Ein Text von: **CARL-JOSEF KUTZBACH**

Notiert am: 26.1.2019 poschd@cajo-kutzbach.de

Big Data

Möchten Sie entmündigt werden?

„Der sieht den Wald vor Bäumen nicht!“ spottete man früher, wenn jemand vor lauter Details das große Ganze nicht erkennen konnte. Heute gibt es Rechenmaschinen und Rechenverfahren, die im Wald – um im Bild zu bleiben – jeden einzelnen Baum erkennen und bewerten können. Da das unsere Denkmöglichkeiten übersteigt, können wir uns das schlecht vorstellen und folglich auch nur schlecht damit umgehen.

Das gleiche Problem tritt auf, wenn man auch nur versucht sich vorzustellen, was andere Leute mit meinen Daten anfangen könnten. „Ich habe doch nichts zu verbergen!“ wird oft von Leuten gesagt, denen nicht klar ist, weshalb sie ihre Daten schützen sollten. Und außerdem würden die Daten doch anonymisiert, es könne also niemand wissen, dass man selbst dahinter steckt. Viele Benutzer von Pornoseiten wundern sich, weshalb sie anschließend entsprechende E-mails mit zweideutigen Angeboten bekamen. In den USA gelang es Forschern aus vielen anonymisierten Kreditkartendaten, auf die Person zurück zu schließen, sobald diese nur drei Einkäufe mit der Kreditkarte getätigt hatte. Also mit der angeblichen Anonymität ist es heute nicht mehr weit her.

Das merken Benutzer von Firmenwagen spätestens dann, wenn die Werkstatt anruft, dass das Fahrzeug einen Mangel gemeldet habe und wann man denn zur Behebung in die Werkstatt kommen wolle. Auch wer ein Leasing-Fahrzeug benutzt, muss damit rechnen, dass das gesamte Fahrverhalten aufgezeichnet und analysiert wird, und man - im Falle eines Unfalles - sehr genau bestimmen kann, wie schnell man fuhr und wann man mit dem Bremsen anfing.

Der damalige Bundesdatenschutzbeauftragte Peter Schaar beschrieb 2005, was Sorgen macht:

> ***„Es gibt eine technologische Entwicklung, die dadurch gekennzeichnet ist, dass wir überall einen Datenschatten hinter uns her ziehen. Das heißt, dass bei der Benutzung des Handys, beim Abheben vom Konto, beim Einkauf im Supermarkt oder beim Surfen im Internet immer Personen-bezogene Daten anfallen, die dann auch zugeordnet werden können, nämlich meinem Verhalten, und dann werden daraus Schlussfolgerungen gezogen, von denen ich gar nichts ahne, in Bezug auf meine politische Meinung, auf meine Vorlieben, oder meine Krankheiten.“***

Dazu gehören so genannte „Smart Meter“ Stromzähler, die genau protokollieren, wann wie viel Strom gebraucht wurde. Wenn man das mit dem Fernsehprogramm abgleicht, kann man vielleicht auf Grund der Zeiten schon erkennen, welche Sendungen angeschaut wurden und daraus auf politische Ansichten schließen. Einfacher ist es natürlich heute, wenn man einem digitalen Assistenten (Alexa, Siri & Co.) befiehlt er möge dies oder das einschalten, denn diese Plaudertaschen melden Vieles an ihre Hersteller, oder könnten auch als heimliche Lauscher im Wohnzimmer missbraucht werden. Weil das so ist, forderte Schaar schon vor 14 Jahren:

> ***„Also ich würde mir wünschen, dass sich jeder Einzelne ein Stück weit für diese Frage interessiert. Das ist die Voraussetzung dafür, dass er dann bewusst handelt. Das heißt, dass es ihm nicht egal ist, wo er seine Spuren hinterlässt, denn er muss letztlich auch damit rechnen, dass diese Spuren gegen ihn verwendet werden, oder - aus einseitigen Interessen heraus - auch aus dem Zusammenhang gerissen werden.“***

Wer zum Beispiel eine billige Wohnung in einem Viertel ergattert hat, dass irgend eine Firma, die Bewertungen erstellt (vielleicht die Schufa), für wenig seriös hält, der muss damit rechnen, dass er bei einem Kreditvertrag, oder einer Versicherung schlechtere Bedingungen bekommt, als jemand aus einem Nobelviertel. Hat man dann noch einen ausländisch klingenden Namen, dann kann das sogar dazu führen, dass man gar keinen Kredit bekommt, weil die Software, die diese Bewertungen macht, auf Grund von Namen und Wohnort auf geringe Kreditwürdigkeit, ja vielleicht sogar auf die Gefahr eines Versicherungsbetruges schließt.

Wie soll man sich aber als Einzelner - der nicht erfährt, was im Hintergrund abläuft - gegen eine derartige verdeckte Diskriminierung wehren? Wie soll man der Bank oder Versicherung nach weisen, dass sie Verfahren benutzt, denen der Gleichheitsgrundsatz und das Diskriminierungs Verbot des Grundgesetzes völlig egal sind, weil die Programme sie gar nicht kennen.

Ähnliches gilt für die Abrechnung von ärztlichen Leistungen durch entsprechende Dienstleister. Auch da wird versprochen, dass die Daten sicher seien. Es mag sein, dass die Namen der Patienten sorgfältig von den Krankheits- und Behandlungsdaten getrennt werden. Aber für die Forschung sind natürlich große medizinische Datensammlungen um so wertvoller, je mehr man über die Patienten weiß (Alter, Krankheitsgeschichte, Wohnort, Laster). Dabei muss man wissen, dass heute mit Hilfe von „Data Mining“ (das Untersuchen großer Datenmengen auf bestimmte Inhalte hin) auch eine Nadel im Heuhafen gefunden werden kann. Bei seltenen Erkrankungen, die in einem Jahr nur wenige Mal auftreten, dürfte es leicht fallen heraus zu bekommen, welche Person das war. Ähnliches gilt, wenn jemand mehrere Erkrankungen zugleich hat, wie das vor allem bei Älteren auftritt. Sucht man in den Daten, dann ist die ursprüngliche Anonymisierung sehr schnell kein ausreichender Schutz davor, dass man diese Person finden könnte.

Das, was für die Forschung gut ist, wäre auch für die Krankenkassen oder Rentenversicherungen interessant, weil sie aus den Daten ableiten könnten, welche Kosten bei welchem Patienten auf sie zu kommen, oder gar, wer wahrscheinlich bald stirbt. Wer in jungen Jahren schwer erkrankte, bekommt bestimmte Versicherungen gar nicht mehr, weil den Versicherungen das Risiko zu groß ist. Wenn aber der wirtschaftliche Nutzen für die Firmen groß genug ist, dann wächst die Gefahr, dass man versucht, an solche Daten heran zu kommen. Der Ankauf von Daten, die Steuerhinter zieher vor Gericht brachten, zeigte das ja.

Selbst, wenn die Abrechnungsfirmen völlig korrekt arbeiten und sich größte Mühe geben, ist nicht garantiert, dass sich ein Kenner der Materie nicht unerlaubt Zugang zu den Daten beschafft und damit eventuell viel Geld verdient. Dabei spielt auch eine Rolle, dass die Tendenz besteht möglichst viele Daten auf einem Großrechner zu versammeln. Dort lohnt sich für Hacker ein Datendiebstahl am ehesten und Großrechner sind relativ gut in ihrem Aufbau und ihren Funktionsweisen dokumentiert, allerdings meist auch gut gesichert. Die Esten, die bei der Digitalisierung weit voran geschritten sind, haben aus einem Datenklau beim Großrechner gelernt und die Einwohner-Daten auf viele dezentrale Rechner verteilt.

Der verstorbene englische IT-Fachmann Paul Liller meinte, dass jeder, der ins Netz geht, gehackt werden könne, sobald jemand sich die dafür nötige Mühe machen würde. In den USA bekommt man angeblich schon für 9 $ alle möglichen Daten über eine Person. Wenn man bereit ist genügend Geld zu bezahlen - ab 1200.- € aufwärts - bekommt man im Darknet das Profil eines Journalisten, stellte Peter Welchering in einem Beitrag des DJV-Blickpunkt fest. Damit kann man dann versuchen Druck auf Journalisten auszuüben.

Trotz aller Debatten um Vorratsdaten-Speicherung und Aufbewahrungsfristen bei uns, vergisst das Internet wenig, zumal interessierte Firmen ihre Daten eben in Ländern mit weniger strikten Vorgaben speichern. Daher befürchtete Peter Schaar schon früh:

> ***„Wenn irgend jemand im Internet vor Jahren in einem Chatroom eine unbedachte Äußerung gemacht hat, dass die ihm noch nach Jahren nachhängt, dass er etwa nicht zu einem Vorstellungsgespräch eingeladen wird, dass er möglicherweise fürchten muss seinen Arbeitsplatz sogar zu verlieren. Das sind alles Konsequenzen, die man jeweils bedenken muss, wenn man bestimmte Technologien benutzt, oder wenn man beispielsweise mit seinem Namen bestimmte Äußerungen macht.“***

Wenn man aber gar nicht erfährt, weshalb man benachteiligt wird, kann man sich auch nicht dagegen wehren und seine Rechte nicht wahrnehmen. Hier wird das Recht unterlaufen.

Man kann verstehen, dass deshalb Manche im Internet nur unter Pseudonym auftreten, aber das verhindert zugleich eine ehrliche menschliche Begegnung mit dieser Person. Und andere meinen, sie könnten im Schutz der Anonymität mal so richtig „die Sau raus lassen“ und sind erstaunt, wenn man ihnen das dann doch anlasten kann, weil auch sie in vielen Fällen eine Datenspur hinterlassen. Big Data (wörtlich „große Daten“, meint die Verarbeitung und Analyse riesiger Mengen) ermöglicht nicht nur die Suche nach der Nadel im Heuhaufen, sondern auch zu prüfen, zu wem diese oder jene Daten nicht passen und so auch all jene auszuschließen, nach denen man nicht sucht, bis dann ganz wenige übrig bleiben, die verdächtig sind.

Weil der Bürger die erstaunlichen Möglichkeiten der Analyse von riesigen Datenbeständen nicht kennt, sind ihm die Gefahren seines Verhaltens nicht bewusst. Peter Schaar riet schon 2005:

> ***“Ich würde mir wünschen, dass man, wenn man eine Kundenkarte benutzt, dass man sich überlegt, bei welcher Gelegenheit man das tut. Ob man das bei jedem Kleineinkauf macht, oder ob man das nur macht, wenn man größere Anschaffungen tätigt, wenn man überhaupt davon Gebrauch machen will. Es gibt durchaus manche Punkte, wo man sagen kann: Ja, da bin ich mit einverstanden, oder, dort möchte ich nicht registriert werden. Da zahl ich bar, dort zahl ich mit der Kreditkarte. Solche Wahlmöglichkeiten sind ja zum Glück immer noch gegeben.“***

In Skandinavien aber, wo man heute schon fast Alles mit der Karte bezahlt, macht man sich mit Bargeld fast schon verdächtig. Dort könnte man an Hand der Kartendaten ziemlich gut belegen, wann jemand wo war, und für was er, wie viel, bezahlt hat.

Verbindet man das mit den Daten, die schon ein Handy hinterlässt, dass sich ja ständig beim Rechner des Anbieters melden muss, damit der Telefonate zum Handy durchstellen kann, dann entsteht ein ziemlich genaues Bewegungsprofil dieser Person. Wenn man ein Smart-Phone

benutzt, das ständig die Daten auch an den Hersteller, Kartendienste und Programmierer weitergibt, damit man es orten kann und weiß, wo man ist, dann sind die Daten noch genauer.

Schon 2005 zeichnete sich ab, dass immer mehr Plastik-Karten mit einem Chip ausgestattet werden würden, der es erlaubt die Daten auszulesen, ohne, dass man die Karte dazu an ein Lesegerät halten muss. Das ist so ähnlich, wie die Funketiketten (RFID) in Kaufhäusern, die einen Ladendiebstahl verhindern sollen, bei denen es dann an der Eingangstür piepst, wenn das Etikett nicht richtig „entschärft“ wurde.

Bank- und Kreditkarten mit Chip sollen das Einkaufen erleichtern, Patientenkarten mit Chip die Abrechnung des Arztes, Fahrkarten mit Chip das Bezahlen oder die Abrechnung beim Fahren mit öffentlichen Verkehrsmitteln und Ausweise mit Chip, die Kontrolle beschleunigen. Dabei weiß der Laie nie, welche Daten auf seinem Chip gespeichert sind und welche von den Lesegeräten ausgewertet werden. Krankenkassen teilen einem zwar mit, was sie auf dem Chip speichern, aber kaum jemand wird ein Lesegeräte anschaffen, um das auch zu überprüfen.

Das zweite Problem mit solchen Karten mit Chip ist, dass man als Laie nicht spürt wer wann wo die Karte ausliest. Deshalb tragen Vorsichtige entsprechende Ausweise und Karten in einer Hülle, die für die Funkwellen undurchdringlich sein soll (etwa eine geeignete Metallfolie) oder verzichten wo möglich gleich auf den Chip. Manche Banken stellen auch Karten ohne Chip aus.

Seit private Rechner sehr leistungsfähig geworden sind, bieten Bildbearbeitungsprogramme Gesichtserkennung an. Die Software ordnet dabei im Hintergrund das Gesicht der Tante Frida alle Gesichtern zu, die es für ähnlich hält. So ähnlich funktioniert auch der Versuch in Berlin, bei dem an einem Bahnhof mittels Videokamera Gesichter von Menschen „erkannt“ werden sollen. Im Versuch soll die Software nur diejenigen erkennen, die freiwillig mitmachen. Aber das Ziel ist klar, man möchte große Ströme von Fussgängern nach bestimmten Menschen durchsuchen können. Das dient angeblich der Terrorabwehr. Aber das verhindert keinen Terror, sondern im besten Fall kann man hinterher feststellen, wer am Tatort war.

In England gibt es etwa eine Videokamera für vier Bürger. Das macht klar, weshalb man so viel Wert auf automatische Gesichtserkennung legt: Kein Mensch wäre in der Lage so rasch so viele Videos zu sichten. Das geht nur mit automatisierter Datenanalyse. Dass es dabei auch darum geht dem Bürger ein Gefühl von Sicherheit zu geben und die Politik damit Handlungsfähigkeit demonstrieren will, spielt sicherlich auch eine Rolle, denn es gab eine Meldung, dass 80 % der britischen Kameras keine brauchbaren Bilder lieferten.

Man muss sich darüber im Klaren sein, dass unter dem Deckmantel der Terrorbekämpfung die weitgehende Überwachung aller Bürger betrieben wird. In gewissem Sinn haben damit die Terroristen mehr erreicht, als durch einen Terroranschlag allein: Sie erzeugen mit Hilfe der Politik und entsprechender Unternehmen für Sicherheitstechnik eine Stimmung des Misstrauens und der Angst. Ob das die klügste und angemessene Antwort auf Terror ist, darf bezweifelt werden. Damit soll keinesfalls das Leid von Opfern gering geachtet werden, sondern die Frage stellt sich, ob man nicht durch andere Maßnahmen dem Terror den Boden entziehen könnte, etwa in dem man versucht weltweit faire und auskömmliche Lebensbedingungen zu schaffen, so dass Hass und Verzweiflung weniger Nährboden finden.

Diese Beispiel der doch recht langsamen Fußgängerströme zeigt, wozu man auch die Mautbrücken an Autobahnen und Bundesstraßen benutzen könnte: Automatische Analyse der Kennzeichen und damit das Erstellen von Bewegungsprofilen von Autofahrern. Prompt fordert die Politik, bei Verbrechen, man müsse diese Daten auch zu Verfolgung von Straftätern einsetzen, obwohl man genau dies ursprünglich strikt abgelehnt hat. Ähnlich ist es mit der bei Hannover eingerichteten Geschwindigkeitskontrolle über eine Strecke, indem man am Anfang die Autos erfasst, diese Bilder mit Aufnahmen vom Ende der Strecke vergleicht und all jene heraus fischt, die dort früher ankommen, als es bei Einhaltung der Geschwindigkeitsbegrenzung überhaupt möglich wäre. Dass alle fotografierten Fahrzeuge einen Menschen am Lenkrad sitzen haben, der ein „Recht am eigenen Bild“ hat, das hier aber ausgehebelt wird, ist nicht jedem klar. Auch die Video-Überwachung allerorten (an der Haustür, Kaufhäuser, Läden, Banken, Gaststätten, Straßen) setzt sich über das Recht des Einzelnen hinweg und erklärt ihn „vorsorglich“ zum Verdächtigen. Damit wird aber der Rechtsgrundsatz „Im Zweifel für den Angeklagten“ ins Gegenteil verkehrt und jeder Bürger zum Verdächtigen abgestempelt.

Auch bei der Nutzung von Telefon, Mobiltelefon, E-mail, Internet und fast all seinen Diensten werden die Daten gespeichert (und der Nutzer zum Verdächtigen), um im Falle eines Falles hinterher sagen zu können, wer wann mit wem kommuniziert hat und wo Beide sich zu diesem Zeitpunkt befanden. Das erleichtert zwar die Fahndung, löst aber das grundlegende Problem nicht, dass man eigentlich Vorbeugung bevorzugen müsste, die es erst gar nicht zu schweren Rechtsverstößen kommen lässt. Manchmal, das muss auch gesagt werden, helfen die gespeicherten Daten auch Ansprüche der Verbraucher zu belegen (bei Ausfall des Netzes), oder Unschuldige vor Anklagen zu bewahren, etwa, wenn deren Daten missbraucht wurden.

Die Illusion, dass das Internet zu einer weltumspannenden freien Kommunikation führen werde, die den Frieden und das gegenseitige Verständnis fördert, ist längst zerstoben. Einerseits weil es Staaten, wie China, gibt, die das Internet und seine Nutzer zensieren. Andererseits, weil im Internet längst Firmen die Macht übernommen haben, die ihre eigenen Gewinne höher schätzen, als den Nutzen für die Bürger. Nur ein paar Namen: ebay, Amazon, Google (mit Android, Gmail, Google Chrome, Youtube (eine Videoplattform, die dank US-Recht auch der vermutlich größte Hehler von eigentlich urheberrechtlich geschütztem Material ist). Facebook, ein so genannter „Sozialer Dienst“, hat durch Werbung seinen Gründer reich gemacht. Der hat weitere Firmen (Instagram, WhatsApp) gekauft und ist bestrebt diese zu verknüpfen, obwohl er das beim Kauf bestritten hatte. Skype (Bildtelefonie) gehört zu Microsoft, iTunes gehört zu Apple und verkauft vor allem Musik, erledigt aber auch die Synchronisation von Dateien. Die meisten dieser Dienste arbeiten mit Rechenverfahren, bei denen die Daten der Nutzer erfasst werden. Das ist teilweise nicht zu vermeiden, etwa wenn eine Verbindung zwischen zwei Nutzern hergestellt werden soll, ähnlich wie schon früher beim Telefon. Aber in vielen Fällen werden eben auch Daten erhoben, die für das Funktionieren nicht notwendig wären.

Wobei die Firmen natürlich stets so tun, als ob sie ihre – scheinbar kostenlosen – Dienste der Allgemeinheit zur Verfügung stellen. In Wirklichkeit geht es darum Daten der Menschen zu sammeln und sie zu Geld zu machen. Ein Weg dafür ist, dass man die Werbung auf den Nutzer zuschneidet (Apple-Kunden bekommen im Netz Apple-Werbung zu sehen, Microsoft-Kunden

die für Windows, wer eine Vorliebe für bestimmte Farben hat, wird Werbung für Produkte in dieser Farbe bekommen.). Die gezielte Ansprache erspart den Werbenden Aufwand und bringt weitere Erkenntnisse darüber, ob der Nutzer die Werbung wahrnahm, wie lange und ob er sie vielleicht sogar anklickte. Hier wird deutlich, weshalb Suchmaschinen und andere Seiten, etwa Medien, Daten sammeln und das Verhalten der Nutzer analysieren. Je besser die Nutzer durchschaut werden, desto mehr kann man sie durch Werbung (oder auch Software-Roboter) beeinflussen. Und desto mehr Geld geben die Auftraggeber (Werber, oder Politik) denen, die sich die Daten der Nutzer aneignen.

Andreas Geldner schrieb am 25.1.2019 in der Stuttgarter Zeitung unter der Überschrift:

> *Daten und Algorithmen verändern die Wahrnehmung* ***Die Dressur des Menschen***
>
> *„Der Leser wird gläsern. Wer jemals einen Blick auf eines der am weitesten verbreiteten Gratiswerkzeuge zur Analyse des Online-Verhaltens geworfen hat, der kommt aus dem Staunen nicht heraus: Wer welchen Text geklickt hat – das ist ja noch vergleichsweise trivial. Aber die Fieberkurven zeigen auch, woher er kommt, aus welchem Land, aus welcher Stadt, wie alt er ist oder ob er ein Mann ist oder eine Frau. Mit einem Blick ist zu erkennen, aus welchen sozialen Kanälen er auf den Text gefunden hat. Wann liest er, wer ist neu, wer kommt wieder? Und mit wenigen Klicks ist das Ranking perfekt, bis hinters Komma: Vom ersten bis zum zehntausendsten Text lässt sich in Sekundenschnelle säuberlich sortieren, was beim Leser angekommen ist und was nicht. Wenn etwas geklickt wird, kann man schnell reagieren und dem „User" mehr vom populären Gleichen bieten."*

Im Klartext: Der Nutzer bekommt, was er gerne möchte, nicht, was für ihn nützlich wäre. Damit verändert sich seine Sicht auf die Welt. Aber weil er meint, alle bekämen dasselbe (wie früher bei Zeitung, Radio und TV), wie er zu sehen, glaubt er alle müssten die Welt auch so sehen, wie er. Aber sie haben unter Umständen eine völlig andere Darstellung gezeigt bekommen. So entstehen dann Vorwürfe, wie „Lügenpresse", obwohl es die Suchmaschinen und so genannten „Sozialen Dienste" sind, die dem Nutzer das zeigen, wovon sie meinen, dass er es gerne sähe.

Längst sind es nicht mehr nur Suchmaschinen und Medien, die das Nutzerverhalten mit Hilfe von „Big Data" analysieren, sondern auch Läden, die Waren über das Internet verkaufen wollen. Auch sie wollen möglichst viel über ihre Kunden erfahren, natürlich „nur" um sie noch besser bedienen zu können. In Wirklichkeit geht es um Geschäfte, die Geld bringen sollen.

Da der Mensch keinen Sinn hat, mit dem man digitale Daten direkt wahrnehmen könnte, kann man nur mit Hilfe von technischen Hilfsmitteln feststellen, ob Daten abgezogen werden, oder auf das eigene Gerät übertragen werden. Das zu untersuchen ist unbequem und wird deshalb von den Wenigsten gemacht. Vorsichtige Internetnutzer gehen mit einem Firewall und einem Antivieren-Programm ins Netz, dass die Übertragung von Schadsoftware auf das eigene Gerät unterbinden soll und ständig aktualisiert werden muss. Wer das Ausführen von Befehlen (Scripten) auf dem eigenen Rechner unterbinden möchte, wird NoScript aktivieren und staunen, an wen die eigenen Daten alles weiter gegeben werden sollen, wenn man es nicht unterbindet. Wer weiß, dass Werbung häufig als eine Art „trojanisches Pferd" missbraucht wurde, um Schadsoftware zu übertragen, oder wer auch nur den Diebstahl an Lebenszeit durch Werbung vermeiden möchte, benutzt einen Werbeblocker (ungefähr ein Drittel der Nutzer, fast genau so

viele, wie am Briefkasten Werbung ablehnen). Mittlerweile werden die Verfahren, die auch Werbeverweigerern Werbung unterzuschieben versuchen immer raffinierter und der Laie staunt, wenn er sich anzeigen lässt, was im Hintergrund läuft, wenn er eine Seite mit Werbung aufruft.

In jüngster Zeit werden von Programmierern von Webseiten (aber auch Apps, also Programmen) immer öfter Cookies (kleine Softwareschnipsel, die Daten speichern können) benutzt, obwohl diese schon seit Langem als Einfallstor für Schadsoftware berüchtigt sind. Es erscheint dann ein Banner, dass man der Nutzung von Cookies zustimmen solle, oder dies automatisch durch die weitere Nutzung der Seite tue. Wieder ist der Laie, der die Cookies nicht analysieren kann, der Dumme. Zwar kann man im Browser (in dem man die Webseiten betrachtet) einstellen, dass man keine Cookies akzeptiert, aber ob das auch wirklich funktioniert, oder ob man dann die Seite nicht oder nur eingeschränkt nutzen kann, ist nicht sicher.

Cookies dienen unter anderem dazu auszuspionieren von welcher Seite der Nutzer kam und zu welchen Seiten er weiter zieht. Da der Bau einer Webseite immer komplizierter wurde, je mehr Möglichkeiten es gibt, nutzen die meisten Laien die Dienste von Programmierern, wissen also oft nicht einmal, was ihre eigene Webseite mit deren Besuchern macht. Kein Wunder, wenn manchmal Seiten lange zum Laden brauchen, weil da so viel im Hintergrund passiert, für das der Nutzer auch mit seiner Stromrechnung für Router und Rechner bezahlt. Auch Router (Geräte, die die Verbindung zischen Rechner, Telefon und Telefonnetz herstellen) wurden schon angegriffen. Aber viele Anbieter verlangen, dass man den Router ständig am Netz lässt, weil man ja sonst nicht mehr über Telefon, WLAN, etc. erreichbar wäre. Außerdem können die Anbieter so ständig auf den Router zugreifen und neue Software aufspielen, wann es ihnen passt. Der normale Benutzer merkt das gar nicht, außer er geht dabei etwas schief.

Wenn man mal davon ausgeht, dass die meisten Menschen 8 Stunden arbeiten und 8 Stunden Freizeit haben und ebenfalls 8 Stunden schlafen, dann läuft bei ihnen der Router 16 Stunden, in denen er eigentlich ausgeschaltet sein könnte, weil die Leute schlafen, oder am Arbeitslatz sind. Zwei Drittel des Strombedarfes der Router ließe sich also vermeiden, wenn man sie ausschalten würde. Nur kämen dann – wegen der Nutzung des Internets beim Telefonieren (Voice over IP) – eben auch keine Anrufe durch, die den Schlafenden wecken, oder, während der Arbeitszeit, auf dem Anrufbeantworter landen. Wenn man bedenkt, dass der Standby-Betrieb aller Fernseher in Deutschland ein ganzes Kraftwerk erforderte, dann dürfte der Betrieb der Router auch nicht viel weniger Strom verbrauchen. Wie kommen überhaupt die Anbieter dazu dem Kunden vorzuschreiben, dass sie mehr Strom verbrauchen sollen, als eigentlich nötig?

Das klassische Telefon hatte seine eigene Stromversorgung und man konnte damit auch bei Stromausfall telefonieren und trotzdem funktionierten Bildschirme und Beleuchtung.

Diese kurze Übersicht zeigt, dass die Bequemlichkeit alle Bedenken besiegt, dass aber auch die Anbieter viel zu wenig tun, um dem Nutzer zu helfen wirklich nur die Daten heraus zu geben, die notwendig, oder sinnvoll sind. Die unvollständige Übersicht auf der folgenden Seite belegt, dass es viel zu einfach ist, dem Nutzer die Schuld am zunehmenden Datenmissbrauch zu geben:

Liste der Dienste und Daten, bei denen man die Nutzung gründlich überlegen sollte:

Das Internet, das einst als Verbindungsnetz gedacht war, hat sich zu einer Art weltweitem Spinnennetz entwickelt, an dem alles hängen bleibt, was nahe genug kommt. Anders als bei normalen Spinnennetzen, die nur hie und da auf Beute lauern, ist es heute für Durchschnittsbürger kaum mehr möglich sich vom Internet fern zu halten. Natürlich könnte man darauf verzichten, wäre damit aber auch von vielen Dingen ausgeschlossen, denn das Fahrplanbuch der Bahn, wurde längst durch eine elektronische Auskunft ersetzt, an die man eben am Einfachsten über das Internet heran kommt. Versandhaus-Katalogen ging es ebenso.

Ein Mensch wurde 2007 verhaftet und ihm vorgeworfen, er gehöre einer militanten Gruppe an. Was war geschehen? Ein BKA-Beamter hatte durch Eingabe der Begriffe "Gentrification" und "Prekarisierung" einen Hinweis auf diese Person bekommen, aber wohl übersehen, dass diese wissenschaftlichen Begriffe zum beruflichen Wortschatz eines Stadtsoziologen gehören.

Ein Google Manager meinte mal, „Google will die 3 Gehirnhälfte seiner Nutzer werden und ihnen schon beim Anziehen sagen, was sie heute tragen sollen“. Allein das Bild der „dritten Hälfte“ zeigt schon, wes Geistes Kind der Mann ist. Die Aussage bestätigt aber auch den Größenwahn, dass nämlich Algorithmen dem Menschen das Denken abnehmen könnten.

Dass Google sich über die Interessen der Menschen gern hinweg setzt, zeigte sich schon bei Streetview (also der fotografischen Aufnahme vieler Straßenzüge samt deren Gebäuden und der Passanten). Trotz erheblicher Proteste wurden die Aufnahmen angefertigt und zur Verfügung gestellt. Privatsphäre interessiert Google nicht, weil, wie Google in einem Prozess argumentierte es heute sowieso keine Privatsphäre mehr gebe. Die Bürger wurden dazu nicht gehört!

Google gab 2009 bei einer Anhörung zu, dass sie systematisch E-mails analysieren, um so ganz gezielt Werbung an den jeweiligen Benutzer bringen zu können. Apple beantragte 2009 ein Patent, das es einem Betriebssystem erlauben würde nur dann weiter zu arbeiten, wenn der Benutzer zuvor „brav“ Werbung geschaut hätte. Manche Anbieter von Software machen das heute bereits und wer deren Apps (= Application = Anwendung) benutzt, bekommt immer wieder Werbung zu sehen.

Da es bei der Werbung um viel Geld geht (allein für Werbung in Deutschland werden über 21 Mrd. Euro ausgegeben, die natürlich auf die Kunden umgelegt werden, also über 250 Euro pro Kopf und Jahr), lohnt sich das Geschäft für die großen Werbevermarkter, wie Google. Da deren Gewinne um so höher sind, je weniger Aufwand sie treiben, lagern die Daten häufig auf Großrechnern, wo sie Hacker anlocken. Ob auch bei der Sicherheit gespart wird, ist nicht klar, aber sehr wahrscheinlich, denn mehr als 2,2 Mrd. Datensätze von E-mail-Adressen samt deren Passworten sind zur Zeit als „geklaut“ bekannt, also fast jeder Dritte Mensch ist betroffen.

Hier kann man seine E-mail-Adresse prüfen:

Auf deutsch beim Hasso-Plattner-Institut in Postdamm: Webseite

Auf englisch von einem Mitarbeiter von Microsoft: Have I Been Pwned

Beide sind kostenlos!
Warum wird so viel Werbung betrieben? Erstens, weil sie wirkt. Zweitens, weil sie der Kunde bezahlt. Es ist also Ziel derjenigen, die mit Hilfe von Werbung Geld verdienen wollen, das

Verhalten der Kunden zu beeinflussen. Das gelingt nicht immer gleich gut, aber wenn man über genügend Kenntnisse verfügt, kann man jemand ziemlich leicht verführen etwas zu tun, was der eigentlich gar nicht will. Das wissen schon Kinder, die ihre Eltern oder Großeltern um den Finger wickeln, wenn sie von ihnen etwas haben wollen.

Was bei den Kindern meist noch harmlos ist, wird aber problematisch, wenn durch geeignete Werbung das Kaufverhalten, die Politik oder das Wahlverhalten beeinflusst werden soll. Die Werber sagen zwar, dass sie nur das tun, was ihre Auftraggeber wollen, aber das sind in der Regel Leute mit Geld oder Macht oder beidem, wie im amerikanischen Wahlkampf zu sehen war, als man Bots (Roboter, die nur aus Software bestehen und unabhängig im Netz arbeiten) dazu benutzte Menschen vorzugaukeln, sie wären ebenfalls Menschen und hätten gute Argumente für oder gegen einen zur Wahl stehenden Kandidaten. Wenn aber gekaufte Maschinen in einer Demokratie mit darüber entscheiden, wer die nächste Regierung bildet, dann ruiniert das die Demokratie, aber auch das Vertrauen in die Mitmenschen, bei denen man im Netz ja nun nicht mehr weiß, ob das wirklich Menschen sind, oder Software, die nur einen Menschen vorspielt.

Dann entscheidet nicht mehr die Meinung der Wähler die Wahl, sondern – vor allem, wenn die Ergebnisse knapp sind – derjenige, der sich die meisten virtuellen Meinungsmacher (Bots) leisten kann. Dass die frühere Firma Cambridge Analytica Millionen von Nutzerdaten von Facebook bekam, um so Einfluss nehmen zu können, ist der erste Skandal. Der zweite war, dass die Firma sich nicht an die Absprachen mit Facebook hielt. Und der dritte Skandal ist, dass die Firma nicht nur beim Brexit und den US-Wahlen die Finger im Spiel hat, sondern auch beim Niedergang der Demokratien in Afrika. Die Firma hat 2018 offiziell Insolvenz angemeldet, scheint aber unter neuem Namen (Emerdata) weiter zu arbeiten.

Das Beispiel zeigt, wie „Big Data“ benutzt werden können um Demokratien zu schädigen und die Entscheidungen des Einzelnen zu beeinflussen. Wenn aber jemand für mich entscheidet und ich nichts mehr zu sagen habe, dann nennt man das „**Entmündigung**“! Es sieht so aus, als ob es höchste Zeit wäre sich gegen diese schleichende Entmündigung durch die Datenverarbeitung zu wehren und Spielregeln (Gesetze zum Schutz der Bürger) durchzusetzen.

Wenn man auch nur so viel über diese Entwicklung weiß, wie ich hier skizziert habe, dann wird deutlich, dass es bei Autonomem Fahren, bei Industrie 4.0, aber auch beim Mobilfunkstandard G5 nicht nur um Technik geht, sondern auch um Maßnahmen, die zum völlig transparenten Bürger ohne Privatspäher beitragen könnten, also für den Bürger und die Demokratie gefährliche Nebenwirkungen entfalten können. Es versteht sich von selbst, dass derartige mächtige Werkzeuge auch zu erheblichen Schäden führen, wenn sie missbraucht werden.

Das Interesse der Mächtigen am transparenten (gläsernen) Bürger erklärt auch, weshalb so viel Wert darauf gelegt wird diese Techniken rasch einzuführen. Dabei wird übersehen, dass der Bedarf an Rohstoffen und Energie für diese Verfahren so groß ist, dass alle Bemühungen um Energiesparen und Klimaschutz hinfällig werden könnten. Es fehlt schlicht an Technikfolgen-Abschätzung. Sehr wahrscheinlich würde die Umsetzung der kühnen Pläne, die Umwelt stark schädigen, aber keine wirkliche Verbesserung bringen, weil man ja weiß, dass mit wachsendem

Umfang (Komplexität) auch die Fehlerquote steigt. Das gilt für Texte, aber ebenso für technische Systeme.

Da aber, wie eingangs erwähnt, derartige komplexe Techniken und Verfahren für die meisten Menschen kaum gedanklich zu durchdringen sind, passiert viel zu wenig. Der Gesetzgeber erlässt eine „Datenschutz-Grundverordnung“ und weist damit dem Einzelnen eine Aufgabe zu, für die er nicht ausgebildet ist. Außerdem sind die riesigen Mengen an gestohlenen Daten mit großer Wahrscheinlichkeit nicht im mühsamer Kleinarbeit gesammelt worden, sondern, indem man große Systeme knackte (z.B. Yahoo, 2014 wurden 500 Millionen Datensätze gestohlen). Man hat zwar heute mehr Datenschutzbeauftragte (die sich auch sicherlich viel Mühe geben), aber man geht nicht an die Wurzeln des Problems, die man in der Arroganz der Macht der IT-Konzerne suchen müsste. Die Demokratie verträgt es nicht, wenn wirtschaftliche Interessen zu Entscheidungen und Techniken führen, die die Bürger entmündigen.