www.jusletter-it.eu

Hanspeter Thür

Die Privatsphäre im Zeitalter von Big Data

Im Film von Stanley Kubrick «2001: A Space Odyssee» aus dem Jahre 1968 kehrt ein Astronaut von einer Spazierfahrt im All zurück und bittet um Einlass in die Raumstation. Der Computer weist ihn ab: «Sorry, das kann ich nicht tun» und der Astronaut bleibt vor der Tür. Kubrick zeigte vor mehr als 40 Jahren den Computer der Zukunft als künstlich intelligentes Wesen, als Maschine mit menschlichen Zügen, die sich aber gegen den Menschen richten kann. Wo stehen wir heute, 14 Jahre nach Kubricks Deadline? War es eine realistische Vision oder blieb es harmlose Science Fiction?

Kategorie: Beiträge
Rechtsgebiete: Big Data, Open Data & Open Government; Datenschutz; Science Fiction und Utopien
Region: Schweiz

Zitiervorschlag: Hanspeter Thür, Die Privatsphäre im Zeitalter von Big Data, in: Jusletter IT 21. Mai 2015

Inhaltsübersicht

1 Der technische Weg zu Big Data

[Rz 1] Die technische Entwicklung im Bereiche der Informations- und Kommunikationstechnologie verläuft seit Mitte 1960 dramatisch. Die digitale Revolution ist in aller Munde, und wird verglichen mit den epochalen Umwälzungen im Zug der ersten und zweiten industriellen Revolution im 19. Jahrhundert.

[Rz 2] Möglich wurde diese Entwicklung, weil sich in den letzten 50 Jahren die Leistungsfähigkeit von Schaltkreisen und Computer-Chips alle 18 bis 24 Monate gemäss dem Moorschen Gesetz[1] verdoppelte und es noch mindestens ein Jahrzehnt weiter tun wird.[2] Wir werden künftig mit digitalen Assistenten unterwegs sein, die uns alles, was wir jemals gelesen, gesehen und gehört haben, jederzeit zugänglich machen.[3]

[Rz 3] Gleichzeitig reduzierten sich Preis und Grösse der Prozessoren dramatisch.[4]

[Rz 4] Ebenso revolutionär ist die Entwicklung von drahtlosen Kommunikationsmodulen: Sie benötigen immer weniger Energie, werden immer kleiner und können immer mehr Daten immer schneller durch die Luft befördern. Mit RFID kann Fernidentifikation über Funk hergestellt werden. Die Lokalisierung von Gegenständen, etwa mit GPS, und damit auch von Personen wird immer genauer und billiger.

[Rz 5] Die Entwicklung der Sensortechnologie geht in die gleiche Richtung: immer kleiner, billiger und genauer.[5] Werden solche Sensoren grossflächig eingesetzt, erhält man dichte Überwachungsnetze für unterschiedlichste Zwecke.

[Rz 6] Begriffe wie Embedded, ubiquitous oder wearable Computing zeigen die Richtung in eine Welt, wo uns schlaue Alltagsdinge, die in miniaturisierter Form in Kleidung, Armbanduhren, Schmuck und Brille oder sogar dem Körper eingebaut sind, das Leben mit zahlreichen raffinierten Dienstleistungen erleichtern werden.

[Rz 7] Alltagsgegenstände werden immer intelligenter, weil sie mit Informationstechnologie zum Sammeln, Speichern, Verarbeiten und Kommunizieren von Daten ausgestattet werden. Sie wer-

---

1 Gordon Moore, Mitgründer des Chip-Herstellers «intel» behauptete bereits 1965, dass sich die Leistungsfähigkeit der Prozessoren alle 18 Monate verdoppeln wird. Diese Prognose hat sich bis heute vollständig realisiert. Das heisst, seit 1965 sind die Chips 10-milliardenfach leistungsfähiger und entsprechend kleiner. Vgl. http://de.wikipedia.org/wiki/Mooresches_Gesetz (alle Internetquellen zuletzt besucht am 18. Mai 2015).

2 ETH-Professor Friedemann Mattern prognostiziert sogar, dass in den nächsten 40 Jahren Computer ihre Leistungsfähigkeit weiterhin um das Hunderttausend- bis Milliardenfache steigern werden.

3 Friedemann Mattern (Hrsg.), Die Informatisierung des Alltags, Springer-Verlag Berlin Heidelberg 2007.

4 1958 kostete ein Grossrechner von IBM mit 5000 Kilobyte Speicher rund eine Mio. Franken. Zum Vergleich, ein simples I-Phone hat 32 Mio. KB Speicher und kostet höchstens einige Hundert Franken. Heute verfügt bald jeder Haushalt und vor allem jeder Arbeitsplatz über einen PC mit mehreren Gigabyte, also Millionen Kilobyte Speicher.

5 Man spricht bereits von Sensornetzen, wo sich Sensoren auf nahezu unsichtbare Weise miteinander austauschen und vernetzen und vielfältige Phänomene der Welt in nie da gewesener Genauigkeit beobachten können.

den miteinander kommunizieren können, auch via Internet:[6] Das Internet der Dinge steht vor der Tür. Ericsson geht davon aus, dass bis zum Jahr 2020 rund 50 Milliarden intelligente Apparate ans Internet angeschlossen sein werden.[7] Diese Entwicklung wird sehr unterschiedlich bewertet. Während auf der einen Seite das immense wirtschaftliche und gesellschaftliche Potential betont wird,[8] sehen andere grosse Gefahren für Persönlichkeitsschutz und Privatsphäre.[9]

[Rz 8] Namhafte Forscher behaupten, es werde künftig möglich sein, dass wir mit einer Brille die Welt betrachten, die uns automatisch Informationen über das Beobachtete direkt auf das Auge projiziert. Wir werden über Geräte verfügen, die miteinander kommunizieren und sich Informationen vom Internet holen und uns sagen, was wir zu tun haben.[10]

[Rz 9] Es ist also keine Fiktion mehr — um bei der eingangs erwähnten Filmsequenz anzuknüpfen: Die intelligente Maschine der Zukunft wird uns sagen, was wir zu tun haben und sie wird uns möglicherweise bestrafen, wenn wir uns ihr widersetzen.

[Rz 10] Wenn die Kaffeemaschine einfach abstellt, wenn ich sie nicht entkalke oder wenn die Bohrmaschine nur funktioniert, wenn ich den firmeneigenen Helm mit Schutzbrille trage, ist das vielleicht ärgerlich, wenn aber Computer, die in den Finanzmärkten eingesetzt werden, sich verselbständigen, wie das 1987 geschehen ist und in der Folge einen Börsencrash mitverursachten,[11] ist das schon weniger harmlos.

[Rz 11] Schlaue Alltagsdinge bekommen ein «Gedächtnis», wissen wer angerufen hat. Der DVD-Player auf dem Laptop weiss den Namen des zuletzt abgespielten Films. Ein lustiges Feature, das aber auch zu peinlichen Situationen führen kann, wenn der Lehrer am nächsten Tag den Schülern mit dem Laptop ein Video zeigen möchte und das Gerät den Schülern ungefragt mitteilt, welchen Film ihr Lehrer am Abend zuvor konsumiert hat.

[Rz 12] Diese Beispiele zeigen, dass wir uns zunehmend mit einer Digitalisierung der Welt auseinander setzen müssen, die das Potential einer totalen Kontrolle beinhaltet.[12,13]

---

6 Mit der neuen Version IPv6 kann bereits heute jedes Gerät mit einer IP-Adresse versehen werden und kann mit entsprechender technischer Ausrüstung über das Internet kommunizieren.

7 Ericsson White Paper, zitiert in Andrew Keen, «Das digitale Debakel», Deutsche Verlags-Anstalt München 2015, FN 9, S. 23.

8 Vgl. Jeremy Rifkin, Die Null-Grenzkosten-Gesellschaft, Campus Verlag Frankfurt am Main, 2014, der durchaus auch auf die Risiken mit Blick auf den Persönlichkeitsschutz und die Privatsphäre hinweist.

9 Vgl. Andrew Keen, a.a.O. Yvonne Hofstetter, «Sie wissen alles», C.Bertelsmann München, 2. Auflage 2014.

10 Friedemann Mattern, «Hundert Jahre Zukunft — Visionen zum Computer- und Informationszeitalter». http://www.vs.inf.ethz.ch/publ/papers/mattern2007-zukunft.pdf.

11 Handelsstrategien wie das Programme-Trading (namentlich die Portfolio Insurance), welche Investoren vor grösseren Kursverlusten hätten schützen sollen und die Margin Calls, welche die Solvenz der Clearing Häuser hätten garantieren sollen, waren für den Kurssturz mitverantwortlich. Vgl. http://www.nzz.ch/aktuell/startseite/der-boersencrash-von-1987--ein-schock-fuer-die-damaligen-handelssysteme-1.568513.

12 Harald Welzer in der Sternstunde Philosphie von SRF vom 29. März 2015, http://www.srf.ch/sendungen/sternstunde-philosophie/harald-welzer-unsere-freiheit-ist-bedroht. Welzer befürchtet, dass die digitale Welt zunehmend totalitaristische Züge annimmt und Konzernen wie Google, Facebook usw. mit ihrem Drang, die Welt zu verbessern in eine «Weltverbesserungsdiktatur» führe. In seinem Ende April 2015 erscheinenden Buch «Autonomie. Eine Verteidigung» fragt er: «Was aber, wenn der Totalitarismus gar nicht in uniform auftritt?».

13 Für Keen, a.a.O, S. 213 ist das erschreckende an der vernetzten Gesellschaft des 21. Jahrhunderts, dass wie ein elektronisches Panoptikum im Stile Jeremy Benthams errichtet und dies mit seinen utillitaristischen Gedanken von der Quantifizierung der Gesellschaft verbindet, vgl. auch FN 25.

2 Der Nutzer als Datenlieferant

[Rz 13] Grosse Datenmengen kommen auch deshalb zusammen, weil die Nutzer von Geräten und Services von Gratisangeboten Gebrauch machen, die es nur deshalb sind, weil sie den Anbietern sämtliche Nutzerdaten zur Auswertung und Weiterverwendung liefern. Google und Facebook, die ihre Dienste gratis zur Verfügung stellen, sind derzeit die grössten Sammler persönlicher Daten.[14] Vielen Nutzern ist nicht bewusst, dass diese systematisch zur Profilierung ausgewertet und an Dritte verkauft werden. Viele Apps, die man aufs Handy herunterlädt, offenbaren nicht (oder dann in schlecht auffindbaren AGB), dass sie ebenfalls Daten absaugen, auswerten und weiter geben.[15] Den Nutzern ist die Tatsache oft nicht bewusst, dass installierte Software online gewartet wird und dabei ebenfalls Daten weitergibt. Die digitalisierte Kommunikation (E-Mail, Telefon usw.) hinterlässt ebenfalls grosse Datenberge, die von den Anbietern unter Umständen genutzt werden. Nicht zu sprechen von den Datenmengen, die das Internet der Dinge, das sich in den nächsten Jahren auf breiter Ebene durchsetzen wird, über unsere täglichen Gewohnheiten und Verhalten festhalten wird.[16] Vernetzte Autos und Fernsehgeräte, die Nutzergewohnheiten festhalten und weitermelden, sind bereits auf dem Markt. Experten sprechen davon, dass sich die Datenmenge alle zwei Jahre verdoppeln wird.[17]

[Rz 14] In die gleiche Richtung geht die Quantified Self-Bewegung,[18] welche 2007 von Gary Wolf und Kevin Kelly ins Leben gerufen wurde, um ihre Selftracking-Erfahrungen auszutauschen. «The Quantified Self» ist ein Netzwerk aus Anwendern und Anbietern von Methoden sowie Hard- und Softwarelösungen, mit deren Hilfe sie z.B. umwelt- und personenbezogene Daten aufzeichnen, analysieren und auswerten. Ein zentrales Ziel stellt dabei der Erkenntnisgewinn u.a. zu persönlichen, gesundheitlichen und sportlichen, aber auch gewohnheitsspezifischen Fragestellungen dar. Zu diesem Zweck werden unter Umständen auch heikle Gesundheitsdaten ins Netz gestellt.[19]

---

14 Auf diesem Weg sind die beiden amerikanischen Firmen innert weniger Jahre zu den teuersten börsenkotierten Unternehmen aufgestiegen, die jährlich Milliardengewinne erzielen. Noch 2000 verdiente Google wenige Millionen Dollar und Facebook existierte noch gar nicht.

15 Datenmissbrauch durch Apps in «Kommerzielle digitale Überwachung im Alltag» Studie im Auftrag der österreichischen Bundesarbeitskammer 2014, Ziff. 4.1.1., S. 34 ff; Darin wird unter anderem eine Untersuchung von 26 Datenschutzbehörden aus 19 Ländern aus dem Jahre 2014 erwähnt, welche feststellte, dass 31% von 1'200 untersuchten Apps auf Daten zugreifen, ohne dass dies für die eigentliche Funktion der App notwendig wäre. 59% der Apps sind sogar als bedenklich eingestuft worden, da sie die Nutzerinnen nicht ausreichend darüber informieren, welche Daten genutzt und weitergeben werden. Vgl. auch die Studie der Stiftung Warentest (zitiert in http://www.welt.de/vermischtes/weltgeschehen/article106374257/Viele-Apps-uebertragen-ungefragt-Daten.html).

16 Vgl. FN 5 und 7.

17 Klaus Mannhart, IDC-Studie zum Datenwachstum- Doppeltes Datenvolumen alle zwei Jahre. In CIO. 10 Juli 2011 (zitiert in http://www.odoscope.de/operational-intelligence/big-data/).

18 Die Mitglieder der Quantified-Self-Bewegung veranstalten in 35 Ländern weltweit in rund 130 Städten regelmäSSig stattfindende «Meetups». Kern dieser Treffen sind Erfahrungsberichte von Anwendern über Self-Tracking-Lösungen für Sport, Gesundheit und andere persönliche Bereiche sowie Produktpräsentationen von Startups und etablierten Unternehmen. Die Quantified-Self-Gruppen dienen der Vernetzung von Anwendern, Entwicklern und Anbietern digitaler Produkte für Sport, Gesundheit und andere Bereichen der Nutzung persönlicher Daten.

19 http://de.wikipedia.org/wiki/Quantified_Self.

3 Risiken von Big Data Analytics

[Rz 15] Diese grossen Datenmengen sind ja nur deshalb interessant, weil sie dank der technologischen Entwicklung auch ausgewertet werden können. Man findet buchstäblich die Nadel im Heuhaufen.[20] Dabei geht es darum, darin Korrelationen oder Muster (Algorithmen) zu finden, die eine Aussage über ein künftiges Ereignis oder Verhalten erlauben. Dabei geht es nie um Kausalitäten, sondern um mehr oder weniger hohe Wahrscheinlichkeiten.[21]

[Rz 16] Damit ist auch schon Konfliktpotential einer solchen Auswertung skizziert. Zielen diese Vorhersagen nicht auf Personen, sind sie unproblematisch. Wenn beispielsweise das Bundesamt für Strassenverkehr Verbindungsdaten von Mobiles der Swisscom-Kunden auswertet, um den Verkehrsfluss zu verbessern, ist kein Problem zu sehen. Oder wenn Daten ausgewertet werden, um den Verlauf von Epidemien sichtbar zu machen.

[Rz 17] Ganz anders, wenn auf der Basis von Wahrscheinlichkeiten Entscheide gefällt werden, welche einer Person zum Nachteil gereichen. Zum Beispiel, wenn es um ihre Finanzkraft, Gesundheit oder mögliches deliktisches Verhalten geht.

[Rz 18] Gefährlich ist auch der Umstand, dass mittels Big Data Analytics einmal anonymisierte Daten zunehmend wieder deanonymisiert werden können. Das führt zum Schluss, dass es im Zeitalter von Big Data keine harmlosen Daten mehr gibt. Sie können stets zu Korrelationen beitragen, die am Ende auch Aussagen über den möglichen Charakter, die politische Ausrichtung oder sexuelle Orientierung usw. einer Person zulassen.[22,23]

[Rz 19] Ganz abgesehen davon können Entscheide, die lediglich auf der Basis einer Auswertung vergangener Ereignisse gefällt werden, unter Umständen auch falsch sein. Nassim Taleb, ein ehemaliger Finanzmathematiker und Trader hat diese Phänomen eingehend erforscht und die Problematik mit der Metapher des Schwarzen Schwans[24] veranschaulicht: Lange war man überzeugt, dass es keine schwarzen Schwäne gibt, weil man noch nie solche gesehen hatte, bis man sie in Australien entdeckte. Taleb warnt: Der Blick in die Vergangenheit führt immer wieder zu falschen Erkenntnissen, wenn gestütz darauf eine Aussage über die Zukunft gemacht werden soll.

4 Fazit für die Privatsphäre

[Rz 20] Die Schlüsse, die wir angesichts dieser Entwicklung für den Gehalt der Privatsphäre zu ziehen haben, sind offenkundig:

- **Wir erleben eine zunehmende Perfektionierung der Überwachung**
  - Unsere Alltagsdinge bekommen ein Gedächtnis: Sie plaudern unter Umständen ohne

[20] Hanspeter Thür, «Auch du bist verdächtig», Schweizer Monat, November 2013, S. 14.

[21] Beispiele in Viktor Mayer-Schönberger, Big Data, Redline Verlag, S. 67 ff.

[22] Beispiele in Thür, a.a.O., S. 16.

[23] Im Juni 2014 war eine Studie der Cornell University und der University of California in San Francisco veröffentlicht worden, für die Facebook heimlich den Inhalt der Startseite von knapp 700'000 englischsprachigen Nutzern manipuliert hatte. Dabei wurde den nicht eingeweihten Testpersonen im Jahr 2012 eine Woche lang überwiegend positive oder negative Einträge von Freunden angezeigt, um herauszufinden, wie sich dies auf ihre Stimmung auswirkt. http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/der-facebook-boersengang/facebook-managerin-sheryl-sandberg-entschuldigt-sich-fuer-psycho-experiment-13024578.html.

[24] Nassim Nicholas Taleb, Der Schwarze Schwan, Hanser 2008; Kurzzusammenfassung in http://www.getabstract.com/de/zusammenfassung/finanzen/der-schwarze-schwan/11237/.

unser Wissen Dinge aus, die nicht für andere bestimmt sind.
  - Orte, die mit Sensoren bestückt sind, können unaufdringlich im Hintergrund beobachten. Mit der Konsequenz, dass wir nie genau wissen, ob wir in einem bestimmten Augenblick an einem bestimmten Ort beobachtet werden.
  - Eine unsichtbare und allgegenwärtige Überwachungstechnik kann in ihrer Perfektion die delikate Balance zwischen Freiheit und Sicherheit aus dem Gleichgewicht bringen. Konkret: Die umfassenden Überwachungsmöglichkeiten verschieben das politische und wirtschaftliche Machtgefüge der Gesellschaft.
- **Wir erleben eine Perfektionierung des Wissens über Personen**
  - Es können immer exaktere Persönlichkeitsprofile erstellt werden.
  - Big Data Analytics kann implizite Verbindungen in einem grossen Datenbestand zwischen a priori unverbundenen Daten ermitteln und zu neuen Erkenntnissen über eine Person führen. Wenn Google beispielsweise weiss, womit ich mich in letzter Zeit beschäftigt habe und dieses Wissen weiter gibt, erfährt ein Dritter Dinge, die ihn nichts angehen, die er aber mit andern Informationen verknüpfen kann, was mir schaden könnte.
  - Wenn wir zunehmend von smarten Gegenständen umgeben sind (ubiquitous computing, wearables usw.), die miteinander kommunizieren und diese Daten Unbekannten weiter geben, vergrössert sich das Wissen über unsere Verhaltensmuster, Interessen, Präferenzen etc. massiv. Dramatisch ist dies vor allem auch deshalb, weil die Betroffenen selber über dieses Wissen gar nicht verfügen.
  - Privatheit wird zum verhandelbaren Produkt: Genügend finanzielle Anreize (Rabatte, Preisnachlässe bei Versicherungen usw.) oder Komfortvorteile können zum freiwilligen Verzicht auf Privatheit führen. Wie ist das aus der Sicht einer liberalen Gesellschaftsordnung zu beurteilen?
  - Die Möglichkeit zur Anonymisierung wird zunehmend obsolet.
- **Wir erleben den Verlust der Location Privacy**
  - Die GPS-basierten Handydienste machen deren Nutzer jederzeit lokalisierbar. Die Frage stellt sich, ob auf Fernlokalisierung überhaupt noch verzichtet werden kann.
  - Dobson und Fisher sprechen von Geo-Slavery,[25] einer neuen Form von Sklaverei, die durch die Kontrolle des Aufenthaltsorts charakterisiert wird.
  - Es ist noch kaum erforscht, welche Sekundäreffekte diese Entwicklung haben wird.
- **Die Gesellschaft entwickelt sich in Richtung Technologiepaternalismus**
  - Der verselbständigte Computer, ausgestattet mit künstlicher Intelligenz führt zu Kontrollverlusten des Menschen, zum Verlust selbst bestimmten Handelns und führt in einen Technologiepaternalismus, wo nicht mehr der Mensch, sondern die Technik darüber entscheidet, welcher Spielraum dem Individuum verbleibt.
  - Nichtdestotrotz werden über das Technikdesign eines bestimmten Produkts oder Systems stets Menschen an irgendwelchen Schalthebeln entscheiden, die sich unter Umständen einer gesellschaftlichen Kontrolle entziehen. Unsere Gesellschaft wird zunehmend von einer kleinen gut ausgebildeten Elite geführt.
  - Zudem werden wir zunehmend abhängig von einer IT-Infrastruktur, deren Sicherheit

[25] Jerome E. Dobson / Peter F. Fisher, «ResearchPriorities», http://scholar.google.ch/scholar?q=dobson+fisher+geoslavery&hl=de&as_sdt=0&as_vis=1&oi=scholart&sa=X&ei=El83VaruI8rsO5-XgYgI&ved=0CBsQgQMwAA.

und Verlässlichkeit im Krisenfall nicht garantiert ist, was bei einem Ausfall ebenfalls weit reichende Folgen nach sich ziehen kann.[26]

5 Braucht es die Privatsphäre überhaupt?

[Rz 21] Wollen wir gegen die negativen gesellschaftlichen Auswirkungen der digitalen Revolution antreten, hat man sich zunächst darüber zu einigen, ob die Privatsphäre und der damit verbundene Persönlichkeitsschutz als verfassungsrechtlich geschütztes Gut nach wie vor zu verteidigen ist.

[Rz 22] Immer mehr Stimmen bezweifeln, dass die Privatsphäre überhaupt noch zeitgemäss, ist. Die einem machen aus der Not eine Tugend, wie der ehemalige Nasa-Berater und Astrophysiker Prof. Dr. David Brin und erfolgreicher Science-Fiction Autor, der in seinem Buch «The Transparent Society»[27] die Vision einer Gesellschaft entwirft, in der jeder jeden beobachten kann, darf und auch soll und postuliert ein digitales Panoptikum, wie es Jeremy Bentham mit seinem Panoptikum beschrieb.[28]

[Rz 23] Die andern fordern Transparenz mit einem moralischen Ansatz, wie der Philosoph und Publizist Ludwig Hasler, der zum «fremden Blick des Internets» meint: ««Er ertappt mich in meinem bewusstlosen routinierten Treiben. So ertappt, muss ich wählen: Stehe ich zu dem, was ich tue? Muss ich mich unter dem fremden Blick ändern?».[29] So gesehen ist Hasler gar der Auffassung, dass «der fremde Blick meine Freiheit (befördert)». Das Internet als quasireligiöse Instanz, die mir sagt, was ich zu tun und zu lassen habe [...]», folgert Aklin.

[Rz 24] Der fremde Blick als Disziplinierungsmittel und moralischer Imperativ für die totale Transparenz also? Das ist jedenfalls auch die Botschaft der grossen Internetgiganten, die jährlich Milliardengewinne mit der Auswertung von Personendaten einfahren.

[Rz 25] Bei Eric Schmidt, dem Chef von Google, tönt es dann so: «Wenn es etwas gibt, von dem sie nicht wollen, dass es irgendjemand erfährt, sollten sie es vielleicht ohnehin nicht tun.»[30] Nicht minder religiös tönt es bei Facebook-Chef Marc Zuckerberg: «Ich möchte die Welt offener und ehrlicher machen. Die Zeiten, in denen man seinen Kollegen eine Persönlichkeit präsentieren kann und Freunden eine andere, sind vorbei. Zwei oder mehr Identitäten zu haben, beweist einen Mangel an Integrität.»[31]

[Rz 26] Nicht zum ersten Mal werden knallharte Profitinteressen mit moralisch religiösem Anspruch unterfüttert!

---

[26] Marc Elsberg, Blackout — Morgen ist es zu spät, Blanvalet 2012.

[27] David Brin, The Transparent Society, Perseus Books 1998.

[28] Das Panoptikum ist ein von dem britischen Philosophen Jeremy Bentham (Begründer des klassischen Utilitarismus) stammendes Konzept zum Bau von Gefängnissen und Fabriken, das die gleichzeitige Überwachung vieler Menschen durch einen einzelnen Überwacher ermöglicht, der von den Überwachten aber nicht gesehen werden kann. http://de.wikipedia.org/wiki/Panopticon. Vgl. auch FN 13.

[29] Zitiert nach Béatrice Acklin Zimmermann, FdP Politikerin und Leiterin des Studienbereichs Religion, Theologie und Philosophie an der Paulus-Akademie Zürich, «Die Privatheit in Gefahr» in NZZ vom 7. November 2014, http://www.nzz.ch/meinung/debatte/ist-die-privatsphaere-noch-zu-retten-1.18419949.

[30] Eric Schmidt, «Offenheit ist meine Religion», Interview mit Joachim Müller-Jung und Holger Schmidt in der Frankfurter Allgemeinen Zeitung vom 9. September 2010, http://de.wikiquote.org/wiki/Eric_Schmidt.

[31] Zitiert aus Kirkpatrick, The Facebook Effect, S. 314

[Rz 27] Die mit solchen Statements aufgeworfenen gesellschaftlichen Grundsatzfragen werden nach wie vor in einem zu exklusiven Kreis debattiert, haben nach wie vor keine Breitenwirkung und gesellschaftliche Relevanz, während die digitalen Revolution voranschreitet und die Grundlagen unserer liberalen Ordnung in Frage stellt. Das Feld wird weitgehend jenen überlassen, welche konkrete wirtschaftliche (und vermutlich auch politische) Interessen mit dem gläsernen Menschen verfolgen. Die Frage stellt sich, wie sich unsere Gesellschaft angesichts der dramatischen Entwicklung von Technologien verhalten soll, die allesamt das Potential besitzen, die wichtigen Grundsätze des Persönlichkeitsschutzes auszuhebeln und die Privatsphäre nachhaltig zu schädigen.

6 Was bedeutet das für den Persönlichkeitsschutz der Zukunft?

[Rz 28] Neben dem notwendigen gesellschaftlichen Diskurs braucht es klare Antworten auf Verfassungs- und Gesetzesstufe. Die Technik soll nicht alles tun dürfen, was sie tun kann. Es braucht Regeln zu den Vorkehrungen, die jemand treffen muss, der persönlichkeitsgefährdende Produkte auf den Markt bringt. Es braucht Reflexionen darüber, wie angesichts der fortschreitenden Digitalisierung die Autonomie des Menschen gewahrt bleibt und die Gesellschaft keinem Technologiepaternalismus zum Opfer fällt, die von einer hauchdünnen Elite geführt wird. Es geht um die Wahrung unserer demokratischen und liberalen Grundordnung. Wie kann dem Recht auf Vergessen auch im Internetzeitalter Nachachtung verschafft werden? Es ist zu hoffen, dass die «Expertenkommission zur Zukunft der Datenbearbeitung und Datensicherheit»,[32] die noch vor der Sommerpause eingesetzt werden dürfte, diesbezüglich wichtige Impulse zu geben vermag und den längst fälligen Diskurs über die Auswirkungen der digitalen Revolution anschieben kann.

[Rz 29] Was bedeutet das für den Datenschutz in einem engeren Sinne? Zunächst ist darauf zu beharren, dass bei der Auswertung von Big Data die geltenden verfassungsrechtlichen und gesetzlichen Prinzipien einzuhalten sind. Jede Person hat gemäss Art. 13 der Bundesverfassung (BV) Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten. Dieses Grundrecht ist Teil der persönlichen Freiheit und schliesst das sogenannte informationelle Selbstbestimmungsrecht mit ein. Jeder soll selber darüber bestimmen können, wem und aus welchen Gründen er Persönliches offenbart, seien es Lebensdaten, Gedanken, oder Empfindungen. Dieses Grundrecht darf nicht ohne einen Rechtfertigungsgrund eingeschränkt werden: Es braucht die Einwilligung des Betroffenen oder ein überwiegendes persönliches oder öffentliches Interesse. Will der Staat die Privatsphäre einschränken, braucht er stets eine gesetzliche Grundlage. Festzuhalten ist auch an den Grundsätzen von **Zweckbindung, Verhältnismässigkeit, Datensparsamkeit und Transparenz.** Das **Recht auf Berichtigung, Sperrung und Löschung** bleibt ebenso zentral. Das **Recht auf Vergessen ist** durch den Entscheid des EuGH vom 13. Mai 2014[33] massiv gestärkt worden ist.

[Rz 30] Darüber hinaus braucht es angesichts der Herausforderungen von Big Data an verschiedenen Orten eine Stärkung bzw. Präzisierung des informationellen Selbstbestimmungsrechts. Privacy muss bei der Konzeption von Produkten und Dienstleistungen eingebaut werden (**Privacy**

[32] Von Ständerat Paul Rechsteiner mit der Motion 13.3841 «Expertenkommission zur Zukunft der Datenbearbeitung und Datensicherheit» vorgeschlagen.

[33] Urteil des EuGH C-131/12 vom 13. Mai 2014 (*Google Spain*).

by design). Sie sind stets mit den höchsten Privacy-Grundeinstellungen auszuliefern (**Privacy by default**). Zu diskutieren ist bei heiklen Anwendungen ein **Privacy Impact Assessment** und regelmässige **Audits**. Zu prüfen ist die Einführung von **Technologiefolgeabschätzungen (TA)** und der **Zertifizierung** für persönlichkeitsgefährdende Produkte und Dienstleistungen.[34]

[Rz 31] Mit Blick auf Big Data Analytics schlägt Viktor Mayer-Schönberger eine Kontrolle der «Datenbarone»[35] und fordert die Installierung von «Algorithmikern»,[36] Experten in Informatik, Mathematik und Statistik, welche Big Data-Analysen und Vorhersagen bewerten. «Algorithmiker wären per Eid zu Vertraulichkeit verpflichtet, ähnlich wie Wirtschaftsprüfer. Sie würden die Wahl der Daten, die Qualität der Werkzeuge zu Analyse und Vorhersage — einschliesslich der Algorithmen und mathematischen Modelle — und die Interpretation der Ergebnisse überprüfen.» Ein Konzept, das dem Grundsatz der Transparenz im Umgang mit Big Data Analytics zum Durchbruch verhelfen könnte. Er vergleicht das Konzept mit Modellen aus dem Wettbewerbsrecht oder der Nuklear- und Gentechnik.

[Rz 32] Last but not least ist auch eine Stärkung der Datenschutzaufsicht vorzusehen.

---

lic. iur. Hanspeter Thür, Rechtsanwalt, Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter.

[34] Diese Prüfung könnte auf privatwirtschaftlicher Basis durchgeführt werden, vergleichbar mit den Aufgaben des technischen Überwachungsvereins (TÜV), der durch staatliche Gesetze vorgeschriebene Sicherheitskontrollen als privatwirtschaftliche Organisation durchführt. Eine andere Möglichkeit wäre, diese Aufgabe einer staatlichen Organisation wie der TA-SWISS zu übertragen. Ihr Auftrag müsste aber entsprechend erweitert werden. Derzeit beschränkt sich die im Bundesgesetz über die Förderung der Forschung und der Innovation (Forschungsgesetz FIFG) definierte Aufgabe, für Parlament und Bundesrat Entscheidungsgrundlagen bereitzustellen, damit diese möglichst frühzeitig die Folgen neuer Technologien erkennen. TA'S und Zertifizierungen im Einzelfall sind nicht vorgesehen.

[35] Viktor Mayer-Schönberger, a.a.O. S. 229.

[36] Viktor Mayer-Schönberger, a.a.O. S. 226.