Zwangsdigitalisierung - Zwänge zur Nutzung digitaler Geräte

Inhaltsverzeichnis

Dr. Rainer Hammerschmidt, Vorstandsmitglied
MA Beate Baum, Wissenschaftliche Fachberatung

Vorwort

Dies ist die Mitschrift einer Sendung auf AlexTV, dem Offenen Kanal Berlin, über die Zwänge zur Nutzung digitialer Geräte, um am öffentlichen Leben teilnehmen "zu dürfen". Die Sendung läuft am Sa., 12. und Mo., 14. Dezember jeweils ab 08:00 Uhr. Das Video der Sendung ist hier und bei Youtube https://youtu.be/-C8muyZjy6o abzurufen.

Alle unsere Artikel zum Thema Zwangsdigitalisierung lassen sich mit https://www.aktion-freiheitstattangst.org/cgi-bin/searchart.pl?suche=zwangsdigit&sel=meta finden.

Über die unendlich vielen Möglichkeiten die uns Computer, Smartphone und Handy bieten, wird ständig berichtet. Über die Risiken bei der Benutzung wird aber geschwiegen. Wir haben auf unserer Webseite unter der Rubrik Zwangsdigitalisierung bereits zwei wichtige Beispiele genannt:

- der Zwang zur Steuererklärung mit dem Programm Elster
- die Speicherung und Nutzung unserer biometrischen Daten in Ausweis und Pass.

Doch das ist bei Weitem noch nicht alles.

Deshalb möchten wir uns heute in der kommenden Stunde darüber unterhalten an welchen Stellen wir gegen unseren Willen gezwungen werden digitale Geräte zu nutzen und damit unsere Daten staatlichen Stellen oder Privatunternehmen zur Verfügung zu stellen, ohne dass wir das wirklich selbst wollen.

Dafür haben wir uns heute mit Robbi, einer Roboterdame, zusammengefunden, die uns zu diesem Thema zur Verfügung stehen wird. Hallo Robbi!

R: Guten Tag ...

Vielleicht kannst du uns zuerst einmal einen Überblick verschaffen, an welchen Stellen überall die Digitalisierung in unser Leben eingreift.

Videoüberwachung

Da sind zum einen die allgegenwärtige Videoüberwachung im öffentlichen Raum, aber auch in Geschäften und Supermärkten. Diese Videoüberwachung wird auch genutzt, um durch automatische Kennzeichenerfassung auf den Straßen unser Fahrverhalten und damit unsere Bewegungsprofile aufzunehmen.

Hieß es anfangs, dass lediglich zu schnelles Fahren erfasst werden soll, so werden inzwischen durch Verknüpfung mit Fahndungs-Dateien unsere Daten mit staatlichen Datenbanken abgeglichen. Auch wenn anfangs Gerichte dieses Vorgehen als unzulässig verworfen haben, so gibt es inzwischen in vielen Bundesländern die automatische Kraftfahrzeugkennzeichen Erfassung im Regelbetrieb.

Kommen wir zurück zur normalen Videoüberwachung von Menschen. Wir alle erinnern uns an das Pilotprojekt des damaligen Innenministers de Maiziere zur angeblich intelligenten Videoüberwachung auf dem Berliner Bahnhof Südkreuz. 42.000 Menschen laufen täglich über diesen Bahnsteig. Aus ihnen sollte das angeblich intelligente System Gesuchte ausfindig machen. Das Ergebnis war ernüchternd:

Bei einer Fehlerrate von über 20% müsste in jedem Fall eines möglichen Gefährders die Polizei 600 mal am Tag mit einem Einsatzkommando zuschlagen, um hinterher festzustellen, dass sich das intelligente System glücklicherweise geirrt hat.

Damit war das Projekt am Bahnhof Südkreuz bereits die zweite große Verschleuderung von Steuergeldern. 2013 hatte das EU-Forschungsprojekt INDECT eine ähnliche Absicht ebenfalls nicht erfüllen können. Damals wurde versucht, die Daten von Videoüberwachungskameras mit den Daten aus sozialen Netzwerken zusammenzubringen und daraus auf "unnormales Verhalten" zu schließen. Das "unnormale Verhalten" zu definieren ist weder den damaligen Projektteilnehmern gelungen, noch sollte es grundsätzlich Aufgabe des Staates sein, zu bestimmen welches Verhalten Menschen an den Tag legen dürfen oder sollten.

R: Was sollte denn abnormales Verhalten und damit verdächtig sein?

Was ist in einer multikulturellen Gesellschaft "abnormal"? Wieder sollte durch die willkürliche Definition von "normalem Verhalten" Anpassungsdruck erzeugt werden, der die Entwicklung unserer demokratischen Gesellschaft gefährdet. Das EU-Forschungsprojekt INDECT wollte aus dem Erkennen von "abnormalem Verhalten" durch Videoüberwachung, Gesichtserkennung, Identifizierung der Menschen z.B. bei Facebook die Polizei unterstützen. Fehlentscheidungen und Fehlalarme wären vorprogrammiert. Und in der Folge müssen dann Unschuldige ihre "Unschuld beweisen", das ist nicht leicht.

Damit kommen wir zu einem weiteren großen Block, der uns hier beschäftigen muss. Die Qualität der Videoüberwachung ist inzwischen so groß, dass aus über 150 m Entfernung biometrische Fotos von den Gesichtern der Menschen erfasst werden können.

Biometrische Merkmale

Aber biometrische Merkmale gehören jedem Menschen allein. Bereits ihre Aufnahme und Speicherung in Ausweis und Pass ist nach unserer Ansicht eine Verletzung unsere Privatsphäre. Leider hat sowohl das Bundesverfassungsgericht als auch der Europäische Gerichtshof die Speicherung biometrischer Daten, wie das biometrische Foto und den Fingerabdruck im Pass genehmigt.

Für den in Deutschland üblichen Personalausweis war es bisher freiwillig, einen Fingerabdruck abzugeben. Diese Freiwilligkeit endet am 1. August 2021 (Nächstes Jahr: Neuen Ausweis nur gegen Fingerabdruck).

Bereits vor zwei Jahren wurde das Ausweis-Gesetz geändert. Bis dahin war es freiwillig, sich einen elektronischen Schlüssel auf dem Ausweis zu speichern. Nachdem die staatlichen Behörden 10 Jahre lang beobachtet haben, das von 80 Millionen Einwohnern sich nur vier Millionen diesen Schlüssel erzeugen ließen, wurde das Gesetz entsprechend geändert. Nun muss man den Schlüssel deaktivieren, wenn man ihn **NICHT** möchte, was viele nicht machen werden, weil es kompliziert ist oder sie seine Existenz gar nicht kennen.

Wir wollen nicht leugnen, dass es Anwendungen gäbe, die es wert wären, einen elektronischen Schlüssel auf dem Ausweis zu nutzen. Solche Anwendungen gibt es aber bisher praktisch nicht. Es ist jedoch eine Bevormundung, wenn der Staat bestimmt, dass ich einen elektronischen Schlüssel zu besitzen habe, egal ob ich ihn nutzen möchte oder nicht. Wenn ich den Ausweis verliere, muss wieder ich meine Unschuld beweisen, wenn jemand anderes diesen für irgendwelche Geschäfte (Online-Funktionen des Personalausweises gehackt) nutzt - schon wieder eine Umkehrung der Unschuldsvermutung.

Jetzt soll es künftig den Personalausweis auf dem Handy geben (Elektronischer Personalausweis auf dem Handy) und ab 2022 wird es eRezepte, also nur noch elektronische Rezepte auf dem Handy geben - das allein ist schon schlimm genug. Aber das Rezept auf dem Smartphone kann man sich auch gut in Verbindung zusammen mit dem geplanten Personalausweis auf dem Handy vorstellen:

Der Polizist sieht dann bei der Ausweiskontrolle auf dem Handy auch gleich die Rezepte über irgendwelche Psychopharmaka und packt den so Kontrollierten zumindest in seinem Kopf gleich in die passende Schublade.

Die elektronische Patientenakte

Zum Thema Freiwilligkeit passt auch gut die ePA, die elektronische Patientenakte, die mit dem PDSG im Sommer beschlossen und ab 1.1.2021 eingeführt wird. Wir haben darüber in der Engagementwoche auch hier auf dem Sender diskutiert (Elektronische Patientenakte - Top oder Flop?). Auch bei der Speicherung und Weitergabe von unseren Gesundheitsdaten in einer ePA kann es zu Missbrauch führen und wir haben keinen Überblick mehr, wer die Daten zu welchem Zweck öffnet oder gar kopiert.

Die Ärzte sehen alle Daten in der ePA, auch die von anderen, also der Zahnarzt auch die Ultraschalbilder deiner Einerstöcke.

- In Phase 1 (2021) sind die Daten für den Versicherten nur über den Arzt lesbar.
- In Phase 2 (ab 2022) können Versicherte (nur) über Smartphone/Tablet auf ihre ePA zugreifen.

Hilfskräfte dürfen (nur) unter Aufsicht auf die ePA zugreifen – das ist beim üblichen Stress in Krankenhäusern sehr unrealistisch. Und damit addiert sich die Anzahl der Menschen, die eine ePA sehen können bundesweit auf ca. 2 Millionen Menschen - natürlich immer nur diejenigen, die theoretisch etwas mit deiner Behandlung zu tun haben.

Wer eine ePA beantragt, hat seine Datenhoheit verloren. Es gibt nur alles oder nichts. Die Freiwilligkeit endet nach Anlegen der ePA. Der Begriff "technische Zugriffsfreigabe" wie er im PDSG steht, darf nicht als die Einwilligung des Versicherten angesehen werden. Das ist nicht konform zur DSGVO und gesetzlich völlig undefiniert. Zur DSGVO siehe z.B. unseren Artikel Europäische Datenschutzgrundverordnung ab heute in Kraft

Auch das Beschlagnahmeverbot von Gesundheitsdaten - Ärzte dürfen keine Auskünfte zu Patienten geben - ist in Gefahr. Das Zeugnisverweigerungsrecht gilt nur für approbierte Ärzte. Alle anderen, wie z.B. die sogenannten Hilfskräfte könnten sich nicht weigern, Daten herauszugeben, wenn sie darauf Zugriff haben sollten.

Die ePA soll freiwillig sein, aber der Arzt wird dafür bezahlt, wenn er sie für uns anlegt und ob man in gesundheitlich kritischen Situationen in der Lage ist, solche Forderungen des Arztes abzulehnen, ist sehr fraglich. Ist die ePA erst einmal angelegt, wird es schwierig, sie wieder zu löschen. Jede/r sollte sich bald darüber informieren - denn 2021 ist bald.

Zurück zum Personalausweis

Über die darüber hinausgehenden Probleme bei der Ausweisbeantragung und den damit zusammenhängenden Vorgängen haben wir in einem Artikel auf unserer Webseite unter der Kategorie Zwangsdigitalisierung ausführlich berichtet. (Die Odyssee des biometrischen Abbilds)

Dort ist auch beschrieben, wie sämtliche Steuerpflichtige zur Nutzung von Elster, dem Programm für alle Steuererklärungen gezwungen wird. Das gilt sogar für Solo-Selbstständige, Künstler usw., die ihre mageren Einnahmen auch auf dem berühmten Bierdeckel erklären könnten. (Die dunklen Seiten der digitalen Agenda)

Bewegungsdaten

Ein drittes großes Kapitel sind unsere Bewegungsdaten. Allein durch den Besitz eines Smartphones oder Handys sind unsere Bewegungen durch die Landschaft nachzuvollziehen. Die Provider speichern die Position unseres Gerätes relativ zu ihren Antennen-Standorten. Wenn ihnen diese Angaben zu ungenau sind (ca 30 bis 50 m) haben sie die Möglichkeit die GPS Daten unseres Handys zu nutzen, wenn wir die GPS Standorterfassung nicht ausgeschaltet haben. Damit sind wir auf ca 10 Meter genau zu erkennen. Noch genauer wird unser Standort erfasst, wenn wir unser Gerät mit irgendwelchen Apps ausgestattet haben, die von Supermärkten und Geschäften angeboten werden. Dann lässt sich über Bluetooth unsere Position vor einem Supermarktregal auf einen Meter bestimmen.

R: Was hat das noch mit Zwangsdigitalisierung zu tun?

Du hast recht Robbie, wenn wir uns solche Apps installieren, dann sind wir selber schuld. Gerade in den letzten Monaten wurde uns die Corona App schmackhaft gemacht (Corona-App zum Letzten). Damit sollten Kontakte zu eventuell positiv Infizierten nachverfolgbar gemacht werden. Positiv an der Corona App ist immerhin, dass diese Daten in einem festgelegten Zeitraum wieder gelöscht werden. Das gilt für die Supermarkt Apps sicher nicht.

Genauso fragwürdig ist eine Corona Nachverfolgung über QR Codes in Restaurants. Die Anbieter dieser Apps sammeln persönliche Daten von uns und vergessen scheinbar auch öfter das Löschen unserer Daten ("Denken first, digital second" vor Gebrauch von Corona-Listen).

Gefährdung unserer Kommunikation

Ein weiteres Thema ist die Gefährdung unserer Kommunikation. Unsere Privatsphäre hängt wesentlich davon ab, dass wir davon ausgehen können, dass unsere Gespräche Briefe und E-Mails nicht von Fremden abgehört oder gelesen werden. Die europäische Datenschutzgrundverordnung legt feste Regeln vor, die einzuhalten sind. Damit sollte es möglich sein, das eigene Recht an seiner Kommunikation durchzusetzen.

Leider hat der Staat im Rahmen der Anti-Terror-Gesetzgebung nach dem Jahr 2001 viele unserer Grundrechte angeknabbert (Überwachungsgesetze). So wurde 2007 eine Vorratsdatenspeicherung unserer Telefon und Internetverbindungen zum Gesetz und im Jahr 2008

durch die Novelle des BKA Gesetzes ein Lauschangriff auf private Wohnungen erlaubt. Im März 2009 wurde mit dem "Ersten Gesetz zur Änderung des Artikel 10-Gesetzes" sogar die Überwachung Minderjähriger und die Ortung von Handys durch den Verfassungsschutz, also einen Geheimdienst erlaubt.

Während die Vorratsdatenspeicherung sofort als anlasslose Überwachung aller Menschen für illegal erklärt wurde, galt das BKA-Gesetz für weitere acht Jahre, bis auch seine Regelungen in Teilen vom Bundesverfassungsgericht für unzulässig befunden wurden. Erst vor wenigen Wochen: Die Anti-Terror-Gesetze wurden entfristet - damit werden diese Einschränkungen unserer Grundrechte auch noch gelten, wenn es keinen "Terroristen" auf der Welt mehr gibt. Wer glaubt, dass sich Anti-Terror-Gesetze gegen Terroristen richten, glaubt auch an den Weihnachtsmann (Terroristen sind nur Beifang).

R: Ähh, ... noch mal ... was hat das noch mit Zwangsdigitalisierung zu tun?

Oh Robbie, du passt ja wirklich auf! Natürlich können wir sagen, wir verzichten freiwillig auf sämtliche Kommunikation mit anderen Menschen und verkriechen uns in einer Holzhütte im Wald. Dann wird und kann uns niemand abhören. Wollen wir jedoch mit anderen Menschen kommunizieren, so ist es inzwischen natürlich, dafür auch elektronische Mittel zu verwenden. Wir sind schließlich keine Maschinenstürmer. Wir möchten aber diese Geräte dann auch unbeobachtet nutzen können.

Dazu gehört es, dass wir unsere Daten auch auf dem eigenen Rechner, aber vor allem bei der Kommunikation verschlüsselt versenden. Dieser Wunsch hat zuerst einmal nichts mit Misstrauen gegenüber dem Staat zu tun, denn es gibt auch genügend Kriminelle die mittels Hacks versuchen an unsere Daten zu kommen. Deshalb ist eine verschlüsselte Kommunikation ein Grundpfeiler für unser Zusammenleben.

Dagegen hat uns jedoch der Staat erst im Sommer mit dem Zwang zur Passwort-Herausgabe durch die Internetprovider einen großen Stolperstein in den Weg gelegt. (Bundesregierung beschließt Pflicht zur Passwortherausgabe)

Nach der üblichen Salamitaktik wird nun gerade beabsichtigt ein grundsätzliches Verbot einer Ende-zu-Ende-Verschlüsselung durchzusetzen. Dazu hat die EU ein Papier veröffentlicht in dem sie die Provider von Messenger Diensten dazu zwingen will einen Generalschlüssel anzulegen, mit dem jede Ende-zu-Ende-Verschlüsselung unabhängig von der Bereitschaft der Kommunikationspartner lesbar zu machen ist (Angriff auf die Ende-zu-Ende-Verschlüsselung). Damit ist der typische "men in the middle" Angriff, den diese Art der Verschlüsselung gerade verhindern will, wieder möglich.

So ist es nur eine Frage der Zeit bis diese Generalschlüssel von kleinen und großen Kriminellen zum Kauf angeboten werden. Diesen Verlust an Sicherheit können sich weder die staatlichen Stellen in ihrer Kommunikation erlauben und erst recht nicht Banken, Online Portale für Reisebuchungen oder der gesamte Online Handel.

Überwachungsgesamtrechnung

Die Forderung **"macht alles unverschlüsselt" aber macht es digital** - das ist sogar der Gipfel von Zwangsdigitalisierung. Das BVerfG hat in seinem Urteil gegen die Vorratsdatenspeicherung im März 2010 den Begriff der Überwachungsgesamtrechnung definiert (Wie weiter nach dem Karlsruher Urteil zur Vorratsdatenspeicherung?). Mit diesem Begriff will oder wollte das Gericht künftig nicht nur jede einzelne neue Überwachungs-Maßnahme prüfen sondern ob durch die Summe der Maßnahmen nicht ein grundrechtlich erträgliches Maß an Überwachung für den Einzelnen überschritten wird. Auch wenn die einzelne Maßnahme gesetzlich legal ist, so kann durch die Summe der Maßnahmen ein grundrechtlswidriger Zwang auf den Menschen entstehen (Diskussion über den künftigen Datenschutz).

R: Na gut, na gut, ... ich sehe ein, dass du dich bei der Benutzung von digitalen Geräten oder in der Kommunikation mit uns Maschinen unwohl fühlst. ...

Das liegt aber nicht an uns. Wir Maschinen haben feste Gesetze an die wir uns halten müssen.

Meinst du etwa die Robotergesetze von Isaac Asimov?

R: Ja, denn Isaac Asimov formuliert 1942 die folgenden Gesetze

> *Ein Roboter darf kein menschliches Wesen (wissentlich) verletzen oder durch Untätigkeit (wissentlich) zulassen, dass einem menschlichen Wesen Schaden zugefügt wird.*
>
> *Ein Roboter muss den ihm von einem Menschen gegebenen Befehlen gehorchen – es sei denn, ein solcher Befehl würde mit Regel eins kollidieren.*
>
> *Ein Roboter muss seine Existenz beschützen, solange dieser Schutz nicht mit Regel eins oder zwei kollidiert.*

Automatisierung des Krieges

Aber Roboter im militärischen Bereich mit automatischen Waffensystemen, Smart Bombs, Drohnen, Kampfroboter, Drohnenschwärme (Erprobung von Angriffen mit Drohnenschwärmen und Drohnenschwärme über der Ostsee), die Flugzeuge zum Absturz bringen sollen, die folgen diesen Gesetzen nicht. Und gerade das Thema der bewaffneten Drohnen ist eines, was uns seit einigen Jahren schwer beschäftigt. Wir arbeiten gegen solche Mordwerkzeuge mit über 150 Organisationen in der Drohnen-Kampagne zusammen.

Überwachungsdrohnen mit hochauflösenden Kameras können Gesichter noch in 160m biometrisch erkennen. Kampfdrohnen können bis zu 4 Raketen und 2 Bomben tragen, die am Boden einen "lethalen" Radius von 30-60m besitzen. Drohnen bieten für den Verwender den "Vorteil", dass er über eine langen Zeitraum (bei Flugzeiten über 12h) von Ferne das Geschehen beobachten und beeinflussen kann ohne bemerkt zu werden. Dies führt zu Angst und Verhaltensänderungen bei den Betroffenen und senkt die Schwelle bei Konflikten. Kampfdrohnen verletzen darüber hinaus die Menschenrechte und auch das (Kriegs-) Völkerrecht.

Wir sehen in bewaffneten Drohnen, die über den Menschen kreisen, und aus für den Einzelnen unbekannten Gründen plötzlich Raketen oder Bomben abwerfen, eine schwere Menschenrechtsverletzung. Der über tausende Kilometer entfernte Pilot sieht irgend etwas auf seinem Bildschirm und bekommt den Befehl dieses Ziel zu bombardieren. Oft ist einfach die Begründung, dass es sich um einen feindlichen Kämpfer handelt der ausgeschaltet werden müsse. Vielleicht trifft es dann aber auch nur einen Freund oder Familienangehörigen, der in den Besitz des Handys gelangt ist, auf dessen Ortung der Angriffsbefehl beruht.

Damit wird jeder rechtsstaatliche Grundsatz ad absurdum geführt. Der Pilot ist gleichzeitig Ermittler, Richter und schließlich Henker.

Es gibt in diesem Prozess keine Möglichkeit Gegenbeweise oder Widerspruch anzuführen. Darüber hinaus sind die Opfer - und es sind inzwischen über 10.000 Menschen, die von Drohnen weltweit getötet wurden - bis zum Moment ihrer Hinrichtung nicht darüber informiert, dass Ihnen irgendetwas vorgeworfen wird. Auch Kinder werden, ebenso wie Frauen und andere Zivilisten,

Opfer dieser unmenschlichen Kriegsstrategie. Es sind bereits über 500 Kinder davon ca. 136 namentlich bekannt und mehrere Tausend Frauen.

Genau zu diesem Thema der Ermordung von Kindern macht unser Verein seit fast zwei Jahren Ausstellungen in Deutschland. Unter dem Link drohnen-quilts.de stellen wir Patchworkdecken im Angedenken an diese Kinder aus. Auf der Webseite kann man sich darüber informieren und die Ausstellung gegen eine geringe Gebühr ausleihen. Auch die Ausstellung der Drohnen-Quilts war bereits Thema einer Sendung auf diesem Kanal.(Auch bei Youtube https://youtu.be/EDvUBCjH6f0)

Das Drohnen-Thema beschäftigt uns auch, weil die Drohnen und auch andere fast automatische Waffen zu einer Bedrohung für die Menschheit werden können. Ihre Automatisierung schreitet voran und mit dem Argument der künstlichen Intelligenz solcher Maschinen werden ihnen zunehmend mehr Entscheidungsmöglichkeiten gegeben (Keine Drohnen - Slaughterbots - Einstieg in "automatisierte" Kriege).

Dem Zwang unter ihnen zu leben, können sich die Menschen in Pakistan, Afghanistan, Jemen und Mali nicht entziehen. Sie müssen ständig mit der Angst leben getötet zu werden. Wir bei uns regen uns höchstens mal über Überwachungsdrohnen der Polizei oder Tiefflieger der Bundeswehr auf, wie beim G7 Gipfel in Heiligendamm.

Wir wollen keine Kriege und erst recht keine automatischen Kriege.
Doch zurück zu unseren Robotergesetzen.

Die Robotergesetze hat sich der liebe Herr Asiimov 1942 sicher gut überlegt, aber schauen wir uns die automatischen oder teilautomatischen Waffensysteme an, die inzwischen überall in Betrieb sind. Diese Folgen, wie wir gerade erläutert haben, deinen Gesetzen nicht.

R: Du bist unfair ... denn wir sind in unserem Handeln nicht autonom ... wir folgen Programmen und viele Programmierer arbeiten im Auftrag der Militärs.

Genau das ist das Problem. Maschinen folgen Programmen und können bestenfalls mit der sogenannten künstlichen Intelligenz ihre Programme erweitern. die Absichten und Ziele, die die Auftraggeber die Programmierer gesetzt haben, könnt ihr jedoch nicht umgehen. Deshalb ist jeder Zwang zur Nutzung von fremden Programmen und Geräten, über deren wirkliche Absichten und Ziele man selbst noch nicht mal etwas weiß, eine Einschränkung unserer Freiheit und in jedem Falle unserer Privatsphäre.

EU Identität

Ich will da noch gar nicht von der EU Identität sprechen, die Frau von der Leyen für alle europäischen Bürger durchsetzen möchte. Vorher müssen in den einzelnen Ländern ja noch die nationalen

Personenkennzeichen eingerichtet werden. Doch das ist in Deutschland bereits im Gange. ("Personenkennziffer" wird zur "EU-Identität")

Aus der Steuer-ID, die bei ihrer Einführung vor 20 Jahren "nur" ein Schlüssel für das Finanzamt werden sollte (Steuer-ID wird zur Personenkennzahl), soll das vom Bundesverfassungsgericht 1969 verbotene Personenkennzeichen werden, mit dem alle Behörden in Deutschland Zugriff auf die persönlichen Daten eines Menschen bekommen können. Bei uns in Deutschland läuft dies unter dem Begriff "Register-Modernisierung". (Nun also doch die totale Personenkennziffer)

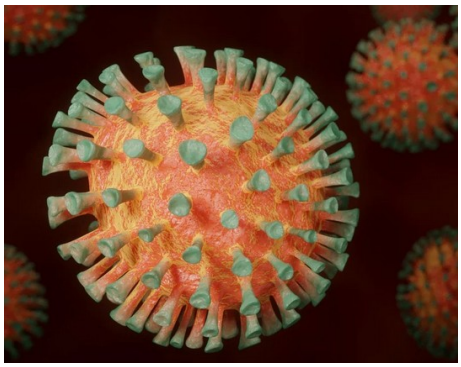
Impfzeugnis und digitale Einreiseanmeldung

Ein Vorgeschmack darauf droht uns mit der im kommenden Jahr bevorstehenden Impfung gegen Corona.

R: Was hat denn das schon wieder mit Zwangsdigitalisierung zu tun?

Nun ja, man muss niemanden mehr zum Impfen verpflichten. Ohne Impfnachweis kann man einfach kein Bahn- oder Flugticket buchen und auch kein Hotel (Australische Fluglinie Qantas plant Impfpflicht für Passagiere). Am Ende bleiben Apotheke, Arzt und Lebensmittelladen als die einzigen Orte, die man besuchen darf. Überall sonst wird der Zugang verwehrt, so wie es heute einem schon in China ergeht ohne eine entsprechende App oder einen Negativtest. Und wir brauchen nicht mit dem Finger auf China zeigen, auch die australische Fluggesellschaft Quantas hat kürzlich ihre Beförderungsbedingungen geändert. Man muss nun zum Flug den Nachweis einer Impfung oder einen Negativ-Test mitbringen.

Nicht der Zwang, das **Ausgrenzen ist das Mittel der Zwangsdigitalisierung**, hier deutlich gemacht am Beispiel der bevorstehenden Impfung.



R: Okay, ich glaube dir ja, dass du die Einschränkungen deiner Bewegungsfreiheit als Zwang empfindest. oh, ich weiß ja gar nicht was glauben ist ...

Aber du musst doch zugeben, dass die Digitalisierung euch eine Menge Zeit erspart, die ihr für sinnvolle Tätigkeiten verwenden könnt. Sieh mal als Beispiel die Digitalisierung bei der Einreise aus Risikogebieten z.B. mit dem Flugzeug.

Bundesinnenminister Horst Seehofer hatte dazu in der Mitte Oktober gesagt: "Mit der digitalen Einreiseanmeldung beenden wir endlich die Zettelwirtschaft im Reiseverkehr". Nun müsst ihr nur noch diese Einreise-Anmeldung auf eurem Smartphone eingeben und es muss kein Zettel ausgefüllt und den Stewardessen zum mühsamen Einscannen übergeben werden.

Sorry, Robbie, das ist leider kein gutes Beispiel. Den Zettel kann ich während des ganzen Fluges ausfüllen, wo das Handy nicht funktioniert. Nach der Landung beim Aussteigen ist sicher nicht die Zeit dafür, ich muss es vor dem Einsteigen in den Flieger machen.
Außerdem: ich habe gar kein Handy, was mache ich dann? In Singapur muss ich in solchen Fällen einen aktiven RFID-Chip mit mir tragen, der mich jederzeit identifizieren soll.

Viel schlimmer ist jedoch was auch dieses Beispiel wieder einmal zeigt, dass wir Schritt für Schritt zur Nutzung solcher Techniken angelernt werden. Wer sagt mir denn, dass die Daten meiner Anmeldung nur an die Gesundheitsämter weitergegeben werden und nicht Geheimdienste oder Meldebehörden mitlauschen - besonders dann, wenn es künftig keine Ende-zu-Ende-Verschlüsselung mehr geben sollte.

Die Enthüllungen von Edward Snowden

Auch die verbreitete Meinung, dass sich unsere Daten in dem riesigen Heuhaufen der Datensammler sowie so nicht mehr finden lassen, ist leider falsch. Unser Ehrenmitglied, der Whistleblower Edward Snowden, hat 2013 aufgedeckt, dass sich mit dem Programm XkeyScore von den Geheimdiensten in diesen Daten suchen lässt und beliebige Zusammenhänge auffindbar sind.

R: Kannst du uns etwas mehr über Edward Snowden erzählen? Ich habe gehört, dass er sogar bei euch im Verein ist.

Ja das ist eine interessante Geschichte. Edward Snowden hat im Juni 2013 in der Öffentlichkeit über seine Arbeit bei den US Geheimdiensten berichtet. Sofort wurde er zum meistgesuchten Menschen auf der Welt. Während seines Fluges von Honkong nach Südamerika wurde bei der Zwischenlandung in Moskau sein Pass durch die US-Behörden für ungültig erklärt, so dass es ihm unmöglich war, seine Reise weiter fortzusetzen.

Seitdem lebt er gegen seinen Willen im Exil. Nach jährlichen Verlängerungen hat ihm die russische Regierung inzwischen seinen dauerhaften Aufenthalt in Russland erlaubt. In dem Jahr nach seinen Veröffentlichungen haben überall auf der Welt Menschen gegen die totale Überwachung durch die US-Geheimdienste demonstriert - auch wir. Mit unserem Transparent wurden wir damals auch Teil des "Snowden" Films über ihn.

Da wir seine Veröffentlichung für unsere Themen als absolut wichtig betrachten, haben wir auf unserer Jahresmitgliederversammlung im Juni 2014 beschlossen, ihn zu unserem Ehrenmitglied zu ernennen. Er hat uns über seinen Anwalt mitteilen lassen, dass er dies gerne annimmt. Seine Enthüllungen sind so wichtig, dass wir die Kernpunkte davon in unsere Publikation "Überwachung durch den Staat" aufgeschrieben haben. Auch dazu lief vor einigen Wochen eine Sendung auf diesem Kanal.

Kurz zusammengefasst kann man sagen, dass die US-Geheimdienste zusammen mit ihren Verbündeten, den sogenannten five eyes (Großbritannien, Kanada, Australien, Neuseeland) die gesamte Kommunikation auf der Welt, egal ob es Telefongespräche oder die Kommunikation über Computer sind, abhören und sogar speichern können. Erst vor wenigen Jahren wurde ein riesiges Speicherzentrum im US-Bundesstaat Utah fertiggestellt, das während der Regierungszeit von Präsident Obama geplant wurde (NSA Sumpf trocken legen und Stromschwankungen in Überwachungszentrum).

R: Ja, ... ich habe auch einen großen Speicher aber was soll man mit diesen vielen Daten anfangen?

Richtig, Daten sammeln allein hilft wenig. Das haben wir bei unseren Geheimdiensten auf der Suche nach Terroristen oft genug bemerkt. Und hier schließt sich der Kreis zu dem Programm xkeyscore. (XKeyscore ist Super-Google und Verfassungsschutz und XKeyscore? und Der Yahoo XKeyScore-Selector)

False Positives

Damit ist es möglich in dieser unglaublichen Fülle von Daten sinnvoll zu suchen. Das heißt leider nicht, dass dadurch die Arbeit der Geheimdienste sinnvoll wird. Sie können viel finden, aber ob es sich um sinnvolle und in dem Zusammenhang richtige Ergebnisse handelt, müssen wieder Menschen entscheiden und die machen, wie du weißt Fehler.

Und solche Fehler führen wieder dazu, dass Unschuldige ihre Unschuld beweisen müssen, denn die Behörden setzen voraus, dass sie im Recht sind. Solche falschen Treffen, auch False Positives genannten Fehler in den Suchergebnissen haben dann oft keine Gelegenheit ihren Kopf aus der sich schließenden Schlinge zu ziehen.

Das wohl krasseste Beispiel für so einen Fall zeigt die "Operation Ore", bei der europäische Polizeibehörden mit dem FBI zusammen arbeiteten. Über 5000 Personen wurden allein in Großbritannien im Rahmen dieser Aktion wegen des Besitzes von Kinderpornografie festgenommen. Viele von ihnen wurden verurteilt, 33 von ihnen begingen Selbstmord. Erst später stellte sich im Laufe weiterer Ermittlungen heraus, dass ihre Kreditkartennummern von den wirklichen Kriminellen missbraucht wurden. Ihre einzige Gemeinsamkeit war, dass sie in einem normalen Onlineshop ihre Kreditkartennummern verwendet hatten. Für mindestens 5000 Menschen war dadurch ihr bisheriges Leben zerstört und meist auch das ihrer Familie.

Du siehst also, auch die beste angeblich "künstliche Intelligenz" bringt nichts.

R: Danke für deine Ausführungen, ich habe einiges gelernt - hoffentlich löscht niemand meinen Speicher.

Es war auch nett mit dir zu reden, aber auch dabei kann ich mir nicht sicher sein, dass niemand unsere Kommunikation mitgehört hat oder dass du sie vielleicht sogar für Google & Co oder irgendwelche Dienste gespeichert hast.

R: Ich finde es inzwischen auch seltsam, dass Menschen sich eine Alexa oder ähnliches ins Wohn- oder gar Schlafzimmer stellen und ihre Wünsche oder Fragen mit Amazon, Apple, Google & Co teilen. (Digitalen Assistenten wie Alexa oder Siri vertrauen? und Menschen hören bei Sprachassistenten mit und Innenminister wollen Alexa als Beweismittel zulassen und "Smart Relax" mit dem ständigen Zuhörer)

Aber ich verspreche dir, dass außer den Zuschauern am Fernsehschirm niemand unser Gespräch belauscht hat.

Das beruhigt mich sehr. Robbi, ich danke dir für dein Interesse und hoffe, dass wir auch die Zuschauer nicht gelangweilt haben. **Aktion Freiheit statt Angst** beschäftigt sich mit noch vielen weiteren Themen zum Schutz unserer Grundrechte. Schauen Sie bei Interesse doch mal bei uns auf die Webseite a-fsa.de

R: Auf Wiedersehen