Freitag, 02. August 2024, 13:00 Uhr
~26 Minuten Lesezeit

Big Brothers Lebenslauf

Vom Volkszählungsurteil über das PRISM-Programm des NSA zur künstlichen Intelligenz — durch diese Entwicklungen zieht sich ein roter Faden hindurch.

von Das Gewerkschaftsforum
Foto: Maxx-Studio/Shutterstock.com

Als der Bundestag 1983 die Durchführung der Volkszählung beschlossen hatte, entbrannte in der

Bundesrepublik Deutschland zum ersten Mal der Kampf um den Datenschutz, und es formierte sich der Widerstand gegen den „gläsernen Bürger“. Erstmals wurden auch Computer eingesetzt, um die persönlichen Umfragedaten zu speichern und mit den Melderegistern abzugleichen. Es entstand eine große Boykottbewegung, die am Ende sogar das Bundesverfassungsgericht bemühte, das mit seinem neu formulierten „Recht auf informationelle Selbstbestimmung“ jedem einzelnen Menschen das Recht zugestand, selbst darüber entscheiden zu dürfen, wer Daten von ihm erhebt, speichert, verwendet und weitergibt. Seither haben sich die Dinge verändert — und überwiegend zum Schlechteren. Eine kurze Geschichte der Massenüberwachung in Deutschland.

30 Jahre später enthüllte Edward Snowden die Internetüberwachungsprogramme PRISM und Upstream Collection, mit denen Geheimdienste und Konzerne weltweit massenhaft Kommunikationsdaten abgriffen, sammelten, auswerteten und weitergaben.

Dann wurde das ID2020-Projekt aufgelegt, und dazu hatte der Bundestag im Januar 2021 das sogenannte Registermodernisierungsgesetz beschlossen. Mit dem Gesetz wird der Onlinezugang relevanter Daten der Verwaltungsregister durch die persönliche Steueridentifikationsnummer verankert. Diese Nummer ist eine weltweit einheitlich lesbare, biometrisch eindeutig unterlegte Identifikationsnummer, die für die globale Bevölkerungsüberwachung über Ländergrenzen hinweg von zentraler Bedeutung ist. Mit der zentralen Nummer sind die

Voraussetzungen für die automatisierte Schleppnetzüberwachung von Milliarden Menschen durch die amerikanische National Security Agency (NSA, deutsch: Nationale Sicherheitsbehörde, der größte Auslandsgeheimdienst der USA), Microsoft, Facebook und andere Organisationen und Konzernen geschaffen.

Nur mit der Identifikationsnummer können sie die Informationen, die es in vielen tausend verschiedenen Datenbanken über all die Menschen gibt, verlässlich zusammenführen. Als weitere Schritte in diese „schöne neue Welt“ wurde der digitale Impfpass namens „CovPass“ europaweit gestartet, der Taschenspion Smartphone weiter entwickelt und mit künstlicher Intelligenz verfeinert.

Nach dem Ende der bipolaren Welt im Jahr 1989 und dem Abhandenkommen von Gegnern und Grenzen wurden unter der Regie der USA auch alle Einschränkungen im Verkehr von Gütern und Kapital aufgehoben. Dies zu einem Zeitpunkt, an dem sich fast die Hälfte der Staaten der Welt erstmalig dem ausländischen Kapital öffnete, das dann auf ein riesiges Angebot an billigen und qualifizierten Arbeitskräften, ein enormes Vorkommen an Naturschätzen und einen noch nicht dagewesenen großen Absatzmarkt traf. Das kam vor allem dem Kapital der USA, als neue unipolare Macht, zugute. Gleichzeitig bekam die Verbreitung des Neoliberalismus einen Schub, bei dem das Kapital von Einschränkungen befreit und der Arbeitsschutz, die öffentliche Daseinsvorsorge und der Sozialstaat nachhaltig abgebaut wurden.

> ***Vor dem Hintergrund des globalen Kapitalismus mit seinen sozialen Desintegrationsprozessen wurden parallel dazu internationale Strategien entwickelt, um zu gewährleisten, dass die Machtverhältnisse auch stabil bleiben. Dazu wurde vor allem die Polizei militarisiert, das Militär im Inneren einsetzbar gemacht, und es gibt mittlerweile kaum ein gesellschaftliches Problem mehr, auf das seitens der Politik nicht mit der Verschärfung des Strafrechts reagiert wird.***

Gleichzeitig wurde ein Überwachungssystem errichtet, in dem die Bevölkerung total überwacht, von jeder Person massenhaft Informationen gesammelt, sie erpressbar gemacht und ein immenses Meinungs- und Unterhaltungsangebot mit dem Internet aufgebaut werden, damit die Massen beschwichtigt und abgelenkt sind.

Volkszählungsurteil 1983

Einige Leser, vor allem die älteren, werden sich erinnern: Auf dem Titelbild sind die Codezahlen der Fragebögen zur Volkszählung 1987 zu sehen. Diese Zahlenfolge war auf jeder Seite des Fragebogens aufgedruckt und sollte die Anonymität der Volkszählung gewährleisten. Doch an dem Schutz der Daten der einzelnen Person wurden schnell Zweifel laut. Im Gegensatz zur heutigen Zeit, in der fast jeder alles von sich bereitwillig ins Internet stellt, gaben damals 40 Prozent der Bevölkerung an, sich um die Datensicherheit bei der Volkszählung Sorgen zu machen.

Im Jahr 1983 hatten viele Menschen bereits am Widerstand gegen Großprojekte wie der Startbahn West/Frankfurter Flughafen und dem Ausbau des Rhein-Main-Donau-Kanals teilgenommen, gegen die Atompolitik protestiert oder gegen die Stationierung der Mittelstreckenraketen demonstriert. So war es nicht ungewöhnlich, dass innerhalb ein paar Wochen nach Bekanntgabe der Fragebögen sich bereits einige hundert Bürgerinitiativen zum Boykott der Volkszählung gegründet hatten. Der Hauptknackpunkt lag den Kritikern zufolge in der Absicht, die in der Volkszählung erhobenen Daten für eine Korrektur der Meldedaten zu verwenden.

Sofort wurde auch gerichtlich gegen das Vorhaben vorgegangen. Die Kläger beanstandeten, dass die Ausführlichkeit der Fragen bei ihrer Beantwortung Rückschlüsse auf die Identität der Befragten

zulasse und damit den Datenschutz nicht gewährleisten würde. Es bestand die Befürchtung, dass ein weiterer Schritt hin zum „Gläsernen Bürger“ und in Richtung Überwachungsstaat getan würde.

> ***Das „Volkszählungsurteil“ von Mitte Dezember 1983 ist im Rückblick mittlerweile historisch bedeutsam geworden.***

Nach dem Bundesverfassungsgericht verstieß die Volkszählung, so wie sie organisiert werden sollte, gegen das Grundrecht auf informationelle Selbstbestimmung, das sich aus der Menschenwürde und dem Recht auf freie Entfaltung der Persönlichkeit nach dem Grundgesetz ableitet. Die Zählung, die für den 27. April 1983 geplant war, wurde dann gemäß dem Urteil untersagt. Nachdem die Befragung neu konzipiert wurde, die personenbezogenen Angaben von den Bögen getrennt wurden und die Anonymität besser gewährleistet sein sollte, gab es einen neuen Stichtag für die Befragung, den 25. Mai 1987.

Die groß angelegte Imagekampagne „Zehn Minuten, die allen helfen“ zeigte aber wenig Erfolg. Inzwischen standen für viele Menschen die Themen wie der begonnene Rückbau des Sozialstaates, die Einforderung von mehr Eigeninitiative und Eigenleistung – „privat vor Staat“ –, der Abbau demokratischer Rechte, der maschinenlesbare Ausweis, ein zentrales Verkehrsinformationssystem, Personenkennzeichen im Sozialversicherungsausweis, Personalinfosysteme in der Privatwirtschaft/Überwachung der Beschäftigten und die ausufernde Datensammlungswut bei Polizei und Geheimdiensten im Vordergrund. Den Kritikern der Volkszählung ging es vor allem auch um mehr Mitbestimmung sowie den Kampf gegen die Beschränkung von Bürgerrechten und gegen eine Entwicklung in Richtung technokratischen Staat. Es bildeten sich weitere Bürgerinitiativen und Boykottgruppen, die auch durch öffentliche Aktionen immer

mehr Unterstützung erlangten.

Trotz umfangreicher Repressionen und der Androhung von Bußgeldern bis zu 10.000 DM wuchs die Zahl der Volkszählungsboykott-Initiativen von 350 Mitte 1986 auf über 1.100 im April 1987 an. Auch die Beschlagnahme von Flugblättern, die Überwachung der Aktivisten durch den Verfassungsschutz, die über 100 Hausdurchsuchungen bei Volkszählungsgegnern wegen angeblichen „Aufrufs zur Sachbeschädigung“ – gemeint war die Sachbeschädigung durch das Abschneiden der Kontrollnummer auf den Volkszählungsbögen – schreckten kaum ab. Die persönlichen Daten von über 900 Volkszählungsgegnern wanderten in die „APIS“-Dateien des Bundeskriminalamts; allein in Baden-Württemberg wurden 653 Personen im „polizeilichen Meldedienst“ gespeichert. Die überwiegende Mehrzahl der Strafverfahren wurde zwar 1988 eingestellt, aber die Reaktion des Staates hatte insgesamt die Argumente der Volkszählungsgegner geradezu bestärkt und er sich selbst vorgeführt.

Dann war es so weit: Über eine Million Menschen folgten damals dem Boykottaufruf. Viele andere machten bewusst falsche Angaben, sodass bis heute die statistischen Ergebnisse der letzten großen Volkszählung höchst umstritten sind. Während die statistischen Ämter der Befragung eine gute Qualität bescheinigten, sprachen unabhängige Informatiker von einem „Daten-Gau“.

> ***Was die Volksbefragungsboykottbewegung erreichte, war aber, dass die Sensibilität der Menschen in den 1980er-Jahren für das Aushorchen der Bürger durch den Staat größer geworden und die Notwendigkeit der gesetzlichen Regelung des Datengebrauchs erforderlich war sowie ein noch immer aktuelles Urteil des Bundesverfassungsgerichts (BVG) erstritten wurde.***

Diese Bewegung wird auch gern als ein weiteres Beispiel dafür

herangezogen, dass eine Bewegung, die sich ursprünglich gegen einen konkreten Missstand gründet, auch eine Erweiterung von Grund- und Freiheitsrechten erstreiten kann. Erstreiten durch das Engagement des Einzelnen, im Verbund mit dem gemeinsam geschaffenen gesellschaftlichen Druck von unten der vielen. Allerdings konnte damals niemand erahnen, wie es mit dem Datenverkehr in der digitalisierten Welt 30 Jahre später im Jahr 2013 aussehen würde.

Die Enthüllungen von Eward Snowden – Internetüberwachungsprogramme PRISM und Upstream Collection der US-Geheimdienste

Mit der Einführung des Überwachungsprogramms PRISM konnte die NSA Daten in einer unglaublich hohen Anzahl sammeln. Sie generiert sie aus E-Mails, Fotos, Video- und Audiochats, Webbrowsing-Inhalten, Anfragen an Suchmaschinen und allen Daten, die in den Clouds gespeichert sind. Dazu kommen noch die routinemäßig gelieferten Daten von Google, PalTalk, YouTube, Microsoft, Yahoo, Facebook, Skype, AOL und Apple.

PRISM ist nicht allein eine Software oder ein Datenzentrum, es besteht aus mehreren Komponenten. Die wichtigste davon ist eine Ausleitungsschnittstelle, über die Daten von den Firmen an die Dienste übergeben werden. Dabei funktioniert die Schnittstelle wie ein elektronischer Briefträger.

Das Programm Upstream Collection ermöglicht die permanente Datensammlung unmittelbar aus der Internetinfrastruktur des privaten Sektors, hervorgeholt aus den Switches und Routern, die den Internetverkehr aus den am Meeresboden verlegten Kabeln

oder über die Satelliten abwickeln. Das Programm ist mit seinen Werkzeugen in der Lage, ganz nah an der überwachten Person und seiner Privatsphäre zu operieren. Jedes Mal, wenn die Person eine Website besucht, einen Webbrowser öffnet, die URL eingibt, geht die Anfrage auf Serversuche. Bevor die Anfrage den entsprechenden Server erreicht, muss sie aber die mächtigste Waffe der NSA, die sogenannte TURBULENCE, durchlaufen. Bei dem Durchlauf muss die Anfrage einige „schwarze Server“ überwinden, die übereinander gestapelt kaum größer als ein Quadratmeter sind und in allen verbündeten Staaten in besonderen Räumen der Telekommunikationsunternehmen aufgestellt sind, ebenso auf US-Militärstützpunkten und in US-Botschaften rund um den Globus.

Die TURBULENCE enthält zwei wichtige Werkzeuge:

1. TURMOIL betreibt die „passive Datensammlung“, indem es Kopien der durchlaufenden Daten sammelt, und mit seiner Wächterfunktion untersucht es die Metadaten, ob sie etwas enthalten, was „prüfungswert“ erscheint, bis hin zu bestimmten Schlüsselwörtern. Werden die Daten als verdächtig eingestuft, gibt TURMOIL den Internetverkehr weiter an die
2. TURBINE; dieses Werkzeug gibt die Anfrage an die Server der NSA weiter. Dort wird mithilfe von Algorithmen entschieden, welche Schadprogramme der NSA gegen die Person eingesetzt werden. Die Entscheidung wird durch den Typ der Website, die angefragt wurde, begründet oder durch die Software des Computers und die Art der Internetverbindung. Das ausgewählte Schadprogramm wird dann wieder an die TURBINE gesendet. Diese führt das Schadprogramm zurück in den Kanal des Internetverkehrs und liefert sie dem Anfragenden frei Haus zusammen mit der gewünschten Website. Der gesamte Vorgang dauert weniger als 680 Millisekunden, ohne dass der Nutzer etwas davon mitbekommen hat. Ab diesem Zeitraum gehört das gesamte digitale Leben des Nutzers dem Geheimdienst.

Beide Programme können durch die obligatorische Datensammlung auf den Servern der Provider (PRISM) und durch die unmittelbare Datensammlung aus der Internetinfrastruktur (Upstream Collection)

über den gesamten Globus Informationen überwachen, egal ob sie gespeichert oder übermittelt wurden.

Der nächste Schub

a. Einheitliche Identifikationsnummern für alle Zwecke

Das Hauptproblem beim Datenschutz ist gar nicht mehr so sehr der Überwachungsstaat, wie noch bei der Volkszählung befürchtet. Viel umfassender sammeln Konzerne Daten und überwachen die einzelne Person. Sie verfügen über unzählige Daten, die sie sich ohne Probleme zusammenkaufen können. Über die Mehrzahl der Erdenbewohner existieren bereits komplette Dossiers.

Ein Problem bestand bisher darin, dass die Datenbanken nicht so gut zusammengeführt werden können und eine sichere automatische Identifizierung nicht gewährleistet ist. Mit der Etablierung der einheitlichen Identifikationsnummer für alle Zwecke wird das Problem dahingehend gelöst, dass die Unternehmen ihre Konsumenten mit deren Identifikationsnummer in den Datenbanken haben und sie zielsicher ansprechen können.

Finanzierer dieser ID2020-Initiative sind die Gates- und Rockefeller-Stiftungen, die auch die Harmonisierungsbemühungen der Weltgesundheitsorganisation (WHO) bezüglich digitaler Impfnachweise bezahlt haben.

Die Initiative ID2020 strebt an, bis 2030 alle Menschen auf der Welt mit digitalen, biometrisch unterlegten Identitätsnachweisen auszustatten, die für viele verschiedene öffentliche und private Zwecke verwendbar sein sollen. Am Ende wird es sich um miteinander vernetzte Mega-Datenbanken handeln, in denen alle Menschen mit einer Nummer und ihren biometrischen Merkmalen eindeutig und maschinenlesbar identifiziert sind und schließlich alle

Informationen über diese Menschen leicht zentral abrufbar werden.

Der Bundestag hat Anfang 2021 einen entscheidenden Schritt bei der Umsetzung des sogenannten ID2020-Projekts von Microsoft, Accenture und Rockefeller-Stiftung getan, indem er die Steuer-Identifikationsnummer zur „einheitlichen Bürgernummer“ für alle Behörden gemacht hat. Das Ganze wurde schnell durchgesetzt, obwohl alle Datenschutzbehörden warnten, dass das Gesetz verfassungswidrig sein könnte. Der wissenschaftliche Dienst des Bundestages hatte ebenfalls „erhebliche Schwierigkeiten“ gesehen. Auch das Bundesverfassungsgericht hat sich mehrfach gegen eine solche Nummer ausgesprochen. Doch die Bundesregierung hat erst gar nicht wirklich nach alternativen, datenschutzfreundlicheren Modellen gesucht, sondern von Anfang an auf die Steuer-ID als Kennzahl gesetzt.

Mit dem Gesetz ist es möglich, den Onlinezugang relevanter Daten der Verwaltungsregister durch die persönliche Steueridentifikationsnummer zu verankern. Damit wird gewährleistet, „dass Basisdaten natürlicher Personen von einer dafür verantwortlichen Stelle auf Inkonsistenzen geprüft, verlässlich gepflegt, aktualisiert und bereitgestellt werden“. Zur eindeutigen Zuordnung in den Registern soll die Steueridentifikationsnummer als „einheitliches, nichtsprechendes Identifikationsmerkmal“ verwendet werden. Für die Transparenz soll ein sogenanntes Datencockpit aufgebaut werden, das eine „einfache und zeitnahe Übersicht über zwischen Behörden vorgenommenen Datenübermittlungen ermöglicht“. Mit so einer Form der umfassenden Datenerfassung und des Datenaustauschs wird ein perfektes totalitäres Überwachungs- und Kontrollsystem geschaffen.

> ***Demnächst werden überall Felder zum Eintrag der Bürger-ID eingebaut; die Bundesregierung warb und wirbt wieder einmal damit, alles diene nur der***

> ***Bequemlichkeit für die Menschen, und mit der Nummer ginge alles einfacher und schneller.***

Wieder beteuert die Regierung, dass eine Zusammenführung der Register nicht geplant und wegen der dezentralen Datenhaltung gar nicht möglich sei, doch die Erfahrung zeigt, dass einmal installierte Überwachungsmöglichkeiten später ausgeweitet werden, zur Freude von Geheimdiensten und Polizeibehörden. Als die Steuer-ID-Nummer eingeführt wurde, versprach man noch hochheilig, dass sie nur für Steuerangelegenheiten genutzt werden sollte. So ist durchaus davon auszugehen, dass demnächst auch die Hürden bei der Personenkennzahl fallen und die Daten aus den Registern und Datenbanken zusammengeführt werden, weil vorgeblich dies für die Digitalisierung der Behörden erforderlich sei.

Einheitliche Identifikationsnummern für alle Zwecke innerhalb eines Landes sind der erste Schritt in Richtung einer global einheitlichen Nummer, mit der auch private Unternehmen ihre Datenbanken einfacher und viel zuverlässiger als bisher zusammenführen können, damit ein lückenloses Profil des einzelnen Menschen entsteht.

b. Der „grüne CovPass“ – Ausweis über den Gesundheitszustand

Am 1. Juli 2021 startete der digitale Impfpass namens CovPass europaweit. Er sollte sowohl als neue Funktion in der Corona-Warn-App als auch als eigenständige App eingeführt werden. Wer den CovPass nutzt, kann mit einem QR-Code nachweisen, dass er geimpft, genesen oder negativ getestet ist.

Bei den völlig überzogenen Maßnahmen gegen das Coronavirus erlebten wir eine große Spaltung der Gesellschaft. Um am gesellschaftlichen Leben wieder teilnehmen zu können, muss der einzelne Mensch sich erst einmal über seinen ihm zugestandenen gesellschaftlichen Status klar werden: Gehört man zu den „Gesundeten und Geimpften“ oder zu den Kranken

beziehungsweise Nichtgeimpften, zu denjenigen, die die Maßnahmen der Behörden befolgen, oder zu den Verweigerern und Aufmüpfigen, zu den Guten oder Bösen im Staat? Je nachdem werden die schweren Eingriffe in die Persönlichkeit erleichtert oder beibehalten und der Zugang zum gesellschaftlichen Leben gegeben oder verwehrt.

Bei den Coronamaßnahmen spielten auch die Contact-Tracing-Apps für Smartphones eine große Rolle. iPhones bieten diese Funktion seit September 2020 (iOS 13.7) an. Die über Bluetooth Low Energy (BLE) gesammelten Informationen bildeten die Grundlage für die Contact-Tracing-Apps. Auch die deutsche Corona-Warn-App nutzte den intransparenten Datenpool. Dafür konnte das Programm über eine Schnittstelle alle Begegnungen der vergangenen 14 Tage auslesen. Ende 2020 entwickelten bereits über 20 Länder Tracking-Applikationen, um die von Big Tech gesammelten Bewegungs- und Begegnungsdaten auslesen und in ihren COVID-Apps darstellen zu können.

> ***Obwohl die Pandemie bereits ausdrücklich – oder implizit – für beendet erklärt wurde, wird weiter an der Überwachungsagenda gearbeitet, und man will elektronische Impfpässe weltweit zur Voraussetzung für das internationale Reisen machen.***

Die Überlegung dahinter aber ist, später beliebige gesundheitspolitische oder sonstige Vorwände zu nutzen, um die vorhandene Überwachungsinfrastruktur auch im Inland wieder für vielfältigste Aktivitäten zur Voraussetzung zu machen.

Die Zusammenarbeit der großen Pharmakonzerne, Nationalstaaten und Europäischer Union in Verbindung mit den ihnen ergebenen Medien soll dem einzelnen Menschen den massiven Eingriff mit dem digitalen Impfpass in die Persönlichkeitsrechte als Erleichterung und weniger Kontrolle verkaufen. In der Realität wird

der digitale Impfpass aber als ein Bewegungsmelder funktionieren, der „richtiges oder falsches Verhalten“ erfasst und weitergibt, die Gesellschaft nachhaltig spaltet und dabei hilft, ein europäisches Sozialkreditsystem aufzubauen.

Uneingeschränkte Unternehmensmacht gekoppelt mit unkontrollierbaren staatlichen Diensten

Das Internet ist eine grundlegende Infrastruktur für die Ausübung zahlreicher Menschenrechte. Konzerne wie Facebook und Google sind Torhüter dieser digitalen Welt. Sie haben eine historisch einmalige Macht über den „digitalen öffentlichen Platz“ und bestimmen auch, unter welchen Bedingungen und mit welchen Einschränkungen Meinungs- und Informationsfreiheit online ausgeübt werden kann und welchen Preis man dafür zahlen muss. Die Dominanz von Onlinediensten, wie sie IT-Riesen wie Google und Facebook anbieten, geben diesen Unternehmen eine nie dagewesene Macht über die persönlichsten Daten von Millionen Menschen: 2,8 Milliarden Personen pro Monat nutzen einen Facebook-Dienst, mehr als 90 Prozent aller Internetsuchen finden auf Google statt, und mehr als 2,5 Milliarden Handys nutzen das Google-Betriebssystem Android.

Konzerne wie Facebook und Google sammeln Daten in einem unfassbaren, nie dagewesenen Ausmaß – unbeschränkt, dauerhaft. Dies umfasst nicht allein freiwillig zur Verfügung gestellte Informationen, sondern die digitale Erfassung und Überwachung aller Aktivitäten, weit über die Nutzung einzelner sogenannter Social-Media-Plattformen hinaus. Auch ist das Sammeln nicht auf die Daten derer beschränkt, die sich bewusst dafür entschieden haben, diese Dienste zu nutzen.

> ***Während internationales Recht und Verfassungen elementare Menschenrechte garantieren, staatliche Behörden reglementieren und diese einer rechtsstaatlichen Gewaltenkontrolle unterwerfen, haben die Internetkonzerne ein privates Überwachungsregime geschaffen, welches sich der unabhängigen öffentlichen Kontrolle weitgehend entzieht.***

Parallel zum Ausbau des weltweiten Überwachungssystems, in dem die Bevölkerung total ausgehorcht, von jeder Person massenhaft Informationen gesammelt wird, sie erpressbar macht, wurde nebenbei ein immenses Meinungs- und Unterhaltungsangebot mit dem Internet aufgebaut, mit dem man die Massen beschwichtigen und ablenken will. Dazu kommt, dass die USA und auch die europäischen Staaten über ein Heer von Einflussjournalisten in Kooperation mit der monopolisierten Medienmacht verfügen, die die globale Kommunikation weitgehend steuern.

Dabei wurden diese Big-Tech-Konzerne systematisch von der US-Regierung und dem US-Militär aufgepäppelt. Es wird immer wieder erzählt, wie junge Männer in ihren Hinterhofgaragen den Grundstein für die Megakonzerne gelegt hätten. Ihr genialer Erfindergeist war lediglich nur das Zurückgreifen auf jeweils aktuellen US- Militärentwicklungen. Alles, ob Sensoren, Chips, Siri, Touchscreen oder Batterien, wurde von der US-Regierung und dem dortigen Militär finanziert und entwickelt. Schon vor über 12 Jahren konnte man in den USA nachlesen, wie erfolgreich das Investmentinstrument der CIA – In-Q-Tel – bei der Gründung von Google, Facebook, Twitter und den anderen Senkrechtstartern Regie führte und die Unternehmen seither für seine Zwecke instrumentalisierte.

Smartphone – Tyrann und Spion im Taschenformat

„*Die Gefahr, dass der Computer so wird wie der Mensch, ist nicht so groß wie die Gefahr, dass der Mensch so wird wie der Computer*“ (Konrad Zuse).

Seit der Jahrhundertwende hat kaum ein Gegenstand so eine erfolgreiche Karriere hinter sich wie das Mobiltelefon. Weltweit haben 6,92 Milliarden Menschen ein solches Gerät derzeit in Gebrauch, das waren Ende 2023 gut 86 Prozent der Weltbevölkerung, die mit dem Telefon nicht mehr vorrangig telefonieren, sondern sich je nach Region, zwischen zwei und knapp sechs Stunden pro Tag im Internet aufhalten.

Zunächst herrschte die Freunde am mobilen Telefonieren und der neuen Technik des kleinen Gerätes vor. Schnell kam die SMS-Funktion hinzu, dann auch die Möglichkeit, mobil eine E-Mail zu verschicken und auch außerhalb der Wohnung ins Internet gehen zu können. Ein weiterer Entwicklungssprung kam dann mit dem iPhone.

> ***Für die Multifunktionen der heutigen Smartphones bezahlen die Menschen mit der Preisgabe von Freiheit. Sie werden von den Telefonen nicht nur ausspioniert, auch ihr Bewusstsein wird stark beeinflusst.***

Die Mehrheit der Bevölkerung kann sich den Alltag ohne Smartphone kaum noch vorstellen; sie glaubt, ohne das Gerät zum Beispiel auf Dienste wie Nachrichten- und Informationsbeschaffung, Video- und Musikstreaming, Wetterbericht, Routenplanung und Navigation, komplette Kommunikation, Zahlungsverkehr, Anfertigen und Sammlung von Fotos und Filmen alternativlos verzichten zu müssen.

Die Angst vor der Abhängigkeit vom eigenen Gerät scheint berechtigt, denn die Entwicklung ist schon weiter fortgeschritten, als jeder Nutzer eines Smartphones wahrhaben will:

- Smartphones werden schon seit 2012 kaum noch zum Telefonieren genutzt.
- 6,92 Milliarden Menschen besitzen derzeit ein Smartphone. Das entspricht 86 Prozent der Weltbevölkerung.
- Je nach Region verbringen die Nutzer zwischen zwei und knapp sechs Stunden pro Tag mit ihrem Gerät.
- Der weltweite Durchschnitt für Menschen im Alter von 16 bis 64 Jahren liegt aktuell bei sechs Stunden und 58 Minuten Bildschirmzeit pro Tag.
- Über hundert Mal, mit steigender Tendenz, greift man in diesem Zeitraum nach dem Gerät.
- 60 Prozent des gesamten Internetverkehrs sowie 55 Prozent der weltweiten Webseitenzugriffe finden mittlerweile über die Mobiltelefone statt.
- 98 Prozent der Geräte laufen entweder auf Android oder iOS.

- 92,3 Prozent aller Internetnutzer greifen von ihrem Mobilcomputer aus auf das Internet zu, und
- 35,2 Prozent der Nutzungsdauer verbringen iPhone- und Android-Kunden auf dem sogenannten Social-Media-Angebot.

Die mittlerweile exzessive Nutzung des Geräts in allen möglichen Lebenslagen ist zu einer gesellschaftlichen Plage mit einem hohen Suchtfaktor geworden. Doch gegen eine Sucht kann man ankämpfen und sie überwinden, gegen eine stetige, lückenlose Observation, Manipulation und Transformation der Gesellschaft hat niemand eine Chance. Da geht es nur um hilfloses Ausgenutztwerden, weil die Smartphones sich längst zu tief in die sozioökonomischen Strukturen unserer Zeit gefressen haben.

Was ein Smartphone so alles kann

Weil die Entwicklung in den vergangenen Jahren so rasant war, werden im Folgenden die Möglichkeiten moderner Smartphones ausführlich aufgezeigt:

- Die US-amerikanischen Internetkonzerne kennen nicht nur alle unsere Kontakte, Bewegungsdaten, Lieder, Fotos, Videos, Bankverbindungen, Kontostände und E-Mail-Anhänge, sondern speichern auch unsere Suchanfragen, politischen Ansichten, Sorgen, sexuellen Präferenzen, vertraulichen Nachrichten und intimen Gespräche. Diese Informationen zeichnen nicht nur ein detailliertes Bild vom sozialen Netzwerk jedes Nutzers, sondern auch ein psychologisches Profil, das exakter kaum sein könnte.
- Über 72 Millionen Datenpunkte sammeln die Megakonzerne für Digitalwerbung in den USA pro Kind bis zu dessen 13. Lebensjahr. Facebook zum Beispiel hortet mindestens 52.000 Einträge je Nutzer. Das harmloseste Ergebnis dieser Datensammlung ist zielgerichtete Werbung, die uns auf Basis von Daten und Nutzungsverhalten auf Plattformen und Webseiten angezeigt wird.
- Heftiger sind die Auswirkungen durch Datenmissbrauch, mentale Manipulation, digitale Währungen, algorithmisierte Zensur, elektronische Ausweise, Sozialkreditsysteme, CO2-Budgetierung und Geofencing. Diese Sammlungen wären ohne Smartphone überhaupt nicht möglich.
- Wer permanent seinen Standort an eine Zentrale übermittelt, ist auch einfach zu kontrollieren. Die Smartphone-Nutzer erfahren dies ganz direkt, wenn zum Beispiel viele Inhalte, die in der Schweiz oder anderen Nicht-EU-Ländern angezeigt werden, in EU-Staaten unterdrückt werden oder ein Musiktitel sich nicht mehr abspielen lässt, wenn man auf Reisen ist.
- Smartphones überwachen und dokumentieren die Position ihres Nutzers auch, wenn alle GPS-Funktionen deaktiviert sind oder das Gerät komplett ausgeschaltet ist. Das optionale Abschalten von Standort- und Ortungsdiensten oder der Hintergrundaktualisierung in den Smartphone-Menüs bezieht sich in der Regel nur auf Dienst- und Drittanbieter-Apps. Verkauft werden solche Lokationsdaten bevorzugt an Regierungen und Geheimdienste.

- Die Ortungsdienste von den Konzernen lassen sich nicht abschalten; unklar ist auch, was mit den Daten geschieht. In der alltäglichen Praxis ist es beispielsweise möglich, dass eine gesamte Reiseroute auf den Meter genau bei Google Maps dokumentiert wird, obwohl alle Tracking-Funktionen deaktiviert sind, und selbst im hintersten Winkel der Erde, wo sich mit dem Smartphone keine Datenverbindung herstellen lässt, wird der Weg aufgezeichnet.

- Mit so einem Programm ist es durchaus möglich, digitales Geld oder moderne PKW demnächst so zu programmieren, dass sie auch nur in einem vordefinierten Radius funktionieren.

- Die jüngsten Entwicklungen für Android-Smartphones zeigen zum Beispiel mit dem „Google Play Protect“, wie eine Betriebssystemsoftware, die vor „schädlichen“, oder „unbekannten“ Drittanbieter-Apps warnt, sie scannt und deren Installation verhindern soll, angeblich zur Sicherheit des Nutzers. Da ist es nicht mehr weit, dass auch unliebsame Applikationen zum Beispiel von RT, *Al Jazeera* oder anonyme Krypto-Wallets rasch auf der Liste schädlicher Software landen und nicht mehr verwendbar sind.

- Seit 2021 ist Apple in der Lage, mit seinem „Client Side Scanning“ auf iPhones und iPads installierten Erweiterungen sämtliche Fotos zu scannen, die auf iCloud hochgeladen werden. Damit sollte die Verbreitung von Kinderpornografie erschwert werden. Das Internet Architecture Board (IAB) warnte damals eindringlich vor diesem skandalösen Paradigmenwechsel im Hinblick auf die Privatsphäre und Datenverschlüsselung. Nach einigem Protest nahm Apple offiziell Abstand von diesem Vorhaben, doch installierte die Software trotzdem. Das Programm befindet sich also heute auf jedem Apple-Gerät mit aktuellem Betriebssystem. Apple versichert aber blauäugig, das Programm sei nicht aktiviert.

- Eine Privatsphäre für Fotos gibt es nicht mehr. Jedes Foto, das mit einem iPhone, iPad oder Mac aufgenommen wird, wird lokal gescannt. So kann das Gerät Gesichter identifizieren und für einzelne Alben vorschlagen. Dann wird jedes Bild mit sogenannten Neural Hashes versehen, also mit klaren Identifikatoren, die beim Upload in die Cloud übertragen und katalogisiert werden. Auch wenn die Cloud-Dienste nicht aktiviert sind, übertragen Apple-Geräte die Transkripte der Neural-Hash-Datenbank nachts heimlich an die Zentrale. Wie allgemein bekannt ist, lassen sich Bilder in der Cloud nicht so einfach löschen. Löscht man das Foto selbst manuell, wird das Foto nicht wirklich gelöscht, sondern nur in der User-Ansicht ausgeblendet. Wie lange Apple und Google die Daten auf ihren Servern speichern, ist nicht bekannt.

- Google plant, künftig alle Anrufe seiner Nutzer zu scannen und zu speichern, vorgeblich um seine Kunden so vor Telefonbetrügern warnen zu können.

- Die umstrittene Vorratsdatenspeicherung ist nicht mehr aktuell. Neuerdings arbeiten neben den privaten Megakonzernen auch die transatlantisch ausgerichteten Überwachungsinstitutionen in der EU, Großbritannien und den USA an Gesetzen, die Client Side Scanning und anlasslose Totalüberwachung legalisieren.

- Vorläufiger Höhepunkt sind Smartphones, die sich mit Gesichtserkennungssoftware wie „Face ID“ entsperren lassen, sie fertigen alle fünf Sekunden ein Infrarotbild von ihrer Umgebung an, auch dann, wenn der Bildschirm gesperrt oder verdeckt ist. Nach Angaben von Apple ist das erforderlich, um das Gerät zügig per Blick auf den Bildschirm entsperren zu können. Die von Face ID angefertigten Fotos werden in mathematische Strukturen umgewandelt und auf dem Telefon abgelegt. Das Gerät schickt jede Nacht gegen drei Uhr unaufgefordert nicht einsehbare Datenpakete an Apple.

- Erschreckend ist auch die Entwicklung bei den Kameras. Mittlerweile können sie zum Beispiel dem Blick des Smartphone-Nutzers folgen, um dessen Befehle entgegenzunehmen, seine Tätigkeiten nachzuvollziehen oder seine Mimik zu deuten. Apple nennt diese Fähigkeiten „Aufmerksamkeitssensible Funktionen“, die vor allem für biometrische Kontrollen genutzt werden können.

- Auch sind die eingebauten Mikrophone weiterentwickelt worden. Das Smartphone hört permanent zu, um immer zu wissen, wann der Nutzer etwas vom ihm will. So ist es kein Zufall, dass Werbeanzeigen und Social-Media-Inhalte exakt das widerspiegeln, was im Umfeld des Gerätes in den letzten Stunden besprochen wurde. Weil die Sprachaufzeichnungen als Datenmenge für die Übertragung an die Megakonzerne zu groß sind, nutzen die Smartphones Textdateien mit Transkripten, die man sehen kann, wenn man mit iMessage eine Voicemail aufnimmt und diese in Sekundenbruchteilen als Text im Display erscheint.

- Die neuen KI-basierten Anwendungen können sogar autonom funktionieren, wenn das Smartphone seine Kameras, Bewegungssensoren und Mikrofone permanent nutzt, um seine Umgebung zu überwachen. Das einzelne Gerät überwacht dann nicht mehr nur den einzelnen Nutzer, sondern auch sein gesamtes Umfeld.

- Um das Umfeld überwachen zu können, beherrschen die Geräte die Kommunikation untereinander perfekt; sie können seit vier Jahren jeden Kontakt mit einem anderen iPhone aufzeichnen und bilden daraus Netzwerkkarten zu Bewegungen und Begegnungen ihrer Besitzer. Sie tauschen Informationen wie IMEI-Nummern, IP-Adressen und Kontaktdaten flächendeckend über das Betriebssystem aus.

- Im Laufe der Zeit sind immer mehr Datenkraken entstanden. So zeichnen zum Beispiel Googles Android-Geräte seit Ende 2020 jede Begegnung mit anderen Android-Geräten auf, und damit entstanden zwei riesige Mesh-Netzwerke, in denen Maschinen ohne Zutun ihres Besitzers untereinander kommunizieren. In Deutschland verwenden aktuell 66,1 Prozent der Smartphone-Nutzer Android und 33,2 Prozent iOS von Apple. 99,3 Prozent der Bevölkerung sind damit kartografiert. Seit Neuestem verstehen sich die beiden bisher getrennt voneinander spionierenden Betriebssysteme von Google und Apple nun auch gegenseitig.

> ***Dies alles zeigt nur noch die schaurige Perspektive auf, dass es kein Zurück mehr gibt und der einzelne Mensch der permanent sich ausbreitenden Smartphone-Überwachung durch die Megakonzerne mit ihren verschlüsselten Messengerdiensten nicht mehr***

> ***entkommen kann.***

Die aktuellen KI-Dienstprogramme wie Recall haben eine weitere Stufe der Überwachung erklommen. Vorgeblich sollen diese Programme dem Benutzer bei der Suche nach Dateien helfen, nur lokal gespeichert und nach drei Monaten gelöscht werden. Für den neuen KI-Dienst werden alle paar Sekunden Screenshots gemacht und damit alles aufgezeichnet, was auf dem Computer passiert. Trotz aller Beteuerungen ist es weiter ein Leichtes, einen Zugriff auf den einzelnen Computer zu bekommen. Beispielsweise muss ein Hacker nur Recall aufrufen, um Zugang zu Passwörtern oder anderen sensiblen Daten zu erhalten. Programme wie Recall zeigen, dass auch technisch sichere Messenger ganz einfach überwacht werden können. Für eine Überwachung müssen die Messenger-Nachrichten nicht mehr auf dem Server abgefangen und entschlüsseln werden, sondern werden einfach nur stetig auf dem Smartphone fotografiert und zur Übertragung in Textdateien umgewandelt.

Künstliche Intelligenz (KI) – das mächtige Geheimdienst-Werkzeug

Bereits vor 15 Jahren gab es ein öffentlich bekanntes Programm des Militärs der USA mit dem Name Life Log, das genau die Speicherung und Aufzeichnung unserer alltäglichen Aktivitäten zum Ziel hatte, die heute durch Goggle, Apple und die anderen US-Konzerne wie nach einer Blaupause umgesetzt wurde. Ein weltumspannendes Aushorch- und Überwachungssystem unter der Obhut des US-Militärs und Geheimdiensten. Doch die angeleitete Entwicklung ging schnell weiter.

Ende 2015 wurde OpenAI mit der erklärten Vision gegründet, eine künstliche Intelligenz zum Wohle der Menschheit zu entwickeln.

Gründer von OpenAI waren unter anderem die Multimillionäre und -milliardäre Sam Altman (Loopt, Y-Combinator), Ilya Sutskever (technischer Mastermind von OpenAI, zuvor KI-Experte bei Google) und Elon Musk (Tesla, SpaceX). Elon Musk zog sich 2018 aus dem Unternehmen zurück und verkaufte seine Anteile an Microsoft. Der Konzern investierte im Jahr 2019 bereits eine Milliarde US-Dollar in OpenAI, weitere zwei Milliarden 2021 und weiter zehn Milliarden 2023.

Als Ende November 2022 OpenAI seinen KI-basierten Chatbot „ChatGPT“ der Öffentlichkeit vorstellte, löste das einen KI-Hype aus und erlangte sofort eine sehr hohe Popularität. Auch hier zeigte sich wieder die enge Verbindung zu den US-amerikanischen Behörden. OpenAI hatte sich kürzlich den erst vor Kurzem abgetretenen Chef des US-Auslandsgeheimdienstes NSA in den Vorstand geholt – des Geheimdiensts, der den Anspruch hat, alles zu erfahren, was auf dem gesamten Globus vorgeht. Mit Paul M. Nakasone zieht ebenfalls ein Geheimdienstler in den Vorstand von OpenAI und wird maßgeblich im Sicherheitskomitee von OpenAI mitarbeiten. Der Mann war von 2018 bis zum Februar 2024 Leiter des US-Geheimdienstes NSA und langjähriger Leiter von USCYBERCOM, der obersten geheimen Datenüberwachungsorganisation der Regierung.

Mit diesem Personal ausgerüstet kann die neue Technologie vor allem bei Microsoft, Google und Apple wie auch anderen US-Konzernen zur weltweiten Anwendung kommen. Es wird bereits davon geträumt, mit KI Dinge wie digitale Wahlen oder ein universelles Grundeinkommen, das aus der Wertschöpfung von künstlicher Intelligenz gespeist werden soll, verwirklichen zu können.

Auch Elon Musk ist wieder dabei: 2023 gründete er sein eigenes KI-Unternehmen „xAI“, mit dem er fortschrittliche KI-Systeme, unter anderem einen Supercomputer, bauen möchte. 24 Milliarden US-Dollar Wagniskapital hat Musk inzwischen für dieses Unternehmen

eingeworben. Da wird nicht gekleckert, sondern geklotzt.

Wie Musk ist vor allem Sam Altman hyperaktiv. Gemeinsam mit dem deutschen Physiker Alex Blania gründete er 2019 das Unternehmen „Tools For Humanity“. Schnell waren 240 Millionen Dollar Wagniskapital eingesammelt, um die Kryptowährung Worldcoin (WLD) und eine Hardware namens „Orb“, zum Scannen der Iris entwickeln zu können. Die beiden Männer möchten mit ihrem Projekt „das größte Finanznetzwerk der Welt“ erschaffen und eine zuverlässige Möglichkeit entwickeln, Menschen von KI-Systemen unterscheiden zu können. Für diesen Zweck ist ein digitaler Identitätsnachweis namens „World ID“ vorgesehen. Die Nutzer können sich die „World App“ installieren, ihre Iris an einem Orb in der Nähe scannen lassen und erhalten dafür ihre digitale Identität sowie ein paar Worldcoins im Wert von etwa 100 Euro gratis. Etwa 5,5 Millionen Menschen, vorwiegend aus Entwicklungsländern, haben dies inzwischen getan.

Schöne neue Welt!

Zur Erinnerung

Mit dem Volkszählungsurteil von 1983 schuf das Bundesverfassungsgericht das Grundrecht auf informationelle Selbstbestimmung. Danach verstößt es gegen die Menschenwürde, also den ersten und wichtigsten Artikel des Grundgesetzes, wenn der Staat selbst Persönlichkeitsprofile anlegt oder dies zulässt.

Redaktionelle Anmerkung: Dieser Beitrag erschien zuerst unter dem Titel „**Vom Volkszählungsurteil über das PRISM-Programm**

des NSA zur einheitlichen Identifikationsnummer für alle Zwecke, zum Taschenspion Smartphone und Künstlicher Intelligenz (https://gewerkschaftsforum.de/vom-volkszaehlungsurteil-ueber-das-prism-programm-des-nsa-zur-einheitlichen-identifikationsnummer-fuer-alle-zwecke-zum-taschenspion-smartphone-und-kuenstlicher-intelligenz/)“ beim ***Gewerkschaftsforum*** *(https://gewerkschaftsforum.de)*.

Das **Gewerkschaftsforum** ist ein Internetjournal, das sich vorrangig mit gewerkschaftlichen Themen, aber auch mit sozial- und wirtschaftspolitischen Fragen kritisch auseinandersetzt. Es wurde Ende 2013 von Gewerkschaftsaktivisten in Dortmund gegründet und möchte auf die Interessen der Mächtigen aufmerksam machen, den gewerkschaftlichen Kampf der Beschäftigten begleiten und den immer leiser gewordenen erwerbslosen und armen Menschen eine Stimme geben. Weitere Informationen unter **gewerkschaftsforum.de** (https://gewerkschaftsforum.de).