1 Informationelle Selbstbestimmung ein fast vergessenes Menschenrecht

Axel Stolzenwaldt

1.1 Einleitung

Im Jahre 1983 war ich Betreiber einer kleinen Buchhandlung in einer kleinen Stadt in Hessen. Ein Bestseller in diesem Jahr war die Dystopie "1984" von George Orwell. der eine Diktatur beschreibt, in der die Menschen bis in den privatesten Bereich verfolgt und überwacht werden. Dass dieser Roman in Deutschland damals von vielen gelesen wurde, ließ sich nicht nur auf die Jahreszahl des Titels - 1984 - zurückführen. Vielmehr hat zu dem Erfolg dieses Buches beigetragen, dass 1983 von der damaligen Bundesregierung eine Volkszählung geplant wurde, die alle Bürger bis in kleinste Details ihres Privatlebens ausforschen sollte.

Diese Volkszählung wurde 1983 gestoppt, sie kam wegen der Proteste sehr vieler Bürger gegen die Ausforschung der Privatsphäre nicht zustande. Bestätigt wurde dieser Bürgerprotest durch ein Urteil des Bundesverfassungsgerichts, das in der Volkszählung eine Verletzung des Rechts auf Privatheit und der Freiheit der individuellen Lebensführung sah.

1.2 Was ist "Würde"?

Versetzen wir uns die Zeit des Absolutismus: Ein Landesherr hatte jedes Recht, mit seinen Untertanen zu verfahren, wie er wollte. So vermietete der Hessische Landgraf Friedrich II seine zwangsrekrutierten Soldaten an den britischen König, der die Aufständischen im Unabhängigkeitskrieg in Nordamerika 1776 niederschlagen wollte.

Gegen diese Willkürherrschaft des Adels deklarierten die Vertreter der Aufklärung das Recht jedes Menschen auf Freiheit, Gleichheit und - ja auch das - Brüderlichkeit.

Diese grundlegenden Freiheitsrechte beinhalten auch das Recht auf persönliche Entscheidungsfreiheit und das Recht auf einen geschützten Bereich des Privaten.

Dass diese Rechte auch in neuerer Zeit den Menschen genommen wurden, hat in unserem Land der Nationalsozialismus gezeigt. Die Würde des Menschen, die Achtung seiner grundsätzlichen Menschenrechte wurde während der Herrschaft der Nationalsozialisten und auch in den späteren Jahren in der DDR, mit Füßen getreten.

Vor diesem geschichtlichen Hintergrund erhält im Grundgesetz die Achtung vor der persönlichen Würde und Entscheidungsfreiheit des Individuums einen besonders hohen Stellenwert:

Artikel 1 Absatz 1:

Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

Artikel 2, Absatz 1 und 2:

Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt. Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

Um die Bedeutung der Privatheit für die Würde des Menschen für Sie auch erfahrbar zu machen, möchte ich ein kleines Experiment veranstalten.

Bitte beantworten sie folgenden Fragen wahrheitsgemäß und überlegen Sie sich bitte, ob sie die Antworten öffentlich machen würden

- Was haben Sie heute morgen zum Frühstück getrunken ?
- Haben Sie ein Auto?
- Wie ist der Geburtsname Ihrer Mutter?
- Wo waren sie letzte Nacht?
- Haben Sie schon mal Pornographie geschaut?
- Welche Farbe hat Ihre Unterwäsche?
- Wann haben Sie zum letzten Mal gekifft?
- Werden Sie heute Abend Beischlaf haben?

Ich denke, dass Sie jetzt eine konkrete Vorstellung davon entwickeln können, was "Würde" und "Privatsphäre" bedeuten.

1.3 Geschichte des Datenschutzes

In den 70er Jahre gab es schon vor dem wegweisenden Urteil des Bundesverfassungsgerichts 1983 Datenschutzgesetze.

1970, also zu einer Zeit als von Hessen anders als heute noch Impulse für eine fortschrittliche Gesellschaft ausgingen, verabschiedete der Hessische Landtag das weltweit erste Datenschutzgesetz, dass unter anderem auch die Einrichtung eines Datenschutzbeauftragten beinhaltete.

1983 erfolge das bereits angesprochene Urteil des Bundesverfassungsgericht.

1995 wurde die EU-Richtlinie 95/46/EG veröffentlicht. Richtlinien sind Vorgaben an die Regierungen in der EU, die Inhalte einer solchen Richtlinie in nationale Gesetze umzusetzen. Die Richtlinie 95/46/EG wurde von den Bundesregierungen unter Helmut Kohl und Gerhard Schröder nicht umgesetzt, erst ein Vertragsverletzungsverfahren zwang die Bundesrepublik 2001 zur Umsetzung in ein neues Datenschutzgesetz.

2004 hat das Bundesverfassungsgericht (BVerfG) akustische Wohnraumüberwachung (Großer Lauschangriff) für verfassungswidrig erklärt, weil sie den unantastbaren Bereich privater Lebensgestaltung verletzte.

2006 und die folgenden Jahre gab es immer wieder Versuche sowohl von der EU-Kommission als auch von der Bundesregierung die Vorratsdatenspeicherung einzuführen. Vorratsdatenspeicherung heißt, dass ohne jeden Anlass personenbezogene Daten durch öffentliche Stellen gespeichert werden können, also ohne Anfangsverdacht oder konkrete Gefahr. Der zugrunde liegende Gedanke ist, dass jeder Mensch grundsätzlich verdächtig ist, kriminelle Handlungen vollbringen zu können.

Nach langer Diskussion hat zuletzt 2016 der EUGh (Europäischer Gerichtshof) eine vom EU-Parlament verabschiedetet EU-Richtlinie zur Vorratsdatenspeicherung gekippt. Dies wurde 2016 vom EUGh noch bekräftigt und am 22.6.2017 hat das OLG Nordrhein-Westfalen ein 2015 vom Bundesparlament eingebrachtes Gesetz für illegal erklärt.

2015 wurde das Safe-Harbour-Abkommen zwischen den USA und der EU vom EUGh für ungültig erklärt. Was ist das Safe-Harbour abkommen? Ursprünglich durften personenbezogene Daten gemäß der EU-Richtlinie 95/46/EG (1995) aus der EU nur in Länder übermittelt werden, die ein ähnliches Niveau des Datenschutzes haben wie die EU selbst. Da es in den USA so gut wie keinen Datenschutz gibt, wäre die Übertragung personenbezogener Daten nicht rechtmäßig. Daraufhin wurde eine Vereinbarung zwischen der EU und den USA geschlossen, nach der US-Unternehmen sich freiwillig verpflichten, die Datenschutzstandards der EU einzuhalten. Zur Registrierung dieser Selbstverpflichtung konnten US-Unternehmen sich in eine Liste des US-Handelsministeriums eintragen lassen.

Das Recht auf Vergessenwerden hat der EUGh im Juni 2017 bestätigt. Danach können Nutzerinnen aus der EU von Google, Bing und Co. verlangen, dass Suchanfragen, die ihren Namen enthalten, nicht mehr in den Ergebnislisten angezeigt werden. Wenn dritte Webseiten Informationen von dem betreffenden Nutzer, der betreffenden Nutzerin enthalten, den diese/r nicht mehr im Netz haben will, so muss er/sie sich direkt an den Webseitenbetreiber wenden.

2018 wird die EU Datenschutz-Grundverordnung in Kraft treten. Sie gilt unmittelbar, das heißt, sie ist in allen Ländern der EU sofort gültig und muss nicht erst in nationales Recht umgewandelt werden. Ziel dieser Verordnung ist die Vereinheitlichung der unterschiedlichen Regelungen in der EU. Sie regelt Rechtsgrundlagen der Datenverarbeitung, die Rechte der Betroffenen und die Pflichten der Verantwortlichen sowohl im öffentlichen als auch im privatwirtschaftlichen Bereich. Bei Verstößen gegen diese Verordnung drohen Bußgelder in Höhe von bis zu 4 Prozent des weltweiten Unternehmensumsatzes.

Sie soll insbesondere auch Gültigkeit für Unternehmen haben, die ihren Sitz außerhalb der EU haben, aber ihre Angebote auch an EU-Bürger wenden. Dies zu verhindern gab es umfangreiche Lobbyarbeit vor allem von US-Firmen. Es gab ca. 4000 Änderungsanträge. Sie lehnen das Löschen von personenbezogenen Daten aus Konzerndatenbanken (Recht auf Vergessenwerden) und die ausdrückliche Einverständniserklärung zum Sammeln personenbezogener Daten ab. Sie befürchten einen *California Effect*: Durch strenge Umweltgesetze in Kalifornien wurden die Mindeststandards für den Umweltschutz in allen US-Standards schleichend angehoben. Dieser Effekt würde in der Datenverarbeitung den Datenschutz erhöhen.

1.3.1 Exkurs: Definition Datenschutz

Der Begriff "Datenschutz" wird häufig unklar und manchmal bewusst interessengeleitet verwendet. Dabei werden der Schutz von Daten vor Vernichtung oder Veränderung im Allgemeinen verwechselt mit dem Schutz der personenbezogenen Daten vor Nutzung durch Dritte.

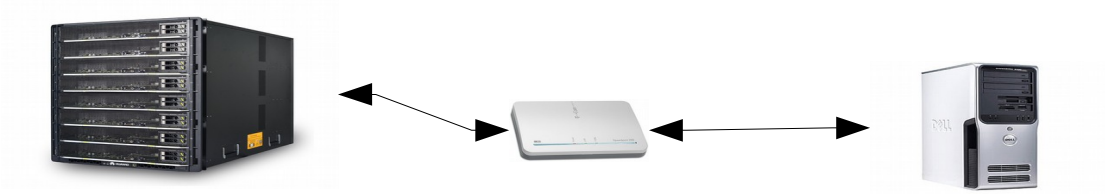
Wenn eine normale Nutzerin ihre Daten vor Verlust schützt, in dem sie eine regelmäßige Datensicherung durchführt, dann hat sie ihre Daten von Vernichtung oder Veränderung geschützt.

Ganz anders liegt der Fall, wenn Daten von Menschen durch andere Menschen und Institutionen gespeichert werden und eventuell an andere weitergegeben werden. Hier erhebt sich sehr schnell die Frage, wem diese personenbezogenen Daten gehören und wer was mit welchem Recht vor dem Zugriff durch Dritte schützt.

1.4 Aktuelle Praxis

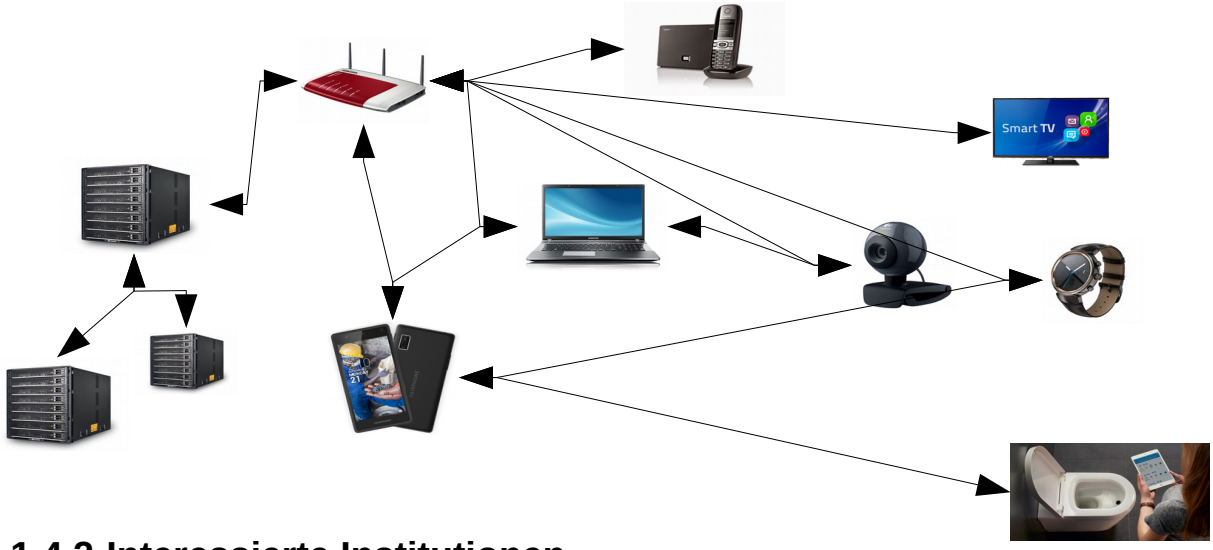
1.4.1 Quellen der Datenströme

In der Steinzeit des Internets, also etwa Anfang der 90er Jahre, gab es einen Zugang zum Netz über ein Modem, das den PC mit dem Netz verband. Es war die Zeit, als Daten mit höchstens 9600 bit/s durch die Telefonleitung krochen. Es war also in der Regel eine einfache Konstellation:



Mittlerweile hat sich die Situation grundlegend geändert: Es ist ein ganzer Gerätezoo, in dem wir Nutzer uns bewegen: zum einfachen PC kommen noch Laptops, Tablets, Assitenten (Siri, Echo, Alexa), das vernetzte Auto, Smartphones, Smart-TV, Smart-Meter und noch vielmehr Smart-Tralala dazu.

...heute IoT (Internet of Things)



1.4.2 Interessierte Institutionen

Wer also ist an den Daten, die unsere Persönlichkeit ausmachen, interessiert? Welche Zwecke werden mit der Speicherung von Daten verfolgt?

Zwei große Bereiche können wir unterscheiden: Staatliche Institutionen und die Privatwirtschaft, hier insbesondere die Digitalwirtschaft.

1.4.2.1 Staat

1.4.2.1.1 Polizei

Natürlich hat die Polizei ein großes Interesse, Daten zu Personen zu erheben und zu speichern, die kriminell geworden sind oder bei denen ein Verdacht besteht, dass sie kriminell werden könnten. In

diesem Zusammenhang ist das Speichern und Verarbeiten von personenbezogenen Daten unter genau definierten Bedingungen legitim, da damit der Schutz der Gesellschaft verbessert werden kann. Wie allerdings eine falsche oder unzureichende Formulierung dieser Bedingungen zu gravierenden Verletzungen der Menschenrechte führen kann, werden wir später noch hören.

1.4.2.1.2 Geheimdienste

Aufgabe der Geheimdienste in Deutschland ist, Personen oder Gruppen in der Gesellschaft ausfindig zu machen, die gegen die Grundordnung der Bundesrepublik verstoßen. Dafür sollen sie neben der Beobachtung öffentlich erhältlicher Daten in die Lage versetzt werden, auch im Geheimen Daten über Personen zu sammeln und diese Daten auszuwerten. Auch hier gilt, dass eine genaue Definition der Speicherung und Verarbeitung der Daten zwingend notwendig ist.

Sowohl bei der Polizei als auch bei den Geheimdiensten sollte eine Kontrolle durch Betroffene und Parlamente umfassend möglich sein. Dass Geheimdienste die Parlamente und Regierungen belogen und betrogen haben, konnte man nach den Snowden Veröffentlichungen und bei der Untersuchung der NSU-Morde deutlich sehen.

Zur Zeit wird in Hessen ein neues Verfassungsschutzgesetz im Parlament diskutiert. Ein wichtiges Problem steht dabei im Vordergrund:

Wenn Software zur Quellen-TKÜ (Telekommunkationsüberwachung) oder für die Online-Durchsuchung eingesetzt werden soll, ist es für die Geheimdienste erforderlich, dass diese Software durch Sicherheitslücken einen Zugang zum elektronischen Gerät des zu Überwachenden erhält. Wenn Geheimdienste diese Sicherheitslücken nicht den Herstellern melden, sind alle Systeme unsicher, die diese Lücken aufweisen. Dies gibt Crackern die Möglichkeit, auf fremden Geräten Schadcode auszuführen.

Geschehen ist dies im Mai diesen Jahres: Der Virus "Wanna Cry" befiel rund 230.000 Rechner weltweit mit Verschlüsselungssoftware. Betroffen waren unter anderem die Deutsche Bank, Banco Bilbao, Nissan, Renault, Fedex und das NHS (Natinoal Health Service)in Großbritannien. Genutzt wurde die Sicherheitslücke über fünf Jahre von der NSA, ohne dass diese den Hersteller der sicherheitskritischen Software, "Microsoft" informierte.

Selbst bei Organisationen, die eigentlich unsere Sicherheit erhöhen sollten, können wir daher nicht auf die Absicherung unserer Geräte vertrauen.

1.4.2.1.3 Weitere Interessenten

- Finanzämter
- Agentur für Arbeit
- Kommunale Verwaltungen
- Schulen
- Universitäten
- ...

Bei allen diesen Institutionen gibt es relativ strenge Handhabung des Verfassungsschutzes, wenn auch dieses nicht perfekt ist.

1.4.2.2 Große IT-Anbieter

Wenden wir uns dem vom Umfang der abgefischten Volumen an Daten wesentlich größeren Bereich der Privatwirtschaft zu. Zuerst sind hier die großen Firmen zu nennen, mit denen wir direkt zu tun haben.

Besonders bekannt sind die "Inglorius Bastards of the Internet":

- Apple
- Microsoft
- Amazon
- Facebook (Instagram 2012, Whatsapp- , Oculus VR - 2014, wit.ai (Spracherkennung)- 2015, face.com (Gesichtserkennung) 2012)
- Google
- Snapchat: web beacons (Web-Wanze)

Diese großen Player sammeln Daten und behalten sie meistens im eigenen Zugriffsbereich, weil die gesammelten Daten und die daraus abgeleiteten Informationen ihr Kapital , ihre Geschäftsgrundlage sind, die sie nicht so ohne weiteres hergeben.

1.4.2.3 Datenhändler

Anders sieht die bei den großen Adress- und Datenhändlern aus. Das Geschäftsmodell dieser Firmen beruht darauf, möglichst detailliert personenbezogene Daten einzusammeln und durch möglichst viele beschreibende Merkmale die Daten zu Personen wertvoll zu machen und dann an interessierte Firmen oder andere Institutionen weiter zu verkaufen. Die Firmennamen kennt man kaum, aber unsere Daten sind dort vielfältig gespeichert und ausgewertet.

- AZ Direct
- Deutsche Post Direkt
- Schober Information Group
- Acxiom

Wer sammelt die Daten für diese Datengroßhändler?

Wer sich in der spanischen Küche auskennt, weiß was ein Pulpo ist: Eine Krake, wenn sie gut zubereitet ist eine Leckerei. Es gibt aber auch die Chipirones, die Minikraken. Und so gibt es hundertausende Minidatenkraken, die ihre Daten an die großen Datenhändler verkaufen.

Mehr noch als bei den großen Platzhirschen des Datensammelns wird bei diesen Unternehmen deutlich: Wir sind nicht die Kunden, wir sind die Ware.

1.4.2.4 Übrige Wirtschaftsunternehmen

Neben den Firmen, die direkt mit Daten umgehen oder sie verwerten, gibt es noch weitere Abnehmer der aufgewerteten Daten.

- Banken
- Schufa
- Versicherungen
- Autoindustrie

- ...

Hier geht es also nicht um die direkte Ausnutzung von Daten, um diese gewinnbringend einzusetzen. Daten dienen hier den jeweiligen Geschäftszwecken, die über reine Datenverwertung hinaus gehen.

1.4.3 Techniken der Datengewinnung

Die Gewinnung von Informationen aus Daten geschieht grundsätzlich auf zwei Wegen:

Einerseits werden Daten von Personen mit Hilfe elektronischer Geräte wie Laptop, Smartphone, Internet of Things direkt abgeschöpft. Andererseits werden aus den direkt abgeschöpften Daten der Nutzerinnen Meta-Informationen gewonnen, bekannt sind dazu die Schlagworte Big-Data und Algorithmen.

1.4.3.1 Direktes Abschöpfen durch IT-Geräte

Im Folgenden werde ich einige Methode darstellen, wie Daten von den NutzerInnen abgeschöpft werden.

1.4.3.1.1 Cookies

Das Verfahren ist Ihnen allen sicher bekannt: Wenn Sie auf ihrem Laptop oder Smartphone eine Seite aufrufen, erzeugt diese Seite auf Ihrem Rechner eine kleine Datei. Diese dient dann dem Betreiber der Website, das Surfverhalten des Nutzers zu kontrollieren, zu steuern oder auch Daten über die Nutzung auf den Server des Webseitenanbieters hochzuladen. Welche Daten in einem Cookie gespeichert werden, ist für den Nutzer/die Nutzerin nicht erkennbar.

1.4.3.1.2 Browser-Tracker

Rufen Sie eine Website auf, werden die Nutzungen auch über sogenannte Tracker-Software verfolgt. Die bekannteste und am häufigsten eingesetzte Tracking-Software ist googleAnalytics, sie übermittelt umfangreich Daten über das Nutzungsverhalten an den Webseitenbetreiber. Aber es gibt auch noch weitere Mithörer: ioam, adsense(Google), plista, ...

1.4.3.1.3 App-Tracker

In vielen Smartphone-Apps sind Tracker eingebaut, die zum Teil umfangreich Daten für Drittfirmen einsammeln. Zu den Daten gehören sehr häufig Standortbestimmungen, Surfverhalten, Adressbücher (Whatsapp), Terminkalender,...

1.4.3.1.4 Web-Beacons

Beim Aufruf einer Webseite wird oft ein kleines 1x1 Pixel großes Bild mit übertragen. Webseitebetreiber oder Dritte, die vom Webseitenbetreiber den Zugang zur Webseite erhalten haben, können auf diese Weise das Surfverhalten speichern und kontrollieren

1.4.3.1.5 IoT (Internet of Things)

Die größten Lücken in der Sicherheit von Nutzerinnen haben sich in den letzten Jahren in der Verwendung des IoT aufgetan. Web-Cams, Home-Automations-Geräte, Echo,..., sie alle haben häufig ein eigenes Betriebssystem und Webschnittstellen, die nicht gesichert sind. Es ist keine

Seltenheit, dass Daten unverschlüsselt über das W-LAN übertragen werden oder dass der Zugang dieser Geräte über den User "admin" und das Passwort "admin" möglich ist. Ein wahrlich sicherer Zugang für Dritte. Aber auch die Übersendung von Daten von einem Gerät an der Hersteller findet oft ohne Wissen der Nutzerin statt.

Ein wenn auch extremes Beispiel für die Übertragung von Daten ist der Vibrator "Svakom Siime Eye" der unter anderem mit einer Kamera ausgerüstet ist. Um den Livestream vom Vibrator im W-LAN zu verfolgen ist lediglich das Passwort 88888888 nötig. zusätzlich kann man die gewonnenen Bilder auch in die Cloud hochladen, z.B. nach Snapchat.

1.4.3.1.6 Was wird abgerufen

Bisher haben wir nur abstrakt dargestellt, dass Daten übermittelt werden. An drei Beispielen möchte ich darstellen, in welchem Umfang Daten auf diversen Servern landet.

Snapchat

sammelt ein:

- welche Filter sie einsetzen,
- welche Channels man anschaut
- welche Suchanfragen man absetzt,
- ja allgemein: mit wem man wann wieviel kommuniziert und was man mit den Nachrichten macht.

es wird gespeichert,

- was sie auf der Website von Snapchat eingeben,
- ob Ihre Eingabe angeschaut wurde
- sowie weitere Metadaten (Das kann alles mögliche sein, Snapchat lässt sich alle Möglichkeiten offen)

Auch das von Ihnen genutzte Gerät wird untersucht:

- Welche Smartphonemarke Sie benutzen
- das Betriebssystem
- Verwendeter Speicher
- Geräte ID für Werbezwecke
- eindeutige App-ID
- Geräte ID,
- Welche Apps installiert sind,

- Browsertyp
- Sprache
- Batteriestand
- Zeitzone
- die in einem Handy üblichen Sensoren wie Beschleunigungssensor, Lagesensor, Kompass, Mikrophone (!!!)
- Ob Kopfhörer angeschlossen sind.
- W-LAN Informationen
- Telefonverbindungen
- Signalstärke
- Kamera
- Standort
- Besuchte Internetseiten
- IP-Adresse

Darüber hinaus können alle diese Daten mit Daten anderer Snapchatbenutzer verknüpft werden.

Snapchat behält die Daten nicht für sich, es stellt diese Daten anderen zur Analyse und Verfolgung zur Verfügung. Die auf Snapchat hochgeladenen Bilder sind zwar nicht mehr sichtbar, aber alle weiteren Informationen sind auf den Speichern von Snapchat vorhanden. Mit Snapchat verbundene Bilder bleiben auf dem Gerät selbst erhalten.

Ganz allgemein gesprochen sind die Datenschutzklauseln bei Snapchat so allgemein gehalten, dass Snapchat mit den Daten alles machen kann, was es will.

Microsoft

Microsoft(1) - Windows 10:

Ähnlich ist die Situation, wenn Sie Windows 10 nutzen: Wenn sie nicht ausdrücklich in den Einstellungen zur Privatsphäre bestimmte Sperreinstellungen vornehmen, dann sammelt Microsoft folgende Daten ein:

- Gerätedaten (Prozessor, Kamera, Speicher,...)
- Netzwerkverbindungen (IP, Provider,...)
- Konfiguration des Betriebssystems (Spracheinstellungen, angeschlossene Geräte, ...)
- Benutzte Programme (Word, Filezilla, PDF-Reader,...)
- Angeschaute Filme

- Browsernutzung, Browserhistorie
- Kamera und Mikrophon sind grundsätzlich offen
- Cortana lauscht mit: Kalenderereignisse, Interessen, Standorte, Eingabeverlauf
- Kontakte sind im Zugriff durch Anwendungen

Microsoft ist allerdings zu Gute zu halten, dass man diese Voreinstellungen, anders als bei Snapchat, ausschalten kann. So lassen sich auch Daten, die von Cortana an Microsoft übermittelt wurden, wieder löschen.

Microfsoft(2) - Azure Application Insights

Wenn man auf Grundlage von Microsofts Cloud "Azure" eine Anwendung zur Nutzung anderen Menschen zur Verfügung stellt, kann man als Entwickler folgende Daten auswerten:

- allgemeine Benutzerstatistik
- Nachverfolgen einzelner Sitzungen von Benutzern
- Analysieren, welche Benutzer die Anwendung nutzen
- Analysieren des Benutzerflows

1.4.3.2 Indirektes Ausforschen (Metadaten)

Was aber fangen die Datensammler mit dem ungeheuren Berg an Daten an, um Informationen zu gewinnen? Die Stasi zu den Zeiten der DDR war teilweise funktionsunfähig, weil sie mit den ungeheuren Mengen an Daten über ihre Bürger nichts anfangen konnte. Erst wenn solche Daten strukturiert und ausgewertet sind, können sie für Kontrolle oder Einflussnahme genutzt werden.

1.4.3.2.1 Exkurs Big Data - KI

Die Strukturierung und Auswertung von Daten wird oft mit den Schlagworten von Big-Data und Algorithmen beschrieben. Was Big-Data bedeutet, ist deutlich geworden, als wir uns angeschaut haben, welche Daten eingesammelt werden.

Die Bearbeitung der gigantischen Datenbestände wird mit dem Ziel der Mustererkennung und Prognose aufgrund von Wahrscheinlichkeitsrechnung (Bays'sche Formel der bedingten Wahrscheinlichkeit) vorgenommen.

Grundlage dieser Verfahren sind in der Regel die "Neuronalen Netze". Es handelt sich um eine grob vereinfachende Simulation der Neuronenverknüpfung im menschliche Gehirn.

Dabei bilden die Hirnzellen in einem gerichteten Netz die Knoten, die Synapsen werden als gewichtete Kanten modelliert. Wie das Zusammenspiel dieser Knoten, die Änderungen in den Gewichtungen der Kanten und die Verarbeitung der Daten in den Knoten stattfindet, wird durch Algorithmen gesteuert.

Einem solchen System werden die zu untersuchenden Daten vorgegeben. Aber: Das fällt nicht vom Himmel. Es sind Menschen - Teams, einzelne Entwickler, Manager, Politiker, Sachbearbeitungen,

Fachabteilungen - die entscheiden, welche Daten ausgewertet werden sollen. Mit der Auswahl der zu bearbeitenden Daten gehen Wertvorstellungen, Ziele, Zwecke in die KI ein, die von Menschen, Firmenzielen, politischen Vorgaben bestimmt werden.

Genauso verhält es sich mit den Algorithmen. Da heißt es "Algorithmen beherrschen uns", "Wider die Herrschaft der Algorithmen", "Algorithmen sind gefährlich". Nonsens!! Algorithmen sind nichts anderes als Berechnungsverfahren. Wenn ein Kind in der Schule lernt, wie man schriftlich multipliziert, dann lernt es einen Algorithmus. Wenn ich nach einem Rezept eine neue Art von Tomatensoße koche, dann führe ich einen Algorithmus aus.

Das bedeutet, dass Algorithmen von Menschen gemacht sind und von Menschen angewandt werden. Es ist immer die Entscheidung desjenigen, der ein neuronales Netz programmiert, welchen Algorithmus er verwendet. Auch hier, wie bei der Auswahl der Daten, spielen wirtschaftliche, politische, interessengeleitete Vorgaben eine Rolle, welche Algorithmen bei der Anwendung eines neuronalen Netzes angewandt werden.

Und da landen wir bei dem, was seit jeher ein Grundprinzip der Anwendung von Software ist: Das GIGO Prinzip "Garbage in - Garbage out". Wenn die Auswertung von Daten auf unzureichend vorbereiteten Datengrundlage beruht oder die falschen Algorithmen ausgewählt wurden, bekommt man nur sehr bedingt vernünftige Informationen heraus.

Damit wird auch unsere Ausgangsfrage deutlich: Was ist "informationelle Selbstbestimmung"? Wenn ich nicht weiß, wer die Auswahl der Daten, die mich betreffen, und die Bestimmung Algorithmen, die Auswirkungen auf mein Leben haben, wie kann ich dann selbstbestimmt leben?

Wie können wir uns gegen den Identitätsdiebstahl wehren, der täglich von den großen und kleinen Datenkraken durchgeführt wird?

Was kann ich machen, wenn ich aufgrund fehlerhafter Auswahl von Algorithmen falsch charakterisiert werde?

1.4.4 Verwendung

Unbestritten ist die Nützlichkeit neuronaler Netze und die Auswertung von Daten. Besonders in der Forschung, aber auch im Einsatz in der Industrie, bei Verkehrsproblemen, Optimierungen von Verwaltungsabläufen. Wichtig ist aber immer: Wer setzt diese Technologie ein, welche Daten bilden die Basis, welche Algorithmen werden angewandt und ist eine wirkliche Qualitätssicherung vorhanden.

1.4.4.1 Staat

1.4.4.1.1 Polizei

Wenn die Speicherung von personenbezogenen Daten von potentiell kriminellen Personen in Beziehung gesetzt wird mit Ergebnissen einer "Predictive Policing" Software auf Grundlage von Neuronalen Netzen, die nicht vollkommen von den benutzenden Poizeibehörden verstanden wird, besteht die Gefahr der Fehlinterpretation.

Dass Polizeibehörden nicht immer fehlerfrei in ihren Interpretationen sind, haben leider die Morde des NSU gezeigt: Die Ermordeten wurden einfach zu Tätern gemacht, indem man vermutete, dass

sie in einem kriminellen Umfeld tätig gewesen seien und/oder es sich um Rachemorde gehandelt habe.

Die hessische Landesregierung hat übrigens die Eigenentwicklung einer solche Vorhersagesoftware in Auftrag gegeben. Zu untersuchen wäre sicherlich, wie die Datenbasis dieser Software gebildet werden soll und welche Algorithmen genutzt werden sollen. Und eine weitere Klärung wäre notwendig, in welchen Bereichen diese Software zur Predictive Policing eingesetzt werden soll. Ob da z.B. auch Wirtschaftskriminalität mit beobachtet wird?

Problematisch ist die Einbeziehung privatwirtschaftlicher Unternehmen in die polizeiliche Arbeit mit massenhaft gespeicherten Daten. So wurde am 30.10 bekannt, dass die Bayerische Polizei eine Privatfirma beauftragte, kinderpornographisches Material zu sichten . Diese Firma wiederum hatte Mini-Jobber eingestellt, um diese Arbeit erledigen zu lassen. Offen natürlich ist die Frage, in welchen Bereichen mit welchem Ergebnis die Polizei Mini-Jobber welche Daten auswerten lässt.

1.4.4.1.2 Geheimdienste

Natürlich sind die spektakulären Offenlegungen der Tätigkeiten der Geheimdienste durch Snowden bekannt..

Aber auch in Deutschland verstoßen die Geheimdienste permanent gegen bestehende Gesetze. Bereits im Juli 2015 hat dies die Datenschutzbeauftragte der Bundesregierung den BND gerügt. In einer weiteren Untersuchung 2016 hat sie 18 massive Rechtsverstöße festgestellt, "die herausragende Bedeutung haben und Kernbereiche der Aufgabenerfüllung des BND betreffen".

1.4.4.2 Privatwirtschaft

Große Firmen sind nicht primär wie Regierunge an einer funktionierenden Staatsgewalt und Gesellschaft interessiert. Sie haben die Aufgabe, Gewinn zu erwirtschaften und daher ist ihr Vorgehen anders und auch anders zu bewerten.

1.4.4.2.1 Werbung

Hauptzweck der Datensammelei der Wirtschaftsunternehmen ist Werbung zur Umsatzsteigerung. Die Beeinflussung des Nutzerin hat zum Ziel, weitere Umsätze zu generieren.

Dabei gibt es zwei Wege:

Zum einen die direkte Ausnutzung von Nutzungsdaten wie zum Beispiel Amazon. Wer hat sich nicht schon einmal beeinflussen lassen, wenn man ein Buch gekauft hat und gesehen hat, was es sonst noch in der Richtung gibt?

Durch indirekte Ausnutzung Ansprache an mögliche Kunden. Dies tritt uns z.B entgegen, wenn wir auf eine Website gehen und dann dort auf unsere Person ausgerichtete Werbung sehen. Das ist auch bei der Nutzung von Bots bei Facebook oder Twitter der Fall. Wer ist wirklich frei in seinen Entscheidung, wenn er/sie zielgerichtete Werbung über E-mail erhält?

Bei allen diesen offenen und verdeckten Werbemaßnahmen sollte man sich klar machen, dass die Angebote ein Ausschnitt aus der gesamten Realität sind. Amazon zeigt nur Bücher, die durch Amazon beziehbar sind, Google zeigt nur die Suchergebnisse, die in seinen Speichern vorhanden sind.

1.4.4.2.2 Nudging

Die Daten über unser Verhalten führen nach dem Ansatz der Verhaltensökonomie zu einem rationaleren und für das Individuum vorteilhafteren Verhalten.

So hat die Generali Versicherung 2014 eine App entwickelt, die das Verhalten der Versicherten beobachten und an die Versicherung übermitteln soll. Menschen, die sich gesünder verhalten, sollen auf Grundlage von Big-Data und algorithmischen Auswertungen Vergünstigungen erhalten. Nun ist es aufgrund des Geschäftsmodells einer Versicherung sicher legitim, Risikobewertungen vorzunehmen und darauf abgestimmt die Versicherungsprämie zu berechnen.

Neu ist, dass das individuelle Verhalten ständig vermessen wird, dass die Auswertung in Echtzeit geschieht und dass es zu einer zielgerichteten ökonomischen Sanktionierung kommt. Kürzere Perioden "ungesunden Verhaltens" (dreimal hintereinander Party während der Karnevalszeit gemacht) führt sofort zum Verlust von Vergünstigungen.

Und die Verwendung einer App erzeugt bei leichtgläubigen Menschen, unter den Anhängern der Datenglaubens, den Eindruck: Die Daten sagen es aber, da kann man keine Zweifel haben.

Wir sollten uns aber erinnern: Die Auswahl der gemessenen Parameter und die Algorithmen sind von Menschen, Teams, Managern ausgewählt auf Grund der Interessen der Firmen. Es gehen also die Firmeninteressen und mögliche Fehler mit ein.

1.4.4.2.3 Weltverbesserung und Zensur

Mark Zuckerberg:

Im Frühjahr diesen Jahres hat Mark Zuckerberg, der Chef von Facebook, ausführlich dargelegt, was für ihn die Ziele sind, die er mit Facebook verfolgt. Wenn man das liest, kann man den meisten Forderungen zustimmen: Meinungsfreiheit, Solidarität, Hilfe bei Katastrophen. Leider entspricht das nicht der realen Machtausübung facebooks.

Zwei Beispiele:

1. Anzeigen, die man in facebook veröffentlichen will, können bewusst bestimmten Zielgruppen vorenthalten werden. So wurde in New York von Aktivisten testweise die Annonce für eine Mietwohnung aufgegeben. Mitglieder von facebook, die Hispanics, Afro-Amerikaner oder Asiaten waren, wurden von der Ansicht dieser Anzeige ausgeschlossen.

2. Facebook zensiert alle Bilder, die weibliche Nacktheit zeigen. Eine moralische, puritanische Vorstellung, die in den USA weit verbreitet ist und sich von dern europäischen Menschenbild unterscheidet. Dies führte dazu, dass das Bild eines Mädchens, das vor dem Napalmangriff einer US-Mililtäreinheit im Vietnamkrieg flüchtet, aus facebook entfernt wurde.

Larry Page:

Google baut mit Larry Page an der Spitze an einer Gesellschaft, in der alle Ereignisse und Vorgänge durchgehend digitalisiert und technisch begründet sind. Geprägt ist dies von einem starken Glauben

an den Fortschritt der Technik. Es ist auch der Glaube daran, dass die perfekte technische Welt auch die Welt ist, die den Menschen den höchsten Grad an Freiheit gibt.

Anders als Apple sucht Google die Auseinandersetzung über die weitere Entwicklung der Technik auch mit seinen Kritikern.

Trotzdem bleibt ein totalitärer Anspruch, alles aus der Sicht des Konzerns lösen zu können. Der Wahlspruch "Don't be evil" definiert, dass alles, was Google tut, gut ist. Allerdings fehlt dann die Definition, was Google unter Böse versteht.

Und da hat Google doch ein paar schwarze Flecken: Steuervermeidung in Europa, Mangel der internen Diskussionskultur, Monopolstellung bei den Suchmaschinen.

Über den Google Browser Chrome. Android, Youtube, Google Home sammelt Google so viel Daten ein, wie kein anderer Konzern weltweit. Ziel ist, den vollkommen berechenbaren Nutzer, dem man sagen kann, was für ihn gut ist: "The goal is to enable Google users to be able to ask the question such as ‘What shall I do tomorrow?’ and ‘What job shall I take' " (Eric Schmidt, früherer Chef von Google)

Beide, Zuckerberg und Page, mögen gute Vorsätze haben, die Umsetzung aber führt zu einer Entmündigung der Menschen. Freie Entscheidung, die Grundlage einer demokratischen Entwicklung und das, was den Menschen ausmacht, wird auf diese Weise ausgehöhlt.

So lange die gespeicherten Informationen und deren algorithmische Verwendung nicht von mir einsehbar und kontrollierbar sind, ist der Kernbereich der menschlichen Autonomie gefährdet.

Und noch eine abschließende Frage ist offen: Zur Zeit werden diese Daten nicht zur direkten Unterdrückung genutzt. Was ist aber, wenn diese Daten, wie dies zur Zeit in China geschieht, von kommenden Generationen von Managern und Politikern genutzt werden, um deren wirtschaftliche und politische Ziele durchzusetzen?

Zu glauben, dass das wohl nicht passieren wird, ist reichlich naiv.

1.5 Konsequenzen

Die wichtigste Konsequenz:

- Denken Sie selbst.
- Lassen Sie sich nicht von KI, Algorithmen, Datengläubigkeit beeindrucken.
- Verfallen Sie nicht in das bequeme Gegenteil, dem Anhängen an Verschwörungstheorien.
- Gehen Sie den steinigen Weg, jedes Mal neu zu schauen:

  Was kann ich wissen?
  Was soll ich tun?
  Was darf ich hoffen?
  Was ist der Mensch?

Und was kann ich ganz konkret machen ? Hier ein kleine Auswahl:

1.5.1 individuell

- Datensparsamkeit
  - z.B. DuckDuckGo statt Google
  - Coockies ausschalten
  - Reduzierung der Nutzung von Instagram, Snapchat, facebook, Whatsap,...
- Technische Vorkehrungen treffen
  - Adblocker im Browser
  - Verschlüsselung der Mail
- Daten anfordern
  - Daten von Datensammlern anfordern (wird ab 25. Mai 2018 leichter)
- Sich informiern

1.5.2 gesellschaftlich

- Öffentlich diskutieren
  - Freunde
  - Familie
  - Foren
  - Versammlungen
  - Universitäten
  - Meinung äußern
- Initiativen unterstützen
  - Chaos Computer Club
  - Initiave "none of your business" ("geht Dich nichts an")
  - Digitale Gesellschaft

1.6 Schlusswort

Ich habe jetzt so viel Schreckliches erzählt, da könnte es einem wirklich grausen. Aber

"Wo aber Gefahr ist, wächst das Rettende auch." (Hölderlin, Patmos)

Lassen Sie sich den Spaß an der Nutzung neuer Medien, am Programmieren, an der Entwicklung neuer Ideen nicht verderben.

Ich persönlich fange jetzt an, mit dem Raspberry Pi zu experimentieren, gleichzeitig lerne ich Python und beschäftige mich mit den Grundprinzipien neuronaler Netze.

Viel Spaß bei Ihren Experimenten und Erfahrungen.

1.7 Links

Einige wenige Hinweise:

1.7.1 Inglorius Bastards:

Snapchat: https://www.snap.com/en-US/privacy/privacy-policy/
Windows: https://docs.microsoft.com/de-de/azure/application-insights/app-insights-tutorial-users

1.7.2 Adresshändler:

http://www.az-direct.com/site/
http://schober.de/analytics/

1.7.3 Schutzsoftware:

Firefox Addons:

- uBlock Origin
- Lightbeam

1.7.4 Totes Holz

Steffen Heuer/Pernille Tranberg: "Mich kriegt ihr nicht!"
Yvonne Hofstetter: "Sie wissen alles : wie Big Data in unser Leben eindringt und warum wir um unsere Freiheit kämpfen müssen"

1.7.5 Sonstiges

https://www.golem.de/news/fraunhofer-fokus-metaminer-soll-datensammelnde-apps-aufdecken-1711-131291.html
https://digitalegesellschaft.de/
http://www.tagesschau.de/inland/bnd-315.html