Hans G. Zeger[1],

Big Data statt Big Brother - Endlich Schluss mit Privatsphäre!

Warum gibt es überhaupt Datenschutz/Privatsphäre? - Datenschutz war historisch die Abwehr der Gefahr der Diktatur einer technischen Elite - Kombinatorik, Wahrscheinlichkeitsrechnung, Scoring und Vorratsdatenaufzeichnung sind Vorboten von Big Data - das "Real-Individuum" wird durch das "Funktions-Individuum" abgelöst - unser bisheriges Verständnis von Individuum und persönlichen Daten wird in einer Big Data - Gesellschaft obsolet - Welche Antworten kann/soll eine den Grundrechten verpflichtete Gesellschaft geben?

Sehr geehrte Damen und Herren,

erlauben Sie mir vorab einige grundsätzliche Anmerkungen zum Themenkomplex Überwachung, Datenschutz und Privatsphäre, ich werde dann zu den spezifischen Big-Data Fragestellungen kommen.

IDEE DER PRIVATSPHÄRE

Europa hat eine rund 350-jährige Erfolgsgeschichte der Grund- und Menschenrechte hinter sich. Von der amerikanischen Unabhängigkeitserklärung (1776), der Französischen (1789) und der bürgerlichen (1848) Revolution, dem Staatsgrundgesetz in Österreich (1867), der UN-Charta der Menschenrechte (1948) bis in die Gegenwart reicht die Entwicklung der Menschenrechte.

Die Idee, das Menschen Privatsphäre haben, ist ein modernes Konstrukt und wurde 1890 erstmals öffentlich formuliert. Samuel D. Warren und Lois D. Brandeis, zwei Bostoner Anwälte veröffentlichten in der Harald Law Review den Artikel "The Right of Privacy".

Kern der Argumentation ist das Recht "allein gelassen zu sein" ("the right to be let alone"). Lange vor dem Computereinsatz entstand damit die Idee einer individuellen Privatsphäre.

Aufgenommen wurde dieser Gedanke auch in der Europäischen Menschenrechtskonvention, 1950 verabschiedet, ist sie in Österreich seit 1958 in Kraft. Im Artikel 8[2] wird dieser Anspruch auf Privatsphäre formuliert: 'Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.'

Diese Konstruktion der Privatsphäre bereitete bis Anfang der 70er-Jahre kaum Schwierigkeiten. Eingriffe in die Privatsphäre wurden als physische Übergriffe staatlicher Organe, ungerechtfertigte Hausdurchsuchungen, Zensurmaßnahmen und persönlich durchgeführte Observation verstanden. Die Erhaltung der Privatsphäre war eine mehr oder minder persönliche Auseinandersetzung von Individuen mit greifbaren Staatsorganen.

---

1 Lektor am Juridicum Wien, Mitglied des Datenschutzrates im Bundeskanzleramt und Geschäftsführer der "e-commerce monitoring GmbH", Obmann der "ARGE DATEN - Österreichische Gesellschaft für Datenschutz", Studium Philosophie, Mathematik, Sozialwissenschaften, Autor von "MENSCH.NUMMER.DATENSATZ. Unsere Lust an totaler Kontrolle", Residenzverlag 2008, "Paralleluniversum Web2.0", Kremayr&Scheriau 2009 und zahlreicher weiterer Fachpublikationen (http://www.zeger.at)

2 Der MRK-Artikel komplett: 'Artikel 8 - Recht auf Achtung des Privat- und Familienlebens
(1) Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.
(2) Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.'

GEFAHR DER TECHNISCHEN DIKTATUR

Erst mit der Ausbreitung der EDV Anfang der 70er-Jahre wurde die Idee der Privatsphäre neu hinterfragt. Die scheinbar grenzenlosen Speichermöglichkeiten der Computer ließen die Befürchtung aufkommen, dass es einmal möglich sein müsste, alles über einen Menschen zu wissen oder - wie es ein deutscher Innenminister Ende der 70er-Jahre formulierte - vor dem Täter am Tatort zu sein.

Eine Erhebung des statistischen Zentralamts brachte 1975 223 personenbezogene Datenverarbeitungen zutage, mit der Prognose, in Zukunft würde die Zahl - auf Grund der massiven Zentralisierungsgewinne - weiter absinken. In den westlichen Staaten entstand - auch unter dem Eindruck des Kalten Krieges - die Befürchtung, dass es einer technischen Elite gelingen könnte mit Hilfe der Computer die Herrschaft zu übernehmen.

Mit der Idee des "Datenschutzes" sollte diesen monströsen Datenverarbeitungen ein Gegengewicht entgegengesetzt werden. Mehrere Länder, voran Deutschland, relativ spät Österreich, hatten daher bis 1984 Datenschutzgesetze erlassen.

Auch in der OECD und im Europarat war zu Beginn der 80er-Jahre Datenschutz ein Thema und relativ ähnliche Bestimmungen und Empfehlungen wurden verabschiedet. Am 28. Jänner 1981 verabschiedete der Europarat die Konvention "zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten"[3]. Zusammengefasst wurde diese Formulierung mit dem Begriff "Datenschutz".

Wir finden diese Idee auch im Artikel 1 Abs. 1 der europäischen Datenschutzrichtlinie[4] ähnlich formuliert: "Die Mitgliedstaaten gewährleisten nach den Bestimmungen dieser Richtlinie den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten."

Weniger klar findet sich diese Idee im § 1 DSG 2000[5], der den Artikel 8[6] der Europäischen Menschenrechte zitiert und im Verfassungsrang steht.

SCHUTZ DES IDENTIFIZIERTEN INDIVIDUUMS

Analysiert man alle bisherigen Datenschutzbestimmungen, gehen sie mehr oder minder klar vom Schutz der Privatsphäre identifizierter natürlicher Personen aus. Das identifizierte Individuum, so das Konzept, darf weder von einem staatlichen, noch einem privaten "Big Brother" durchleuchtet werden. Egal wie viele Daten für die Erfüllung einer Aufgabe erforderlich sind, niemals darf eine Stelle "alles" über eine Person sammeln.

---

3 Artikel 1 lautet "Zweck dieses Übereinkommens ist es, im Hoheitsgebiet jeder Vertragspartei für jedermann ungeachtet seiner Staatsangehörigkeit oder seines Wohnorts sicherzustellen, daß seine Rechte und Grundfreiheiten, insbesondere sein Recht auf einen Persönlichkeitsbereich, bei der automatischen Verarbeitung personenbezogner Daten geschützt werden".

4 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

5 § 1 DSG 2000 Grundrecht auf Datenschutz
(1) Jedermann hat, insbesondere auch im Hinblick auf die *Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten*, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.
(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in *Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958*, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden. ...

6 Der MRK-Artikel komplett: 'Artikel 8 - Recht auf Achtung des Privat- und Familienlebens
(1) Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.
(2) Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.'

Wenig bewusst ist den meisten Menschen, inklusiven vielen "Fachleuten" der Informationsverarbeitung und -regulierung, dass sowohl die Datenschutz-Richtlinie der EU als auch das DSG 2000 auch den Schutz bestimmbarer Personen vorsieht. Es sind auch Daten schützenswert, die zwar aktuell nicht einer bestimmten Person zugeordnet werden, aber durch Zusatzerhebungen und -auswertungen irgendwann schon.

Im Zusammenhang mit staatlichem Handeln eine wenig bedeutsame Bestimmung, noch leben wir in einer Gesellschaft, in der bestimmte Täter zur Verantwortung gezogen werden und nicht auf Grund besonderer Merkmale bestimmbare Personengruppen. In der vormodernen Zeit nannten wir so etwas Sippenhaftung, vor etwa 80 Jahren Rassenhygiene.

Die Frage des bestimmbaren Personenbezugs gewinnt jedoch immer mehr an Bedeutung bei Internet- und Smartphone-Anwendungen.

VORBOTEN VON BIG DATA

Tatsächlich ist "Big Data" ein Thema lange bevor der Begriff geprägt wurde, ich möchte das an Hand einiger Beispiele verdeutlichen, die Sie vielleicht im ersten Eindruck in den Bereich des nutzlosen Wissens einordnen mögen.

Komplexität und Singularität

Kaum jemand reflektiert in seinem Tagesgeschäft dessen Komplexität. Unsere Tagesabläufe, unsere privaten und geschäftlichen Kontakte, wie wir Feste feiern oder was wir essen, erscheint uns hochgradig ritualisiert und genau umschriebenen Abläufen zu unterliegen. Dieselben Abläufe, wie wir sie bei hunderten, tausenden Mitmenschen ebenfalls beobachten können. Wir fühlen uns in diesem sozialen, politischen oder wirtschaftlichen Milieu anonymisiert und geborgen.

Tatsache ist jedoch, dass schon bei so etwas einfachem, wie dem Mittagessen und wenigen berücksichtigten Parametern[7] mehrere Milliarden Kombinationen entstehen, die Wahrscheinlichkeit ein bestimmtes Mittagessen einzunehmen kleiner ist, als im berüchtigten italienischen Lotto "6 aus 90" zu gewinnen. Dort gibt es "nur" rund 622 Millionen Kombinationen.

Ein ziemlich nutzloses Wissen, werden Sie argumentieren. Zurecht, doch begeben wir uns auf eine technische Ebene. Untersuchungen zeigen, dass Standardcomputer, aber auch Smartphones mit ihrer Installation (Betriebssystem-Version, Browser, Plugins), völlig unabhängig von MAC-ID, IP-Adresse oder Cookies eine Signatur haben, die auf Grund der Unzahl an Kombinationsmöglichkeiten weltweit faktisch eindeutig ist. Im Ergebnis kommunizieren wir im Internet immer als Individuum, in der Regel sogar übereindeutig identifiziert, die Identifikation ist mehrfach abgesichert.

Wahrscheinlichkeit und Verknüpfung

Betrachten wir ein zweites Phänomen, die aktuellen Entwicklungen in der Medizin. Aus dem Handwerk medizinischer Experten, die auf Basis ihrer Erfahrungen Diagnosen stellen und Therapien anwenden, wurde ein wahrscheinlichkeitstheoretisches Projekt.

So gilt eine bestimmte mutierte Form des BRCA2-Gens als Auslöser von Brustkrebs. Jedoch nicht im Sinne einer Ursache-Wirkung-Beziehung, sondern bloß als genetische Prädisposition, d.h. etwa 80% der Frauen werden Brustkrebs haben und "nur" 6% der betroffenen Männer müssen mit Brustkrebs rechnen[8]. Faktum ist aber auch, dass Menschen ohne diese Mutation an den beiden Krebsarten erkranken, in Deutschland mit einer Inzidenzrate von 123 neuen Fällen pro 100.000 Frauen im Jahr bei bei Brustkrebs.

---

[7] Bei uns gängige Fleisch- und Fischarten, davon die üblicherweise genutzten Teile, die üblichen Zubereitungsarten, die gewöhnlichen gemüse- und kohlehydrathaltigen Beilagen und noch beliebte Salatkombinationen und Saucenarten. Mengen, Herkunft der Zutaten, Produktionsform und mehrere Gänge, Vor- und Nachspeise lassen wir unberücksichtigt.

[8] Quelle: ETH Zürich 2012, http://elbanet.ethz.ch:8001/servlet/SBReadResourceServlet?rid=1138177978484_1865281431_231&partName=htmltext

Analysiert man die Krankheitsursachen, dann finden sich neben genetischen Faktoren, hormonelle, umweltbedingte Faktoren, Lebensführung und persönliches Verhalten haben Auswirkungen, ganz besonders natürlich das Lebensalter und sogar die Tatsache, ob die Frau Linkshänderin ist oder nicht (+45% erhöhtes Risiko).

Solange diese Erkenntnisse bloß abstrakt formuliert werden, fallen sie genauso in die Kategorie des nutzlosen Wissens, wie unser Mittagsmenü-Beispiel.

Medizinische Forschung tritt jedoch an, die Lebenssituation individueller Menschen zu verbessern, den Ärzten Werkzeuge zu Therapie oder Diagnostik von Krankheiten zu liefern, den Menschen Hilfen zur Vermeidung von Krankheiten und der Gesundheitspolitik zur Abschätzung der Volksgesundheitskosten in die Hand zu geben.

Die Information, linkshändige Frauen haben ein um 45% erhöhtes Brustkrebsrisiko, ist ganz offenkundig eine nicht personenbezogene Information. Oder?

Nehmen wir den Standpunkt einer Privatversicheurng ein. Der Versicherungsnehmer hat einen Fragebogen auszufüllen, neben Name, Anschrift und Alter vielleicht auch Geschlecht, Gewicht, Größe, berufliche Tätigkeit, Hobbies und auch ob er Links- oder Rechtshänder ist. Alles völlig harmlose Informationen. Oder?

Ob nun die Aussage "45% erhöhtes Brustkrebsrisiko" zu einer personenbezogenen Information wird oder nicht, ist keine Frage der Information allein, wie in der Frühzeit der Datenverarbeitung, in der immer isolierte personenbezogene Datensätze betrachtet werden, sondern welche Verknüpfungen macht das Versicherungsunternehmen tatsächlich.

Damit wird auch deutlich, dass die derzeit heiß diskutierte Frage ob ein bestimmtes Marketing-Unternehmen personenbezogene Gesundheitsdaten erhalten hat oder nicht, völlig am Problem vorbei geht. Ob diese Daten personenbezogen verwertet werden können hängt ausschließlich vom Detaillierungsgrad der Daten, vorhandenem Zusatzwissen und den tatsächlich durchgeführten Verknüpfungen und Auswertungen ab.

Rating und Scoring

Wir sind damit direkt beim dritten Phänomen, die Verwendung von Bewertungsverfahren. Rating bzw. Scoring bedeutet die Reduktion komplexer persönlicher und wirtschaftlicher Zusammenhänge auf einen einzigen (meist nummerischen) Wert.

Der Scoringgedanke ist heute allgegenwärtig und findet nicht nur bei der Bonitätsbeurteilung, in der kreditgebenden Wirtschaft oder den Versicherungsunternehmen Anwendung.

Scoring ist der Versuch aus vergangenen statistischen Erfahrungswerten einer breiten Gruppe von Personen auf das individuelle Verhalten einer bestimmten Person zu schließen.

Was wird zum Scoring[9] herangezogen? Ob jemand jung oder alt, Beamter, Angestellter oder Arbeitsloser ist, in Eigenheim oder Mietwohnung wohnt, Autobesitzer oder Öffie-Freak (Vorsicht Grüner!), aber auch in welcher Straße und welchem Haus jemand wohnt.

Ein Auskunftsdienst berichtete einmal in einer Anti-Fraud-Veranstaltung stolz, dass bei ihren Telekom-Kunden ein rotes Warnsignal leuchtet, wenn am selben Tag drei Leute aus demselben Haus einen Handy-Vertrag wollen. In der Vergangenheit wäre das oft dieselbe Person unter unterschiedlichen Namen gewesen.

[9] Wäre das Gesamtausfallsrisiko aller Kredite bei einem Promille (einer von eintausend vergebenen Krediten wird nicht zurückgezahlt), dann wäre die individuelle Rückzahlungswahrscheinlichkeit bei 0,999. Steigt bei der kritischen Scoringgruppe das Ausfallsrisiko um 100%, dann wäre die Rückzahlungswahrscheinlichkeit immer noch 0,998, also immer noch praktisch ident zur Gesamtgruppe. Es wäre nicht nachvollziehbar, dass diese Personengruppe mit drastisch schlechteren Kreditkonditionen bestraft würde. Die Trennschärfe zwischen "positiver" und "negativer" Bewertung die wesentliche Verschlechterungen der Kreditkonditionen oder eine Ablehnung rechtfertigen, müsste zumindest so hoch sein, dass in der Gruppe der "negativen" Bewertungen zumindest eine Ausfallswahrscheinlichkeit von mehr als 50% besteht, also der Ausfall wahrscheinlicher ist, als die Rückzahlung.

"Können wir sowas auch haben", war die spontane Reaktion der anwesenden Polizisten.

Und so fördert die EU seit Jahren das Projekt INDECT. Kern des Projekts ist die automatisierte Analyse öffentlichen Verhaltens nach verdächtigen Vorfällen. Nun gehört es zu den besonderen Abscheulichkeiten von Kriminellen, sich zu tarnen und nicht mit Kriminalitäts-Abzeichen herumzulaufen. Also wurde in der ersten Phase des Projekts, in der Phase der Kategorisierung, festgehalten, was denn eigentlich "verdächtiges Verhalten" ist.

Dazu ein kleiner Auszug der Verdachtsfälle:
- überqueren der Straße, abseits vom Zebrastreifen
- in der Öffentlichkeit Dose in der Hand halten
- stehen in Hauseingängen, vor Häusern, Bahnhöfen, ...
- stehenbleiben vor einem Auto
- gehen von einem Auto zum nächsten
- längeres Herumstehen allgemein
- Laufen im Stadtgebiet
- Bewegen mehrerer Menschen aus verschiedenen Richtungen auf einen Punkt zu

Die Wiener Polizei steht dem nicht nach, verdächtig ist nach deren Vorstellung, wer Socken (saubere!) in seiner Handtasche/Aktentasche bei sich trägt.

Strukturanalyse und Vorratsdaten

Damit dieses Konzept Kombinatorik, Wahrscheinlichkeit und Rating funktioniert benötigen wir Daten, Daten, Daten. Je mehr und je länger auf Vorrat, desto genauer sind unsere Berechnungen, so das große Versprechen.

Und so werden Telefonverkehrsdaten, E-Mail-Verkehrsdaten, Banküberweisungsdaten, Reisedaten oder Einkaufsdaten auf Vorrat gesammelt. Wenn nicht heute, dann irgendwann wid man aus diesen Daten schon Muster erkennen können.

Jede Institution hofft dabei auf ihren individuellen Check-Pot:
- die ultimative kaufkräftige Einkaufsgruppe
- den Hard-Core-Internet und -Technik-Junkie
- den sicheren, weil niemals kranken, Versicherungsnehmer
- den sicheren, weil niemals insolventen Kreditnehmer
- die wirklichen Top-Terroristen und auch alle ihnen hörigen "Schläfer"
- die wirklichen Pläne der Konkurrenz
- alle Hendldiebe und Neffen-Betrüger

....

FUNKTIONALE IDENTIFIKATION STATT "INDIVIDUUM"

Nutzer wähnen sich im Internet anonym. Sie können sich nicht vorstellen, ohne Personalnummer, ohne zentrale Behörde identifiziert zu werden und dass ihre Interessen ausgespäht werden können.

Faktum ist, das Sammeln von Online-Daten ist heute ein unglaublich komplexes großtechnisches Unterfangen, das die Vorstellungsskraft der Laien überfordert. Am ehesten ist es noch mit der Komplexität von Wetter- und Klimamodellen oder von Erdbebenvorhersagemodellen vergleichbar. Die logistischen Herausforderungen einer Mondlandung oder des Manhattenprojekts sind ein Klacks gegenüber dem Ziel aus Milliarden Online-Daten nützliche Erkenntnisse zu gewinnen.

Im Newspeach der Online-Industrie geht es um "behavioral targeting"[10], "retargeting"[11], "contextual targeting"[12], "demographic targeting"[13], "geo targeting"[14]. Internetbenutzer sind aufzuspüren, ihrem Verhalten nachzuspüren, sie sind zu identifizieren und, sollte ein Benutzer versuchen seine Identität abzuschütteln, dann ist die Fährte eines verlorenen Nutzers wieder aufzunehmen.

Alle diese Schritte funktionieren ohne Real-Identifikation, also ohne Verknüpfung mit einem "Real-Individuum" mit Namen, Anschrift, Sozialversicherungsnummer und Kontonummer. Wir sprechen von einem "Funktions-Individuum".

Aus der Sicht eines Targeting-Unternehmens ist es egal, ob es weiß, dass "Franz Maier" aus Berlin sich für schnelle Autos, teure Handys und Olaf Benz Tangas interessiert oder der Benutzer "0ec583f8f69b880d". Wesentlich sind Umfang und Genauigkeit der recherchierten Interessen ("behavioral targeting"). Gelingt es, die Person "Franz Maier" alias "0ec583f8f69b880d" zu einer Konsumentscheidung zu bewegen, muss sie spätestens zu diesem Zeitpunkt auch ihre reale Identität preisgeben, entweder über eine Zustelladresse, eine Kontonummer oder über die Kreditkartennummer.

Jeder Zugriff auf die Webseiten eines Betreibers wird analysiert, im Hintergrund werden die mitgeschickten Signaturdaten aufgelöst und schon sieht er, dass sich "Harald W****, Wien, Austria am 1. Mai 2008 um 13:59 die Pornoseite fetish-live" angesehen hat, oder jemanden aus dem Innenministerium der 'Vienna Gentlemens Club' interessiert.

Die praktische Umsetzung erfolgt durch Spezialisten wie der AdLINK Group[15]. Vermutlich sagen Ihnen http://www.bluelithium.com/, http://www.zanox.com oder http://www.affili.net nichts. Nie davon gehört? Sie haben diese Seiten noch nie aufgerufen? Tatsächlich gehören sie zu den weltweit reichweitenstärksten Internetseiten. Diese Seiten - wie zehntausende andere - sind Sammelstellen der Milliarden Informationssplitter, die unser "Funktions-Individuum" hinterlässt.

Entscheidend ist nicht mehr das vorhanden sein von Information, sondern welche Kapazitäten zur Auswertung, Verwertung und Verknüpfung der Daten. Ob eine Information personenbezogen ist oder nicht, ist nicht mehr aus dem einzelnen Informationssplitter, sondern nur mehr aus dem Gesamtsystem ableitbar.

Nicht Kontrolle/Überwachung im klassischen Sinne ist Ziel der Online-Tracker, sondern Verhaltenssteuerung.

Die gerade aktuelle Diskussion um die NSA-Überwachung zeigt, wie in der Informationsverarbeitung die Kluft zwischen politischem Verständnis und wirtschaftlicher Realität immer weiter auseinander klafft.

Der naive Bürger glaubt, es gehe um das Sammeln von vertraulichen Daten, wie Kontodaten, Reisepassnummern, Vermögens- oder Einkommensdaten. Mitnichten, tatsächlich hinterlässt jeder Internetnutzer täglich zehntausende, für sich genommen, nichtssagende Informationssplitter. Diese Splitter, richtig zusammengeführt, erlauben - so die Protagonisten - das Netzwerk der Beziehungen und Kontakte, die geheimen Wünsche und Sehnsüchte, Vorurteile und Klischees aufzudecken. Beim Privaten sind es verdächtige Kontakte zu unsicheren Zeitgenossen, bei Unternehmen sind es ihre Geschäftspartner, ihre zukünftigen Projekte, ihre Forschungsziele, ihre Handelsbeziehungen und ihr wirtschaftlicher Status.

Das Sammeln ist bloß der leichteste Teil der Übung, Stufe zwei ist das Verdichten, Stufe drei das Verknüpfen der Daten. Erst dann kann die eigentliche analytische Arbeit der Geheimdienste beginnen. Dabei steigen von Stufe zu Stufe die rechentechnischen Anforderungen, insbesondere was die Auswertungsgeschwindigkeit

10 Identifikation des Verhaltens eines Internetnutzers
11 Wiederaufnahme der Spur eines verlorenen Internetnutzers
12 Erkennen und Identifizieren von Interessenszusammenhängen, z.B. Reiseinteressen und Fotoausstattung, Sportinteressen und Modemarken, Hobbys und politische Einstellungen, Gesundheitsinteressen und Ernährung, ...
13 Identifikation bildungsbedingter, kultureller, einkommensorietierter, sozialer und statusbedingter Merkmale eines Internetbenutzers
14 Identifikation regionaler, standortbezogener Informationen und Interessen eines Internetbenutzers: "*Geo-Targeting trifft in Europa lebende türkische User präzise*" (http://www.teleint.com/)
15 "Mit Angeboten in 7 europäischen Ländern betreibt affilinet eines der führenden Affiliate-Netzwerke Europas und das erfolgreichste im deutschsprachigen Raum. Es bietet Online-Werbetreibenden (Advertiser) einen effektiven digitalen Vertriebskanal und den registrierten Vertriebspartnern (Publisher) attraktive Verdienstmöglichkeiten. Europaweit sind bei affilinet rund 1.500 Affiliate-Programme und mehr als 400.000 Websites registriert." (aus der Website der ADLINK-Group)

betrifft, gewaltig. Schon vor Jahren produzierten die Sozialen Medien wie Facebook und Co öffentlich zugänglichen Content, für dessen bloß oberflächlichen Betrachtung ein geübter Nutzer 65.000 Jahre benötigt und das täglich. Der für den naiven Nutzer unsichtbare Internetteil, das "hidden" Internet, muss mit etwa dem Faktor tausend größer angesetzt werden.

Tatsächlich können nur wenige private Unternehmen die Stufen eins bis drei bewältigen, unter anderem Google, Facebook und mit Einschränkungen Yahoo. Selbst die top ausgestatteten US-Geheimdienste wären damit überfordert. Es macht daher Sinn mittels Projekten wie PRISM oder X-KEYSCORE die privaten Datensammlungen an die Kandare zu nehmen. Da die wichtigsten privaten Datenverarbeiter in den USA sitzen ist auch leicht erklärt, warum EU-Behörden und noch mehr österreichische neidvolle Zuschauer bleiben.

WAS IST FÜR DIE ZUKUNFT ZU TUN?

Wir sollten den ursprünglichen Grundrechtsgedanken nicht aus dem Auge verlieren, besonders wenn wir heute wissen, dass die Vorstellungen über die Fähigkeiten der automatisierten Datenverarbeitung falsch waren und wir statt eines "großen Bruders" in Form von Smartphones, User Targeting, Social Media, Big Data und dem "Web der Dinge" viele Millionen hilfreiche kleine Schwestern haben, die global vernetzt, für uns wirken.

1983 wurde durch das Volkszählungsurteil vom Bundesverfassungsgericht Deutschland das bis dahin gültige Konzept "Datenschutz" hinterfragt und durch den Begriff der "informationellen Selbstbestimmung" ersetzt. Der Einzelne soll entscheiden dürfen, wer welche Informationen über ihn hat, 93 Jahre nach "The Right of Privacy" wurde das Recht "allein zu sein" für das Informationszeitalter neu interpretiert. Die Gestaltung der Verwendung persönlicher Daten durch das Individuum steht im Vordergrund.

Das deutsche Verfassungsgericht hatte im Trojanerurteil 2008 (25 Jahre nach dem Volkszählungsurteil) die Unverletzlichkeit der persönlichen Informationsinfrastruktur als weiteres selbständiges Grundrecht definiert. Der persönliche Computer wird als Teil der Privatsphäre angesehen, der nicht nur ein technisches Gerät ist, sondern als „Verlängerung“ der eigenen Persönlichkeit verstanden wird.

War "Datenschutz" bis 2009 ein Zusatz zum Recht auf Privat- und Familienleben und stark technisch orientiert, wurde mit der EU-Grundrechtecharta ein eigenständiges "Datenschutz"-Grundrecht formuliert: "Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten." (Art. 8 Abs. 1[16])

2033 wäre es wieder so weit, folgt man den Zeitabständen zwischen der "Erfindung" neuer Grundrechte durch den deutschen Bundesverfassungsgerichtshof.

Ich kann nur hoffen, dass wir nicht so lange warten müssen, damit das Phänomen des "Funktions-Individuums" und der Frage des strukturellen Personenbezugs einer brauchbaren rechtlichen Regelung unterworfen wird.

Und so wäre heute eine "Grundrechtscharta der Informationsgesellschaft" erforderlich, in der das "Recht auf unversehrte persönliche Informationsinfrastruktur" genauso verankert ist, wie "Schutz vor willkürlichen Datenverknüpfungen" oder das "Recht auf Entsorgung von Information" ("Recht auf Vergessen werden") und der Anspruch erhalten bleibt "ungefiltert auf alle öffentlichen Informationen eines Netzwerkes zugreifen zu können".

Die jetzt in Diskussion stehende EU-Datenschutz-Grundverordnung wäre der optimale Anlass die besonderen Fragestellungen von Web 2.0, Big Data und dem "Web der Dinge" zu regeln, sonst passiert uns dasselbe wie mit der derzeitigen EU-Richtlinie Datenschutz. Diese konnte im Jahr ihrer Verabschiedung, zeitgleich dem Jahr des Beginns des Internet-Booms, keine geeigneten Regelungen zum persönlichen Datenschutz im Internet formulieren.

---

[16] Der Artikel 8 der "CHARTA DER GRUNDRECHTE DER EUROPÄISCHEN UNION (2010/C 83/02)" komplett: Artikel 8 Schutz personenbezogener Daten
(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.