Eine bedenkliche Begleiterscheinung der Corona-Politik ist die Einführung von Mitteln der Massenüberwachung. Gleichzeitig gerät die Idee des Datenschutzes prinzipiell unter Druck. Dazu kommt, dass viele Bürger diese Entwicklungen unter dem Eindruck der „Pandemie"-Bekämpfung eher akzeptieren. Von **Tobias Riegel**.

Dieser Beitrag ist auch als Audio-Podcast verfügbar.

https://www.nachdenkseiten.de/upload/podcast/210127_Corona_und_massenhafte_Ueberwachung_NDS.mp3

Podcast: Play in new window | Download

Das Recht auf den Schutz der eigenen Daten gerät im Zuge der Corona-Politik unter den Druck eines vielstimmigen Chores. Hier folgen einige ausgewählte Stimmen. So forderte der Chef des Mobilfunk-Konzerns Vodafone Deutschland gerade, beim Thema Datenschutz „über unseren Schatten zu springen", wie Medien berichten: Mobilitätsdaten könnten helfen, die Krise schneller und besser zu bewältigen. Aktuell sei dies aber wegen des "hiesigen Datenschutzes" nicht gestattet. Er frage sich angesichts der aktuellen „Fallzahlen" aber, "ob wir jetzt nicht mal über unseren Schatten springen sollten". (…) "Personalisierte Daten wären ein weitreichender Schritt, selbst darüber sollte man aber nachdenken und reden können."

Der CDU-Politiker Friedrich Merz erklärte kürzlich laut Medien, dass Politik und Recht „viel zu viel auf den individuellen Datenschutz" ausgerichtet seien, auch wenn dies auf Kosten der Allgemeinheit gehe. Die Corona-Warn-App, so Merz, sei wirkungslos, da sie eine Nachverfolgung der Infizierten nicht ermögliche. Eine Tracking-App, wie sie etwa in Südkorea oder Japan erfolgreich zum Einsatz gekommen sei, sei „viel effizienter". In einem Gastbeitrag in der „Welt" wird so argumentiert:

> „Unser Datenschutz verhindert eine wirksame Corona-Warn-App: Die Bundesregierung ist der Ansicht, dass es am Datenschutz keinerlei Abstriche geben darf – während die anderen Grundrechte massiv eingeschränkt werden. Doch es ist nicht zulässig, ein einzelnes Grundrecht zu verabsolutieren und die anderen Grundrechte dafür zu opfern."

Die Floskel vom „falsch verstandenen Datenschutz"

Und die NZZ ist erstaunt, dass „die Informationstechnik nicht ausreichend zur Bekämpfung der Corona-Pandemie genutzt“ werde. In verschiedenen asiatischen Ländern – insbesondere Südkorea und Taiwan – würden Bewegungsprofile basierend auf den Handydaten zur Kontaktverfolgung und zur Isolierung Infizierter benutzt, so die Zeitung. Nicht nur China betreibe eine informationstechnische Beobachtung der Bevölkerung zur Seuchenbekämpfung, sondern auch demokratische Staaten. Weil manche dieser Länder mit ähnlichen Instrumenten aber auch die politische Zuverlässigkeit der Menschen sichern wollten, würde in westlichen Rechtsstaaten auf die entsprechenden Techniken verzichtet, beklagt die NZZ und fragt:

> „Und besteht in Deutschland (oder seinen europäischen Nachbarländern) wirklich die ernsthafte Gefahr, dass eine autoritäre Regierung sich daranmacht, die Bürger total zu überwachen? Diese These wird von einigen besorgten Datenschützern vertreten. Sie ist hier und heute durch nichts begründet.“

Nicht immer wird die neue Technik begeistert begrüßt, was auch an Missbrauch durch Sicherheitsbehörden liegt. So gibt es in Singapur aktuell großen Unmut darüber, dass die erhobenen Daten nicht nur zum „Gesundheitsschutz“ genutzt werden, sondern auch zur Strafverfolgung, wie Medien berichten: „Das Innenministerium bestätigte, dass die Daten von der Polizei für strafrechtliche Ermittlungen eingesehen werden könnten.“ Dieser Vorgang erinnert an die von der deutschen Polizei beschlagnahmten Gästelisten aus Gaststätten – eine Praxis, die ebenfalls den Ankündigungen, die Listen dienten nur dem „Gesundheitsschutz“, widersprach. Die NachDenkSeiten haben in dem Artikel „Die Polizei und die Corona-Gästelisten: Mit Täuschung in die Vorratsdatenspeicherung?“ über den Vorgang berichtet :

> “Zusätzlich besteht die Gefahr, dass auf solch umstrittenen Wegen erhobene Daten (wenn sie einmal verfügbar sind und die Nutzung für ein begrenztes Feld erlaubt wurde) dann auch außerhalb des einst eingegrenzten Feldes genutzt werden könnten. Die Floskel vom ‚falsch verstandenen Datenschutz‘ kennt man bereits von der Debatte um die Rechtfertigung der Voratsdatenspeicherung.“

„Der Staat muss Bewegungsprofile auswerten dürfen“

Zu Wort gemeldet hat sich auch Stefan Dräger, der Chef des größten Herstellers von Beatmungsgeräten weltweit, wie die „Welt“ berichtet: „Der Staat muss Bewegungsprofile

auswerten und nutzen dürfen." Laut Medien sagte Dräger weiter:

> „Um besser mit Corona leben zu können, könnte man darüber nachdenken, den Datenschutz aufzuweichen und dem Beispiel asiatischer Länder zu folgen. Nur traut sich kaum einer, das zu sagen."

Der Staat müsse Bewegungsprofile auswerten und das Wissen darüber nutzen dürfen, wer mit wem an welchem Ort Kontakt habe, so Dräger. Schützenhilfe für diese weitreichenden Überwachungs-Pläne erhält er von Uwe Brandl, Präsident des Bayerischen Gemeindetags, wie Medien berichten. Brandl hält den coronabedingt geltenden 15-Kilometer-Bewegungsradius für schwer kontrollierbar. Als Alternative schlägt er vor, Bewegungsprofile aus Handys auszulesen.

„Wegen Corona": Zugriff auf Standorte, Bewegungsprofile und Adressbücher

Wohin die Reise auch für uns gehen könnte, wenn man den hier zitierten Stimmen folgt, kann man an den abschreckenden Beispielen vieler Länder sehen: „Die Corona-Pandemie beschleunigt die digitale Massenüberwachung rasant", erklärt etwa die Initiative „Brot für die Welt" und führt aus:

> „In vielen Ländern kontrollieren Apps Bewegungen und Kontakte großer Teile der Bevölkerung. Manche Regierungen missbrauchen die Daten, um kritische Stimmen zu unterdrücken. Schätzungsweise eine Milliarde Menschen nutzen allein in China und Indien Tracing- und Tracking-Apps. Die Regierungen haben so Zugriff auf Standortdaten, Bewegungsprofile und im Fall der indischen App Aarogya Setu auch auf die Adressbücher der Nutzerinnen und Nutzer. Es fehlen Angaben zur Verwendung der Daten, Löschfristen und die Zusicherung, die Daten unter Wahrung der Anonymität auszuwerten. Offiziell gilt die Nutzung der Apps zwar als freiwillig, aber praktisch wird sie erzwungen."

Auf die Gefahr der Verstetigung der „Corona-Maßnahmen" weist „Amnesty International" hin:

> „Die jetzt getroffenen Maßnahmen könnten die Krise überdauern und bestimmen, wie Überwachung in einer Welt nach COVID-19 aussieht. (…) Sind

> Daten erst einmal gesammelt, besteht die Gefahr, dass sie auch für andere Zwecke eingesetzt werden als zum Schutz der Gesundheit."

Die Initiative fährt fort:

> „Einige Regierungen arbeiten mit Unternehmen zusammen, die in der Vergangenheit den Respekt vor den Menschenrechten vermissen ließen. Die umstrittenen US-amerikanischen Anbieter von Überwachungstechnologie Clearview AI und Palantir befinden sich Berichten zufolge in Gesprächen mit US-Behörden. Das israelische Überwachungsunternehmen NSO Group, das seine Produkte an Regierungen mit erschreckender Menschenrechtsbilanz verkauft, vertreibt jetzt ein Big-Data-Analysetool, das angeblich die Ausbreitung des Virus über die Bewegungsdaten der Menschen nachvollzieht."

Kontrolle und Zensur

Begleitet wird diese Entwicklung hin zu mehr Überwachung von einer Verengung des Debattenraums in fast allen großen Medien und einer sich verschärfenden Praxis von Löschungen der Beiträge Andersdenkender in den sozialen Medien. Diese Entwicklung ist in Deutschland nicht zu leugnen, in anderen Ländern ist sie teils noch weiter fortgeschritten. So habe die „Corona-Pandemie zu einem ‚dramatischen Verfall' der Freiheit im Internet geführt" – zu diesem Ergebnis kommt die teils fragwürdige US-Organisation „Freedom House", wie die „Süddeutsche Zeitung" bereits im Herbst berichtete. Bei dem Absatz ist aber zu beachten, dass sich die Zensur zumindest hierzulande nicht gegen „Informationen über die Ausbreitung der Pandemie" richtet, sondern gegen kritische Standpunkte gegenüber der offiziellen Corona-Politik:

> „Dieses Jahr zeige sich ein 'besonders düsteres' Bild. Staatliche und private Akteure in zahlreichen Ländern hätten die Krise genutzt, um online veröffentlichte Informationen zu steuern, kritische Berichte zu unterdrücken und neue Technologien zur sozialen Kontrolle zu installieren. Behörden hätten in mindestens 28 von 65 untersuchten Ländern Websites gesperrt oder einzelne Nutzer, Plattformen oder Online-Publikationen gezwungen, Informationen über die Ausbreitung der Pandemie zu löschen. In mindestens 13 Ländern sei das Internet zeitweise ganz abgeschaltet worden, besonders häufig in Regionen, in denen Minderheiten leben. Neue Gesetze zur Eindämmung vermeintlich falscher

> Nachrichten über das Infektionsgeschehen oder zum Erhalt der öffentlichen Ordnung würden vielfach missbraucht."

Zur Massen-Kontrolle über „Corona-Warn-Apps" in anderen Ländern schreibt die Zeitung:

> „Es ist möglich, diese Apps so zu programmieren wie die von Datenschützern gelobte deutsche Corona-Warn-App. (…) In mindestens 54 Ländern aber existieren laut dem Bericht nur minimale Vorkehrungen gegen den Missbrauch solcher sensiblen Informationen, die zudem vielfach mit bereits existierenden, öffentlich oder privatwirtschaftlich erhobenen Daten über die Bürger gekoppelt und an verschiedene Behörden weitergegeben würden. (…) In pakistanischen Geheimdienstberichten sei die Rede von abgehörten Telefonaten in Krankenhäusern, mit denen ermittelt werden solle, ob Freunde und Bekannte von Patienten ebenfalls Symptome zeigen. (…) Südkoreanische Beamte griffen auf Kreditkartenabrechnungen, Handystandorte und Sicherheitskameras zu, um die Ausbreitung des Virus zu überwachen."

„So überwacht der Arbeitgeber seine Mitarbeiter! Fünf Methoden im Test"

Ein weiteres potenzielles Feld der zukünftigen Massenüberwachung ist der Arbeitsplatz. Dass Corona als „Türöffner für Überwachung der Mitarbeiter" genutzt werden kann, haben die NachDenkSeiten im gleichnamigen Artikel beschrieben:

> „Die Einführung eines ‚Ökosystems' an Werkzeugen zur betriebsinternen Überwachung der Mitarbeiter wird von PWC mit dem ‚Schutz der eigenen Mitarbeiter in Bezug auf Hygiene und Infektionsrisiken' begründet. (…) Laut DLF haben auch andere IT-Firmen oder Unternehmensberatungen wie die Boston Consulting Group (BCG) erkannt, dass Firmen einen Bedarf an ‚Pandemie-Kontrollsystemen' hätten, und würden diese nun anbieten. (…) Dabei proklamieren die meisten Unternehmen, die Nutzung der Apps beruhe auf Freiwilligkeit der Mitarbeiterinnen und Mitarbeiter. Doch diese ‚Freiwilligkeit' ist gegenüber dem Arbeitgeber nicht gegeben."

Aktuell untersucht „Stiftung Warentest", welche Mittel hier gerade noch legal wären. Laut Medien heißt es dort: „Was ist erlaubt, was nicht? So überwacht der Arbeitgeber seine

Mitarbeiter! Fünf Methoden im Test“. Der Bericht fährt fort:

> „Webcam-Aufzeichnungen: Manche Software ermöglicht es, Beschäftigte über die Kamera des Rechners zu kontrollieren. Eine solche Videoüberwachung ohne jeglichen Anlass ist in aller Regel verboten. Besteht etwa der Verdacht, dass Beschäftigte bei den Arbeitszeiten betrügen, kann eine heimliche Überwachung ausnahmsweise und zeitlich eng begrenzt zulässig sein, erklärt Stiftung Warentest. Allerdings nur dann, wenn sie das einzig mögliche Mittel ist, den Arbeitszeitbetrug nachzuweisen.“

Viele Menschen würden die in diesem Text thematisierten Kontrollmaßnahmen eigentlich nur vorübergehend und nur zur akuten Gefahrenabwehr akzeptieren. Unter dem Eindruck einer angstschürenden Medienkampagne sieht das aber schon anders aus. Der oben zitierte Bericht von Freedom House schließt mit der berechtigten Warnung vor einer Verstetigung der offiziell als nur temporär dargestellten Maßnahmen:

> „Die Autoren des Berichts schreiben, dass es ‚schwierig, wenn nicht unmöglich’ sein werde, solche Instrumente zur Überwachung wieder außer Betrieb zu nehmen, nachdem das Virus bezwungen ist. Die Geschichte zeige, ‚dass neue staatliche Vollmachten für gewöhnlich die ursprüngliche Bedrohung überdauern‘.“

Titelbild: DedMityay / Shutterstock

Mehr zum Thema

Corona als Türöffner für Überwachung der Mitarbeiter

Niemand hat die Absicht, einen Immunitätsausweis einzuführen

Corona: Der „freiwillige“ Zwang gegen die Bürger

Massen-Kontrolle: „Alle nutzen Google und Facebook und haben jetzt plötzlich Datenschutz-Bedenken“

„Clearview“: Die Realität der massenhaften Überwachung

Gesichtserkennung: Mit Populismus in den Überwachungsstaat

Rosige Zeiten für Zensoren und Spione: Der Großangriff des Überwachungsstaates

„Kontinuierliche, automatische Überwachung“: Die EU, die Zensur und das Urheberrecht

Die Polizei und die Corona-Gästelisten: Mit Täuschung in die Vorratsdatenspeicherung?

Willkommen in der „neuen Normalität“