Osnabrücker Jahrbuch Frieden und Wissenschaft 22 / 2015

GRENZÜBERSCHREITUNGEN

- OSNABRÜCKER FRIEDENSGESPRÄCHE 2014
- MUSICA PRO PACE 2014
- BEITRÄGE ZUR FRIEDENSFORSCHUNG

Herausgegeben vom Oberbürgermeister der
Stadt Osnabrück und dem Präsidenten der
Universität Osnabrück

V&R unipress

Verantwortlicher Redakteur: Dr. Henning Buck
Redaktionelle Mitarbeit: Joachim Herrmann, Dr. Michael Pittwald, Jutta Tiemeyer
Einbandgestaltung: Bruno Rothe / Tevfik Göktepe

Wir danken für freundliche Unterstützung der Osnabrücker Friedensgespräche 2014-2015

- der Stadtwerke Osnabrück AG
- der Sievert-Stiftung für Wissenschaft und Kultur
- dem Förderkreis Osnabrücker Friedensgespräche e.V.

Redaktionsanschrift: Geschäftsstelle der Osnabrücker Friedensgespräche
Universität Osnabrück, Neuer Graben 19 / 21, D-49069 Osnabrück
Tel.: + 49 (0) 541 969 4668, Fax: + 49 (0) 541 969 14668
Email: ofg@uni-osnabrueck.de – Internet: www.friedensgespraeche.de

Die Deutsche Nationalbibliothek – Bibliografische Information: Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über ›http://dnb.ddb.de‹ abrufbar.
1. Aufl. 2015

Printed in Germany: Hubert & Co., Robert-Bosch-Breite 6, 37079 Göttingen.
Gedruckt auf säurefreiem, total chlorfrei gebleichtem Werkdruckpapier; alterungsbeständig.

ISBN: 978-3-8471-0517-6
ISSN: 0948-194-X

Inhalt

III. BEITRÄGE ZUR FRIEDENSFORSCHUNG

IV. ANHANG

Auf dem Podium: Markus Löning, Volker Lüdemann, Katharina Morik,
Arnulf von Scheliha und Zoë Holz

Persönliche Freiheit und Sicherheit im Internet

Podiumsveranstaltung in Kooperation mit dem Politik-Prüfungskurs des 12. Jahrgangs des Ratsgymnasiums Osnabrück[1] am 27. November 2014 in der Aula der Universität

Markus Löning	Menschen- und Bürgerrechtsexperte, Beauftragter der Bundesregierung für Menschenrechtspolitik a.D., Berlin
Prof. Dr. Katharina Morik	Lehrstuhl für Künstliche Intelligenz, Technische Universität Dortmund
Prof. Dr. Volker Lüdemann	Wirtschaftsjurist, Datenschutzexperte, Hochschule Osnabrück
Prof. Dr. Arnulf von Scheliha *Zoë Holz*	Universität Osnabrück, gemeinsam mit Schülerin am Ratsgymnasium – Gesprächsleitung
Dalal Ahmed, Rahel Birkner *Darius Mewes*	SchülerInnen am Ratsgymnasium

Vorbemerkung: Zur Einführung in das Thema wird ein von SchülerInnen des Kurses produzierter Kurzspielfilm gezeigt, der mögliche Konsequenzen einer Auswertung der Internetnutzung eines jugendlichen Jobbewerbers durch eine Personalagentur veranschaulicht. Der Titel des Films: *Das Bewerbungsgespräch oder Spuren im Netz. Ein Film von Mitgliedern des Politikkurses po61 des Ratsgymnasiums Osnabrück*.

Arnulf von Scheliha: Die Handlung ist frei erfunden, aber doch möglich. *Wie* ist das möglich?

Zoë Holz: Wir wissen nicht, ob das im Film Gezeigte heute möglich ist oder morgen möglich sein wird. Dazu inspiriert hat uns der Artikel *Software scannt Facebook-Profile von Bewerbern* aus der Zeitung *Die Welt*.[2] Das geschah wohl nur zu wissenschaftlichen Zwecken. Eine Studie hatte

ergeben, dass eine fünf- bis zehnminütige Konzentration eines Facebook-Profils aussagekräftiger sei als ein Interview mit einem Stellenbewerber.
Arnulf von Scheliha: Was ist eigentlich *Maik Tappe*, der Hauptfigur des Films, passiert? Was wurde ihm vorgeworfen?


Zoë Holz und Arnulf von Scheliha

Zoë Holz: Anhand seiner Internetnutzung wurde sein ›Profil‹ erstellt: Morgens schaut er schon Fernsehen, und zwar ein eher unseriöses Privatfernsehprogramm, später wird von einem Freund über den Messaging-Dienst *WhatsApp* gefragt, ob er abends für das Amüsement sorgen könne, woraufhin er im Netz nach einem Rezept für Hasch-*Cookies* sucht. Außerdem besitzt er einen internetfähigen Kühlschrank, der ihm meldet, dass nur Bier, Ketchup und Mayo im Kühlschrank vorrätig seien, was nicht unbedingt für eine gesundheitsbewusste Ernährungsweise spricht. Das Navigationsgerät in seinem Auto meldet seine anschließende Fahrt zum Frühstück bei McDonalds, was auf einen zweifelhaften Charakter schließen lässt, weil man da normalerweise nicht frühstücken sollte. Und dann postet er noch einen politisch völlig inkorrekten Kommentar über eine vor einem Supermarkt liegende, schwer unfallverletzte Frau, was auch nicht für seinen Charakter spricht. Insgesamt entsteht das Bild eines chaotischen Kiffers, den die Personalchefin in der Designabteilung nicht haben möchte.

Arnulf von Scheliha: Ist so etwas technisch möglich? Ist es rechtlich erlaubt? Sind unsere Grund- und Menschenrechte in Gefahr, wenn es erlaubt und technisch möglich wäre? Darüber wollen wir heute Abend diskutieren mit unseren Gästen, die Ihnen jetzt vorgestellt werden.

Darius Mewes: Frau Morik richtete 1991 an der Technischen Universität Dortmund den Lehrstuhl für Künstliche Intelligenz ein. Hier befasst sie sich seitdem mit maschinellem Lernen und *Data Mining*. *Data Mining* ist die Anwendung von Algorithmen auf Datenbestände, um Muster zu erkennen und so nutzbare Informationen zu gewinnen. Ein anderer Begriff in

diesem Zusammenhang ist *Big Data*. *Big Data* beschreibt große, komplexe und manchmal auch sich schnell verändernde Datenmengen, welche durch die andauernde digitale Revolution zwar einerseits durch Menschen, aber zu einem großen Teil auch automatisch, z.B. durch Sensoren, erzeugt werden. Andererseits bezeichnet *Big Data* Technologien, mit denen man diese Daten sammeln, filtern, verbinden und auswerten kann. Auch mit der Erforschung neuer Verfahren zur Filterung wertvoller Informationen beschäftigt sich Frau Morik. Vielleicht hört sich das Ganze recht abstrakt und theoretisch an; aber es gibt durchaus konkrete Anwendungsmöglichkeiten. Beispielsweise arbeitet Frau Morik am europäischen Projekt *Insight*, das es sich zum Ziel gesetzt hat, Daten, die u.a. aus sozialen Netzwerken und von Verkehrssensoren stammen, zu verbinden und zu analysieren. Dadurch soll die Verkehrsplanung bei Katastrophen wie etwa großen Überschwemmungen verbessert werden. Auch das ist ein Beispiel für die Anwendung von *Big Data*.

Darius Mewes

Katharina Morik: Vielen Dank für die Einführung, die schon viele Informationen enthalten hat. *Big Data* nennen wir zum einen sehr große Datenmengen. Die von uns untersuchten medizinischen Daten z.B. weisen pro Beobachtung 230.000 Attribute auf, sodass eine einzelne Beobachtung schon ein großes Aufkommen an Daten mit sich bringt; wir haben aber Daten sehr vieler Beobachtungen. Wir haben aber auch realzeitlich einströmende Daten, Sensorströme aus unterschiedlichen Quellen, die wir verbinden. Das fordert die Algorithmen schon sehr heraus. Um zu zeigen, was *Big Data* sind, gibt es eine Faustregel: *Big Data* sind solche Datenmengen, die man schneller mit einem Schiff als mit einem Satelliten überträgt, und diese Definition dürfte jedermanns Phantasie inspirieren. Es geht hier um das *IceCube Project* am Südpol. Wir versuchen Teilchen aus dem Weltall zu bestimmen, die durch die Erde hindurch und dann durch einen drei Kilometer langen Tunnel aus Eis geflitzt sind, worin Spezialkameras die Bewegung der Teilchen aufnehmen. Von diesen Teilchen sind die

Neutrinos interessant, weil sie Rückschlüsse auf Ereignisse im All zulassen. Sie sind aber sehr selten und schwer in der Masse nicht interessanter Daten zu finden. 90% Rauschen enthalten 10% interessante Information, aus der man auf Ereignisse im Weltall schließen kann. Diese Daten mit dem Satelliten vom Südpol zur *University of Wisconsin* in Madison zu übertragen, dauert 10 Jahre, sie auf Festplatten per Schiff zu transportieren, nur 28 Tage. Das sind die großen Datenmengen, die wir untersuchen. Ihren Wert haben sie für die Wissenschaft: Wir können damit z.B. den *Krebsnebel*, der sowohl ein Überrest einer Supernova als auch ein Pulsarwind-Nebel im Sternbild Stier ist, besser bestimmen, um herauszufinden, wie unser Universum entstanden ist.

Ein anderes, von der Bauhaus-Universität Weimar stammendes Beispiel ist das Programm *Netspeak*. Für jemanden, der eine Rede schreiben möchte, ist dieses Programm sehr praktisch. Es geht nicht mehr von den Regeln der deutschen Grammatik aus, sondern stellt einfach ans Internet eine Frage wie z.B.: Welche Worte erscheinen zwischen *waiting* und *answer*? Weil die nicht regelrechten Sätze sehr viel seltener sind als die wohlgeformten, regelrechten, kommt man schon zu brauchbaren Ergebnissen, ohne ein Grammatikprogramm schreiben zu müssen.

Hinsichtlich der Wissenschaftlichkeit solcher Untersuchungen stellt sich allerdings ein Problem. Wissenschaftliche Ergebnisse müssen überprüfbar sein. Da wir in Deutschland aber weder die Rechenkapazität noch etwa die Daten von Google haben, können die Google-Wissenschaftler ihre Ergebnisse publizieren und niemand kann kontrollieren, ob sie stimmen. In seiner Studie von 2012 beschreibt der Londoner Professor *Muki Haklay* die Trennung der bürgerlichen Teilhabe, ›*digital divide*‹: Bestimmte reiche, mächtige, gebildete, meist männliche Personen gestalten das *web*, und wir als Nicht-Dazugehörige sind benachteiligt. Dies gilt auch für den wissenschaftlichen Wettbewerb und wird leider überhaupt nicht öffentlich diskutiert. Schon vor 20 Jahren haben europäische Wissenschaftler darum gebeten, dass mehr EU-Fördergelder in diesen Bereich investiert werden. Das ist nicht geschehen, und inzwischen ist der Vorsprung, den Google erreicht hat, für uns kaum noch einzuholen. Forschungsergebnisse, die Google publiziert, können nicht mehr der kritischen Analyse unterzogen werden. Kritische Analyse bedeutet üblicherweise, ein Experiment zu reproduzieren oder auch zu modifizieren. Wenn wir weder die Daten noch die Rechenkapazität haben, um Forschungen im Google-Maßstab durchzuführen, nachzuvollziehen, können wir publizierte Ergebnisse nicht überprüfen. Gerade dies ist aber zwingend erforderlich, um Wissenschaft zu betreiben. Hier besteht die Gefahr wachsender Abhängigkeit.

Einen Wert haben die zu erhebenden Daten übrigens auch für die Bewegung des *quantified self*, eine erstaunliche Neigung von Menschen, sich selber immer wieder zu optimieren, indem man die eigenen Signale notiert und darüber Datenanalysen macht.

Ein weniger überraschender Nutzen der Daten wird in dem schon angesprochenen Projekt *Insight* deutlich, das wir in Kooperation mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) betreiben. Tatsächlich verbreiten sich Informationen über Facebook schneller als über offizielle Kanäle, die das BBK ansonsten verwendet. So konnten sich z.B. während des jüngsten Elbhochwassers im Jahr 2013 viele Einzelpersonen und ganze Nachbarschaften, die beim Auffüllen von Sandsäcken und bei der Unterbringung von Leuten ihre Hilfe anbieten wollten, schnell organisieren. Das Interessante ist das *crowdsourcing*: Man kann direkt über Facebook jemanden ansprechen und fragen, wie der Wasserstand ist und ob der Deich noch hält; einen Helikopter hinzuschicken, ist nicht nötig. Das wollen wir in der Weise optimieren, dass möglichst wenig Fragen gestellt werden müssen, um möglichst viele Informationen zu bekommen, damit Fluthilfe in Echtzeit gelingt.

Katharina Morik

Der Wert der Daten für soziale Netzwerke zeigte sich auch im Zusammenhang mit den Protesten um den Gezi-Park in Istanbul. Sobald die örtliche Verwaltung jeweils erneute Vorbereitungen traf, den Park zu roden, kursierten schon die ersten *Twitter*-Meldungen darüber. Bald nach Eintreffen der Bagger war auch die Bevölkerung da. Der Protest war erfolgreich: die Bäume stehen noch. Den Vorteilen stehen auch Nachteile gegenüber, die man vermeiden muss. So kann Twitter auch Falschmeldungen und Gerüchte in die Welt setzen, und es gibt ›Stille-Post‹-Effekte.

Der Schutz der Privatsphäre ist natürlich ein Riesenthema im Zusammenhang mit der Erhebung persönlicher Daten. Vielleicht kennen Sie die Studie des GRÜNEN-Politikers *Malte Spitz*, der 2009 recherchierte, wie seine Datenspur im *web* verläuft, insbesondere die Spur seiner Aufenthaltsorte, die sich aus den Verbindungsdaten seines Mobiltelefons ergab. Planungs- und Verwaltungsinstitutionen, die solche Daten nutzen, brauchen sie eigentlich nur für statistische Zwecke. Sie interessieren sich nicht dafür, wo Malte Spitz war. Sie wollen wissen, welche Pendlerverkehrsströme wo existieren, um damit Fahrpläne für Verkehrsmittel zu optimieren. *Rakesh Aggrawal* und *Ramakrishnan Srikant* haben in ihrem Aufsatz *Privacy Preserving Data Mining* eine Methode vorgestellt, mit der man sicherstellen kann, dass eine Einzelperson wie der Bewerber im eingangs gezeigten Film nicht identifiziert werden kann. Mithilfe statistischer Auswertungen können Antworten z.B. auf folgende Fragen gegeben werden: Wie viele Menschen wollen eine bestimmte Strecke fahren? Wo wird besonders viel Kommunikation abgefragt? Wo müssen Sendemasten gebaut werden etc.

Gefragt ist eine statistische Datenauswertung, bei der das Individuum nicht identifizierbar ist. Man möchte die Daten zum Vorteil nutzen und mögliche Nachteile technisch einfach blockieren. Ein Beispiel: Auf einem digitalen Stadtplan von Manhattan liefert in einer Freitagnacht jeder Fahrradfahrer eines Pizzalieferdienstes, der gerade unterwegs ist, ein kleines Sensorsignal. Anhand der aufleuchtenden Punkte könnte man eine Wegstrecke rekonstruieren und diese einer Person zuordnen. Das wollen wir gerade nicht. Vielmehr geht es hier darum, jeweils die benötigte Anzahl von Pizzen an jenen Auslieferstationen bereitzuhaben, an denen sie nachgefragt werden. Technik kann so gestaltet werden, dass ein Bedarf ermittelt wird und Privatheit geschützt bleibt. Das Beispiel verdeutlicht, warum *Big Data* große Chancen bietet und *Small Data* auch gefährlich sein kann.

Es kommt auch vor, dass man gerne Daten hätte. Die EU bietet den Bürgern Information über 36 Länder. Um aus diesen Daten verständliche Information zu erschließen, gibt es die Bürgerbewegung CODE. Manchmal möchten die Bürger Daten haben, die sie nicht bekommen. Dies fällt nicht in den Bereich der Methoden, sondern fordert die gesellschaftliche Willensbildung, also die Politik. Dann ist auch der Gesetzgeber gefragt, um etwas wie z.B. die Privatheitsverordnung amerikanischer Bauern von 2014 auf den Weg zu bringen. Methodisch machbar ist Privatheit und Transparenz, aber es muss von uns eingefordert werden.

In der Informatik werden, zusammengefasst, die folgenden Fragen diskutiert:

- Wem gehören die Daten? (*privacy*)
- Wer nutzt die Daten? (*value*)
- Welche Daten will ich sehen? (*transparency*)
- Wer dominiert das Web? (*digital divide*)
- Wer hat genügend Rechenressourcen, um den Wert der Daten tatsächlich zu schöpfen? (*research reproducibility*)


Rahel Birkner

Rahel Birkner: Herr Lüdemann hat sich u.a. mit dem Problem auseinandergesetzt, welche Daten ein Auto über den Fahrer sammelt und wie sie weitergegeben werden können.

Herr Lüdemann, ich habe eine Frage an Sie bezüglich des Films. Darin wurde gezeigt, dass die Personalchefin wusste, dass der Protagonist bei McDonalds war, und ich möchte Sie gern fragen, wie das überhaupt möglich ist.

Volker Lüdemann: Wir haben im Film eigentlich zwei Phänomene gesehen: einmal das ›Internet der Dinge‹ – und das betrifft auch das Auto – und zum anderen *Big Data*. ›Internet der Dinge‹ bedeutet: Nicht mehr der Mensch kommuniziert mit einer Maschine oder einem Computer, sondern – und das ist relativ neu – die Maschinen kommunizieren untereinander. Das hat eine vollkommen neue Qualität. Wenn der Mensch mit einer Maschine kommuniziert, ist er Subjekt: Er kann das tun, z.B. Facebook nutzen, er muss es aber nicht. Man kann auch ein Smartphone links liegen lassen. Bei einer Maschine-Maschine-Kommunikation ist das anders: Hier wird der Mensch in der Regel zum Objekt. Die personenbezogenen Daten gehen z.B. im Fall des Autos automatisch ihren Weg, sobald das System einmal autorisiert und eingeschaltet ist. Oftmals weiß man gar nicht, was da vor sich geht, und manche wissen nicht einmal, *dass* die Autos überhaupt kommunizieren. Das ist das eine Phänomen.

Das andere Phänomen ist *Big Data:* Weil digitaler Speicherplatz fast nichts mehr kostet und die Rechner immer schneller werden, lassen sich rund um die Uhr die verschiedensten Datenarten aufzeichnen, miteinander verknüpfen und korrelieren. Damit sind vielfältige Dienstleistungen möglich, sogenannte *Smart Services*: Waschmaschinen, die genau dann waschen, wenn der Strom günstig ist, Kühlschränke, die Milch und Butter bestellen, oder eben Dienstleistungen rund um das Auto: Versicherungstarife, die vom Fahrverhalten abhängen, Fernüberwachung der Fahrfunktionen, elektronischer Notruf oder das Übertragen von Gesundheitsdaten – ja, auch das macht unser Auto.

Dreh- und Angelpunkt für das Internet der Dinge und für die Nutzung von *Big Data* sind *Sensoren*, die kleinsten technischen Bausteine. Sie erheben die Daten und stellen sie dann bereit. In einem modernen Auto sind heute mehr als 80 Sensoren verbaut. Sie messen unser Fahrverhalten, die Sitzbelegung, die Beschleunigung, die Atemluft, unser Gewicht, wissen um unsere Rückenprobleme, kennen unsere Fahrtziele und unseren Standort. Wussten Sie, dass die *Smart Meter*, die intelligenten Zähler im Keller, bei 15-minütigem Ablesen mehr als 35.000 Datensätze pro Jahr liefern und bei sekundengenauer Ablesung, die technisch möglich ist, über 30 Mio. Daten ausgeben? Früher wurde der Zähler einmal im Jahr abgelesen, jetzt sendet er 30 Mio. Daten. Die einzelne Beobachtung mag harmlos sein. Der gezeigte Film zeigt aber auch: Wenn man alles mit allem kombiniert und auswertet, kann das zu folgenschweren Verletzungen der Privatsphäre führen. Damit werden die Sensoren zum Rechtsproblem: Mit ihrer Sammeltätigkeit greifen sie permanent in unser Grundrecht auf informationelle Selbstbestimmung ein.

Dieses Grundrecht steht nicht im Grundgesetz. Das Bundesverfassungsgericht hat es erst 1983 mit seinem Volkszählungsurteil entwickelt, abgeleitet aus den Artikeln 1 und 2 unserer Verfassung zur »Menschenwürde« und zum »Recht auf freie Entfaltung der Persönlichkeit«. Jeder Mensch soll grundsätzlich bestimmen, so damals das Bundesverfassungsgericht, wer was wann über ihn weiß. Man stelle sich nun die Sensoren vor und die, die die Sensordaten auslesen. Eingriffe in das Grundrecht auf informationelle Selbstbestimmung sind, wie bei anderen Grundrechten auch, nur unter engen Voraussetzungen möglich. Beim Grundrecht auf informationelle Selbstbestimmung – das macht den Datenschutz so einfach – braucht man im Grunde nur einen Satz zu wissen: Es ist alles verboten, was nicht erlaubt ist – soweit die Vorgabe des Bundesverfassungsgerichts.

Erlaubt werden kann es auf zwei Wegen: per Gesetz oder per Einwilligung des Betroffenen. Schaut man sich nun diese famosen *Smart Services* an, stellt man fest: Ein Gesetz, das ihnen die Erhebung personenbezogener

Daten erlaubt, gibt es nicht. Nur für einige, ganz wenige gibt es bisher Ansätze dafür. Bleibt die Einwilligung der Betroffenen, nach der sich die Zulässigkeit der *Smart Services* bemisst. Aber eine rechtswirksame Einwilligung liegt in der Regel ebenfalls nicht vor. Denn für die Einwilligung gelten enge Voraussetzungen. So muss die Einwilligung in Schriftform erfolgen, was in der Praxis häufig schwierig ist. Zudem muss es eine *informierte* Einwilligung sein, d.h. um wirksam einwilligen zu können, muss man wissen, wer wann in welchem Umfang und zu welchem Zweck mit welchem Ziel die erhobenen Daten verarbeiten wird. Schließlich muss die Einwilligung höchstpersönlich gegeben werden, niemand kann stellvertretend für andere einwilligen. Es reicht also nicht, dass der Geräteeigentümer z.B. eines Fahrzeugs, einwilligt, sondern auch der Fahrer, der Mitfahrer und eventuell sogar der, zu dem Sie fahren, müssten einwilligen, denn sie alle sind von der Datenerfassung betroffen. In der Praxis sehen wir: Diese Anforderungen sind kaum zu realisieren.

Volker Lüdemann

Obwohl die *Smart Services* damit derzeit in den meisten Fällen rechtlich unzulässig sind, nimmt die Anzahl der uns umgebenden Sensoren sprunghaft zu: *Smart Watch*, schlaue Kleidung, all die kleinen aktiven und passiven Helferchen mit dem vorangestellten Kürzel *Smart*. Aus der rechtlichen Dimension betrachtet, wird damit das Grundrecht auf informationelle Selbstbestimmung immer häufiger ausgehöhlt, sozusagen jeden Tag und in zunehmendem Maße. Dabei würden wir es gerade jetzt dringend brauchen, denn erstmals besteht mit *Big Data* und dem Internet der Dinge wirklich die Gefahr, dass wir zu ›gläsernen‹ Bürgern werden. Das war 1983 beim Volkszählungsurteil gar nicht der Fall, als die Leute auf die Barrikaden gingen. *Jetzt* ist die Gefahr wirklich real. Und erstmals sind durch die Datenverarbeitung unsere Freiheit und unsere bisherige Lebensweise in ihren Grundfesten bedroht.

Das Gefährdungspotenzial und deshalb vielleicht auch die Widerstände, etwas dagegen zu tun, erhöhen sich durch die wirtschaftliche Bedeutung. Es herrscht Goldgräberstimmung. Allein für *Smart Services* rund um das Automobil wird das Umsatzvolumen für die nächsten Jahre auf über 100 Mrd. Euro geschätzt. Ganz unabhängig von der Datenschutzproblematik stellt sich die Frage: Wem gehören die Daten im Einzelfall eigentlich, die automatisch erhoben und maschinell interpretiert werden? Sie haben ja einen durchaus bedeutenden wirtschaftlichen und auch gesellschaftlichen Wert. Wer hat über diese Daten die Verfügungsgewalt? Und welcher ethische und rechtliche Rahmen soll dafür gelten? Auch hier sind wir in der Diskussion noch ganz am Anfang. Diese Fragen gehen an den Kern unserer Rechtsordnung, an den Kern unseres Zusammenlebens. Hier gibt es noch keine verbindliche Antwort, und auch die soziale, gestalterische und politische Dimension ist völlig ungeklärt.


Dalal Ahmed

Dalal Ahmed: Für das heutige Thema ist wichtig zu wissen, dass *Markus Löning* die Ansicht vertritt, dass sowohl die Meinungs- als auch die Pressefreiheit unveräußerliche Grund- und Menschenrechte sind, die das Fundament jeder Demokratie bilden und deren Wahrnehmung in einer freien Gesellschaft jederzeit möglich sein muss. – Herr Löning, ich möchte Ihnen die Frage stellen, ob nicht der Protagonist in unserem Film seine Meinung über die verletzte Frau frei äußern kann, ohne dass dies im Bewerbungsprozess zu seinem Nachteil verwendet werden darf.

Markus Löning: Ich denke, er hat nichts geäußert, was einen Gesetzesverstoß darstellen würde. Ob seine Aussage aber gegen ihn genutzt werden darf, ist die spannende Frage. Da gibt es den rechtlichen Aspekt: Was darf eine Firma über jemanden recherchieren, wie weit darf sie in die Privatsphäre eindringen und was darf sie zur Grundlage einer solchen Entscheidung machen? Und es gibt darüber hinaus die ethische Frage, weil nicht alles, was vielleicht gesetzlich zulässig ist, auch menschlich anständig ist. Das spielt in diesem Bereich oft eine Rolle: Wie balancieren wir diese

Dinge aus? Wie lässt sich der Spannungsbogen deutlich machen zwischen dem, was die neuen digitalen Technologien für uns alle tun, und ihren Gefahren?

Mein neues Handy z.B. wäre vor 25 Jahren noch ein Festnetztelefon gewesen, und zusätzlich ein Plattenspieler, ein Schallplattenladen, ein Reisebüro, ein dickes Kursbuch der Deutschen Bahn, ein Zeitungskiosk, die Unibibliothek, ein Buchladen. Es wäre etwas gewesen, was ich niemals mit mir hätte herumtragen können. Der Umgang mit den neuen *smartphones* mag für viele vor allem einen spielerischen Reiz haben, aber mein Leben hat es auch leichter und reicher gemacht. Ich habe Zugang zu Informationen, habe Möglichkeiten, mein Leben zu gestalten, die ich früher so nicht hatte. Die digitale Technologie in Form dieses *smartphones* hat mein Leben fraglos vereinfacht und bereichert. Deswegen ist es wichtig, auf der einen Seite die Potenziale von *Big Data* zu erkennen, und die Potenziale der neuen Technologien insgesamt, auch der neuen Verkehrstechnologien. Das Potenzial, Energie einzusparen, und das Potenzial, den CO_2-Ausstoß zu reduzieren, sind enorm. Ein Auto mit Sensorik, mit integriertem Rechner, kann wesentlich energieeffizienter fahren. Wir können über statistische Auswertungen Verkehrsströme viel zeit- und energieeffizienter steuern. Wir können Staus vielleicht nicht völlig abschaffen, aber minimieren, wir können also einen Gewinn an Lebensqualität erreichen durch diese Art von Datensammlung und Datenverarbeitung. Das gilt auch für andere Bereiche, außerhalb der Mobilität: Ähnliches kann im Bereich der Energie erreicht werden, Stichwort ›smarte‹ Waschmaschine. Man kann z.B. von auswärts die Heizung steuern. Insgesamt lässt sich der Energieverbrauch in Haushalten mit diesen neuen Technolo-

Markus Löning

gien stark optimieren, und das lässt sich auf die gesamte Wirtschaft übertragen. Auf Dauer ist hier eine sehr viel bessere Energieeffizienz erreichbar.

Allerdings stellt sich auch die Frage: Wie stark ist der Eingriff in das persönliche Leben? Wenn ich ein *smart meter* habe und Energie optimal einsetzen möchte, ist es aus technischer Sicht gut, möglichst viele einzelne, individualisierte Daten zu haben. Aus Sicht des Persönlichkeitsschutzes muss ich das aber ablehnen. Ich möchte nicht, dass ein Angestellter der Elektrizitätswerke nachschauen kann, wann ich ins Bett oder auf die Toilette gegangen bin, wann ich geduscht oder gekocht habe oder wann meine Frau und meine Kinder nach Hause gekommen sind. Das sind hochsensible Daten, und ich möchte nicht, dass irgendjemand darauf Zugriff hat – und zwar nicht, weil ich etwas zu verbergen hätte!

Das muss man in dieser Debatte immer wieder deutlich machen: Es geht nicht darum, ob man etwas zu verbergen hat, sondern es geht schlicht um unser Recht auf Privatsphäre. In der *Allgemeinen Erklärung der Menschenrechte* ist der Schutz der Privatsphäre als konstitutives, wesentliches Menschenrecht festgelegt. Das ist aus einer menschlichen Perspektive gut erklärbar: Wir brauchen Privatheit, wir brauchen den Schutz unseres Privatbereiches. Deswegen stellt sich die Frage: Wie bringen wir die Verfügbarkeit über diese Technologien, die unser Leben so viel besser machen können, in den nächsten Jahren und Jahrzehnten mit unserem Interesse am Schutz von Privatsphäre zusammen?

Als Menschenrechtsbeauftragter bin ich viel gereist, habe Flüchtlingslager besucht, aber auch Menschen bei Protestaktionen, zuletzt in Hongkong bei den jungen Leuten des *Umbrella Movement*. Sie versuchen, Demokratie in ihrer Stadt, in ihrem Land, durchzusetzen. Sie nutzen die neuen Technologien, um sich zu organisieren, um die Welt darüber zu informieren, was dort stattfindet. Das funktioniert sogar aus einem abgelegenen Dorf in Indonesien oder aus Aserbaidschan, wo die Staatsmacht versucht, solche Kontakte zu unterbinden. Mich haben Menschen aus dem Iran und aus China erreicht, wo von staatlicher Seite versucht wird, das Netz zu kontrollieren. Trotzdem gelangen Informationen heraus. Die neuen Kommunikationstechnologien besitzen ein großes Potenzial auch im Bereich Menschenrechte, Zustände und Vorgänge zu dokumentieren und der Welt mitzuteilen, sich zu organisieren und damit die Verhältnisse zu verbessern. Gleichzeitig verfügen die Polizei und die Geheimdienste leider ebenfalls über gute technische Möglichkeiten, den Aufenthaltsort Einzelner festzustellen und deren Kommunikation zu überwachen. So lassen sich Netzwerke und Freunde identifizieren und Profile erstellen, die weit über das hinausgehen, was wir anfangs im Film gesehen haben. Was in diesem Film halb überraschend, halb lustig war, ist für jemanden, der in einem autori-

tären Land lebt, unter Umständen die Frage von Freiheit oder Gefängnis. In einem autoritären Land ist die *trackability*, die Verfolgung, die aufgrund dieser Datenmengen entstehen kann, extrem gefährlich.

Was können wir tun? Nehmen wir noch einmal das Auto als Beispiel: 1888 fuhr *Bertha Benz*, Ehefrau von *Karl Benz*, mit dem ersten Auto von Mannheim nach Wiesloch. Sie hatte weder Airbag noch Sicherheitsgurt, wohl eine Bremse. Es gab keine Straßenschilder und wahrscheinlich keine Verkehrsregeln, und einen Führerschein wird Bertha Benz nicht gehabt haben. Eine neue Technologie, völlig unreguliert! Man konnte damals wohl nur in Ansätzen das Potenzial dieser Technologie erahnen. Aber zweifellos hat das Auto die Lebensqualität von Millionen und Abermillionen von Menschen sprunghaft verbessert, auch wenn damit gleichzeitig neue Gefahren verbunden waren. Im Laufe der Zeit wurden alle möglichen Vorrichtungen entwickelt, um diesen Gefahren zu begegnen und sie zu verringern. So wird es auch mit dem Internet und anderen digitalen Technologien gehen. Hier ist offensichtlich viel Potenzial, aber wir können noch nicht genau abschätzen, wie sich Nutzen und Gefahren entwickeln werden. Wir müssen also daran gehen, Regeln zu entwickeln, um die Gefahren in den Griff zu bekommen:

Zum einen muss der *Gesetzgeber* versuchen, Sicherheit im Netz durch gesetzliche Regelungen, aber auch durch Kontrolle dieser Gesetze, durch Aufsicht über das Netz, zu verbessern. Das ist nicht leicht in einer Situation einer sehr schnell sich weiterentwickelnden Technologie. Die Frage ist schwierig: Wie macht man das regulatorisch richtig, sodass man die Potenziale erhält und die Gefahren beschränkt? Zum Zweiten brauchen wir aber auch Technologie, die schützt. Sehr viele *smartphone*-Besitzer nutzen den *Messaging*-Dienst *WhatsApp*. Am Markt gibt es aufgrund der Nachfrage von Verbrauchern, denen an einem besseren Schutz ihrer Daten liegt, durchaus technologische Alternativen. Man kann auch den Dienst *Threema* oder andere nutzen. Auch die Industrie ist hier aufgefordert, Angebote zu machen, um die Privatsphäre und Daten besser zu schützen.

Drittens kommt es auf uns selber an: Vieles liegt in unserer eigenen Hand, auch das Nutzerverhalten und z.B. die Erziehung unserer Kinder zum Thema Umgang mit Daten ist eine Aufgabe der Gesellschaft. Auch wir selbst entscheiden, wie wir mit unseren Daten umgehen. Wir müssen uns überlegen: Was machen wir und was lassen wir lieber.

Volker Lüdemann: Frau Morik, Sie sagten, bei *Big Data* gehe es nicht um individuelle Daten. Das klingt für mich ein bisschen nach einem Mythos. *Big Data* soll unsere Umwelt sauberer machen, unser Verhalten rationeller, uns selbst gesünder, die Politik intelligenter. *Big Data* wird oft als giganti-

sche Weltverbesserung dargestellt. In Wirklichkeit geht es aber, wie ich meine, zumindest bei den neueren Anwendungen, absolut um Individualisierung, man spricht sogar von Hyperindividualisierung. Ein Beispiel, das viele Schüler vielleicht kennen: In Amerika gibt es eine Firma namens *BlueKai*, die 150 Millionen Profile von amerikanischen Verbrauchern gespeichert hat. Was macht sie damit? Es geht darum, Werbung zielgerichteter einzusetzen. Ein Profil einer bestimmten Person ist nötig, um ihr die ›richtige‹ Werbung zuspielen zu können. Das macht diese Firma allein in Amerika 80 Mrd. Mal im Jahr: Wer mit *Google* etwas sucht, dessen Profil wird herangezogen, um über die Suchanfrage bzw. die Webseite, die anschließend aufgerufen wird, Werbung zu verkaufen. In Millisekunden wird im Hintergrund Werbung versteigert, die der Internetnutzer auf Grundlage seines Profils angezeigt bekommt. Darum, so meine ich, kommt es schon bei *Big Data* sehr auf das individuelle Profil an. Das ist für mich der Kernpunkt: Wenn *Big Data* wirklich nur auf anonyme Datenmassen setzen würde, wäre das rechtlich unproblematisch. Dann würden keine personenbezogenen Daten erhoben. Aber nach allem, was ich höre, geht der Trend dahin, personenbezogene Daten zu haben, am liebsten von jedem Einzelnen, um ihn zu beglücken – oder eben auch nicht.

Katharina Morik: Wir Informatiker bieten *privacy preserving data mining* an und arbeiten an *privacy by design*-Methoden, die dem Schutz der Privatsphäre dienen. Für die Forschung existiert hier keine Goldgräberstimmung. Es gibt sehr unterschiedliche Interessen, und es kommt auf den politischen Willen an. Was will die Gesellschaft? Womit wollen wir die Dienste von Google bezahlen und womit nicht? Wem gehört das Internet, warum werden Methoden an einer Stelle genutzt und an anderer nicht, obwohl sie angeboten werden? Wann wollen wir Personalisierung und wann nicht?

Um den Unterschied zu verdeutlichen: Im Sonderforschungsbereich 876 beschäftigt man sich z.B. auch mit *smart clothing*, ein Anwendungsgebiet im doppelten Sinn nah am Menschen, man denke etwa an den plötzlichen Kindstod. Es gibt einen kleinen Sensor für Säuglinge, den man in die Babykleidung einnähen kann und der registriert, ob das Baby atmet. Sobald es einen kurzen Moment lang nicht atmet, geht ein Alarm los. Dieses Signal wird aber nicht an irgendeine *Cloud* gesendet, sondern bleibt in der Wohnung, bei den Eltern. Nicht anders ist es mit einem Rechner an meinem Kühlschrank, den ich einfach nur abfrage, was fehlt. Da ist kaum ein Unterschied zum Einkaufszettel. Wenn solche Daten in eine zentrale Speicherung gelangen sollen, muss es eine kryptologische Verschlüsselung

geben, derart, dass die Person des Urhebers nicht ermittelt werden kann. Das bedeutet *privacy preserving by design*.

Ich teile durchaus die verbreitete Skepsis gegenüber der Datensicherheit. Ich habe nur versucht zu zeigen, was technisch alles möglich ist, damit Sie es einfordern können. Die Frage an die Politik ist: Warum, bitteschön, wird so wenig unternommen? – Warum? Weil man von Google abhängig ist und in Europa nicht rechtzeitig Alternativen gefördert wurden. – Das sind Ziele, die ich mit der Community der Wissenschaftler teile.

Arnulf von Scheliha: Wir müssen also unterscheiden zwischen dem, was Wissenschaftler tun, methodisch einfordern und machen können, und dem, was kommerziell gemacht wird. Das sind offenbar zwei Welten.

Markus Löning: Das angesprochene Beispiel ist interessant, weil natürlich die Übersendung einer personalisierten Werbung noch keinen Grundrechtsverstoß darstellt. Das ist eine uralte Technik, jeder Werbetreibende fragt sich: Welche Zeitung liest meine Kundschaft? Schon seit Langem kann man Adressen von Leuten kaufen, von denen man weiß, dass sie bestimmten sozioökonomischen Gruppen oder mit einer gewissen Wahrscheinlichkeit einer Kirche oder Partei angehören. Ebenso kann man Berufsgruppen ansprechen. Das wird durch neue technische Möglichkeiten nun gewaltig gesteigert, weil die ganz persönlichen Vorlieben des Einzelnen aus seiner Internetnutzung ermittelt werden können.

Die Frage ist: Gibt es dafür eine Grenze und von wo an ist deren Überschreitung für die Gesellschaft nicht mehr akzeptabel? Wenn ich eine Werbung erhalte, nur weil ich eine Webseite aufgerufen habe, so ist das noch keine Einschränkung meines Grundrechts, aber ich möchte es vielleicht nicht. Ich möchte vielleicht nicht, dass jemand über mich so vieles weiß, auch weil ich Angst vor Missbrauch habe, z.B. davor, dass jemand meine Daten betrügerisch missbraucht oder dass jemand im Streit mit einem Freund oder Nachbarn kompromittierende Details aus deren Leben im Internet postet. Solche ethischen und gesellschaftspolitischen Fragen sind zu diskutieren. Es muss gesetzlich geregelt werden, wie weit Unternehmen in die Privatsphäre eindringen dürfen. Aber: Wir können das alles natürlich in Deutschland wunderbar regeln. Google wird sich denken: Na, regelt mal schön – wir sammeln trotzdem und speichern die Daten auf dem Server in Seattle oder anderswo. Google hat in Deutschland immerhin einen rechtlichen Unternehmenssitz, andere Firmen haben nicht mal das und werden insofern nicht von deutschen Gesetzen erreicht. Der Bundestag wird nichts verändern können, wenn ihm die politische und juristische Durchschlagskraft fehlt. Ein solches Rechtsproblem hat es früher nicht

gegeben. Also müssen wir auch die Frage diskutieren, wie international tragende Vereinbarungen getroffen werden können. Als Europäer können wir es versuchen, aber eigentlich geht es nur mit den Amerikanern, in einer globalen Vereinbarung.

Katharina Morik: Mehr als *Google* gibt eigentlich das Versandunternehmen *Amazon* Anlass zur Kritik. Das sind zwei Unternehmen mit ganz unterschiedlichen Haltungen und Techniken. Amazon bietet Dritten seine *cloud* als Rechnerressource an, und dann hat es deren Daten. Es gab an der TU Dortmund den Vorschlag, statt eigene Rechner anzuschaffen, alles auf Rechnern bei Amazon zu rechnen, das sei billiger. Das hielt ich für sehr gefährlich, weil ich der Ansicht bin, dass dem Unternehmen in puncto Datensicherheit nicht getraut werden sollte. Inzwischen habe ich in Stockholm ein Rechenzentrum mit dem Namen *bahnhof.net* gefunden, das mit dem Slogan »*We are NSA-free*« wirbt. Es verbürgt sich dafür, keinen Missbrauch mit diesen Daten zu betreiben.

Markus Löning: Diese Lösung halte ich für unrealistisch, denn auch in diesem Rechenzentrum werden doch amerikanische Technik-Komponenten etwa der Firma Cisco verbaut sein.

Katharina Morik: Die juristische Lage ist jedenfalls so: Der Firmensitz ist in Europa. Wer dort rechnet, schließt einen europäischen Vertrag ab, dessen Datenschutz-Verpflichtungen das Rechenzentrum zu erfüllen hat.

Markus Löning: Das ist ja nicht allein eine juristische Frage. Ich hoffe für Sie, dass dort nicht auch chinesische Komponenten verbaut sind.

Volker Lüdemann: Aus dem amerikanischen Rechtsverständnis heraus agieren Firmen wie Amazon oder Google alles andere als böse, sondern ganz normal. Man muss einfach sehen: Beim Datenschutz geht es ja nicht um den Schutz der Daten, sondern es geht aus unserer Sicht um die Wahrung unserer Grundrechte – übrigens auch aus der Sicht der meisten anderen Länder. Das ist eine kulturgeschichtlich gewachsene Sicht. Im angelsächsischen Raum sieht man eher den Eigentumsaspekt als den Aspekt des Verbraucherschutzes. Das gilt allerdings nicht für Fälle von Spionage oder andere Regierungsaktivitäten, die in den USA nicht als problematisch angesehen werden. Diese Sichtweise dagegen haben wir vor allen Dingen hier in Europa und ganz besonders in Deutschland, denn wir führen den Datenschutz auf die Menschenwürde zurück, auf ein ethisches Fundament, und das halte ich auch für richtig.

Markus Löning: Deutschland hat den Missbrauch durch die Gestapo und durch die Staatssicherheit erlebt. Wir haben gesehen, dass staatliche Macht, die Konzentration von Wissen und Information, Missbrauch nach sich ziehen kann, der zu schlimmen Rechtsverletzungen führt. Das kennen Amerikaner und Briten aus ihrer Geschichte so nicht. Selbst die Niederländer sehen das unproblematischer.

Volker Lüdemann: Andererseits ist der Begriff der Menschenwürde in Europa relativ einheitlich, aus der Aufklärung und der Kulturgeschichte insgesamt heraus. Bei uns wird die Menschenwürde stärker betont, die – änderungsfest – in Artikel 1 des Grundgesetzes verankert ist. Das ist der Kern unseres anthropozentrierten Rechtsbildes, die Intimsphäre, auch wenn diese juristisch nicht recht fassbar ist. Und genau dazu gehören eben viele der personenbezogenen Daten.

Zoë Holz: In den Medien wurde vor einiger Zeit über einen Vater berichtet, der durch personalisierte Werbung unabsichtlich von der Schwangerschaft seiner Tochter erfuhr. Man wurde auch über einen Mann informiert, der auf mehrere Menschen geschossen hatte und durch die Sammlung und Auswertung persönlicher Daten gefasst werden konnte. Die Daten stehen also dafür zur Verfügung, und es wird gemacht. Wie ist aber derzeit die rechtliche Situation? Ist das erlaubt? Was ist erlaubt? Gibt es überhaupt Gesetze, die das regeln?

Volker Lüdemann: Die rechtliche Situation stellt sich wie folgt dar: Ein deutsches Unternehmen, das in Deutschland Daten verarbeitet, ist rechtlich gebunden. Es muss sich an die Gesetze halten, d.h., es ist alles verboten, was nicht erlaubt ist. Gesetzlich zulässig sind aber Datenerhebungen, die staatlicherseits im Namen eines allgemeinen Interesses für nötig befunden werden, z.B. die Meldedaten. Gesetzlich erlaubt ist auch, bei einem Kaufvertrag etwa die Abrechnungsdaten zu erheben, andernfalls könnte man *online* keinen Kaufvertrag schließen. Auf der Ebene der EU gibt es 28 verschiedene, teils einander widersprechende Datenschutzgesetzgebungen. Große Firmen wie Amazon, Twitter, Facebook gehen dann z.B. nach Irland, wo das geringste Niveau des gesetzlichen Datenschutzes gilt. Wenn international tätige Unternehmen ihren Sitz außerhalb Europas haben, können sie ihre Prozesse auch so gestalten, dass sie überhaupt nicht europäischem Recht unterliegen. Dann ist man zwar nicht im rechtsfreien Raum, aber in Amerika, und Amerika ist keineswegs rechtsfrei! Im Datenschutzrecht ist es allerdings sehr schwach. Dort hat man einfach ein anderes Grundverständnis darüber und denkt: *business first*. Deshalb hilft die

Regelung, in Deutschland Datenschutzgesetze zu machen, ein Stück weit, aber das wird Google, Amazon, Facebook nicht bremsen.

Arnulf von Scheliha: Frau Morik, Sie unterscheiden zwischen ›guten‹ Wissenschaftlern und der kommerziellen Verwertung durch die angesprochenen Konzerne. Als Universitätslehrerin bilden Sie diejenigen mit aus, die später in diesen Unternehmen arbeiten und dazu beitragen, dass solche Dinge passieren, wie wir sie beklagen. Wie können die Ethik der akademischen Lehre und die Standards, die in der wissenschaftlichen Community gepflegt werden, so weitergegeben werden, dass möglicherweise auch in den Konzernen so etwas wie eine ethische Ausrichtung wirksam wird?

Katharina Morik: Ich lehre die für den Datenschutz geeigneten, schon genannten Techniken *privacy by design* und *privacy preserving data mining*. Anders als in der normalen Gesellschaft, die bei Facebook ganz beherzt alles Mögliche veröffentlicht und Daten durch die Welt schickt, werden innerhalb der Universität, auch in meinem Fach, diese Themen intensiv diskutiert. So wird ein Bewusstsein geschaffen, auch darüber, was man selber tun kann, um seine Privatheit zu schützen. Ich berate auch Firmen in diesem Sinne. Man muss sich im Einzelfall dafür einsetzen, die Firmen auf die Techniken hinweisen, die diese häufig verwenden wollen. Es sind ja nicht alle Firmen böse.

Markus Löning: Es ist leicht, abfällig über *Google* zu reden. Man muss aber anerkennen, dass Google ein enormer Technologie- und Fortschrittstreiber war und ist, durch die schiere Größe und durch den Betriebsgewinn, der in die Entwicklung neuer Technologien investiert wird, in einem Ausmaß, wie wir das staatlicherseits und seitens unserer Unternehmen derzeit nicht können. Beo Google mögen andere Vorstellungen vom Schutz der Privatsphäre bestehen, aber es steht auch ein starker Drang dahinter, neue Dinge zu entwickeln, um die Lebensqualität allgemein zu verbessern.

Zoë Holz: Wir reden jetzt viel über Konzerne, die eine Art Oligopol über die existierenden und zukünftigen Datenmassen besitzen. Vor wem muss ich mehr Angst haben – vor der Regierung, die mich kontrolliert, oder vor der gesellschaftlichen Macht von Konzernen wie Google oder Facebook?

Markus Löning: Angst ist überhaupt nicht angebracht. Wir müssen einfach klären, was im Einzelnen an unserer Internetnutzung problematisch ist und was man tun kann, um das zu ändern. Wir reden jetzt über Google, NSA etc. Was Geheimdienste angeht, so bin ich der Ansicht, dass der russische

und der chinesische Geheimdienst in weit größerem Maß Sorge bereiten als die NSA. Mit diesen Diensten kann man nicht darüber diskutieren, was sie tun und ob es dafür eine überprüfbare Rechtsgrundlage gibt.

Wer bei uns Einwände gegen das Handeln von NSA oder deutschen Geheimdiensten hat, kann zumindest eine Debatte darüber anstoßen, kann darüber in der Zeitung schreiben, kann versuchen, etwas zu bewegen. Meine Freunde in China haben keine solche Chance. Sie werden in Arbeitslager gesperrt, wenn sie das zum Thema machen. Das bringt, so meine ich, auch eine Verpflichtung mit sich, hier bei uns etwas zu tun, d.h. für uns diese *Privacy*-Debatte zu führen. Datenschutzregeln für die Firmen festzulegen, ist letztlich Aufgabe des Gesetzgebers bzw. des Staates. Wir als Gesellschaft müssen der Politik sagen: So und so sollen die Regeln aussehen, nach denen gespielt werden muss. Die heutige Diskussion, die Sie organisiert haben, kann einen wichtigen Beitrag zur Meinungsbildung leisten: Was finden wir als Gesellschaft gut? Was finden wir schlecht? Und wie wollen wir verhindern, dass die schlechten Dinge geschehen?

Publikum: Das Leben sei mit den neuen digitalen Techniken besser und einfacher geworden, hieß es. Ist das die Wahrheit? Brauche ich eine ›intelligente‹ Waschmaschine? Hat sich unser Stromverbrauch dadurch reduziert? Nein, wir verzeichnen einen höheren Energieverbrauch. Wir brauchen ständig neue Handys. Stets müssen neue Ressourcen angezapft werden, um den geweckten Bedarf zu decken. Der CO_2-Ausstoß ist gestiegen, nicht gesunken.

Volker Lüdemann: Die Vorteile neuer Techniken kann man kaum leugnen: Wir nutzen den Komfort unserer *Smartphones.* Mit *smart grids*, smarten Stromnetzen, können wir große Infrastrukturprojekte überflüssig machen. Aber wir müssen auch fragen, was wir bei all diesen Vorteilen am Ende verlieren. Heute sieht es aus, als würden wir zu ›gläsernen Bürgern‹, wenn die Entwicklung sich fortsetzt. Unsere Grundwerte wie etwa die Menschenwürde müssen gesichert werden, darauf wollen wir nicht verzichten. Vielleicht muss Europa dies stärker gegenüber den USA als dem Sitz der derzeit größten Internet-Unternehmen betonen. Deutsche Firmen müssen sich heute strikt an das amerikanische Recht halten, amerikanische Firmen aber nicht an das europäische. Europa hält nicht wirklich dagegen, weil wir nicht mit einer Stimme sprechen können. Das zeigt auch das angestrebte Freihandelsabkommen TTIP mit seinen Schiedsgerichten, die nicht in unsere Rechtsordnung passen, wie ich meine. *Big Data* hat einen weiteren Nachteil, der ein ethisches Problem berührt: Wenn mithilfe von *Big Data* z.B. einzelne Personen aussortierbar werden und keine Angebote mehr

bekommen oder keine Krankenversicherung, dann ist das diskriminierend. Wir Menschen werden dadurch nicht gleicher, sondern ungleicher, denn durch den Vergleich der Profile wird jede Ungleichheit offenbar. Wir müssen nicht leben wie die *Amish People* und ganz auf moderne Technik verzichten. Aber wir müssen bedenken, wie weit die Folgen unseres Tuns reichen und was wir anderen damit antun. Wer jederzeit zahlungsfähig ist, ist bei *Big Data* gut aufgehoben: Man weiß z.B., dass Besitzer von *Apple*-Computern, wenn sie ein Produkt im Internet suchen, im statistischen Durchschnitt bereit sind, dafür höhere Preise zu zahlen. Ihnen werden sofort auch andere Werbeanzeigen geliefert. Solche Praktiken fordern den Kern unseres Menschenbildes heraus: Sind wir bereit, für einen Zugewinn an Luxus in Kauf zu nehmen, dass an anderer Stelle Menschen aus der Gesellschaft herausfallen?

Markus Löning: Am Beispiel der Autoversicherung ist das gut nachvollziehbar: Bei einer individualisierten Autoversicherung werden die im Auto generierten Daten an die Versicherung übergeben. Fährt man vorsichtig und hält sich an die Regeln, bekommt man z.B. einen Beitragsrabatt von 30%. Alle finden das großartig und machen mit. Dadurch wächst der Druck auf jeden Einzelnen, und wer das Geforderte nicht erreicht, muss höhere Beiträge zahlen. Dieses Modell könnte in die Aufforderung des Staates münden, alljährlich am 31. Dezember den USB-Stick mit den Fahrverhaltensdaten des abgelaufenen Jahres abzugeben, damit nachträglich werden kann, ob man sich immer an die Verkehrsregeln gehalten hat. Damit würden Bußgeldbescheide auch im Nachhinein noch möglich!

Hier ist zu fragen: Wie begrenzen wir solchen möglichen Missbrauch?

Publikum: Wir erfahren ja schon seit einiger Zeit, dass Firmen oder Geheimdienste uns überwachen und unsere Daten sammeln. Wie ist es zu erklären, dass es keinen größeren Widerstand in der Gesellschaft gibt?

Sind wir zu bequem, oder überschauen wir als Normalbürger die technisch anspruchsvollen Verfahren einfach zu wenig?

Volker Lüdemann: Früher waren die technischen Aspekte weniger kompliziert. Man bemerkt eine Entsolidarisierung, ziviler Ungehorsam gehört nicht mehr zu den obersten Werten. Wir sind alle ein bisschen angepasster.

Publikum: Aber gegen wen sollen wir demonstrieren? Bei der Volkszählung in den 1980er Jahren war das klar. Geht es heute gegen Google, gegen die NSA, gegen Geheimdienste? Ich habe den Eindruck, wir wissen gar nicht, wer eigentlich verantwortlich zu machen wäre. Da ist etwas

total außer Kontrolle geraten. Der Protest gegen die Volkszählung war zu recht klar an den Staat adressiert. Heute ist das nicht mehr so eindeutig.

Katharina Morik: Technisch ist heute alles möglich, und ich frage mich wirklich: Warum gibt es in dieser Sache keine Riesendemos? Würde der Gesetzgeber *privacy preserving* zur Pflicht machen, würden dies die Firmen ganz schnell umsetzen. Man muss es ihnen nur gesetzlich vorschreiben!

Markus Löning: Es ist die Pflicht des Staates, d.h. der Bundesregierung, der Landesregierungen, aller Parlamente, die Grundrechte der Bürger zu schützen. Daran müssen die Parlamentarier ab und zu erinnert werden. Sie wollen wiedergewählt werden und werden vor allem dann tätig, wenn sie wissen, dass die Wähler sauer sind. Anzusprechen sind die für die Kontrolle der Geheimdienste zuständigen Abgeordneten. Diese Dienste werden aus meiner Sicht nicht ausreichend kontrolliert. Niemand weiß genau, was der BND und die Verfassungsschützer machen. Ich will nichts unterstellen, aber in einer Demokratie muss es eine effektive, vernünftige Kontrolle geben, durch Parlamente und durch Gerichte. Dann sollten wir mit unseren europäischen Freunden sprechen. Es ist immer von der Wertegemeinschaft in Europa die Rede: Die Würde des Menschen und der Schutz von Bürgerrechten sind von zentraler Bedeutung für die EU. Unter uns Europäern muss klar sein: Wir spionieren uns nicht gegenseitig aus, wir respektieren die Grundrechte anderer, es wird nur abgehört, wenn es einen richterlichen Beschluss bzw. ein rechtsstaatliches Prozedere gibt. Das müssen wir von der Politik einfordern. Leider interessiert das derzeit die Verantwortlichen in Berlin, im Bundestag und in der Bundesregierung wenig. Wenn wir Europäer eine Einigung in diesen Fragen erzielen, würde das Bewegung in die Debatte in den USA bringen. Auch in den USA gibt es Bürgerrechtsorganisationen und eine Menge Interessierter, die versuchen, die Dinge in Bewegung zu bringen. Mit denen kann man zusammenarbeiten.

Publikum: Stimmt es denn, dass Datenschutz heute ein größeres Thema in der Gesellschaft geworden ist und dass die Verbraucher inzwischen vorsichtiger mit ihren Daten umgehen? Oder wird der NSA-Skandal vorbeigehen, ohne dass die Leute aufwachen, vor allem die jüngere Generation?

Markus Löning: Wir reden hier über neue Technologien, und wir sind noch dabei, sie zu entdecken, darüber zu diskutieren und zu verstehen, welche Missbrauchsmöglichkeiten damit verbunden sein können. Die Menschen versuchen, mit der Entwicklung Schritt zu halten. Und auch die Unternehmen wollen vorne bleiben: Apple und Google arbeiten an verbes-

serten Verschlüsselungstechniken. Als Optimist glaube ich, dass auch die Jugendlichen clever sind und lernen, mit neuen Herausforderungen vernünftig und verantwortungsbewusst umzugehen.

Publikum: Wird in den Schulen ausreichend über die neuen Kommunikationstechnologien und neuen Medien aufgeklärt? Unsere Kinder wachsen mit Medien auf, von denen Gefahren ausgehen können. Kinder wissen nicht von selbst, wie sie damit umzugehen haben. Wie kann unsere Gesellschaft die Aufklärung verbessern?

Volker Lüdemann: Es ist wichtig, dass die Schulen ihren Bildungsauftrag wahrnehmen. Wenn die Menschen darüber informiert wären, welche Entwicklungen im Gange sind, würden sie etwas dagegen unternehmen. Jedenfalls – und damit wäre schon viel erreicht – läge es dann im Bereich der eigenen Entscheidung, etwas zu unternehmen. Wenn wir zum Handeln befähigt werden, sind wir wieder Subjekte und nicht reine Objekte des Handelns anderer.

Ich glaube aber, gerade die Medien wollen aufklären. Ich selbst bekomme viele Anfragen von Zeitungen, die ihren Lesern fundierte Informationen über die verschiedenen Aspekte neuer Kommunikationstechnologien bieten möchten. Ein Problem ist allerdings oft die Komplexität technischer Sachverhalte, die schwerlich in einem zweiminütigen Rundfunkinterview erläutert werden können. Aber die Mühe sollte sich lohnen, denn gerade bei den Jugendlichen bemerke ich ein ganz großes Interesse.

Katharina Morik: Der Bildungsauftrag der Schulen ist wirklich sehr wichtig. Im Ergebnis der Auseinandersetzung mit dem Thema wird man vielleicht nicht nur *gegen* etwas demonstrieren, sondern entdeckt auch die Möglichkeit, *für* etwas zu demonstrieren. Die Bürger könnten fordern: Wir möchten nur noch *privacy-preserving*-Techniken, andere akzeptieren wir nicht. Und wir möchten gerne eigene Entwicklungen in Europa sehen, statt von anderen abhängig zu sein. Wir könnten auch fordern, dass die in unseren Autos erfassten Daten nicht an Dritte gesendet werden. Dafür gibt es sicherlich technische Lösungen, aber es muss von den Bürgern gewollt und gefordert werden.

Publikum: Ich gehöre der älteren Generation an und möchte hier drei Erfahrungen einbringen. Viele Durchschnittsdeutsche sagen von sich: Ich habe nichts zu verbergen, und erklären so ihr Einverständnis mit der Überwachung des Internet oder der öffentlichen Räume, Straßen und Plätzen durch Videokameras. Ein Protestpotenzial ist hier also kaum zu

erwarten. Die zweite Erfahrung ist, dass ich als Nutzer des Mediums Computer z.B. bei Facebook unfreiwillig zum Datenlieferanten werde. Wie kann das sein? Die dritte Erfahrung ist, dass ich eine Anwendung auf meinem *Smartphone* nicht deinstallieren kann, auch wenn ich es möchte. Es geht nur um den Preis, dass es nachher nicht mehr funktioniert.

Publikum: Die Frage, warum sich gegen die ungewollte Sammlung von Nutzerdaten keine lauten Proteste erheben, lässt sich mit dem Hinweis auf die Geschwindigkeit beantworten, mit der neue Entwicklungen in den Alltag Einzug halten. Eine Protestbewegung auf die Beine zu stellen, braucht Zeit, selbst wenn sie nur auf Grundlegendes konzentriert ist. Ich habe den Eindruck, dass unsere Gesellschaft durch die Sozialen Netzwerke immer autoritärer wird, wohlgemerkt: die Gesellschaft, nicht unbedingt der Staat. Es gab mal eine Piraten-Partei, die sich ins Programm geschrieben hatte, all das öffentlich zu machen, was hier diskutiert wurde, und eine transparente Demokratie zu schaffen, eine Internet-Demokratie. Dieser Impetus, etwas zu tun für mehr Demokratie im Netz und in der Gesellschaft, hat offenbar keine ausreichende gesellschaftliche Basis.

Markus Löning: Wer glaubt, nichts tun zu können, frage mal die Menschen in Russland oder aktuell in Hongkong. Dort tut sich nämlich etwas. Ich rate allen Interessierten: Werden Sie Mitglied bei den Piraten, bei der FDP, bei der Union, egal wo, machen Sie etwas! Oder gründen Sie eine Bürgerinitiative. Ich weiß, wie mühselig das sein kann und wie langsam es geht, aber wir können etwas tun. Wenn wir dazu bereit sind und Leute finden, die mit uns streiten, gelingt uns das auch. Ich glaube nicht, dass unser Land autoritärer wird. Das liegt in unserer Hand! Wir müssen uns nur auch durchsetzen und keine Angst haben.

Volker Lüdemann: Manche Internet-Ethiker zeichnen das Bild einer im Grunde mittelalterlichen Situation: War es früher der Landbesitz, der die Mittellosen in Abhängigkeit hielt, so kann unsere Unabhängigkeit heute durch die Daten bzw. das dahintersteckende Wissen bedroht werden. Wissen bedeutet zweifellos Macht, und die Konzerne, die neuen Monolithe, sind mächtig. Aber wir haben Erfahrungen, was die Bekämpfung von Monopolen angeht. Es gibt das Wettbewerbsrecht, es gibt die Initiative zur ›Zerschlagung von Google‹. Das Wettbewerbsrecht bietet schon längst Möglichkeiten eines Eingriffs, wenn wir nur wollten. Politiker und die Verantwortlichen an verschiedenen Stellen, auch wir selbst, müssen uns dafür einsetzen, dass etwas geschieht. Auf europäischer Ebene könnten wir unsere Standards durchsetzen, und so klein ist Europa nicht.

Katharina Morik: Schon vor 15 Jahren forderten Informatiker, in Europa eigene Produktionsmittel für die Computertechnik zu entwickeln, quasi Maschinen, die Maschinen produzieren, die Maschinen produzieren. Das ist das, was Google gemacht hat. Unsere Forschungsförderung hat hier nicht Schritt gehalten, deshalb, so befürchte ich, wurden wir abgehängt und können den Vorsprung kaum mehr einholen.

Zoë Holz: Sie haben ja alle drei ein Facebook-Profil und sind dort aktiv. Ich würde gerne wissen: Was raten Sie unserem Bewerber Maik Tappe? Wie soll er sich verhalten? Wie kann er verhindern, dass ihm Ähnliches wieder passiert? Soll er vor Gericht gehen?

Markus Löning: Er sollte sich einen anderen Job bei einer anderen Firma suchen. Ich würde nicht bei einer Firma arbeiten wollen, die derartige Methoden nutzt. Außerdem sollte er seine *privacy*-Einstellungen bei der Internetnutzung überprüfen.

Volker Lüdemann: Dummerweise weiß er ja gar nichts von der Ausforschung seiner Person und kann deshalb nichts machen. Juristisch ist da wohl nichts zu machen, selbst für die Berufung auf den allgemeinen Gleichbehandlungsgrundsatz wären Anzeichen dafür erforderlich, dass etwas Irreguläres passiert ist. Wenn eine solche Recherche clever gemacht wird, kann man nichts dagegen tun, und das führt wieder zu dem Punkt: Wissen bedeutet eben Macht. Deshalb muss man sich gut informieren, was mit den Daten geschieht. Dann ist man ein bisschen mächtiger, man lässt bestimmte Dinge, oder man sucht nach Indizien.

Arnulf von Scheliha: Also sind Aufklärung, Bildung und ein kritisches Bewusstsein, was die Machtverhältnisse angeht, nötig, um sich im Internet bewegen zu können, um die Chancen und die Freiheiten, die es bietet, ausnutzen zu können?

Katharina Morik: Eine passende Metapher für Internet-Kommunikationsplattformen wie Facebook ist das ›globale Treppenhaus‹. Niemand würde doch in einem Treppenhaus nackt herumlaufen, oder? Und jeder sollte im Grunde wissen, welche Gespräche er im Treppenhaus besser nicht führt.

---

1 Kursleitung: Holger Niehoff

2 Vgl. http://www.welt.de/wirtschaft/karriere/article125314665/Software-scannt-Facebook-Profile-von-Bewerbern.html