Virale Überwachung

Die Ausrufung des nationalen Notstands hat in einigen die Angst vor dem überstarken Staat geweckt. Aber eine kurzfristig zu vereinfachter Gesetzgebung ermächtigte Exekutive unter der Kontrolle einer weiter voll funktionsfähigen Legislative stellt nur eine vorübergehende Ausnahme dar, was sich von anderen Maßnahmen zur Volkssicherheit nur bedingt erwarten lässt.

Corona-App

Da sind einerseits die offensichtlich grenzwertigen Maßnahmen zur Rückverfolgung möglicher Infektionswege. Wer wurde wann von wem infiziert und hat dies wohlmöglich wo an wen weitergegeben? Corona-Apps zur freiwilligen Nutzung versprechen zu speichern welche Menschen (oder genauer: Telefone) – ob Bekannte oder Wildfremde – sich in einem bestimmten Zeitraum in der Nähe (des Telefons) einer Nutzerin aufgehalten haben. Sollte einer dieser Kontakte sich dann als Corona-positiv entpuppen würde die App nachträglich über ein Infektionsrisiko informieren. Das deutsche Bundeswirtschaftsministerium unterstützt die Nutzung solcher Apps. Nach dem Aufschrei um die Übergabe von 46 Millionen Handynutzerdaten an das Robert Koch Institut, soll es in Deutschland aber (noch) keine Pläne geben die Nutzung der App zur Pflicht zu machen. In Österreich steht eine solche Pflicht zur Debatte. Die E.U. erwägt eine Rückverfolgung durch Geolokalisierung von Handys. In Israel hat die Regierung nicht gezögert und gleich den Geheimdienst Shin Beth beauftragt die Bevölkerung neben der Geolokalisierung auch mit anderen Instrumenten aus der Terrorismusbekämpfung zu überwachen. Nur der Widerstand des Parlaments verhinderte die Pläne des

Verteidigungsministers, diese Überwachung durch die Zusammenarbeit mit einer für notorische Bürgerrechtsverletzungen bekannte Cyber-Spionagefirma (NSO Group) weiter zu verfeinern. Wer im Verdacht steht infiziert zu sein, wird in die Quarantäne beordert ohne Möglichkeit auf Einspruch, ganz gleich welche wirtschaftlichen oder sozialen Folgen ein Irrtum für die Betroffenen haben kann.

Lock-Down und Datenexplosion

Doch Geolokalisierung und Handyüberwachung oder die Durchsetzung des Lock-Downs anhand von Polizei-Drohnen oder Kameras mit und ohne Fähigkeit zur Gesichtserkennung sind nur die unmittelbarsten und am einfachsten zu verortenden Überwachungsmaßnahmen die der Kampf gegen das Corona-Virus stärkt. Weniger offensichtlich ist die Explosion von Daten die durch die Verstärkung bereits vor der Krise bestehender Verhaltensmuster angetrieben wird.

Da wäre zum Beispiel die Verlagerung fast des gesamten Berufs- und Soziallebens ins Internet. Wussten Anbieter von sozialen Medien, Suchmaschinen und Online-Shopping vorher sehr viel über ihre NutzerInnen, so wissen sie spätestens jetzt fast alles. Die Nutzung von Nachrichtenseiten auf Facebook hat sich unter Corona verdoppelt bis vervierfacht und der Messagingverkehr auf Facebook-Plattformen hat sich je nach Region zwischen 50% und 100% gesteigert. Gruppen-Videoanrufe auf Facebook sind um 70% gestiegen, und auch nicht-interaktive Angebote wie etwa Facebook Live steigen, weil neben Vorträgen etliche Sportkurse, DJ-Sets oder Isolations-Selbsthilfe-Angebote von Kochen bis zur Erstellung von Memes explodieren. Auch Amazons Geschäfte überschlagen sich: allein in den USA sollten mehr als 100.000 Mitarbeiterinnen eingestellt werden

um die Nachfrage bewältigen zu können.

Google veröffentlicht sogar sogenannte Mobilitätsreports auf Grundlage der Trackingdaten von Nutzerinnen von Google-Diensten und Apps, die dazu dienen sollen beispielsweise den öffentlichen Transport an die Anforderungen einer zuhause bleibenden Gesellschaft anzupassen. ZOOM, eine Plattform für Videokonferenzen, wird seit Ausbruch der Krise um 535% mehr genutzt: viele Firmen, Organisationen und sogar Regierungen nutzen sie um Präsenzversammlungen zu ersetzen. Dabei hagelt es Kritik: von der Weitergabe von Nutzungsdaten an Facebook, über fehlende Verschlüsselung und das Auftauchen ungewollter (und oft rassistischer) TeilnehmerInnen bei ZOOM-Meetings (sogenanntes „zoom-bombing“), bis hin zur Fremdnutzung von Webcams und der Übernahme ganzer Computer.

Im Lock-Down generieren wir mehr Daten; Daten, die Geld und Macht bedeuten. Wer wird von wem wann wie kontaktiert? Wofür? Wie lange? Gibt es einen Zusammenhang zwischen der Nutzungsveränderung und der Reaktivität auf Anzeigen oder politische Mitteilungen in den sozialen Medien? Welche Art Toilettenpapier bevorzugt beispielsweise der Amazonkunde der bislang nur Philosophiebücher und Pornographie bestellt hat und zu welchen Uhrzeiten sollten wir ihn per Anzeigen und Rabatten zum Kaufe einer Präsidenten-Biographie verführen?

Ähnliche Fragen können auch die Banken in Luxemburg jetzt beantworten. Nicht nur weil viele Läden geschlossen sind und Onlinekäufe Kartenzahlungen erfordern und so nachverfolgt werden können. Sondern auch weil die noch geöffneten Geschäfte in großen Teilen ebenfalls wegen sanitärer Gründe auf Kartenzahlung bestehen. So sieht dann jetzt auch das Sparkassenkonto, wer lieber beim Supermarkt gegenüber sein

Croissant kauft als beim unabhängigen Bäcker an der Ecke, was nicht nur zum gläsernen Kunden führt, sondern diesen Supermarkt bei der Kreditanfrage gegenüber dem Bäcker klar bevorteilt.

Post-COVID 19 Datendiät?

Wie viele dieser Veränderungen werden nach der Krise wieder rückgängig gemacht? Bleibt die Lautsprecherdurchsage der Polizeidrohne Alltag? Bleiben die Kameras (oder kommen sie wohlmöglich erst noch, wie in Luxemburg vorgesehen)? Verstetigt sich der Blick des Chefs ins eigene Wohnzimmer bei der Videokonferenz? Setzt sich der einfache Amazonkonsum endgültig durch, auch weil der Eckladen die Krise nicht überlebt hat? Wird der Daten-Striptease per Plastikkarte zur Pflicht? In manchen Ländern, etwa den Niederlanden, ist es schon länger mehr als schwierig bar zu zahlen. Das gefällt dem Staat, denn es macht Schwarzarbeit und Steuerhinterziehung ebenso schwieriger wie Kapitalflucht oder Schwarzmarkt. Es gefällt auch dem Chef – sofern er nicht nur Schwarzarbeiter beschäftigt – weil ihm so weder Gauner noch Angestellte aus der Kasse klauen können. Aber es schadet nicht nur der Privatsphäre.

« We must not sleepwalk into a permanent expanded surveillance state now, » warnt der stellvertretende Direktor der Technologieabteilung von Amnesty International, Rasha Abdul Rahim ebenso wie mehr als 100 weitere Bürgerrechtsgruppen. Auch weil viele nach dem 11.September oder dem 13.November als vorübergehend eingeführte Überwachungsmaßnahmen und Polizeigewalten nie wieder rückgängig gemacht wurden. Dabei liegt die Gefahr heute wie damals nicht nur im autoritären Opportunismus der Viktor Orbáns dieser Welt, sondern auch bei

der leidenschaftlichen Kollaboration weiter Teile der Bevölkerung in ihrer Selbstunterwerfung. Nach der Krise brauchen die Regierungen und wirtschaftlichen Profiteure der Krise eine Datendiät, die ihr durch eine disziplinierte Bevölkerung frei von falscher Angst oder Gemütlichkeit zu verordnen ist. Denn die Gefahr der totalen Überwachung geht nicht einfach von einem starken Staat aus, sondern von einem von jeder demokratischen Kontrolle befreiten Apparat ohne jeden Respekt für das Privatleben und andere Grundrechte, ganz gleich ob Staat oder Onlineplattform.

GT Nouvelles Technologies 14/04/2020