zu reagieren. Im Rahmen des CTMA wurde sie mit weitem Ermessensspielraum für die Erteilung von Untersuchungsverfügungen ausgestattet.[19]

Die **indische** Regierung stützte sich auf den *National Disaster Management Act (NDMA*) als Rechtsgrundlage für die Unterstützung der Regierungsinitiativen zur Bekämpfung der Pandemie. Die Regierung nutzte ihre Befugnis, im Rahmen des NDMA Richtlinien und Anweisungen zu erlassen, um die Einrichtung der *Aarogya-Setu*-App zu legitimieren und deren Einsatz zu fördern.[20] Anfang Mai erklärte das Innenministerium die Nutzung der *Aarogya-Setu*-App für Arbeitnehmerinnen und Arbeitnehmer im privaten und öffentlichen Sektor für verbindlich. Außerdem forderte es die lokalen Behörden auf, in den Gebieten mit Zugangs- und Ausgangsbeschränkungen eine hundertprozentige Abdeckung durch die App sicherzustellen.[21]

Die Nationalversammlung **Südkoreas** verabschiedete im Februar 2020 Änderungsvorschriften zum Gesetz zur Kontrolle und Verhütung von Infektionskrankheiten *(Infectious Disease Control and Prevention Act, IDCP),* dem Quarantäne-Gesetz *(Quarantine Act)* und dem Gesetz über den Medizinischen Dienst *(Medical Service Act)*. Das IDCP bildet eine Legitimationsgrundlage für das Vorhalten und die Verarbeitung von persönlichen Daten infizierter Personen und ermöglicht den Behörden den Zugriff auf Aufnahmen von Sicherheitskameras, Kreditkartenaufzeichnungen sowie GPS-Daten von Fahrzeugen und Mobiltelefonen, um die Bewegungspfade von COVID-19-Infizierten zurückzuverfolgen.[22]

Praktische Umsetzung

Die Regierung **Singapurs** hat im Frühjahr die Bevölkerung aufgefordert, die *TraceTogether*-App zu installieren.[23] Diese wurde im März als eine der ersten ihrer Art in der Region eingeführt und funktioniert mittels gegenseitiger Smartphone-Erkennung über Bluetooth, wobei die Kontakte lokal auf dem jeweiligen Gerät gespeichert werden. Im Falle einer Erkrankung entscheidet der Smartphone-Nutzer selbst, ob die Gesundheitsbehörden Zugang zu den gespeicherten Begegnungsdaten erhalten. Die Nutzung dieser App ist derzeit noch freiwillig.[24] Zusätzlich wurde in Singapur auch die *SafeEntry*-App eingeführt, die als nationales digitales Check-in-System fungiert und an allen Arbeitsplätzen genutzt werden *muss*.[25] Seit Anfang Juli werden auch tragbare Ortungsgeräte an die Einwohner verteilt, zunächst vor allem an ältere Bürgerinnen und Bürger, die nicht über geeignete Smartphones verfügen, die die Nutzung der *TraceTogether*-App erlauben würden.[26]

In **Indien** brachte die Regierung die Smartphone-App namens *Aarogya Setu* auf den Markt, um die Nachverfolgung von Kontakten zu ermöglichen. Die Speicherung der Daten erfolgt auf einem zentralen Server der Regierung nach Zuweisung einer Identifikationsnummer. Der Umfang der gespeicherten Daten, die der Identifizierung des Nutzers dienen sollen, ist weiter als in Singapur: Die App überträgt bei der Registrierung den aktuellen GPS-Standort, vollständigen Namen, Telefonnummer, Alter und Geschlecht, Beruf sowie Informationen über die in den letzten 30 Tagen bereisten Länder an den Server. Im Übrigen funktioniert die Interaktion der Smartphones über Bluetooth und die entsprechenden Daten werden lokal auf den Geräten gespeichert. Die Anwendung speichert fortlaufend (in Intervallen von 15 Minuten) die GPS-Ortungsdaten des Smartphones und sieht die Durchführung regelmäßiger Selbstuntersuchungen auf Symptome durch die Nutzer vor, deren Ergebnisse einschließlich der Geolokationsdaten dann an den Server übertragen werden, wenn ein Infektionsverdacht besteht. Die entsprechende Nutzungsvereinbarung sichert im Übrigen die Anonymisierung der Daten zu.[27]

Im Falle **Südkoreas** unterscheidet sich der Ansatz im Umgang mit der Pandemie von dem der beiden beschriebenen Länder. Es wurde bisher keine spezifische Anwendung zur Ermittlung von Kontaktpersonen eingeführt. Bereits nach dem Ausbruch des MERS im Jahr 2015 wurden in Südkorea jedoch die Rechtsgrundlagen im Gesundheitssektor angepasst, um effektiver mit öffentlichen Gesundheitskrisen umzugehen, die durch Infektionskrankheiten[28] verursacht werden. Das Land hat neue Gesetze geschaffen, um Ermittlern von Gesundheitsbehörden Zugang zu persönlichen Daten zu ermöglichen. Die entsprechenden Regelungen lassen Ausnahmen im Rahmen des südkoreanischen Gesetzes zum Schutz personenbezogener Daten *(Personal Information Protection Act)* zu, wenn ein „öffentliches Interesse" daran besteht, unter anderem zum Zwecke der Untersuchung der Verbreitung von Infektionskrankheiten. Durch diese Ausnahmen wurden die Behörden ermächtigt, auf detaillierte persönliche Daten zuzugreifen, darunter z. B. Kreditkarten-transaktionen bei den Banken oder Mobiltelefon-Standortdaten bei Telekommunikationsbetreibern. Die Auswertung der Kombination solcher Daten mit dem Videomaterial der Überwachungskameras wurde zu einer frühzeitigen Identifizierung von Corona-Fällen genutzt.[29]

Während der legislative Ansatz zur Bekämpfung der Pandemie in den drei Ländern unterschiedlich ist, gibt es tatsächliche Gemeinsamkeiten in der Herangehensweise an den Einsatz von Apps zur Ermittlung von Kontaktpersonen. Sowohl Singapur als auch Indien haben Wege gefunden, Arbeitgeber zum Einsatz von Apps zur Ermittlung von Kontaktpersonen zu veranlassen. Die jüngste vom **indischen** Innenministerium herausgegebene Richtlinie enthält eine Bestimmung, die Arbeitgeber dazu verpflichtet, „sicherzustellen, dass *Aarogya Setu* von allen Arbeitnehmern mit kompatiblen Mobiltelefonen installiert wird". Das Mandat ist vom Arbeitgeber „nach besten Kräften" zu erfüllen.[30] Im Falle **Singapurs** muss die *SafeEntry*-App *an allen* Arbeitsplätzen verwendet werden. Branchenaufsichtsbehörden wie die *Monetary Authority of Singapore* haben betont, dass die Arbeitgeber in dieser Hinsicht für die Einhaltung der Vorschriften verantwortlich sind. Sowohl *Aarogya Setu* als auch *SafeEntry* erfassen sensible persönliche Daten wie Namen, persönliche Identifikationsnummer und Mobiltelefonnummer.[31] Diese Maßnahmen übertragen die Verantwortung für die Nutzung der App auf den Arbeitgeber und machen sie für die meisten Beschäftigten im formellen Sektor zu einer Voraussetzung für die Wiederaufnahme der Tätigkeit am Arbeitsplatz. Im Falle **Südkoreas** bietet der invasive Charakter des Verfahrens zur Ermittlung von Kontaktpersonen der Regierung theoretisch reichlich Gelegenheit, auf persönliche Daten von Bürgern zuzugreifen, die nicht im Zusammenhang mit Corona stehen.

Rechtliche Probleme

Einige Experten in **Singapur** haben den Ruf nach einer obligatorischen Nutzung der App laut werden lassen[32] - dies zu einer Zeit, in der die Regierung weiterhin versichert, dass die Nutzung der *TraceTogether*-App nicht obligatorisch gemacht werden soll.[33] Oppositionsparteien haben die Regierung zur Vorsicht in Bezug auf die Privatsphäre der Singapurer aufgerufen.[34] In **Indien** hat die obligatorische Verwendung der *Aarogya-Setu*-App scharfe Kritik von Experten wie dem ehemaligen Richter am Obersten Gerichtshof BN Srikrishna hervorgerufen, der festgestellt hat, dass ein solcher Schritt illegal wäre, da es dafür keine gesetzliche Grundlage gebe.[35] Unterdessen hat die indische Justiz *prima facie* die Ansicht vertreten, dass es in diesen beispiellosen Zeiten möglicherweise nicht angebracht sei, in die Anordnungen der Regierung einzugreifen.[36] Auch im Falle Südkoreas hat die Regierung scharfe Kritik für die Weitergabe von Informationen über infizierte Personen auf sich gezogen, insbesondere bei einem COVID-19-Ausbruch in einem von der LGBTQ-Szene frequentierten Stadtteil.[37]

Schlussfolgerung und Perspektiven

Die Entwicklungen in den drei hier beschriebenen Ländern spiegeln den größeren Kontext und auch den Wettlauf um den Einsatz von Apps zur Ermittlung von Kontaktpersonen in der Region und darüber hinaus wider. Dieser Trend wirft natürlich eine Vielzahl von Fragen mit Blick auf den Schutz der Privatsphäre und den Datenschutz auf. Er bietet Regierungen zugleich die Möglichkeit, ihre Legitimität zu erhöhen, wenn sie auch in Zeiten einer Pandemie Erfordernisse der materiellen Rechtsstaatlichkeit beim Einsatz digitaler Kontaktverfolgungstechnologien berücksichtigen. Jenseits der weltweit bestehenden kulturellen Unterschiede in Bezug auf den Begriff des Datenschutzes sind im Zuge der Debatte auch die genannten Staaten hinsichtlich ihres Umgangs mit dem Recht ihrer Bürger auf Privatsphäre ins Rampenlicht gerückt. Es ist klargeworden, dass ihr Schutz für die Bürger von zentraler Bedeutung ist, damit sie diesen Apps, modernen Technologien insgesamt und auch ihrer eigenen Staatsführung vertrauen können.

III. Lateinamerika

Marie-Christine Fuchs, Magdalena Schaffler

Lateinamerika befindet sich derzeit auf dem Höhepunkt der ersten Pandemiewelle und stellt das neue weltweite Epizentrum des Coronavirus dar. Es wird erwartet, dass die Fallzahlen bis in den September hinein stetig ansteigen. Da das Virus bisher selbst durch extreme, Freiheitsrechte einschränkende Maßnahmen nicht aufgehalten werden konnte, begann etwas später als in Asien und Europa auch in Lateinamerika die Diskussion um die Nutzung von Corona-Tracing- und Tracking-Apps. Auch wenn es zahlreiche Anbieter verschiedener Software gibt, hat bisher noch kein einziger Staat in der Region ein obligatorisches Überwachungssystem für Mobiltelefone eingeführt. Datenschutzrechtliche Erwägungen kamen bisher ebenfalls zu kurz.

Rechtliche Rahmenbedingungen

Ein mit der DSGVO vergleichbares, vereinheitlichtes Datenschutzrecht gibt es in Lateinamerika nicht. Bereits in den 90er Jahren fanden vereinzelt datenschutzrechtliche Regelungen Einzug in die Verfassungen und nationale Rechtsordnungen, so etwa in **Peru**.[38] In **Chile** ist der Schutz personenbezogener Daten seit 1999 geregelt.[39] Die spärliche Rechtsprechung dazu ist jedoch höchst kontrovers.[40] Auch in **Kolumbien** sehen die geltenden Gesetze zum Schutz personenbezogener Daten bisher kein generelles „Recht auf Vergessen" (Recht auf Löschung von Daten) oder zur Etablierung von Datenschutzgremien vor.[41] **Mexiko** hingegen hat mit dem 2010 in Kraft getretenen Bundesgesetz zum Schutz personenbezogener Daten[42] eine der umfassendsten Datenschutzgesetzgebungen in der Region. Neben detaillierten Regelungen zur Erhebung, Nutzung, Übertragung und Speicherung von Daten werden auch Rechte auf Zugang, Berichtigung, Widerspruch und Löschung geregelt. Die mexikanische Datenschutzbehörde, *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*, genießt den Ruf einer der aktivsten Datenschutzinstitutionen in Lateinamerika.[43] Jedoch auch in den Ländern mit Datenschutzbestimmungen scheiterte ein effektiver Schutz bisher weitgehend an der administrativen Umsetzung.[44]

Der Erlass der DSGVO in der EU 2018 hat aber immerhin dazu geführt, dass auch in Lateinamerika eine Reformwelle im Datenschutzrecht stattfand, und viele gesetzlich etablierte Regelungen für den Schutz personenbezogener Daten wurden an die in der EU-Verordnung

festgelegten Standards angepasst. Auch einige Länder, die bis dahin keine eigenen Datenschutzgesetze hatten, so etwa **Brasilien**,[45] zogen nach. Von einem gleich hohen Schutzniveau wie in der EU kann aber weiterhin nicht gesprochen werden.

Praktische Umsetzung

Aufgrund eines eher laxen Umgangs mit personenbezogenen Daten und einer in der Bevölkerung weit verbreiteten Akzeptanz bzw. Hinnahme privater wie auch staatlicher Mobil-telefonüberwachung ist es nicht überraschend, dass die Empfehlung der Nutzung von Corona-Tracking-Apps als Hilfsmittel zur Eindämmung der Pandemie in der lateinamerikanischen Bevölkerung weder Aufsehen noch allzu große Besorgnis erregt. Nur vereinzelt wird die Verwendung solcher Apps von Vertretern der Zivilgesellschaft, NGO und Wissenschaftlern in Frage gestellt und werden rechtliche Grauzonen diskutiert. Kritiker solcher Apps befürchten insbesondere, dass die durch die Installation der Software gesammelten Daten, insbesondere Gesundheitsdaten, von den Regierungen nicht datenschutzkonform verwaltet oder sogar zweckentfremdet verwendet werden könnten, um sie im schlimmsten Fall beispielsweise zu Wahlkampfzwecken oder zur anderweitigen Manipulation der eigenen Bevölkerung zu verwenden.[46]

Davon unbeeindruckt priesen die lateinamerikanischen Regierungen besonders im Zeitraum zwischen Mai und Juni 2020 großflächig die Corona-Tracking-Apps als aussichtsreiches digitales Medium gegen die Verbreitung des Coronavirus' an. Dies geschah nicht nur im Radio und Fernsehen, sondern in **Kolumbien** z. B. auch automatisiert durch eine Ansage vor jedem Telefonanruf.[47] Eine gesetzliche Verpflichtung zur Nutzung von Tracking-Apps in Lateinamerika gibt es nach wie vor nicht, es wird weiterhin auf Freiwilligkeit gesetzt. Neben einigen die ganze Region abdeckenden Apps, wie etwa die von der Interamerikanischen Entwicklungsbank angebotenen „David19"-App,[48] findet man in den einzelnen Ländern sowohl nationale als auch lokal vergleichbare und oft konkurrierende Applikationen besserer und schlechterer Qualität.[49] Als Anbieter und Betreiber dieser Corona-Tracking-Apps treten dabei durchgehend staatliche Institutionen auf, meist die Gesundheitsministerien. Inzwischen sind es auch die Arbeitgeber, ob staatlich oder privat, die die Nutzung von diversen Corona-Tracking-Apps oder damit vergleichbare digitale Fragebögen in der lateinamerikanischen Bevölkerung bewerben.

Rechtliche Probleme

Die Freiwilligkeit der Nutzung von Corona-Tracking-Apps erweckt nach außen hin den Anschein, dass die staatlichen Organe ihre Pflicht, Rechte wie den Schutz personenbezogener Daten zu respektieren, ernst nehmen. Wirft man jedoch einen genaueren Blick auf die Datenschutzerklärungen und Nutzungsbestimmungen der einzelnen Software in der Region, so wird schnell klar, dass dies nicht immer der Fall ist. So nimmt sich etwa das Gesundheitsministerium **Mexikos** als offizieller Anbieter der mexikanischen COVID-19MX-APP[50] das Recht heraus, jegliche Aktualisierungen von Datenschutzbestimmungen ohne vorherige Ankündigung vorzunehmen und die mit der App gesammelten Daten ohne spezifische Gründe an Dritte weiterzugeben. Sich selbst nimmt sie explizit von der zivil- und strafrechtlichen Haftung für etwaigen Datenmissbrauch aus.[51]

Fragwürdig ist auch **Kolumbiens** Informationspolitik zum Schutz personenbezogener Daten bei der „CoronApp". Nach dem kolumbianischen Datenschutzgesetz[52] ist die uneingeschränkte Weitergabe von personenbezogenen Daten in medizinischen Notfällen auch ohne Genehmigung der betroffenen Person erlaubt. Hierunter fallen nach Ansicht der kolumbianischen Regierung auch „sanitäre Notstände".[53] Zwar wird in den Nutzungsbestimmungen der Corona-App auf die Löschung der Daten nach Abklingen der Pandemie hingewiesen, dies allerdings nur, sofern die gesammelten Daten nicht für historische, wissenschaftliche

oder statistische Zwecke aufbewahrt werden müssen.[54] Diese Öffnungsklausel könnte als Vorwand für eine uneingeschränkte Vorratsdatenspeicherung genutzt werden.

Auch die Datenschutzkonformität der chilenischen „CoronApp" wirft aufgrund unpräziser Ausdrücke bei den Datenschutzbestimmungen zumindest Zweifel hinsichtlich der Rechtmäßigkeit der Verarbeitung und Weiterreichung von gesammelten Daten an Dritte auf. Unklar ist bis jetzt, ob es dazu einer ausdrücklichen Zustimmung der Nutzer bedarf, oder ob dem chilenischen Gesundheitsministerium dabei freie Hand gewährt wird.[55] Es wird versucht, die unbegrenzte Datensammlungsabsicht mittels der App mit den Hinweisen zu legitimieren, dass die Daten für historische, statistische, wissenschaftliche sowie Studien- oder Forschungszwecke verwendet werden können oder die Daten auf unbestimmte Zeit, jedoch mindestens bis zu 15 Jahre gespeichert werden können.[56]

Schlussfolgerungen und Perspektiven

Trotz eines in der Bevölkerung weit verbreiteten Misstrauens gegenüber staatlichen Institutionen werden die angebotenen Apps größtenteils ohne kritisches Hinterfragen installiert und insbesondere in Lateinamerikas Mega-Metropolen auch aktiv verwendet. Ungeachtet kritischer Stimmen hinsichtlich der Gefahr für den Datenschutz sind sich die Lateinamerikaner ihrer Grundrechte auf Schutz personenbezogener Daten dennoch weiterhin nicht allumfassend bewusst. Vielerorts herrscht die Haltung, dass die Freiwilligkeit der Verwendung der Apps die Effektivität dieser digitalen Hilfsmittel zur Eindämmung der Pandemie vermindere.[57] Viele Bürger auf diesem von sozialer Ungleichheit und prekären Lebensverhältnissen besonders geprägten Kontinent wissen zudem aufgrund der durch die Pandemie ausgelösten bzw. verstärkten Wirtschaftskrise nicht einmal, wie sie morgen noch ihre Familien ernähren sollen. Sorgen um den Datenschutz treten zurück. Bisher sind so in lateinamerikanischen Ländern, wo ein großer Teil der Bevölkerung nicht einmal Zugang zu Trinkwasser, geschweige denn zu Smartphones hat,[58] flächendeckende Erfolge bei der Eindämmung der Pandemie durch den Einsatz von Corona-Apps fraglich. Die strukturellen Grundbedingungen für eine flächendeckende Datenüberwachung und einen damit einhergehenden positiven Effekt zur Eindämmung der Infektionszahlen sind, anders als in hoch entwickelten Ländern in Asien und Europa, nicht flächendeckend gegeben.

IV. Nahost und Nordafrika

Dr. Malte Gaier, Anja Finke

Vergleichsweise früh wurden in den Maghreb- und Golfstaaten erste Corona-Warn-Apps entwickelt. Gerade in diesen Ländern, oftmals geprägt von einer übermächtigen Exekutive und meist unzureichenden Datenschutzbestimmungen, ist die Gefahr jedoch groß, dass ohne eine klare Rechtslage und effektive Kontrollinstanzen Corona-Warn-Apps auch zur staatlichen Überwachung und der Einschränkung individueller Freiheiten eingesetzt werden könnten.

Rechtliche Rahmenbedingungen

In **Saudi-Arabien** gibt es derzeit keine spezifischen nationalen Datenschutzgesetze, allerdings sollen Scharia-Prinzipien und andere sektorale Gesetze im Bereich der elektronischen Kommunikation die Privatsphäre und die persönlichen Daten von Einzelpersonen schützen.[59]

In den **Vereinigten Arabischen Emiraten** gibt es ebenfalls weder ein nationales Datenschutzgesetz noch eine nationale Datenschutzbehörde. Allerdings regelt Bundesgesetz Nr. 2 (bekannt als das „Gesundheitsdatengesetz“) den Einsatz von Informationstechnologien im Gesundheitswesen. Dies ist das erste Bundesgesetz, das sich direkt mit den Grundsätzen des Datenschutzes befasst. Zudem verbietet das Bundesgesetz Nr. 5 über die Bekämpfung der Cyberkriminalität die Weitergabe von Informationen, die illegal auf elektronischem Wege erlangt wurden. Es ist jedoch zweifelhaft, inwieweit diese Gesetze in der Praxis auch staatliche Eingriffe regulieren.

Das Königreich **Bahrain** führte 2019 mit dem Gesetz Nr. 30 zum Schutz personenbezogener Daten ein weitreichendes Datenschutzgesetz ein.

In **Marokko** existieren ebenfalls Regelungen zum Schutz personenbezogener Daten. Zu erwähnen wären unter anderem das Gesetz 69-99 über Archive, das Gesetz 31-13 über das Recht auf Zugang zu Informationen und das Gesetz 09-08 über den Schutz personenbezogener Daten.

Tunesien nimmt aus datenschutzrechtlicher Sicht eine Sonderstellung ein: Das Datenschutzrecht fand dort bereits im Jahr 2014 eine Verankerung in der Verfassung, der Schutz der Privatsphäre wurde an die Spitze der zu garantierenden Rechte und Freiheiten gesetzt. Im März 2018 wurde dem Parlament zudem ein neuer Entwurf des Gesetzes über den Schutz personenbezogener Daten im Einklang mit der neuen EU-Datenschutz-Grundverordnung vorgelegt, bisher wurde das Gesetz aber nicht verabschiedet. Derweil regelt das Gesetz Nr. 2004-63 vom 27. Juli 2004 den Schutz personenbezogener Daten, welches aber hinsichtlich neuer Technologien als veraltet gilt.

In **Jordanien** ist das Recht auf Schutz der Privatsphäre zwar in der Verfassung verankert, derzeit gibt es aber weder ein spezifisches Datenschutzgesetz noch eine Datenschutzbehörde, welche die Datenverarbeitung durch eine Corona-App regulieren könnte.

Im **Libanon** wurde 2018 ein neues Datenschutzgesetz eingeführt, das aber weit hinter seinen Pendants in der Region und erst Recht den durch die DSGVO gesetzten Standards zurück bleibt und den Schutz personenbezogener Daten nur unzureichend gewährleistet.[60]

Praktische Umsetzung

In den Golfstaaten wurden in den letzten zehn Jahren enorme Ressourcen für die Digitalisierung der Infrastruktur bereitgestellt: Neue Partnerschaften mit Big-Tech-Konzernen wurden geschlossen, die Gesetzgebung angepasst und Fachkräfte ausgebildet. Während die historisch niedrigen Ölpreise und die COVID-19-Pandemie die Wirtschaft im Golf erschüttern, ist letztere zweifellos auch der bisher größte Härtetest für die langjährigen Digitalisierungsmaßnahmen im Gesundheitssektor.

Anfang Juni wurde in **Saudi-Arabien** die App „Tabaud“ („Distanzierung“) veröffentlicht. Die Smartphone-Anwendung wurde vom *National Information Center* der saudischen Behörde für Daten und künstliche Intelligenz in enger Zusammenarbeit mit dem Gesundheitsministerium als Warnsystem und zur Ermittlung von Infektionsketten entwickelt. Sie informiert die Anwender der App, wenn sie in den letzten 14 Tagen mit einer nachweislich positiv auf COVID-19 getesteten Person Kontakt hatten. Hierfür erfasst *Tabaud*, welche Smartphones einander nahegekommen sind, und tauscht via Bluetooth zufällig erzeugte Krypto-Schlüssel aus. Dies hat den Vorteil, dass weder Geo-Daten ausgewertet noch Ortsinformationen übermittelt werden. Die Installation und Nutzung der Anwendung sind kostenlos und freiwillig.

Auch die **Vereinigten Arabischen Emirate** (VAE) profitierten beim Ausbruch der Pandemie erheblich von ihrer systematischen Digitalisierungsförderung der letzten Jahre, so dass vor dem Hintergrund der Nationalen Innovationsstrategie, der Strategie für künstliche Intelligenz und der „Blockchain-Strategie 2021" der Übergang zur Fernarbeit und zum Fernunterricht reibungslos und schnell erfolgte. Bereits im April 2020 initiierte das Gesundheitsministerium der VAE die *TraceCovid-App* mit dem Ziel, Infektionsketten frühzeitig aufzuspüren und den Benachrichtigungsprozess zu automatisieren und zu beschleunigen. Die mobile Anwendung tauscht mit anderen Geräten, auf denen die App installiert ist, einen verschlüsselten *Secure Tracing Identifier* (STI) aus. Dieser besteht aus einem anonymisierten Datums- und Zeitstempel, der lokal für drei Wochen auf den Geräten gespeichert wird. Wird ein Nutzer positiv auf das Virus getestet, wird der STI auf einen zentralen Server hochgeladen.

Zum selben Zeitpunkt führte das Gesundheitsministerium die Smartphone-Anwendung „Stay-Home" ein. Die App ermöglicht es dem Ministerium, über den Aufenthaltsort von Personen, die sich in einer obligatorischen häuslichen Quarantäne befinden, informiert zu bleiben. Der Nutzer muss hierfür den Zugriff der App auf Kamera, Standort, Audio und Anfrufe ermöglichen.

Ende April wurden diese Funktionen schließlich in der App „Alhosn" kombiniert, welche es den Nutzern zusätzlich erlaubt, die Testergebnisse auf dem Smartphone zu erhalten. Die Nutzung der App erfolgt in den meisten Fällen weiterhin auf freiwilliger Basis. Menschen, die in den VAE positiv auf das Corona-Virus getestet wurden, und diejenigen, die mit infizierten Personen in engen Kontakt gekommen sind, müssen jedoch ein elektronisches Armband tragen, das mit der *Alhosn-App* verbunden ist. Wer das elektronische Armband nicht trägt, riskiert bei wiederholtem Verstoß eine Haftstrafe von sechs Monaten und/oder eine Geldstrafe von bis zu 100.000 Dirham (24.260 Euro).

Das Königreich **Bahrain** wiederum machte kürzlich mit seiner „BeAware Bahrain" Warn-App Negativschlagzeilen. Laut einem von *Amnesty International* veröffentlichten Bericht ist die App eine der invasivsten Anwendungen zur Ermittlung von Infektionsketten. Für die Registrierung und Nutzung der Anwendung wird eine bahrainische Ausweisnummer benötigt. Die App führt eine Beinahe-Live-Ortung der Standorte der Nutzer durch und lädt die GPS-Koordinaten auf einen zentralen Server hoch. Hierdurch sollen Risikokontakte der letzten 14 Tage identifiziert werden. Zudem war *BeAware Bahrain* mit einer landesweiten Live-Fernseh-sendung namens „Are You at Home?" verknüpft, in der Preise an Personen vergeben wurden, die während des Ramadans zu Hause blieben. Die Teilnahme an der Verlosung war zunächst verpflichtend, wurde dann aber als zusätzliche freiwillige Funktion angeboten.

Die bahrainische Warn-App lässt sich ferner mit einem Bluetooth Armband koppeln, um sicher zu gehen, dass Nutzer die Quarantänebestimmungen achten. Hierfür werden alle zehn Minuten die Standortdaten auf einen zentralen Server geladen. Das Tragen des Armbands ist für alle Personen, die für häusliche Quarantäne registriert sind, verpflichtend. Bei Verstoß droht eine Haftstrafe von mindestens drei Monaten und/oder eine Geldstrafe zwischen 1.000 und 10.000 BD (ca. 2.345 EUR – 23.500 EUR).

Eine ähnlich frühzeitige Reaktion lässt sich auch in Nordafrika beobachten. Trotz der vergleichsweise geringen Fallzahlen reagierten die Regierungen der Maghreb-Staaten angesichts einer oft unzureichenden Gesundheitsversorgung schon früh und umfassend, um das neuartige Corona-Virus einzudämmen. Neben Reise- und Kontaktverboten sowie strikten Ausgangssperren setzte man auch hier früh auf Warn-Apps.

Im Rahmen der nationalen Strategie zur Bekämpfung der Corona-Pandemie entwickelte in **Marokko** ein multidisziplinäres Team des Gesundheitsministeriums, des Innenministeriums, der Nationalen Regulierungsbehörde für Telekommunikation und der Agentur für digitale Entwicklung in Zusammenarbeit mit marokkanischen Unternehmen und Start-ups die Smartphone-Anwendung „Wiqaytna" („Schutz"). Seit dem 1. Juni hat die marokkanische Bevölkerung die Möglichkeit, die App kostenlos herunterzuladen und somit benachrichtigt zu werden, wenn es in den letzten 21 Tagen zu einem Risikokontakt mit anderen Nutzern gekommen ist. Bei jeder Begegnung mit einem anderen Anwender der App wird via Bluetooth ein zufälliger, anonymer und verschlüsselter Code aufgezeichnet und lokal auf den Geräten gespeichert. Nach Ablauf der 21 Tage werden die Informationen automatisch gelöscht. Wird ein Nutzer positiv auf das Virus getestet, wird er aufgefordert, die Begegnungsdaten in eine zentrale Datenbank hochzuladen. Hierbei sollen unter keinen Umständen die Identität der infizierten Person, der Ort der Begegnung oder der Zeitpunkt der Begegnung preisgegeben werden.

In **Tunesien** kann seit dem 19. Mai die Smartphone-Anwendung „E7mi" („Schützen") heruntergeladen werden. Die Anwendung wurde vom tunesischen Start-Up *Wizzlabs* entwickelt. Sobald ein Nutzer der App positiv getestet wurde, benachrichtigt das *Emerging Diseases Observatory* andere Anwender, die mit dieser Person in den letzten 14 Tagen in Kontakt gekommen sind, und leitet daraufhin die notwendigen Folgemaßnahmen ein. Die App verwendet ebenfalls Bluetooth, um den Kontakt zwischen Nutzern aufzuzeichnen, aber speichert und verarbeitet die verschlüsselten Daten nicht auf dem Gerät, sondern auf einem zentralen Server in Tunesien. Für die Registrierung verlangt die App ausschließlich die Telefonnummer des Nutzers, so dass bei einer nachgewiesenen Infektion weder die Identität der infizierten Person noch der Ort und Zeitpunkt der Begegnung preisgegeben werden. Die Nutzung von *E7mi* ist zum aktuellen Zeitpunkt freiwillig. Allerdings kündigte das tunesische Gesundheitsministerium an, dass die App in öffentlichen Räumen zur Pflicht werden könnte, falls die Installationsrate zu niedrig bleibe. Die Corona-Warn-App unterliegt der Kontrolle der Nationalen Behörde für den Schutz personenbezogener Daten.
In den Ländern Rund um die Ostküste des Mittelmeers scheint sich nach einer ersten langsamen Rückkehr zur Normalität im Laufe des Monats Juli eine zweite Welle des Corona-Virus anzubahnen. Anders als in den Golf- und Maghreb-Staaten ist in der Levante derzeit noch keine eindeutige Tendenz zur Digitalisierung bei der Nachverfolgung von Infektionsketten zu erkennen. Doch gerade in der von Konflikten und politischer und sozioökonomischer Instabilität geprägten Region ist es wichtig, die Pandemie in Schach zu halten, um einer weiteren Destabilisierung vorzubeugen.

Bisher hat nur **Jordanien** am 21. Mai eine freiwillig nutzbare Corona-Warn-App zur Kontaktverfolgung auf den Weg gebracht. Die Anwendung „Aman" („Sicherheit") wurde im Auftrag des jordanischen Gesundheitsministeriums von der „COVID-19 Jotech Community", einer Gruppe technisch versierter Freiwilliger, entwickelt. Nach Angaben seiner Entwickler wird die Anwendung als „datenschutzbewusste App zur Erkennung der Exposition mit dem Corona-Virus" beschrieben, die bei einem Risikokontakt automatische Warnmeldungen an Benutzer sendet. In diesem Fall erhalten die Nutzer über die App Anleitungen bezüglich häuslicher Quarantäne und der Kontaktaufnahme mit den zuständigen Behörden. *Aman* verfolgt einen dezentralen Ansatz der Datenspeicherung, wonach die Daten 14 Tage auf den Geräten der Nutzer gespeichert werden.

Im **Libanon** erfolgt die Erfassung der COVID-19-Fälle bisher analog. Es wurde bereits früh auf weitreichende Kontaktverbote, Ausgangssperren, Grenzschließungen und Maskenpflicht gesetzt. Ein Callcenter der Epidemiologischen Überwachungseinheit des Gesundheitsministeriums und des Rafik-Hariri-Universitätskrankenhauses in Beirut setzt sich mit Personen,

die positiv getestet wurden, in Verbindung, um mögliche Kontaktpersonen mit einem erhöhten Infektionsrisiko nachzuverfolgen und zu benachrichtigen. Am 16. Juli 2020 kündigte das libanesische Gesundheitsministerium allerdings an, gemeinsam mit Experten der *American University of Beirut* und dem Unternehmen *Tedmob* an der Einführung der Corona-Tracing-App *„Ma3an"* zu arbeiten.

Eine besonders bedenkliche Umsetzung erfolgte im kriegsgeschüttelten Nachbarland Syrien. Nach Angaben des US-amerikanischen Unternehmens *Lookout* sollen syrische Behörden über die Präventions-App „Covid19" eine verschlüsselte Malware verwendet haben, um Daten der Nutzer zu sammeln. So soll eine Spyware dem Regime ermöglicht haben, den Standort, Nachrichten, Bilder, Videos und Kontakte der Nutzer zu erfassen und somit Regierungskritiker zu identifizieren und zu orten.

Rechtliche Probleme

Eines der Hauptprobleme stellt die Abwesenheit rechtlicher Regelungen in vielen der untersuchten Staaten dar. Aber auch dort, wo datenschutzrechtliche Regelungen existieren, ist die Verwirklichung des Datenschutzes zweifelhaft. Exemplarisch sei hier **Marokko** genannt: Trotz der bestehenden Datenschutzgesetze ist fraglich, inwieweit ein ausreichender Datenschutz im Kontext der Corona-Pandemie sichergestellt ist. Beispielsweise verwehrt gerade das Gesetz 09-08 über den Schutz personenbezogener Daten den Schutz solcher Daten, die im Interesse der Landesverteidigung, der inneren oder äußeren Sicherheit des Staates und der Verhütung oder Bekämpfung von Straftaten erhoben und verarbeitet werden. Sollte die Bekämpfung der Pandemie auch darunter fallen, was noch unklar ist, könnte der Datenschutz ausgehebelt werden.

Schlussfolgerungen und Perspektiven

In vielen Ländern des Nahen Ostens und Nordafrikas gibt es derzeit entweder keine spezifischen Datenschutzgesetze, oder aber Gesetze, die veraltet sind und sich daher nicht mit den heutigen Gefahren der Datenverarbeitung und Vorratsdatenspeicherung beschäftigen. Durch diesen oft unzureichenden Schutz personenbezogener Daten und die mangelnde Transparenz hinsichtlich der Art und Dauer der Vorratsdatenspeicherung könnten Corona-Warn-Apps daher zum Datenmissbrauch und im schlimmsten Fall zur staatlichen Überwachung verwendet werden. Auch müssten effektive und unabhängige Kontrollinstanzen und Rechtswege den Bürgern ermöglichen, gegen potentielle Eingriffe in ihre Privatsphäre und andere individuelle Freiheiten vorzugehen. In der MENA-Region, deren Länder mit einigen Ausnahmen von übermächtigen Exekutiven geprägt sind, fehlen jedoch oftmals erforderliche Gegengewichte in Form von starken und handlungsfähigen Parlamenten und unabhängigen Gerichten.

V. Subsahara-Afrika

Arne Wulff

Im Unterschied zu Europa oder Asien spielt das Thema Corona-Warn-App auf Smartphones in Subsahara-Afrika nur eine Nebenrolle. Eine nennenswerte Auseinandersetzung damit findet nur in wenigen der 49 Staaten statt. Von der kostenlosen Zurverfügungstellung einer App auf Mobiltelefonen, wie dies z. B. in Deutschland der Fall ist, ist man noch weit entfernt. Stattdessen entwickeln sich in verschiedenen afrikanischen Staaten landesspezifische Lösungen. Vereint sind sie in dem Ziel, Ansteckungen durch rechtzeitige Warnungen zu verhindern bzw. infizierte Personen rechtzeitig zu identifizieren. Die Rechtsgrundlagen im

Bereich des Datenschutzrechts sind jedoch nur rudimentär vorhanden, lediglich eine gute Handvoll von Staaten hat einen entsprechenden rechtlichen Rahmen geschaffen. Aus diesem Grund kann hier nur eine überblicksartige Zusammenfassung gegeben werden.

Praktische Umsetzung

In **Kenia** wurde die App „Fuata" entwickelt, die der in Deutschland entwickelten App am ehesten ähnlich ist. Jeder, der diese App auf sein Smartphone herunterlädt, erhält eine persönliche Identifikationsnummer (ID). Die Smartphones, auf denen diese App installiert ist, kommunizieren miteinander über Bluetooth und zeichnen die ID des jeweils anderen Geräts für einen Zeitraum von 21 bis 30 Tagen auf. Wird dann eine der betreffenden Personen in dieser Zeit positiv auf Corona getestet, kann nachverfolgt werden, welche anderen Menschen, die die App nutzen, in ihrer Nähe waren; diese können entsprechend gewarnt und getestet werden. Die Privatsphäre soll dadurch geschützt werden, dass keine GPS-Geolokalisierung verwendet wird und persönliche Daten des App-Nutzers nicht von Behörden eingesehen werden können. Noch fehlt es dem Entwickler aber an Mitteln, um die App anbieten zu können. Er hofft auf die Unterstützung großer kenianischer Mobilfunkanbieter wie *Safaricom*.

Eine ähnliche App, die aber zusätzlich zu Bluetooth auch GPS-Daten verwendet, wird derzeit in Uganda entwickelt. Auch **Ruanda** will diesen Weg gehen. Die „Rwanda Utilities Regulatory Authority" hat die Entwicklung einer App in Auftrag gegeben, die die Nachverfolgung von Personen ermöglicht, die Kontakt zu Corona-Infizierten hatten. In beiden Fällen werden Bewegungsprofile zur Erkennung der infizierten und gefährdeten Personen genutzt. Die Daten können auch zur Kontrolle der Quarantänebestimmungen und des „Social Distancing" verwendet werden.

Technisch bedingt setzt die Nutzung der Apps ein Smartphone voraus. Der Verbreitungsgrad dieser Geräte ist in Subsahara-Afrika allerdings noch immer recht gering. Zwar ist die Dichte an Mobiltelefonen zwischenzeitlich relativ hoch (z. B. 97 Mobiltelefone pro 100 Einwohner in Kenia, 167 pro 100 in Südafrika, aber auch nur 59 pro 100 in Äthiopien und 44 pro 100 in Angola). Dies gilt aber nicht für Smartphones. Während in Deutschland 79 % der Bevölkerung über ein Smartphone verfügen, sind dies in Südafrika nur 35,5 %, in Kenia 20,9 %,

in Uganda 15,6 % und in Nigeria 13 % (Newzoo Global Mobile Market Report 2018). Dadurch sind die Vorteile einer Corona-Warn-App sehr beschränkt – schließlich ist der Grad ihrer Wirksamkeit abhängig von der Zahl der Nutzer.

Einen anderen Weg geht deshalb ein **südafrikanisches** Start-Up. Das Unternehmen „Automatech" setzt anstatt auf Smartphones auf ein kleines Gerät, das mit Hilfe eigener Software den Kontakt zwischen infizierten Personen dokumentieren kann. Das Gerät zum Preis von ca. 15 Euro wurde bereits von größeren Unternehmen bestellt, um ihr damit ausgestattetes Personal besser vor Ansteckungen durch Kontakte bei der Arbeit warnen zu können. Im Unterschied zu den meisten Apps erkennt das Gerät nicht, wo man sich befindet, sondern nur, mit wem man Kontakt hatte, wenn die betreffende Person ebenfalls mit einem solchen Gerät ausgestattet ist. Dadurch ist es weder dem Anbieter noch der Regierung oder Hackern möglich, die Identität des Nutzers festzustellen oder ein Bewegungsprofil zu erstellen – ein Umstand, der gerade im Hinblick auf den Schutz persönlicher Daten von großer Bedeutung ist.

Rechtliche Probleme

Vieles spricht dafür, dass die Sorge um die Sicherheit der persönlichen Daten einer der Gründe für die geringe Nachfrage nach einer „Tracing-App" in Subsahara-Afrika ist. Zwar sind alle Staaten Afrikas dem Internationalen Pakt über bürgerliche und politische Rechte (ICCPR) von 1966 beigetreten. Dieser schützt u. a. die persönliche Freiheit aller Menschen. Eine Erweiterung des Paktes um ein rechtsverbindliches Instrument für den Datenschutz und den Schutz der Privatsphäre, wie u. a. von Deutschland seit 2013 gefordert, hat es bisher aber nicht gegeben. Zwar haben 24 afrikanische Staaten Gesetze und Regulierungen zum Schutz der persönlichen Daten beschlossen. Darunter sind auch 14 Staaten, die die „Convention on Cyber Security and Data Protection" der Afrikanischen Union unterzeichnet haben. Darin verpflichten sich die Staaten u. a. dazu, einen rechtlichen Rahmen in ihren Ländern zum Schutz der personenbezogenen Daten herzustellen. Tatsächlich haben bisher aber nur sechs Staaten die Konvention ratifiziert (**Senegal, Namibia, Mauritius, Guinea, Ghana** und **Rwanda**). Meistens fehlt es allerdings auch dort, wo nationalstaatliche Regelungen zum Schutz von Daten geschaffen wurden, an der Implementierung. Es wurden z. B. noch keine zuständigen staatlichen Organe und Einrichtungen geschaffen, die den Schutz sicherstellen, oder Datenschutzbeauftragte berufen, an die sich die Bürger wenden könnten. Zusätzlich gibt es Befürchtungen seitens der Nutzer von Smartphones, sich durch das Herunterladen einer Corona-Warn-App noch stärker der ohnehin schon intensiven staatlichen Kontrolle auszusetzen. So gibt es beispielsweise in **Simbabwe** eine angeregte Diskussion darüber, wie es dazu kommen konnte, dass Personen, die ihre Quarantäne unbefugt verlassen hatten, von den Behörden nachverfolgt werden konnten. Es wird vermutet, dass anhand der Daten ihrer Mobiltelefone Bewegungsprofile erstellt wurden, was rechtlich nicht zulässig wäre.

Schlussfolgerungen und Perspektiven

Solange die Verbreitung von Smartphones in vielen afrikanischen Staaten gering ist und die Menschen auf Grund mangelnden Datenschutzes und autoritärer Systeme Sorge davor haben, dass Corona-Warn-Apps weniger ihrem persönlichen Schutz als vielmehr staatlicher Kontrolle dienen, wird die Akzeptanz dieser digitalen Helfer gering bleiben. Dies gilt kurioserweise erst recht in Zeiten der COVID-19-Pandemie: in vielen Ländern missbrauchen staatliche Sicherheitskräfte die prekäre Lage der Bevölkerung bereits jetzt schon. Dem möchte die Bevölkerung durch das Herunterladen einer App nicht auch noch weiteren Vorschub leisten.

VI. Zusammenfassung

Pavel Usvatov, Gisela Elsner, Marie-Christine Fuchs

Die Regierungen fast aller Länder in den untersuchten Regionen haben schon ganz zu Anfang der Pandemie den in ihren Ländern verfassungsrechtlich meist zulässigen Notstand ausgerufen, was der ohnehin sehr mächtigen Exekutive in vielen Fällen noch mehr Befugnisse verliehen hat. Zugleich bestehen aber auch nicht ohne Grund Befürchtungen, dass die vielerorts in den Regionen schlecht ausgebauten Gesundheitssysteme angesichts rapide ansteigender Fallzahlen schnell zusammenbrechen könnten. Viele Regierungen reagierten deshalb mit dem Erlass von Dekreten, die bedenklich weitgehende Freiheitseinschränkungen wie z. B. mehrere Monate andauernde Quarantänemaßnahmen,

strikte Ausgangssperren oder Grenzschließungen vorsahen. Vielerorts ist es schwierig zu beurteilen, ob die Maßnahmen ausschließlich dem Gesundheitsschutz dienen, oder unter diesem Deckmantel der Ausweitung der staatlichen Überwachung Vorschub leisten sollen.

Die mit Entwicklung und Einsatz von Corona-Tracking-Apps verbundenen Möglichkeiten einer flächendeckenden und präzisen Überwachung der Bevölkerung wirft eine Vielzahl von Fragen mit Blick auf den Schutz der Privatsphäre und den Datenschutz auf. Auch darüber hinaus stellen sich generell die Fragen, ob und wie unter diesen Umständen die Grundsätze der Rechtsstaatlichkeit beachtet und der Schutz der bürgerlichen Freiheiten gewährleistet werden können. Zugleich bietet sich den Regierungen aber auch die Möglichkeit, ihre Legitimität dadurch zu erhöhen, dass sie auch in Zeiten einer Pandemie Erfordernisse der materiellen Rechtsstaatlichkeit beim Einsatz digitaler Kontaktverfolgungstechnologien berücksichtigen und einen effektiven Schutz der Bürgerrechte gewährleisten.

Jenseits der weltweit bestehenden gesellschaftlichen und politischen Unterschiede in Bezug auf den Begriff des Datenschutzes sind im Zuge der Debatte auch die hier dargestellten Staaten hinsichtlich ihres Umgangs mit dem Recht ihrer Bürger auf Privatsphäre ins Rampenlicht gerückt. Internationale und nationale Menschenrechtsorganisationen und Vertreter der Zivilgesellschaft weltweit fordern vermehrt, dass die Betreiber der Corona-Warn-Apps die Sammlung der Daten gemäß dem Prinzip der Verhältnismäßigkeit auf das erforderliche Mindestmaß beschränken und eine sichere und anonyme Speicherung garantieren müssen. Jegliche Datenerhebung muss auf die Pandemie-Eindämmung beschränkt sein und sollte nicht für andere Zwecke, insbesondere nicht für Zwecke der Strafverfolgung, nationaler Sicherheit oder Einwanderungskontrolle verwendet werden. Des Weiteren muss sichergestellt werden, dass Daten nicht zur kommerziellen Nutzung weitergegeben werden. Besonderes Augenmerk muss auch der Garantie der freiwilligen Nutzung der Apps gelten. Hierfür sollte gewährleistet sein, dass es nicht zu einem faktischen Nutzungszwang kommt, indem die App zur Voraussetzung gesellschaftlicher Teilhabe wird. Schließlich dürfen die Bürger auch nicht an eine Dauerüberwachung herangeführt und gewöhnt werden. All das ist zur Zeit noch nicht gewährleistet.

Aus praktischer Sicht bleibt die Wirksamkeit der Apps bei der Eindämmung der Pandemie oder der Generierung verlässlicher Daten fraglich, wenn sie nicht durch eine große Mehrheit der Bevölkerung genutzt wird. In dem Maße, in dem die Staaten beginnen, die sonstigen Einschränkungen zu lockern, suchen die Regierungen zunehmend nach Möglichkeiten, die Nutzung der entsprechenden Apps zu fördern. Daher sollte die Berücksichtigung von Datenschutzbedenken Teil der Strategie zur Verlangsamung der Pandemie sein und nicht als Luxusproblem abgetan werden. Unter diesen Umständen bleiben viele schwierige Fragen im Zusammenhang mit diesem Thema unbeantwortet, darunter die Frage, wie Informationen datenschutzkonform gesammelt und gesichert werden können, wer Zugang zu den Daten hat, welche rechtlichen, organisatorischen und technischen Schutzmaßnahmen getroffen werden können, um die Risiken des Datenaustauschs und des Missbrauchs von Daten zu minimieren. Ein Schlüsselaspekt ist darüber hinaus der Umgang der Staaten mit der Sammlung von Daten nach dem Ende der Pandemie: Hier gibt es Absichtsbekundungen von Regierungen, die Daten dann zu löschen und nicht weiter zu sammeln. Gesetzliche Regelungen hierzu, die entsprechende Verpflichtungen enthielten, sucht man aber vergeblich. Es wird aber inzwischen immer klarer, dass der Schutz der personenbezogenen Daten für die Bürger der meisten Länder von zentraler Bedeutung ist, damit sie diesen Apps, modernen Technologien insgesamt und auch ihrer eigenen Staatsführung vertrauen können.

Der Einsatz moderner Technologien wird bei der Bekämpfung dieser und vergleichbarer Pandemien unumgänglich sein. Die entscheidende Frage dürfte deshalb am Ende lauten: Wird durch die nun gemachten Erfahrungen in Zukunft eine Normalisierung des Überwachungsverhaltens von Staaten und Unternehmen in geordneten rechtlichen Bahnen unter Beachtung der Bürgerrechte ermöglicht? Angesichts der vielerorts noch unterentwickelten Rechtsgrundlagen für die Nutzung derartiger Technologien bleibt es zur Zeit noch unklar, welche Mechanismen zum Schutz vor Eingriffen in die Privatsphäre, vor umfassender Überwachung und möglicher Verfolgung bestimmter Personengruppen in den untersuchten Regionen der Welt entstehen werden. Das Bewusstsein hierfür aber wächst – auch außerhalb Europas.

[1] Bundeskanzlerin Angela Merkel im Podcast v. 20. Juni 2020, www.bundesregierung.de/breg-de/themen/coronavirus/je-mehr-mitmachen-desto-groesser-der-nutzen-1762982.

[2] Stand: 27. Juli 2020, www.connect.de/news/corona-warn-app-download-zahlen-3200860.html.

[3] Nicht zu verwechseln mit einer „Tracking-App", bei der ein Standort-Tracking erfolgt, z. B. Anhand der GPS-Geodaten oder über das Mobilfunknetz. Beim „tracing" (engl. u. a. Verfolgung, Aufzeichnung) geht es allein um die Erfassung der Daten darüber, ob überhaupt ein Kontakt erfolgt ist, nicht hingegen den Ort des Kontaktes.

[4] www.waz.de/politik/coronavirus-scheitert-die-tracking-app-fuer-den-kampf-gegen-die-pandemie-id228955653.html.

[5] www.faz.net/aktuell/rhein-main/forscher-entdecken-sicherheitsluecke-bei-corona-apps-16812694.html.

[6] Beispielsweise soll die Übertragung und Speicherung der IP-Adressen in Kombination mit anonymen Daten und der ID Rückschlüsse auf die Identität des Nutzers erlauben können, s. Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V. , Analyse und konstruktive Kritik der offiziellen Datenschutzfolgenabschätzung der Corona-Warn-App, Version 1.0 – 29. Juni 2020, S. 3, 5f. Im Übrigen ist bereits die IP selbst und nicht erst die dahinter stehende Information für den Anbieter ein personenbezogenes Datum, BGH, Urt. v. 16.05.2017, Az. VI ZR 135/13 (noch zu TMG und BDSG), in Fortführung von EuGH, Urt. v. 19.10.2016 – C-582/14.

[7] www.faz.net/aktuell/rhein-main/forscher-entdecken-sicherheitsluecke-bei-corona-apps-16812694.html.

[8] So könnten z. B. Unternehmen die Nutzung der App zur Voraussetzung für den Zutritt zu Geschäftsräumen machen, www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/kugelmann-pocht-auf-freiwilligkeit-der-corona-warn-app-sie-darf-nicht-zur-eintrittskarte-werden.

[9] Für eine umfassende Darstellung mit vielen weiteren Nachweisen s. Joelle Grogan, States of Emergency, verfassungsblog.de/states-of-emergency.

[10] Z. B. : „Die größte Herausforderung seit dem Zweiten Weltkrieg" (Sebastian Kurz), www.rnd.de/politik/kurz-zu-coronavirus-grosste-herausforderung-seit-dem-zweiten-weltkrieg-O2KYRUWHPVHHBCRS5PBHJYNCBM.html; "Wir sind im Krieg" (Emmanuel Macron), www.spiegel.de/politik/ausland/coronavirus-in-frankreich-wir-sind-im-krieg-a-50b0dce2-6f7e-4cba-bda1-87fe05bfc7ca; zusammenfassend www.nzz.ch/feuilleton/corona-und-kriegsrhetorik-ld.1560145.

[11] www.echr.coe.int/Documents/Convention_DEU.pdf.

[12] www.euractiv.com/section/digital/news/slovenian-pm-calls-for-mandatory-coronavirus-app-against-commission-advice.

[13] newseu.cgtn.com/news/2020-05-07/Why-COVID-19-contract-tracing-apps-are-causing-deep-division-in-Europe-Qhq5NSZgTm/index.html.

[14] balkaninsight.com/2020/04/16/north-macedonia-leads-region-in-covid-19-tracing-app.

[15] hr.n1info.com/English/NEWS/a530515/Croatia-presents-its-Stop-COVID-19-app.html.

[16] cep.org.rs/en/blogs/covid-19-tracing-app-in-serbia.

[17] www.balcanicaucaso.org/eng/Areas/Balkans/Not-just-apps-privacy-personal-data-and-COVID-19-in-the-western-Balkans-201814.

[18] So z. B. in Bosnien-Herzegowina, www.kas.de/de/web/rlpsee/laenderberichte/detail/-/content/ausgangssperre-verfassungswidrig.

[19] verfassungsblog.de/singapores-legislative-approach-to-the-covid-19-public-health-emergency.

[20] www.thehindubusinessline.com/news/why-legal-experts-think-aarogya-setu-app-cant-be-made-mandatory/article31621274.ece.

21 indianexpress.com/article/india/aarogya-setu-app-mandate-illegal-justice-b-n-srikrishna-6405535.
22 Nach Artikel 34 bis (1)41 der Akte nach Artikel 76 bis (3) der IDPC-Akte.
23 hbr.org/2020/04/how-digital-contact-tracing-slowed-covid-19-in-east-asia.
24 www.channelnewsasia.com/news/singapore/covid19-trace-together-mobile-app-contact-tracing-coronavirus-12560616.
25 www.bbc.com/news/technology-53146360.
26 www.bbc.com/news/technology-53146360.
27 static.mygov.in/rest/s3fs-public/mygov_159051645651307401.pdf.
28 Lee, Gyooho, Legitimität und Verfassungsmäßigkeit der Ermittlung von Kontaktpersonen bei einer Pandemie in der Republik Korea (7. Mai 2020). Verfügbar bei SSRN: ssrn.com/abstract=3594974 oder dx.doi.org/10.2139/ssrn.3594974.
29 Ebd.
30 scroll.in/article/962687/by-making-employers-responsible-for-ensuring-aarogya-setu-use-state-has-outsourced-law-enforcement.
31 www.gov.sg/article/digital-contact-tracing-tools-for-all-businesses-operating-during-circuit-breaker.
32 www.todayonline.com/singapore/covid-19-governance-expert-says-tracetogether-should-be-mandatory-warns-potential-slippery.
33 www.straitstimes.com/singapore/contact-tracing-device-will-not-track-location-and-people-can-use-tracetogether-if-they.
34 Ebd.
35 www.thehindubusinessline.com/news/why-legal-experts-think-aarogya-setu-app-cant-be-made-mandatory/article31621274.ece.
36 www.thehindubusinessline.com/news/why-legal-experts-think-aarogya-setu-app-cant-be-made-mandatory/article31621274.ece.
37 www.pri.org/stories/2020-05-22/south-korea-s-coronavirus-contact-tracing-puts-lgbtq-community-under-surveillance.
38 Art. 2 Abs. 6 der peruanischen Verfassung in seiner Fassung von 1993: „Toda persona tiene derecho: A que los servicios informáticos, computarizado o no, públicos o privados, no suministren informaciones que afectan la intimidad personal y familiar".
39 Gesetz Nr. 19.628 aus 1999, dessen Hauptaugenmerk auf der Datenverwertung durch Dritte liegt. Überwachungsmechanismen für eine ordnungsgemäße Erfüllung fehlen im Gesetz und auch die in Art. 16 vorgesehene Möglichkeit der gerichtlichen Beantragung zur Löschung von Daten bei deren unrechtmäßiger Verwendung erweist sich bis dato als wirkungslos. Siehe www.leychile.cl/Navegar?idNorma=141599.
40 So etwa: Corte Suprema de Chile, Rol N° 11256-2011, de 27 de enero de 2012, c. 6°.
41 Gesetz Nr. 1.581/2012 und Nr. 1.266/2008 sowie die Dekrete 1377/2013 und 886/2014.
42 stcs.senado.gob.mx/docs/08.pdf.
43 blogs.iadb.org/conocimiento-abierto/es/proteccion-de-datos-gdpr-america-latina.
44 Herzog, Roman: Lateinamerika in der neuen Kommunikationswelt, in: Bodemer, Klaus / Gratius, Susanne (Hrsg.), Lateinamerika im internationalen System: Zwischen Regionalismus und Globalisierung, Springer 2003, S. 259.
45 Bis vor kurzem fehlte in Brasilien ein spezifisches Gesetz zur Regelung des Datenschutzes und sogar eine Definition von personenbezogenen Daten. Stattdessen behielt das Land jahrelang mehrere sektorale Gesetze bei, die allgemeine Bestimmungen über den Schutz von Personen und deren Daten enthielten. Das Verbraucherschutzgesetz zum Beispiel sah einige Datenschutzrechte vor, um auf Verbraucherdaten zuzugreifen und diese zu korrigieren, das Strafgesetzbuch enthält den Rechtsrahmen für die Verarbeitung personenbezogener Daten im Internet. Das im August 2018 erlassene LEI Nº 13.709 trat Anfang 2020 in Kraft. Abrufbar unter: www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-publicacaooriginal-156201-pl.html.
46 www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75.
47 www.elespectador.com/noticias/salud/funciona-o-no-la-coronapp.

48 www.dw.com/es/david19-un-rastreador-digital-contra-la-covid-19-en-am%C3%A9rica-latina/a-53538288.

49 web.karisma.org.co/coronapp-medellin-me-cuida-y-calivalle-corona-al-laboratorio-o-como-se-hackea-coronapp-sin-siquiera-intentarlo.

50 socialtic.org/blog/analisis-app-covid19mx-resumen.

51 socialtic.org/blog/analisis-app-covid19mx-resumen.

52 Art. 10 des Gesetzes Nr. 1.581/2012.

53 sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Compendio%202%20FINAL%20V%2012%20Dic20.pdf, S. 256.

54 archive.org/details/informe-publico-tecnico-coron-app-v-170320-1/mode/2up.

55 Auch der Hinweis, dass „Dritten aufgrund eines Gerichts- oder Verwaltungsbeschlusses Zugang oder Offenlegung zu gewähren ist" ist bedenklich.

56 ciperchile.cl/2020/04/22/problemas-de-proteccion-de-los-datos-personales-de-la-aplicacion-coronapp.

57 So etwa netzpolitik.org/2020/warum-freiwilliges-handy-tracking-nicht-funktioniert.

58 Die Verbreitung von Smartphones wird für das Jahr 2020 auf ca. 69 % geschätzt, https://www.statista.com/statistics/218531/latin-american-smartphone-penetration-since-2008.

59 Königlicher Erlass Nr. M/18: Gesetz über elektronische Transaktionen; Königlicher Erlass Nr. M/17: Anti-Cyber-Kriminalitätsgesetz.

60 https://smex.org/an-ugly-new-data-protection-law-in-lebanon/.

Impressum

Die Autorinnen und Autoren

Dr. Pavel Usvatov ist Koordinator der internationalen Rechtsstaatsprogramme der Konrad-Adenauer-Stiftung (vertretungsweise).

Hartmut Rank, LL.M., MBA ist Leiter des Rechtsstaatsprogramms Südosteuropa der Konrad-Adenauer- Stiftung.

Stanislav Splavnic, LL.M. ist wissenschaftlicher Mitarbeiter im Rechtsstaatsprogramm Südosteuropa der Konrad-Adenauer-Stiftung.

Gisela Elsner war bis Juli 2020 Leiterin des Rechtsstaatsprogramms Asien der Konrad-Adenauer-Stiftung.

Aishwarya Natarajan ist wissenschaftliche Mitarbeiterin im Rechtsstaatsprogramm Asien der Konrad-Adenauer-Stiftung.

Dr. Marie-Christine Fuchs, LL.M. ist Leiterin des Rechtsstaatsprogramms Lateinamerika der Konrad-Adenauer-Stiftung.

Magdalena Schaffler ist Projektkoordinatorin im Rechtsstaatsprogramm Lateinamerika der Konrad-Adenauer-Stiftung.

Dr. Malte Gaier ist kommissarischer Leiter des Rechtsstaatsprogramms Nahost / Nordafrika der Konrad-Adenauer-Stiftung.

Anja Finke ist Projektkoordinatorin im Rechtsstaatsprogramm Nahost / Nordafrika der Konrad-Adenauer-Stiftung.

Dr. Arne Wulff ist Leiter des Rechtsstaatsprogramms Subsahara-Afrika (anglophone Länder) der Konrad-Adenauer-Stiftung.

Für eine vollständige Version dieses Beitrags inkl. Quellenverweisen wählen Sie bitte das PDF-Format.

Konrad-Adenauer-Stiftung e. V.

Dr. Pavel Usvatov
Referent Rechtsstaatsdialog und Völkerrecht
Analyse und Beratung
T +49 30 / 26 996-3948
pavel.usvatov@kas.de

Postanschrift: Konrad-Adenauer-Stiftung, 10907 Berlin

Herausgeberin: Konrad-Adenauer-Stiftung e. V. 2020, Berlin
Gestaltung: yellow too Pasiek Horntrich GbR
Satz: Franziska Faehnrich, Konrad-Adenauer-Stiftung e. V.

ISBN 978-3-95721-762-2