Freiheit und Verantwortung in den IT-Wissenschaften

Workshop

Freitag · 27. Oktober 2017 · 10:30 bis 17:00 Uhr
Darmstadtium
Schloßgraben 1
64283 Darmstadt

Programm

Einführung

Hans-Jürgen Prömel, Präsident der Technischen Universität Darmstadt

(Folie 2)

Liebe Frau Friedrich, lieber Herr Allgöwer, liebe Referentinnen und Referenten, lieber Herr Buchmann, liebe Gäste, ich darf Sie herzlich begrüßen!

Von George Bernard Shaw stammt das Zitat: „Liberty means Responsibility. That is why most men dread it."

Doch das Zusammenspiel von Freiheit und Verantwortung ist seit jeher elementar in Wissenschaft und Forschung und, seriös betrieben, kein Grund zur Furcht.

Die im Grundgesetz verankerte Forschungsfreiheit eröffnet Möglichkeiten und schafft Spielräume. Doch gleichzeitig eröffnen sich dringende Handlungsfelder, um missbräuchliche Verwendung zu unterbinden, vor Risiken und Gefahren zu warnen und die Gesellschaft aufzuklären. Die Entdeckung der Kernspaltung oder die Erfindung des Dynamits sind Beispiele für dieses Spannungsfeld. Auch gibt es Errungenschaften, bei denen Nutzen oder Risiko irgendwann überwiegen und das jeweils andere in den Hintergrund tritt, und das mag sich auf der Zeitachse durchaus ändern: Wir reden hier über Dual Use.

Bei den IT-Wissenschaften – und hier denke ich an die alltägliche Informations- und Kommunikationstechnologie, wie wir sie täglich verwenden – liegen der Nutzen und die Vorteile auf der Hand: Wir können von unterwegs telefonieren, zwischendurch einen Termin beim Arzt ausmachen, per Mausklick ein Buch bestellen oder über unsere App ein Bahnticket buchen. Und auch im öffentlichen und privatwirtschaftlichen Sektor, sei es bei den Banken, in der Industrie 4.0 oder in der Verwaltung, erleichtern innovative IT-Lösungen zunehmend alltägliche Arbeiten und bieten Lösungen für Herausforderungen.

Was jedoch vielen Nutzern nicht immer ganz klar ist oder nur langsam ins Bewusstsein dringt, ist, dass jeder Nutzen auch missbraucht werden kann. Fragen des Datenschutzes, der Spionage oder gar von terroristischen Angriffen auf ganze IT-Systeme kommen einem dabei in den Kopf.

Die Forschung in den IT-Wissenschaften sollte nicht nur auf neue, innovative und bahnbrechende Lösungen Wert legen, sondern auch vor Risiken warnen, Schwachstellen und Sicherheitslücken identifizieren und diese reparieren, wo das möglich ist. Gleichzeitig ist hier der Dialog mit Wirtschaft, Politik und Wissenschaft unerlässlich.

Doch genau hier greift wieder das Spannungsfeld, in dem wir uns befinden: Wenn Sie auf Sicherheitslücken hinweisen, können Sie nicht ausschließen, dass diese die Menschen erst auf die Idee bringen, sie zu nutzen. Wenn Sie eine neue Technologie entwickeln, verhindern Sie nicht automatisch, dass diese nicht missbraucht wird, und wenn Sie Ergebnisse publizieren, verhindern Sie nicht, dass diese missdeutet oder falsch verstanden werden und so vielleicht zu noch mehr Unsicherheit führen.

Deshalb freue ich mich, dass Sie zu Ihrem heutigen Workshop zum Thema Freiheit und Verantwortung in den IT-Wissenschaften in Darmstadt zusammengekommen sind. Darmstadt zählt, was den Bereich IT Security angeht, zu den bedeutenden Standorten nicht nur in Deutschland, sondern in Europa und weltweit. Wir haben an der Technischen Universität Darmstadt in den letzten Jahren diesen Bereich strategisch aus- und aufgebaut und inzwischen einige Erfahrungen in der IT-Sicherheitsforschung. Diese spielt an der Universität auch als Profilbereich eine bedeutende Rolle. Im Profilbereich Cybersicherheit, den

wir als CYSEC bezeichnen, arbeiten Wissenschaftlerinnen und Wissenschaftler, und zwar – das ist ein wichtiger Punkt – nicht nur aus der Informatik, sondern auch aus der Physik, Psychologie, Elektro- und Informationstechnik oder den Wirtschaftswissenschaften gemeinsam mit den Informatikern an aktuellen Herausforderungen der IT-Sicherheit.

Diese Interdisziplinarität ist meines Erachtens besonders wichtig, denn die dringenden Herausforderungen der IT-Sicherheit lassen sich nicht nur von der Informatik allein lösen. Stattdessen müssen Brücken zwischen den Disziplinen geschlagen werden. Und das tun unsere Forscherinnen und Forscher in dem Sonderforschungsbereich CROSSING für Kryptographie in einem Intel-Lab, das gerade in die zweite Phase gegangen ist, wo wir europaweit den Lead haben; oder in dem vom Land Hessen geförderten Projekt NICER [Networked Infrastructureless Cooperation for Emergency Response], in dem erforscht wird, wie infrastrukturlose Informations- und Kommunikationstechnologie im Krisenfall Menschen vernetzen und damit eine Kooperation zur Bewältigung von Krisen ermöglichen kann.

Als Partner im Center for Research in Security and Privacy, das vom Bund und vom Land Hessen gerade verstetigt wurde, tragen wir gemeinsam mit unseren Partnern von der Fraunhofer-Gesellschaft und der Hochschule Darmstadt wesentlich zum Erfolg des Standorts Darmstadt und zur Bedeutung der hiesigen IT-Sicherheitsforschung bei.

Die Verantwortung, die wir hierbei tragen, verlieren wir nicht aus dem Blick. So hat sich die Technische Universität Darmstadt beispielsweise in ihrer Grundordnung eine Zivilklausel gegeben, die darauf ausgerichtet ist, dass Forschung, Lehre und Studium ausschließlich friedlichen Zielen verpflichtet sind und zivile Zwecke erfüllen sollen. Die Ethikkommission an der TU Darmstadt dient zudem als Anlaufstelle für Fragen und Zweifel, liefert Anregungen für Reflexionen und Selbstvergewisserung und prüft die ethische Zulässigkeit von Forschungsvorhaben. Als Ansprechpartner für Gesellschaft, Wirtschaft und Politik versuchen unsere Wissenschaftlerinnen und Wissenschaftler zu beraten, aufzuklären und dabei auch Forschungsergebnisse in für Laien verständlicher Sprache zu vermitteln, wie zum Beispiel zuletzt im Funkkolleg Sicherheit, das vom Hessischen Rundfunk veranstaltet und von der Technischen Universität Darmstadt maßgeblich mitgestaltet wurde.

Ich freue mich also sehr, dass Sie heute weder die Freiheit noch die Verantwortung fürchten, sondern sich diesem wichtigen Thema in dem Workshop widmen. Ich wünsche Ihnen einen spannenden Tag und viele anregende und inspirierende Gespräche. Herzlichen Dank.

Bärbel Friedrich ML, Vorsitzende des Gemeinsamen Ausschusses zum Umgang mit sicherheitsrelevanter Forschung

(Folie 3)

Sehr geehrter Herr Präsident, lieber Herr Prömel, auch ich freue mich, bei Ihnen in Darmstadt zu sein. Sie haben mit Ihrem Grußwort schon eine vorbildliche Einführung in die Thematik gegeben.

Ich danke auch Herrn Buchmann, dem Vertreter hier vor Ort, der Mitglied des Gemeinsamen Ausschusses ist, für die Organisation.

Im Namen der Präsidenten der Leopoldina, der Nationalen Akademie der Wissenschaften, Herrn Professor Hacker, und der Deutschen Forschungsgemeinschaft [DFG], Herrn Professor Strohschneider, möchte ich Sie herzlich begrüßen zu dem Workshop, der in die Dual-Use-Problematik einführen wird.

Mein Name ist Bärbel Friedrich, ich bin derzeit wissenschaftliche Direktorin des Alfried Krupp Wissenschaftskollegs in Greifswald und emeritierte Professorin für Mikrobiologie an der Humboldt-Universität. Ich war sechs Jahre Vizepräsidentin der Deutschen Forschungsgemeinschaft und habe zehn Jahre als Vizepräsidentin in der Leopoldina gewirkt und mich speziell auch mit diesen Fragen befasst.

(Folie 4)

Lassen Sie mich kurz die Leopoldina in einigen Worten vorstellen. Sie ist eigentlich die älteste fortdauernde wissenschaftliche Akademie der Welt und wurde schon im 17. Jahrhundert gegründet. Was für uns wichtig ist: Sie verfügt über 1500 Mitglieder aus allen Disziplinen und aus dreißig Ländern, also ein breites Wirkungsspektrum. Sie wurde nach der Wiedervereinigung 2008 zur Nationalen Akademie der Wissenschaften berufen. Als solche hat sie das Mandat erhalten, die deutsche Wissenschaft international zu repräsentieren und – was heute uns beschäftigt – Politik und Gesellschaft zu beraten.

(Folie 5)

In diesem Zusammenhang hat die Leopoldina seit 2009 nahezu 200 Stellungnahmen, Diskussionspapiere und Reports veröffentlicht, teilweise allein, aber in der Regel mit Partnern wie der Union der deutschen Akademien der Wissenschaften, der Akademie der Technikwissenschaften (acatech), aber auch – und das spielt heute eine Rolle – zusammen mit der DFG.

Hier sehen Sie für die jüngste Publikation: „Ethische und rechtliche Beurteilung des *genome editing* in der Forschung an humanen Zellen“, ein sehr aktuelles Gebiet; „Social Media und digitale Wissenschaftskommunikation“, was vielleicht in den heutigen Bereich hineinreicht, und „Additive Fertigung“. Was uns heute beschäftigt, ist „Wissenschaftsfreiheit und Wissenschaftsverantwortung“, eine Broschüre, die 2014 entstanden ist.

(Folie 6)

Zur Deutschen Forschungsgemeinschaft brauche ich nichts zu sagen. Aber was sie gemeinsam hat mit der Leopoldina: Sie ist eine Selbstverwaltungsstruktur. Die Mitglieder der Leopoldina werden gewählt, und so auch die der DFG. Die Kernaufgabe ist – und da unterscheidet sie sich von der Leopoldina – im Wettbewerb die besten Forschungsvorhaben auszuwählen. Sie ist also eine Organisation zur Forschungsförderung, was die Akademie nicht ist. Aber wie die Akademie hat sie auch Aufgaben in der Beratung von Politik und Öffentlichkeit, denn sie hat die erforderliche Expertise.

(Folie 7)

Zur Dual-Use-Problematik; ich beginne mit 2012. Auslöser der heftigen internationalen Diskussionen waren zwei Veröffentlichungen[1] in *Science* und *Nature* aus dem lebenswissenschaftlichen Bereich, die ungefähr zeitgleich veröffentlicht wurden. Eine Arbeitsgruppe aus den Niederlanden um Ron Fouchier hat Experimente zu dem Hühnergrippevirus H5N1 gemacht; das ging auch durch die Presse. Normalerweise wird dieses Virus nur in engem Kontakt mit Federvieh übertragen. Aber diese Arbeitsgruppe hat – wie auch die Gruppe von Kawaoka in Japan und USA – Experimente dazu gemacht, indem sie dieses Virus genetisch so verändert haben, dass es nunmehr zwischen Säugern über die Luft übertragen wird (Tröpfcheninfektion). Das Testsystem in diesem Fall waren Frettchen.

[1] Herfst, Fouchier et al. (2012). *Airborne transmission of influenza A/H5N1 virus between ferrets*. Science, 336 (6088), 1534–1541; Imai, Kawaoka et al. (2012). *Experimental adaptation of an influenza H5 HA confers respiratory droplet transmission to a reassortant H5 HA/H1N1 virus in ferrets*. Nature 486 (7403), 420–428.

Das hat für Wirbel gesorgt, denn es wurde gefragt: Sind solche Experimente nötig? Es hatte sich herausgestellt, dass lediglich fünf kleine Mutationen im Gen, nur ein Basenaustausch erforderlich war, um diesen Effekt zu erzielen.

(Folie 8)

Auf dieser Folie sehen Sie den mächtigen Herrn Fouchier. Wir haben im Juni 2012 eine Friedrich-Loeffler-Lecture im Alfried Krupp Kolleg in Greifswald veranstaltet und hatten ihn dazu eingeladen; das war, bevor diese Publikationen erschienen waren. Mein Kollege Thomas Mettenleiter vom FLI [Friedrich-Loeffler-Institut] in Riems und ich wirken dagegen geradezu wie Zwerge.

Aber die Gruppen verteidigen ihre *gain-of-function*-Experimente derart, dass sie sagen: Dadurch lernen wir, wie sich solche Viren auch in der freien Natur evolutiv verändern können und dann zu solchen virulenten Produkten mutieren.

(Folie 9)

Daraufhin hat auch die Bundesregierung den Deutschen Ethikrat beauftragt, sich mit dieser Thematik zu beschäftigen; in den USA gab es ähnliche Aktivitäten. Die Definition Dual Use Research of Concern bezieht sich in diesem Fall vornehmlich auf

> „lebenswissenschaftliche Arbeiten […], bei denen anzunehmen ist, dass sie Wissen, Produkte oder Technologien hervorbringen, die unmittelbar von Dritten missbraucht werden können und die öffentliche Gesundheit oder Sicherheit und die natürlichen Lebensgrundlagen bedrohen."

(Folie 10)

Daraufhin hat der Ethikrat ein Positionspapier erarbeitet, das im Mai 2014 erschien mit dem Titel „Biosicherheit, Freiheit und Verantwortung in der Wissenschaft". Darin sind vier Punkte aufgeführt, die ich kurz referieren möchte:

[1] Schärfung des Bewusstseins für Biosecurity-Fragen in der Wissenschaftsgemeinschaft; [2] Erstellung eines bundesweit gültigen Forschungskodex für den verantwortlichen Umgang mit Biosecurity-Fragen; [3] Berücksichtigung von Aspekten des *dual use research of concern* (DURC) bei der Forschungsförderung; und jetzt kommt der vierte Punkte, worüber es andere Ansichten gab, und zwar Erlass von gesetzlichen Regelungen, Einsatz einer nationalen DURC-Kommission und Beratungspflicht für Wissenschaftler.

(Folie 11)

Parallel dazu haben DFG und Leopoldina über diese Situation gearbeitet, und zwar unter dem Titel „Wissenschaftsfreiheit und Wissenschaftsverantwortung". Sie haben ebenfalls Empfehlungen zum Umgang mit sicherheitsrelevanter Forschung ausgesprochen. Die Erkenntnis war, dass sich diese Fragen nicht nur auf lebenswissenschaftliche Probleme konzentrieren, sondern für alle wissenschaftlichen Bereiche gelten, und dass man einen Kodex zum Umgang mit sicherheitsrelevanter Forschung für alle Bereiche entwickeln müsste. Das ist in dieser Broschüre ausführlich beschrieben.

(Folie 12)

Was haben wir für Standpunkte definiert? Die Wissenschaft soll selbst ethische Prinzipien sowie Mechanismen zum verantwortungsvollen Umgang mit Forschungsfreiheit und Forschungsrisiken entwickeln.

Wie ich schon sagte: Die Dual-Use-Problematik gilt für alle Wissenschaftsbereiche. Wir haben exemplarisch einige genannt, zum Beispiel:

– Materialforschung und Nanotechnologie: Angriffswaffen?

- Forschung zu Industrierobotern – diese könnten zum Bau von Kriegsdrohnen verwendet werden;
- Sammlung und Analyse personenbezogener Daten: Verletzung von Persönlichkeitsrechten?
- Verhaltens- und Sozialwissenschaften: gezielte Meinungsmanipulation;
- Neurobiologie und Psychologie: Einflussnahme auf Gehirnfunktionen und Verhalten.

Diese Liste ließe sich beliebig ergänzen.

(Folie 13)

Wir sind von dem Prinzip ausgegangen: Wissenschaft braucht Freiheit – Freiheit erfordert Verantwortung. Die Wissenschaftsfreiheit ist auch gesetzlich manifestiert: Im Absatz 3 Artikel 5 des Grundgesetzes ist die Forschungsfreiheit geschützt. Aber sie wird auch in bestimmten Bereichen eingegrenzt: Wir haben viele gesetzliche Regelungen. Darüber können wir uns in Deutschland eigentlich nicht beklagen (als Biologin kann ich davon ein Lied singen).

Wir haben sie, aber wir können mit diesen Regeln nicht die letzten Risiken unserer Forschung ausschließen, sondern nur in einem begrenzten Umfang erfassen.

Daraus abgeleitet sagen wir: Es gibt eine verantwortliche Selbstregulierung der Wissenschaft. Sie ist von großer Tragweite, da sie es gestattet, flexibel auf Fälle zu reagieren, und zwar mit einer hohen Expertise.

(Folie 14)

Wir haben daraus zehn Empfehlungen abgeleitet. Diese überschneiden sich zum Teil mit dem Papier des Ethikrates, aber sind in einem allgemeinen, weiteren Rahmen gefasst:

[1] Beachtung von ethischen Grundsätzen durch den Forschenden über rechtliche Regeln hinaus; ein Bewusstsein schaffen für eventuelle Risiken, was man eigentlich macht (Awareness).

[2] Risikoanalysen von Forschungsvorhaben, dass diese angestellt werden,

[3] Risikominimierung, das ist zumindest in den Biowissenschaften ein wichtiges Thema,

[4] dass die Veröffentlichungen bereits vor dem Einreichen (wenn sie geplant sind) einer Kontrolle, einer Selbstkontrolle untergezogen werden,

[5] Dokumentation und Mitteilung von Risiken,

[6] die Schulung bereits bei Studierenden, die in die Forschung gehen, Aufklärung und Bewusstseinsschärfung;

[7] Klärung der Verantwortlichkeiten in den Arbeitsgruppen,

[8] Verfügbarkeit von Compliance-Stellen

[9] Definition von Ethikregeln. Die Deutsche Forschungsgemeinschaft hat schon in früheren Papieren gerade im Umgang mit pathogenen Organismen einen Code of Conduct herausgegeben; da müssen sich die Forschungsinstitutionen aktiv einbringen.

[10] Für unsere heutige Diskussion ist wichtig: die Einrichtung von Kommissionen für Ethik sicherheitsrelevanter Forschung [KEF].

Ich habe mit Freude vernommen, Herr Prömel, dass Sie das hier in Darmstadt schon vorbildlich realisiert haben. Zu diesem Teil wird jetzt mein Kollege fortfahren. Lieber Herr Allgöwer, ich bitte Sie nun ans Podium. Vielen Dank.

Frank Allgöwer, Vizepräsident der DFG und Vorsitzender des Gemeinsamen Ausschusses zum Umgang mit sicherheitsrelevanter Forschung

(Folie 15)

Lieber Herr Prömel, meine Damen und Herren, auch ich möchte Sie herzlich im Darmstadtium

zu unserer heutigen Veranstaltung im Namen von DFG, Leopoldina und vor allem des Gemeinsamen Ausschusses für den Umgang mit sicherheitsrelevanter Forschung begrüßen. Mein Name ist Frank Allgöwer, ich bin einer der beiden Vorsitzenden dieses Ausschusses und Vizepräsident der Deutschen Forschungsgemeinschaft. Ich bin Ingenieur, Systemtheoretiker und Regelungstechniker und im Moment im Maschinenbau tätig, aber hatte auch schon eine Professur in einer elektro- und informationstechnologischen Fakultät. Ich bin an der Universität Stuttgart tätig.

(Folie 16)

Bevor ich Ihnen den Ausschuss vorstelle, möchte ich einen Schritt zurückgehen und aus Sicht der DFG noch mal unterstreichen, was bereits Herr Prömel und Frau Professor Friedrich schon gesagt haben: Wir haben in Deutschland – auch durch die Verfassung vorgegeben – ein enormes Maß an Freiheit in der Forschung. Dieses enorme Maß an Freiheit in der Forschung muss mit einer Übernahme von Verantwortung einhergehen. Wir müssen beidem, dieser Freiheit und dieser Verantwortung gerecht werden, und zwar sowohl als Wissenschaftler, jeder Einzelne von uns, als auch die Wissenschaftsinstitutionen, die Universitäten, die außeruniversitären Forschungsinstitutionen, aber auch andere Organisationen, die mit dem Wissenschaftsbetrieb zu tun haben, wie Forschungsförderorganisationen, zum Beispiel die DFG.

Diese Verantwortung gilt in jedweder Hinsicht, aber besonders im Zusammenhang mit sicherheitsrelevanter Forschung.

Die Gefahren im Zusammenhang mit sicherheitsrelevanter Forschung und vor allen Dingen (wie schon Frau Friedrich ausgeführt hat) im Zusammenhang mit der Problematik des Dual Use Research of Concern sind jedoch manchmal nur schwer zu beurteilen. Diese möglichen Gefahren – vor allen Dingen, wenn man kein Bewusstsein für die Gefahren hat – zeichnen sich dadurch aus, dass man in diesem Spannungsfeld zwischen Nützlichkeit der Forschung, interessanter Forschung, schädlicher Forschung, aber auch von möglicherweise zu gefährlichen Auswirkungen führender Forschung schnell nicht mehr beurteilen kann, wo in diesem Spannungsfeld man sich befindet. Speziell bei Dual Use hängt das zusammen mit der unbekannten zukünftigen Handlungskette, die entstehen kann, aber auch mit der Schwierigkeit der Risikofolgenabschätzung und der Abschätzung der Stärke des Risikos,

Der Gemeinsame Ausschuss möchte hier eine Hilfestellung bieten. Er möchte den Wissenschaftlern und vor allen Dingen den Wissenschaftsinstitutionen in dieser schwierigen Problematik eine Unterstützung geben.

Wir haben das gerade schon bei Frau Friedrich gesehen: Diese Thematik wird im Moment stark durch die Lebenswissenschaften dominiert. In den Lebenswissenschaften herrscht ein großes Bewusstsein für die Problematik der sicherheitsrelevanten Forschung. Die Dual-Use-Problematik wird sorgsam beobachtet, es gibt ein Monitoring; es ist insgesamt ein recht verantwortliches Handeln in diesem Wissenschaftsbereich vorhanden, und es gibt dort die nötige Aufmerksamkeit.

Bei den Ingenieurwissenschaften ist dies eher weniger der Fall. Wir sagen spontan: So etwas gibt es bei uns einfach nicht. Aber die Frage ist natürlich, ob dem wirklich so ist; das möchte ich sogar in Frage stellen. Aber selbst wenn wir glauben, dass diese Problematik bei uns nicht so sehr vertreten ist, sollten wir zumindest ein Bewusstsein für die Problematik haben und nach

außen klar dokumentieren können, dass wir uns mit diesem Thema auseinandersetzen.

Es wurden schon Themen genannt: Kerntechnologie, Nanotechnologie, Materialwissenschaften. Im Moment ist mit der Künstlichen Intelligenz ein weiterer Bereich dazugekommen, der wie ein Hype in der Öffentlichkeit im Zusammenhang mit Sicherheitsbedenken diskutiert wird. Das dürfen wir auf keinen Fall auf die leichte Schulter nehmen.

Insofern bin ich froh, dass wir heute diese Veranstaltung haben. Ich bin auch froh, dass so viele von Ihnen gekommen sind. Es sind 80 Personen angemeldet. Man könnte sagen: 80 Personen sind nicht so viel, aber für die Informatik, einen abgegrenzten Bereich der Wissenschaften, ist das eine so große Zahl, dass ich als Ingenieur ein bisschen stolz darauf bin, dass Sie heute den Weg nach Darmstadt gefunden haben.

Jetzt möchte ich etwas zur Arbeit des Gemeinsamen Ausschusses sagen. In erster Linie richtet sich die Arbeit des Gemeinsamen Ausschusses bei der Fragestellung Wissenschaftsverantwortung – Wissenschaftsfreiheit an unterschiedliche Personenkreise: zum einen an die Wissenschaftler, aber auch an die Forschungsinstitutionen und Institutionen wie DFG und Leopoldina. Der Gemeinsame Ausschuss richtet sich speziell an die Forschungsinstitutionen und möchte ihnen eine Hilfestellung geben.

(Folie 17)

Die Forschungsinstitutionen tragen Verantwortung für ihre Forschungstätigkeiten sowohl in inhaltlicher Sicht: dass sie für die Arbeit, die in den jeweiligen Einrichtungen durchgeführt wird, Verantwortung zeigen müssen, aber auch in struktureller Sicht: Es müssen die Voraussetzungen geschaffen werden, dass die Wissenschaftler auch tatsächlich arbeiten können; Frau Friedrich hat schon die Einrichtung von Kommissionen bei Ethik in der Forschung betont. Das ist in diesem Zusammenhang eine wichtige Institution.

(Folie 18)

Was macht nun der Gemeinsame Ausschuss, welche Ziele hat er? Der Gemeinsame Ausschuss soll den Institutionen eine Hilfestellung bieten im Hinblick darauf, diese Problematik bekannt zu machen, sie in ihren jeweiligen Institutionen ins Bewusstsein zu rücken und damit aktiv umgehen zu können.

Unter anderem soll ein Monitoring betrieben werden; das macht unser Ausschuss. Wir unterstützen die Institution bei der sachgerechten Implementierung der Empfehlungen, die in den Dokumenten, die Frau Friedrich schon vorgestellt hat, gegeben wurden, speziell im Zusammenhang mit der Einrichtung von Kommissionen in der Ethik in der Forschung.

Wir stellen Informationen über Ansprechpartner bereit, sodass Wissenschaftler auch wissen, an wen sie sich wenden können. Allerdings soll die Verantwortung für einzelne Problemfälle bei der jeweiligen Forschungsinstitution verbleiben und nicht beim Ausschuss.

(Folie 19)

Nur in besonders schwierigen oder bedeutsamen Fällen wird die Kommission Unterstützung leisten, indem sie die Leopoldina bei der Einrichtung von Ad-hoc-Arbeitsgruppen unterstützt, die dann bei der Risiko-Nutzen-Bewertung auch in Einzelfällen Unterstützung leisten kann.

Ganz wichtig ist die Bewusstseinsbildung. Diese wird auch durch regelmäßige Veranstaltungen gefördert, wie wir sie heute haben. Das scheint zu funktionieren: Sie sind da, und wir können bei Ihnen ein Bewusstsein für diese Problematik wecken.

Weiterhin beobachten wir diese Problematik deutschlandweit und empfehlen DFG und Leopoldina, wie entsprechend vorzugehen wäre.

(Folie 20)

Der Gemeinsame Ausschuss wird geleitet von zwei Vorsitzenden, die jeweils vom Präsidium von Leopoldina und DFG benannt werden, und besteht aus einer Reihe von Wissenschaftlern, die Sie hier auf dieser Folie sehen.

Hier sind die ethischen und juristischen Aspekte dieser Problemstellungen stark vertreten, aber auch die Problemstellungen, wie sie in den einzelnen Gebieten vorkommen. Besonders hervorgehoben ist hier Herr Buchmann von der Technischen Universität in Darmstadt, der Kenntnisse und Umsetzungsfragen der Informatik, aber auch eine breite ingenieurwissenschaftliche Expertise in den Ausschuss einbringt. Herr Buchmann, Ihnen noch einmal herzlichen Dank für Ihr Engagement im Ausschuss und bei der Konzeption der heutigen Veranstaltung.

(Folie 21)

Wie arbeitet dieser Ausschuss? Ist er erfolgreich? Klappt es mit der Einrichtung von Kommissionen in der Ethik in der Forschung? Sie sehen hier, wie die Universitäten auf diesen Aufruf reagiert haben.

Sie sehen, dass ungefähr 110 Universitäten und außeruniversitäre Einrichtungen Ansprechpartner benannt haben, die mit der Kommission zusammen dieses Thema an den Institutionen weitertreiben können. An 24 Institutionen wurden bereits Kommissionen für Ethik in der Forschung etabliert. Weitere 34 Universitäten und außeruniversitäre Forschungseinrichtungen haben die Etablierung von KEFs geplant oder diskutieren diese zumindest. An 26 Institutionen wird diese Aufgabe von anderen Kommissionen übernommen, zum Beispiel von Ethik-Kommissionen. An acht Institutionen soll in einer Art Ad-hoc-Vorgehensweise dieser Bereich abgedeckt werden.

Insgesamt können wir sehr zufrieden sein.

Allerdings gibt es 17 unter diesen 110 Institutionen, die keine Aktivität oder keinen Bedarf sehen. Unser Ziel muss natürlich sein, dass die Balken, die da oben in dem Diagramm aufgeführt sind, deutlich größer werden, dass die Gesamtzahl noch deutlich größer wird und dass auch mehr Aktivitäten an den jeweiligen Standorten zustande kommen.

(Folie 22)

Der Ausschuss unterhält auch eine Webseite, die auch bei der Leopoldina angesiedelt ist. Die Geschäftsstelle des Gemeinsamen Ausschusses liegt bei der Leopoldina. Hier sehen Sie ein Bild dieser Webseite. Hier ist auch Darmstadt hervorgehoben, wie das Frau Friedrich gerade schon gemacht hat. Sie dürfen also sehr zufrieden sein: Sie sind vorbildlich in der Umsetzung dieser Empfehlungen.

Zum Schluss möchte ich nochmals die Wichtigkeit des Ausschusses und seine Bedeutung betonen. Der Gemeinsame Ausschuss soll kein von oben installiertes Kontrollgremium oder kein Genehmigungsgremium sein – genauso wenig wie die KEFs übrigens. Der Gemeinsame Ausschuss soll beraten und Hilfestellung bei der Umsetzung leisten. Er kontrolliert nicht, sondern soll die transparente Übernahme von Selbstverantwortung durch die Wissenschaft befördern.

Die Wissenschaft soll selbst hier die Verantwortung zeigen. Es muss uns wichtig sein, dass wir dies machen, aber auch nach außen in der Öffentlichkeit und gegenüber der Politik dokumentieren. Denn nur auf diese Art und Weise wird es uns gelingen, die Forschungsfreiheit, die uns gegeben wurde, für die Zukunft zu verteidigen und

beizubehalten, nur dann, wenn wir diese Verantwortung tatsächlich wahrnehmen.

Es ist mir klar, dass ich hier Eulen nach Athen trage. Denn Sie alle tragen offensichtlich Verantwortung für dieses Thema, indem Sie hier sind. Aber ich möchte Sie auch aufrufen, wenn Sie wieder zurück an Ihre Institution gehen: Werben Sie in Ihren Institutionen für diese Thematik und für den Umgang mit dieser Thematik. Falls Sie von einer Institution kommen, die noch nicht auf dieser Webseite zu finden ist, versuchen Sie Ihre Hochschulleitung zu kontaktieren, damit diese auch solche Kommissionen installiert und den Kontakt zum Gemeinsamen Ausschuss sucht.

Wenn Sie Fragen haben: Die Geschäftsstelle in der Leopoldina, Herr Dr. Fritsch, Frau Borchert, stehen zur Beantwortung von Fragen zur Verfügung. Sie dürfen natürlich auch mich selbst jederzeit gern ansprechen.

Aber ich möchte nun nicht mehr Zeit von diesem interessanten Programm, das wir heute haben, wegnehmen. Vorher aber möchte ich Ihnen allen danken und betonen, dass ich sehr froh bin, dass so viele von Ihnen gekommen sind. Ich möchte speziell Herrn Buchmann und den Fachkollegien der DFG für Informatik danken für die Konzipierung, der Geschäftsstelle des Gemeinsamen Ausschusses für die Organisation und last but not least der Universität Darmstadt, Herr Prömel, für die freundliche Aufnahme hier und für den Empfang, den wir später am Tag genießen dürfen.

Nun kommt der interessante inhaltliche Teil, der von einem Moderator moderiert wird. Bevor ich übergebe, möchte ich darauf hinweisen, dass die Veranstaltung aufgenommen wird. Bitte berücksichtigen Sie dies bei allem, was Sie sagen.

Der Moderator des heutigen Tages wird Manfred Kloiber sein. Er ist IT- und Netzjournalist und arbeitet viel mit Deutschlandfunk, ARD usw. zusammen. Ich übergebe jetzt an Sie und bedanke mich für Ihre Aufmerksamkeit.

Session 1: Nutzen und potentielle Risiken

Moderation: Manfred Kloiber, Deutschlandfunk

Vielen Dank. Ich begleite Sie heute durch den Tag. Sie werden zwei Sessions erleben. Die erste Session beschäftigt sich in drei Vorträgen mit den konkreten Problemaufschlägen, den drei verschiedenen Fachbereichen der Informatik. Nach einer Mittagspause von einer Stunde gehen wir in die zweite Session, wo wir konkret über ethische Fragestellungen diskutieren werden. Nach der Kaffepause werden wir in einer Podiumsdiskussion versuchen, dieses Thema in die Praxis zu übertragen.

Wir wollen nicht große Worte machen, sondern steigen sofort in die erste Session ein, nämlich zu Fragen des Nutzens und der potenziellen Risiken von unterschiedlichen Forschungsbereichen. Ich begrüße Wolfram Burgard von der Albrecht-Ludwigs-Universität Freiburg, Institut für Informatik. Er ist ausgewiesener Experte für autonome Systeme, und aus seinem Schaffenskreis werden wir jetzt hören, wie sich die Fragestellung dort für ihn ergibt.

... der Forschung zur Robotik

Wolfram Burgard ML, Albert-Ludwigs-Universität Freiburg / Institut für Informatik

Danke für die Einleitung. Es ist immer etwas schwierig, bei einer solchen Veranstaltung der Erste zu sein. Normalerweise gilt: Die Ethik kommt immer zum Schluss. Das ist heute nicht so, und das ist auch gut so. Trotzdem bin ich kein Ethiker, sondern Informatiker. Ich habe

aber insbesondere als Robotiker mit der Dual-Use-Problematik zu tun, weil Künstliche Intelligenz [KI] und Robotik derzeit in einem starken Dual-Use-Kontext gesehen werden und derzeit in aller Munde sind.

Man sagt: Wir leben in so einer destruktiven Zeit. Tatsächlich ist es so, dass diese Technologien im Moment viel verändern, in unserem täglichen Leben, aber auch in der Industrie. Ich werde ein bisschen die wissenschaftliche Komponente anschauen und an ein paar Stellen versuchen, insbesondere am Schluss Überleitungen zu diesem Dual-Use-Gedanken zu machen, von dem ich glaube, dass es, wenn man sich das im Detail anschaut, manchmal schwer zu definieren ist, wo die Grenze ist. Aber das ist vielleicht eine Diskussion, die wir am Ende noch führen können.

(Folie 2)

Grundsätzlich geht es uns darum, in der Informatik Roboter- oder Künstliche-Intelligenz-Systeme zu bauen, die ihre Umgebung wahrnehmen und in ihr agieren, und das auf eine möglichst intelligente Weise. Das ist der berühmte Perceive-Act-Cycle.

(Folie 3)

Das passiert typischerweise dadurch, dass die Systeme bei Robotern Sensoren haben, dass sie sich in der Umgebung bewegen und möglicherweise Dinge manipulieren können.

Das ist das, was wir gern erreichen möchten: intelligente Systeme, denen wir Aufgaben geben können und die sie für uns erfüllen und uns dadurch möglicherweise das Leben einfacher machen.

(Folie 4)

Wenn man die Künstliche Intelligenz [Artificial Intelligence, AI] betrachtet: Ein großer Teil der KI-Forschung befasst sich damit, diese Agenten möglichst clever zu machen und ein möglichst gutes, robustes Handeln zu produzieren. Das erreicht man typischerweise dadurch, dass man versucht, Agenten zu bauen, die irgendein Performanzmaß maximieren. Das ist eine Funktion, die die Güte beschreibt, mit der eine Aufgabe ausgefüllt wird. Das, woran wir interessiert sind, ist, diese Performanz zu maximieren.

Wenn Sie an Ihr Navigationssystem denken, dann können Sie da unterschiedliche Bewertungsfunktionen einstellen, zum Beispiel kürzester Weg, geringster Spritverbrauch oder schnellster Weg. Das sind unterschiedliche Bewertungsfunktionen, die Sie auswählen können. Genau das versucht man auch in der Informatik, in der Künstlichen Intelligenz oder in der Robotik zu machen, um solche möglichst intelligenten Robotersysteme zu realisieren.

(Folie 5)

In unserem Leben haben wir mit der KI an allen möglichen Stellen zu tun:

- Sprachverstehen: Das kennen Sie wahrscheinlich alle, wenn Sie mit Ihrem Mobiltelefon reden.
- Navigationssysteme, wie gerade erwähnt. Der Kernalgorithmus, der in Navigationssystemen realisiert ist, kommt im Wesentlichen aus der KI.
- Buchstabenerkennung (Optical Character Recognition),
- Face Classification: Das sind Dinge, die wir nützlich finden, wenn wir beispielsweise unsere Fotos sortieren und automatisch die Bilder unseres Lebenspartners oder unserer Kinder in unserer Bibliothek finden, um die entsprechend darzustellen.
- Ranking von Websites ist ein berühmtes Beispiel für Künstliche Intelligenz, die dafür sorgt, dass wir Webseiten angeboten bekom-

men, die möglichst nahe an dem sind, was uns möglicherweise interessiert.

– Auch Recommender-Systeme geben uns Empfehlungen darüber, was wir möglicherweise interessant finden. Das gibt es schon für Musik oder Filme. Wenn Sie bestimmte Musik-Abonnements machen und Ihre Musik-Library freigeben, dann empfehlen die Ihnen Musikstücke, die wahrscheinlich Ihrem Geschmack entsprechen. Das basiert im Wesentlichen alles auf Techniken der Künstlichen Intelligenz.

(Folie 6)

AI in Games ist einer der großen Bereiche, wo man das Wort AI direkt benutzt: Die Gamer sprechen immer davon, wie gut die AI in diesem Spiel ist. Ich finde den Begriff schrecklich, weil das eigentlich ein Forschungsfeld ist und nicht ein Stück Software. Aber hier kann man sehen, dass da viele Probleme auftauchen: hier oben beispielsweise Suche, aber auch Navigation. Wenn Sie in der Simulation mit einem Helikopter kollisionsfrei durch so eine Welt navigieren wollen, und das möglicherweise in Reaktion auf den Spieler auf der anderen Seite, dann spielen Techniken der Künstlichen Intelligenz eine wesentliche Rolle.

(Folie 7, 8)

Wir wissen, dass wir damit in den letzten Jahren sehr weit gekommen sind. Gerade in den letzten zehn Jahren hat es über diesen Deep-Learning/ Big-Data-Hype Dinge gegeben, die uns auch überrascht haben. Das ist das Beispiel für menschliche Intelligenz, beispielsweise diese Quizshows, wo jeder glaubt, dass man, um da zu gewinnen, wirklich intelligent sein muss, und es stellte sich heraus: Wenn man einen entsprechend großen Computer mit entsprechend viel Information zur Verfügung stellt, dann kann man damit tatsächlich die Topspieler der Welt schlagen. Das ist in dem Fall WATSON, der in dem Spiel Jeopardy die beiden bis dahin erfolgreichsten Spieler geschlagen hat, mit Millionen von Dokumenten, Dictionaries, Wikipedia beispielsweise, Nachrichtenartikeln usw.

Wir sind also tatsächlich so weit, dass wir in bestimmten Einzelfällen das erreichen können, was man als Super Human Performance beschreiben kann.

(Folie 9)

Wir hatten selbst (deswegen hab ich diese Folie) vor zwei oder drei Jahren noch in unserer KI-Vorlesung, wo es um Spiele ging, den Satz drin, dass Go wahrscheinlich doch zu weit entfernt ist davon, als Computer besser zu werden, als der Mensch spielt. Vor zwei Jahren hat sich herausgestellt, dass das auch nicht der Fall ist, weil wir auch im Go mit Methoden der Künstlichen Intelligenz bereits die Qualität von Topspielern erreichen.

(Folie 10)

Die Frage ist: Wie sieht das jetzt in der Robotik aus? Was können wir in der Robotik erreichen? Das ist, wenn Sie so wollen, die physikalische Implementierung solcher Software-Agenten, die dafür sorgt, dass möglichst intelligentes Verhalten generiert wird.

Das sind ein paar Beispiele, in denen wir Robotersysteme sehen. Sie sehen da auch einige Dual-Use-Aspekte, beispielsweise Exoskeletons oder Explorationssysteme. Das sind Dinge, in denen man Robotertechnologie glaubt sinnvoll einsetzen zu können, aber auch andere Dinge wie Staubsauger, Rasenmäher oder Logistiksysteme.

Es gibt Märkte (*self-driving cars*, Logistik), bei denen man nahe dran ist, diese Technologie aus der Künstlichen Intelligenz einzusetzen, um unser Leben besser zu machen, Autofahren sicherer

zu machen oder Produktionsprozesse effizienter zu machen.

Das hat auch einen massiven Einfluss auf die Wirtschaftsstärke eines Standorts. Wenn wir beispielsweise solche Technologien nicht nutzen, werden wir möglicherweise im Bereich der Logistik von der Effektivität und der Produktivität her zurückfallen hinter andere Wettbewerber. Deswegen ist man teilweise gezwungen, diese Technologie zu benutzen, um wettbewerbsfähig zu bleiben.

(Folie 12)

Das sind ein paar Dinge, die man braucht. Hier sehen Sie einen autonomen Staubsauger. Wenn Sie den einfachsten kaufen, ist das zufälliges Herumfahren; das hat nichts mit Intelligenz zu tun. Aber dieser hier hat eine kleine nach oben gerichtete Kamera. Der guckt sich die Welt an, merkt sich, wo die Lichtquellen sind, baut daraus eine Karte (das werden wir gleich noch sehen) und kann einfach intelligenter reinigen.

Bei Rasenmähern gibt es das auch. Eine Firma aus Deutschland hat einen intelligenteren Rasenmäher als die, die nur zufällig durch die Gegend fahren. Das braucht man auch; ab einer gewissen Rasengröße kann man nicht mehr effizient den Rasen abdecken, ohne dass man systematisch fährt, und dafür braucht man diese Technologie.

(Folie 13)

Self-Driving Cars basiert im Wesentlichen darauf, dass Autofahrzeuge wissen, wo sie auf der Straße sind. Dies sagt schon, worum es geht: Um effizient fahren zu können, muss das Fahrzeug wissen, wo es sich befindet. Alle selbst fahrenden Autos – nehmen Sie die deutschen oder die amerikanischen – benutzen diese Technologie für das Positionieren von Fahrzeugen auf der Straße: in dem Fall hier einen Laserscanner auf dem Dach, die in neueren Versionen ins Fahrzeug integriert werden, und dann werden die Fahrbahnmarkierungen benutzt, weil man hochpräzise Karten von der Umgebung hat, um das Fahrzeug zu positionieren.

(Folie 14, 15)

Das ist ungefähr das, was das Fahrzeug sieht (nur um einen Eindruck von diesem Laserscanner zu bekommen). Die Aufgabe des Vehikels ist, daraus zu ermitteln, was als Nächstes gemacht werden soll. Sie benutzen auch mehrere Sensoren, also noch Kameras und Radar, aber im Wesentlichen ist der Laserscanner das, was im Moment noch dominant ist.

Man weiß aus der Robotik: Wenn ein Roboter so einen Pfad fährt, dann misst er den normalerweise so, und wenn das die Wahrnehmungen von so einem Scanner sind und da ist ein bisschen Dynamik, dann sieht man, dass da viele Fehler und Rauschen drin sind.

(Folie 16, 17)

Um Ihnen einmal die Magie zu nehmen: Was sich dahinter verbirgt, ist reine Mathematik. Das sind im Prinzip zwei Gleichungen, die dem zugrunde liegen, und wenn die Fahrzeuge berechnen, wo sie sind, benutzen sie im Prinzip diese Gleichung hier. Das ist das Stück AI, was in dem Fahrzeug funktioniert und dafür sorgt, dass das Fahrzeug weiß, wo es sich befindet.

(Folie 18)

Damit kann man tolle Sachen machen, beispielsweise robuste Roboter lokalisieren. Der findet dann heraus, wo er ist, und kann präzise navigieren.

(Folie 19)

Ich kann Ihnen das hier in dem Video in einem Logistikkontext zeigen. Hier ist ein Laserscanner in 2D, der hochpräzise an diesem schwarzen Punkt andockt. Von dem weiß der Roboter

nichts; der ist nur da, um zu demonstrieren, wie genau diese Positionierung ist.

(Folie 20)

Das hat eine enorme industrielle Bedeutung, auch wissenschaftlich, hier beispielsweise an den Experimenten mit dem 20-Tonner-Vehikel, was einen Prototyp darstellt und eine hochpräzise Lokalisierung erlaubt.

(Folie 21)

Dann wird es in der Praxis in Produktionsprozessen beispielsweise bei Boeing in Seattle eingesetzt, um den Rumpf der 777 durch die Transporthallen zu transportieren.

(Folie 22)

Sie werden sich fragen: Was hat das eigentlich mit der Dual-Use-Problematik zu tun? Dazu werden wir gleich kommen.

Das Ganze geht nicht nur auf Robotern, sondern das können Sie auch auf Ihrem Smartphone haben. Diese Technologie können Sie auch für eine Indoor-Positionierung nutzen. Das ist eine meiner Studentinnen, die sich damit befasst, mit dem Smartphone herauszubekommen, wo man ist.

Da kann man sich alle möglichen Anwendungen vorstellen: Social Media oder sonst irgendwas, dass man halt präzise angeben kann, wo man sich befindet, auch personalisierte Werbung und solche Dinge.

(Folie 23–27)

Dann müssen die Systeme auch Karten bauen. Ich will das kurz machen; das hatte ich schon erwähnt. Das ist letztendlich Mathematik.

(Folie 28)

Diese Gleichung muss man lösen. Das ist aber nichts anderes als Number Crunching, wie man neudeutsch sagt.

(Folie 29, 30)

Damit kann man solche Karten einer Parkgarage bauen. Dann können Sie beispielsweise mit so einem Fahrzeug autonom einparken. Sie können sich also vorstellen, dass das Fahrzeug einen zusätzlichen Knopf hat, der sagt: Park dich selbst. Sie drücken den Knopf, das Fahrzeug entschwindet in der Garage, fährt drei Stockwerke rauf und parkt dann auf einem vorgegebenen Parkplatz oben auf dem Garagendach. Das ist das, wo man im Moment ist.

Hier können Sie diese Messungen sehen, die das System benutzt, um sich in der Garage, wo es typischerweise kein GPS gibt, hochpräzise zu positionieren.

(Folie 31)

Das sind Anwendungen: Das sind Stadtroboter, ein System, was wir gebaut haben. Das ist ein Delivery-Roboter für innerstädtische Bereiche, den man jetzt auch finden kann.

(Folie 32)

Darüber hinaus gibt es auch im Kontext von Wahrnehmung Fortschritte, nicht nur in der Navigation. Mit dem Deep-Learning-Ansatz kann man hochpräzise Menschen detektieren und segmentieren. Das ist für solche Robotersysteme hochgradig nützlich, hat aber auch ein Potenzial für Dual Use.

Anwendungen davon sind beispielsweise Assistenzroboter, die Menschen helfen, beispielsweise als Drinking Assistant: Wenn Sie eine gelähmte Person haben und wollen, dass der Roboter dieser Person etwas zu trinken serviert, dann kann man das über Brain-Machine-Interface machen. Sie sehen hier, wie der Roboter feststellt, wo sich das Gesicht befindet und wo der Mund ist, um dann einschenken zu können.

Das wird über dieses Interface gesteuert. Es ist noch nicht optimal, wie Sie sehen, aber es muss ja noch Aspekte für Forschung geben.

(Folie 33)

Dies hier bezeichne ich als Brain-controlled Robots: Das sind Roboter, die durch Gehirnsignale gesteuert werden.

(Folie 34)

Es gibt aber auch den umgekehrten Fall: Robot-controlled Brains. Das ist der Fall, wenn Sie beispielsweise den Roboter benutzen wollen, um wieder Wahrnehmungen ins Gehirn zurückzuführen.

Hier ist ein solches Experiment. In diesem Lifehand-Projekt war auch ein Kollege aus Freiburg drin gewesen. Ihnen ist es gelungen, über den Anschluss an Nerven im Arm eine Klassifikation von Objekten zu erreichen, die der Roboter gegriffen hat. Der Roboter greift also ein Objekt, und der Benutzer kann über die Kabel, die an seinen Nervenenden angeschlossen sind, und die Signale, die dadurch ins Gehirn eingespeist werden, fühlen, was für ein Objekt der Roboter in der Hand hat.

(Folie 35)

Das ist eines der wohl schillerndsten Projekte, was in eine ganz andere Richtung geht und auch im Kontext von Ethik immer wieder diskutiert wird: Das ist Hiroshi Ishiguro mit seinem Roboter. Hier geht es darum, Roboter zu bauen, die nicht mehr von Menschen unterscheidbar sind.

Es gibt Leute, die sagen, das dürfte niemals so sein. Aber die Szenen, die wir im Film sehen, haben natürlich nie so stattgefunden. Früher waren auch Fotos noch authentisch; heute weiß man, dass Bilder in Zeitungen nicht so zeigen, wie es tatsächlich war. Vielleicht wird es das irgendwann einmal physikalisch geben, dass wir nicht wissen, ob uns ein Roboter gegenübersteht oder ein Mensch.

(Folie 36)

Hier sieht man eine japanische Nachrichtensprecherin. Links ist sie in Echt, und rechts ist das Robotersystem, das so aussieht wie sie.

(Folie 37)

Das können wir weglassen.

(Folie 38)

Ich hatte versprochen, dass ich am Schluss noch einmal über Dual Use spreche. Die Dual-Use-Technologie, die wir gesehen haben, sind im Prinzip Self-Driving Cars.

Das ist ein Projekt von Waymo, ein Google-Spin-off. Das ist einer ihrer Leute, die immer die Experimente machen. Er ist blind, darf also selbst nicht mehr fahren, und wird von diesem autonomen Vehikel durch die Gegend gefahren.

Links unten ist ein Fahrzeug, das der IS gebaut hat. Die haben eine Zeit lang solche Fahrzeuge, Jeeps, gepanzert und sind dann mit Sprengstoff in irgendwelche Gebäude gefahren. Die haben sie deswegen so gepanzert, weil sie dann durch herkömmliche Waffen, die Verteidigungslinien typischerweise haben, fast nicht mehr gestoppt werden können.

Jetzt kann man sich vorstellen, wenn man ein autonomes Navigationssystem darin hat, muss man noch nicht mehr einen Selbstmordkandidaten in diesem Fahrzeug haben, sondern kann den Zielpunkt angeben und das Fahrzeug fährt selbst dahin.

Dasselbe gilt auch für Technologie wie hier den City Explorer Robot, den wir haben.

Rechts unten, das habe ich letzte Woche erst gelernt: Es gibt schon Roboterwaffen, und zwar in der Demarkationslinie zwischen Nord- und Südkorea. Das ist ein automatischer Schussroboter,

der in der Grenzlinie steht. Er trackt Menschen über eine Thermokamera mit möglicherweise solchen Klassifikationsalgorithmen, wie wir sie eben gesehen haben. Man muss sich diesem Roboter ausweisen, indem man irgendein Passwort ruft. Und wenn einem das nicht gelingt, wird auf einen geschossen oder – ich weiß nicht genau was. Zur Not wird man tatsächlich erschossen von dem System.

(Folie 39)

Es gibt auch viele andere Dinge wie die Exoskeletons. Das ist ein Japaner, der für sich selbst ein Exoskeleton gebaut hat. Diese werden von der DARPA [Defense Advanced Research Projects Agency] für das Enhancement von Soldaten erforscht. Der Transfer von der menschlichen, sozialen Unterstützung oder den sozialen Zwecken solcher Systeme auf militärische Zwecke ist dann sehr einfach.

Rechts oben hat man den Roboter, der in Fukushima für die Erkundung in dem Reaktorgebäude eingesetzt wurde.

Die gleichen Roboter – hier unten ist er noch mal – wurden auch in Afghanistan eingesetzt für die Erkundung von Höhlen, in denen man Kämpfer vermutet hat.

Es gibt aber auch andere Anwendungen von diesen Robotern. Beispielsweise hat man am Ende des Jugoslawienkriegs solche Systeme benutzt, um Häuser zu erkunden. Denn die geflüchteten Besatzer hatten darin Sprengfallen installiert, und wenn die Bewohner wieder zurückkamen und den Kühlschrank aufgemacht haben, ist ihnen das Haus um die Ohren geflogen.

Da kann man sehen, dass es schwierig ist, die Grenze zu finden. Das ist eine militärische Verwendung, aber mit einer Komponente, die versucht, das Leben von Menschen zu schützen, indem sie die Sicherheit solcher Häuser untersucht.

(Folie 40)

Es gibt auch Bestrebungen in der Robotik – in den letzten Jahren hat sich eine Gruppe herausgebildet, die in so einem Kontext einen offenen Brief formuliert hat. Dieser offene Brief der Roboter- und AI-Forscher, den ich auch unterzeichnet habe, endet mit diesem Satz, den ich Ihnen einfach zum Lesen überlassen möchte.

> ["In summary, we believe that AI has great potential to benefit humanity in many ways, and that the goal of the field should be to do so. Starting a military AI arms race is a bad idea, and should be prevented by a ban on offensive autonomous weapons beyond meaningful human control."]

Ich habe versucht deutlich zu machen, dass es spannende Forschung gibt, die ein enormes Potenzial für unsere Gesellschaft hat, aber dass der Dual-Use-Aspekt hier extrem groß ist. Es stellt ein Dilemma dar, dass wir für unsere Gesellschaft etwas Wichtiges tun müssen, um nicht zurückzufallen, aber auch versuchen müssen, diese Dual-Use-Komponente im Blick zu halten. Wie uns das gelingt, ist mir nicht ganz klar. Ich hoffe, das klären wir heute. Danke schön.

Manfred Kloiber

Vielen Dank, Herr Burgard. Sie haben nach jeder Session die Gelegenheit, Fragen zu stellen. Wir hatten auf die Tonaufnahme hingewiesen. Es wäre nett, wenn Sie warten, bis eine Kollegin zu Ihnen kommt und Ihnen das Mikrofon hinhält.

Stephan Becker

Mein Name ist Stephan Becker aus Marburg, ich bin Virologe. Gibt es ein Regelwerk für die Künstliche Intelligenz, was gemacht werden darf, was nicht gemacht werden darf? Wird da eine Grenze vom Gesetzgeber gezogen oder gibt es außergesetzliche Regelwerke, an die sich Ingenieure, Entwickler von Künstlicher Intelligenz halten können?

Wolfram Burgard

Nicht dass ich wüsste, also zusätzlich zu dem, was es an ethischen Aspekten gibt, dass Universitäten sagen: Wir machen keine aktive Militärforschung oder so. Das ist etwas, was wir nicht tun.

Auch die Kooperation mit bestimmten Firmen wird schon kritisch gesehen wird. In Freiburg gibt es einen Ableger von Northrop Grumman, die, soweit ich weiß, für die Missiles und die Drohnen die Navigationssysteme bauen, also Kreiselkompasse usw. Die machen auch andere Dinge wie beispielsweise Tracken von Bohrköpfen bei Bohrungen, damit sie hinterher auch das Target finden. Das hat einen Dual Use, und da ist es schon so, dass unsere Studierenden und auch wir diskutieren, ob man in dem Fall tatsächlich eine Kooperation machen sollte.

Rüdiger Grimm

Rüdiger Grimm vom Fraunhofer-Institut SIT [Sichere Informationstechnologie] hier in Darmstadt. Über die bekannte Gefahr der Fehlprogrammierung von Robotern hinaus gibt es eine Fantasie der Science Fiction, dass Roboter einen eigenen Willen entwickeln könnten. Gibt es Überlegungen in Ihrer Richtung, wie da die Entwicklung sein könnte?

Wolfram Burgard

Das ist diese Diskussion zur Singularity. Ich bin da äußerst skeptisch. Im Moment schreiben wir ein paar Gleichungen hin und haben eine Funktion, die optimiert wird. Wenn man sich die Programme anschaut, kann man an der Architektur der Software noch absehen, was das Ding kann. Es ist illusorisch, zum jetzigen Zeitpunkt zu glauben, dass da irgendwann etwas entsteht, was verhindert, dass wir den Stromstecker ziehen oder den Ausknopf drücken.

Es wird bestimmt mal jemanden geben, der so etwas macht. Es gibt auch Robot Wars und solche Dinge; man kann sich so ein Szenario tatsächlich vorstellen. Davon sind wir aber, auch was Wahrnehmungen angeht, sehr weit entfernt. Das ist zumindest meine persönliche Meinung.

Bärbel Friedrich

In biologischen Systemen versucht man schon, in risikosensitiven Bereichen Rückholmechanismen einzubauen, die das korrigieren. Wenn ich mir das selbstfahrende Auto anschaue – für den IS ist es nicht schwer gewesen, das für diese Zwecke zu verwenden.

Wolfram Burgard

Nein. Es *wäre* nicht schwer; sie haben das …

Bärbel Friedrich

Das ist theoretisch, aber dieser Gedanke, den Sie entwickelt haben, ist ja nicht so abwegig. Muss man den möglichen Missbrauch mit in diese Entwicklungen einbeziehen?

Wolfram Burgard

Sagen wir so: Es ist ein interessanter Gedanke. Ich habe einen Ethikantrag stellen müssen für ein Robotersystem, das autonom durch einen Wald navigieren sollte und so groß war wie ein Smart. Da war die Befürchtung, dass irgendjemand auf dieses System eine Waffe schraubt, es fernsteuert und damit einen Angriff auf andere Menschen durchführt.

Da haben wir tatsächlich so etwas gemacht: Wir haben ein verstecktes GPS-System eingeführt, das automatisch Nachrichten verschickt, wenn das Robotersystem den Campus verlässt.

Wir haben auch argumentiert, dass die Software, die unsere Studierenden schreiben, so ist, dass nur ganz wenige Leute die starten können. Ich könnte sie nicht starten, wenn sie mir nicht zei-

gen würden, wie das geht. Insofern gibt es da Mechanismen, die man implementieren kann.

Ich könnte mir vorstellen, dass man das bei selbstfahrenden Fahrzeugen ohnehin machen wird. Wenn die irgendwann mal nicht weiterwissen, ist ein Modell, dass man sich von außen aufschaltet und dann das Auto fernsteuert aus der Situation und anschließend wieder selbst fahren kann. In dem Kontext könnte man sich vorstellen, dass diese Fahrzeug überwacht und auch disabled werden können. Das wäre etwas, was man in dem Kontext diskutieren könnte.

Christoph March

Mein Name ist Christoph March, ich bin vom Bundesministerium für Bildung und Forschung. Sie haben viele Beispiele gebracht vom missbräuchlichen Nutzen von Robotern und autonomen Systemen, vor allem aus dem militärischen Bereich. Können Sie sich auch im nichtmilitärischen Bereich eine missbräuchliche Nutzung vorstellen? Es gibt zum Beispiel einen Chatbot, den Microsoft entwickelt hat, der autonom gelernt hat und sich irgendwann rechtsradikal äußerte, basierend darauf, was dort gefüttert wurde. Sind solche Systeme für Sie auch missbräuchlich oder würden Sie das ausblenden?

Wolfram Burgard

Das ist schon eine Art Missbrauch. Das passt aber mehr in den Vortrag, den wir nachher hören werden, über den Missbrauch von Social Media, wo Leute solche Systeme benutzen, um andere zu beeinflussen. Da kann es eine Rolle spielen, dass ein Roboter nicht mehr von einem Menschen unterscheidbar ist, was die Vertrauensbasis angeht von Menschen gegenüber solchen Systemen. Das hat auch Potenzial für Missbrauch.

In allen Fällen, die ich diskutiert habe, ist es so, dass Menschen diese Systeme bauen und installieren, um diese Dinge zu tun. Das ist auch bei diesem Wahlbeeinflussungssystem so gewesen. Das ist etwas, was man sich genau anschauen und hinterfragen muss, inwiefern solcher missbräuchliche Nutzen tatsächlich möglich ist, wobei wir das alles nicht immer vorhersehen können. Wir haben auch nicht gesehen, dass die Einflussnahme über die sozialen Medien tatsächlich so massiv sein kann.

Manfred Kloiber

Ich habe noch eine Frage. Ich habe bei vielen RoboCups erlebt, dass die Studenten da unheimlich viel machen und viel Engagement zeigen. Bei vielen Robocups gibt es auch ein Versuchsfeld für Rescue-Roboter, die autonom arbeiten sollen. Das ist eigentlich ein Feld, wo man genauso gut militärisch operieren kann. Ist das den Studenten, die da mitmachen, klar? Diskutieren sie darüber?

Wolfram Burgard

Ich bin mir sicher, dass ihnen das klar ist. Aber ich finde auch, dass man dieses humanitäre Konzept dem anderen gegenüberstellen muss. Jetzt müsste man sich fragen: Sollen wir diese Forschung lassen und dann möglicherweise nicht mehr in der Lage sein, in Fukushima etwas zu unternehmen und Menschen zu helfen? Das ist ein kompliziertes Spannungsfeld.

Ich hoffe, dass die Studenten das wissen. Meine wissen es, weil wir oft darüber sprechen. Vielleicht muss es aber noch stärker thematisiert werden.

Manfred Kloiber

Vielen Dank für die Antworten, Herr Burgard.

... der Forschung zu Data Analytics

Manfred Kloiber

Wir machen weiter mit dem Nutzen und den potenziellen Risiken von Data Analytics. Darüber wird Volker Markl sprechen. Er leitet die Arbeitsgruppe für Datenbanksysteme und Informationsmanagement an der TU Berlin, ist Direktor des Berlin Big Data Centers [BBDC] und hat einen Lehrstuhl am Institut für Softwaretechnik und Theoretische Informatik.

Volker Markl, Technische Universität Berlin / Institut für Softwaretechnik und Theoretische Informatik

(Folie 1)

Ich möchte über das Themenfeld Data Analytics und Big Data sprechen.

(Folie 2, 3)

Meinen Vortrag habe ich folgendermaßen eingeteilt: Nach einer Einführung in einige Aspekte zu Data Analytics (da geht es über die drei Arten der IT-Wissenschaften, die neue Qualität von Data Analytics und insgesamt Data Analytics als eine neue Qualität der Wissenschaft) komme ich zu Nutzen und Risiken von Data Analytics, zu einigen Beispielen von Fehlern und Problemen, die auftreten können, zu Überlegungen und Thesen zum verantwortungsvollen Datenmanagement und letztendlich zu einer Konklusion.

(Folie 4)

Wir haben schon mehrfach gesprochen über das Spannungsfeld zwischen der im Grundgesetz für die Wissenschaft gegebenen Freiheit, also Unabhängigkeit und Ungebundenheit, und der Verpflichtung, einen möglichst guten Verlauf der Forschung zu haben, das Prinzip des Nichtschadens.

(Folie 5)

Gerade im Hinblick auf Data Analytics, aber auch für andere Bereiche ist es wichtig, drei Arten von IT-Wissenschaften zu unterscheiden:

[1] In der Systemforschung geht es im Wesentlichen darum, Technologien und systemorientierte Grundlagen zur Verarbeitung und Analyse von Daten zu entwickeln. Das sind beispielsweise informatische Felder wie Rechnerarchitektur, Datenbanksysteme, verteilte Systeme, Rechnernetze, Big-Data-Plattformen, die sich mit so etwas befassen.

[2] In der Algorithmenforschung geht es darum, „intelligente“ Algorithmen oder neuartige Methoden der Datenanalyse zu entwickeln, beispielsweise in den Gebieten des maschinellen Lernens, der Signalverarbeitung, der Sprachverarbeitung, der Bildverarbeitung.

[3] Letztendlich kommen diese beiden Dinge in einer Anwendung mit Daten zusammen. Das ist häufig die Aufgabe eines Data Scientist, also eines datengetriebenen, datenintensiven Wissenschaftlers, der diese Methoden und Systeme in einen konkreten Anwendungsfeld anwendet, beispielsweise in der Physik, der Chemie oder in anderen Bereichen, häufig in diesen Bindestrich-Informatik-Disziplinen.

Ich werde versuchen abzuleiten, dass in diesem Bereich noch andere Aspekte zu sehen sind.

(Folie 6)

Big Data ist auch eine neue Qualität der Data Analytics, denn wir haben durch komplexe Simulationen, Sensoren und die zunehmende Digitalisierung immer mehr Daten zur Verfügung und damit eine erheblich höhere Komplexität im Rahmen dieses Datenanalyseprozesses, der schon vorhanden ist: Er geht von Datenquellenidentifikation über Datenintegration und Datenhaltung, was eher die Systemforschung abdeckt,

während die Algorithmenforschung den Bereich der Datenanalyse und die Anwendung der Analyseergebnisse umfasst, um Entscheidungen zu treffen und neue Erkenntnisse in der Wissenschaft abzuleiten.

Wir haben diese höhere Komplexität, die auch neue Fehlerquellen und Manipulationsmöglichkeiten schafft. Gleichzeitig haben wir die alten Probleme, die schon immer existiert hatten, in den Bereichen Datenqualität und Statistik. Diese bleiben als Grundproblematiken bestehen und können jetzt unter Umständen in einer höheren Skalierung, in einer höheren Menge auftreten und sind vielleicht in einigen Bereichen auch etwas weniger transparent. Das werde ich gleich noch mit ein paar Beispielen untermauern.

(Folie 7)

Ein wichtiger Aspekt ist in diesem Kontext für die Wissenschaft das sogenannte vierte Paradigma, das von Jim Gray, dem Turing-Preisträger, geprägt wurde. Er postulierte die These, dass wir einen Übergang und eine Revolution in den Wissenschaften erleben von der empirischen Forschung über die theoretische Modellbildung, die lange die Wissenschaft getrieben hat, über das wissenschaftliche Rechnen, das komplexe Phänomene simuliert, hin zu einer datenintensiven Wissenschaft: Das ist dieses vierte Paradigma, wo man massive Datenmengen, die über Messungen oder Simulation erzeugt werden, analysiert, mit Software exploriert und Informationen durch Methoden des Datenmanagements und der Statistik des maschinellen Lernens analysiert, um daraus Erkenntnisse abzuleiten.

Ein populäres Beispiel, was auch Jim Gray losgetreten hat, ist der Sloan Digital Sky Survey [SDSS], wo astronomische Daten bereitgestellt wurden, um daraus der gesamten astronomischen Gemeinschaft wissenschaftliche Arbeiten mit diesen Daten zu ermöglichen. Das gibt es heute in vielen Bereichen: in den Materialwissenschaften mit dem NOMAD-Projekt [Novel Materials Discovery], der Genomforschung usw.

(Folie 8)

Wir haben von meinem Vorredner schon etwas über wissenschaftlichen Nutzen gehört: In diesem Kontext gibt es die Möglichkeit, durch dieses vierte Paradigma neue Erkenntnisse zu erlangen allein auf der Basis der Daten, die man durch Experimente erhalten hat.

Gleichzeitig können in der Medizin aufgrund von großen Datenbasen zum Beispiel komplexe Wirkzusammenhänge und neue Korrelationen analysiert und erkannt werden.

Auch in den Geistes- und Sozialwissenschaften, den Digital Humanities, gibt es neuartige Möglichkeiten, insbesondere durch ein Konzept, das teilweise Probleme mit sich bringt (darüber werden wir uns gleich noch unterhalten): das Konzept des Participatory Sensing. Dabei geht es darum, dass man über Sensoren, beispielsweise über das Smartphone, das Verhalten von Nutzern analysieren kann, um daraus Aussagen zu treffen. Da gibt es Möglichkeiten, von statistisch signifikanten Datenmengen Erkenntnisse abzuleiten und neuartige Verknüpfungen durchzuführen, aber auch mit Problemen.

(Folie 9)

Doch zunächst noch ein weiterer Aspekt zum gesellschaftlichen Nutzen. Es ist klar – das klang schon an –, dass wir einen großen Nutzen aus Data Analytics ziehen können:

[1] in der Wirtschaft durch Vermeidung von Ausschuss und Überproduktion und durch die Steigerung der Innovationskraft und Wettbewerbsfähigkeit;

[2] im Bereich der Gesundheit durch Senkung der Gesundheitskosten, Entlastung der Ärzte oder

[3] im Bereich des Verkehrs durch Entlastung der Verkehrsinfrastrukturen, wiederum durch Kostensenkung oder Optimierung.

Das sind viele Chancen in diesen eher klassischen Bereichen, aber mit einer völlig neuen Dimension der Wissenschaft durch datenintensive Forschung.

(Folie 10)

Wie gesagt gibt es auch erhebliche Risiken. Ich habe versucht, sie in fünf Bereiche einzuteilen: Das sind Fehler, also klassische Analysefehler, die aufgrund der Daten zustande kommen (das ist handwerklich schlechte Arbeit, wenn man so will); Manipulationen, die eine bewusste Beeinflussung beabsichtigen; Angriffe; das Thema Dual Use, das schon mehrfach genannt wurde; und das Thema Datenmonopole, das auch ein gewisses Risiko gerade im Hinblick auf Chancengleichheit und Zugang bedeuten kann.

[1] Im Bereich der Fehler sind viele der klassischen Statistikfehler, von Bestätigungsfehlern über Ausreißer, das Simpson Paradoxon, nicht normalverteilte Daten, fehlerhafte Annahmen und falsche Schlüsse. Das sind Herausforderungen, die insbesondere dann, wenn eine Art Datenfundamentalismus betreibt (der heutzutage populär ist), zu Problemen führen können, wenn man blind den Daten oder den Ergebnissen vertraut, weil das ja so berechnet worden ist. Dieser Datenfundamentalismus kann bei derartigen Fehlern zu einem Problem führen. Außerdem gibt es Haftungsfragen und weitere.

[2] Im Bereich der Manipulation haben wir einige Beispiele gesehen: Fake News, Wahlbeeinflussung usw. Hier besteht die Gefahr, dass man durch verschiedene Arten von kriminellen Eingriffen (wie Fake News) oder visuelle Verzerrung von Ergebnissen einen verstärkten Einfluss auf Politik, Konsum und Öffentlichkeit ausübt und somit das Vertrauen beschädigt wird.

[3] Über Angriffe und Sicherheit wird Anja Feldmann noch mehr sagen. Klar ist: Datenlecks, Missbrauch, Softwarefehler oder Cyberattacken können zur Verletzlichkeit von Menschen, Unternehmen oder der Gesellschaft insgesamt führen und sind Herausforderungen,

[4] Im Bereich Dual Use ist ein großes Thema im Bereich Data Analytics die unrechtmäßige Verwendung der Daten. Aber auch Terrorismus, Spionage, Verletzung von Persönlichkeitsrechten oder Diskriminierung insgesamt können zu einem Problem führen.

Die Frage ist hier: Kann man ethische Prinzipien durchsetzen? Das wird auch ein großer Teil der Nachmittagsdiskussion sein. Die Frage ist letztendlich auch, weil das häufig eine Abwägungsentscheidung sein wird: Wie sollen die Gefahren beurteilt und die Gefahren-Nutzen-Analyse jeweils umgesetzt werden?

[5] Als Letztes das Beispiel der Datenmonopole. Eine weitere Herausforderung im Big-Data-Bereich ist, dass die Daten, die erzeugt werden – entweder in den Wissenschaften oder im Internet oder bei Unternehmen –, nicht immer jedermann zugänglich sind. Die Gefahr ist, dass es einen selbstverstärkenden Zyklus von überlegenen Diensten und Datensammlungen gibt im Prinzip Monopole oder Oligopole, die dann eine fehlende Chancengleichheit hervorrufen, sodass nicht jeder Datenanalysen durchführen kann und die Datennutzung auch schwerer kontrollierbar ist.

Da ist die Frage: Kann durch Regulierung diese Problematik abgewendet werden, um das Prinzip der Fairness und der Chancengleichheit zu ermöglichen?

(Folie 11)

In dem Kontext gibt es im Bereich der Datenanalyse und des maschinellen Lernens einige Fehlerquellen. Generell tritt die Grundproblema-

tik immer auf, wenn die Systeme, die Algorithmen und die Daten zusammenkommen. Algorithmen sind in den meisten Fällen per se nicht böse, sondern erst durch die Daten entstehen gerade im Bereich des maschinellen Lernens Probleme.

[1] Wenn man sich die Daten ansieht: Was sind da potenzielle Schwierigkeiten?

Ein Beispiel wäre mangelhafte Auswahl. Wenn ich bei meiner Datenauswertung nur Autofahrten berücksichtige und keine Fahrradfahrten, erhalte ich unter Umständen in einer Studie falsche Ergebnisse, verzerrte Ergebnisse. Das heißt, wenn Daten unvollständig, fehlerhaft oder veraltet sind (was bei Daten häufig der Fall ist) oder die Datenaufbereitung unkorrekt gemacht wird, können aufgrund von Fehlern Probleme, falsche Ergebnisse entstehen.

Verzerrung ist ein weiteres Beispiel. Das kann auch zu Diskriminierung führen. Wenn man zum Beispiel soziale Studien im Bereich Participatory Sensing durchführt, indem man die Smartphone-User trackt und mit deren Daten eine Auswertung macht, ist eine Gefahr dadurch da, dass nicht jeder in der Bevölkerung ein Smartphone hat. Gerade in den USA gibt es darüber eine große Diskussion im Bereich Participatory Sensing, dass das bedeuten könnte, dass gerade Minderheiten und ärmere Bevölkerungsgruppen von diesen Studien nicht erfasst würden. Da muss man aufpassen.

Das kann effektiv bedeuten, dass man zum Beispiel eine Wiederholung historischer Verzerrungen erreicht. Ein typisches Beispiel: Ich stelle Personen ein, die zur Unternehmenskultur passen. Das ist unter Umständen ein sich selbst verstärkender Zyklus. Das wurde von der Obama-Administration im Kontext von Daten-Diskriminierung herausgearbeitet. Dieses Thema wird auch schon in den Wissenschaften beachtet, gerade in der Data-Mining-Community. Es gab auch ein Tutorial von Francesco Bonchi. Gerade die Konferenz ist eine der großen Konferenzen im Bereich des Data Mining, die diese Thematik herausarbeiten.

[2] Ein weiteres Problem besteht auf der Seite der Algorithmen, und zwar dadurch, dass Algorithmen unter Umständen Personalisierungs- und Empfehlungsdienste anbieten, die die Möglichkeiten der Benutzer nicht erweitern, sondern einschränken, weil man immer fokussierter in eine bestimmte Richtung geführt wird, was eine Beeinflussung darstellt.

Oder dass Entscheidungen aufgrund von „Korrelation impliziert Kausalität“ getroffen werden, Scheinkorrelationen (dazu kommen wir gleich noch) beispielsweise, die zu falschen Schlüssen und Handlungen führen können.

Oder dass Algorithmen handwerklich schlecht designt sind, sodass sie nur einen mangelhaften Ausgleich von Fehlern in den Daten oder Verzerrungen in den Daten durchführen, sodass beispielsweise überproportionale Anteile von bestimmten Populationen in den Daten nicht ausgeglichen werden, was wiederum eine Form von Verzerrung oder Voreingenommenheit verursachen könnte.

Oder mangelhaftes Matchmaking bei Algorithmen, die vielleicht Diversität nicht richtig berücksichtigen und dann Ergebnisse liefern, die nicht die Breite der Datenbasis darstellen.

Oder (das ist ein großes Problem insbesondere im Bereich Deep Learning, im Bereich der neuronalen Netze) dass die Ausgaben und Modelle schwer verständlich oder interpretierbar, nachvollziehbar sind, sodass man gar nicht genau sagen kann, warum es zu diesem Ergebnis kam. Deshalb gibt es Schwierigkeiten, ein System in Bezug auf seine Fähigkeit und auf das Problem

des Nichtschadens zu bewerten, und auch Auswirkungen auf die Rechtssicherheit, weil man schlecht rechtlich argumentieren kann, dass sich dieses System entsprechend verhält.

(Folie 12)

In diesem Kontext möchte ich kurz zehn Beispiele benennen, wo Probleme aufgetreten sind. Einige davon wurden vorher schon andiskutiert.

(Folie 13)

Ein Beispiel ist Stichprobenverzerrung. Eines der prominentesten Beispiele, das es dafür gibt, ist Policing. Im Bereich des Policing ist die Idee, dass die Einsatzplanung der Polizeikräfte optimiert werden soll dadurch, dass ich Daten über Kriminalität habe. Die Herausforderung ist aber, dass diese Kriminalitätsstatistiken häufig inhärent verzerrt sind: Sie haben häufig ein Bias, weil die stark kriminalitätsbelasteten Orte in diesen Daten überrepräsentiert sind. Das bedeutet, dass viele Empfehlungen zum Polizeieinsatz in diesen Bereichen stattfinden, was wiederum dazu führen könnte, dass da mehr Festnahmen stattfinden. Dann kommt man in so einen Zyklus.

Das ist auch eine große Diskussion in den USA, wo das in einigen Städten eingesetzt wird, wo sich viele Wissenschaftler gerade im Bereich von verantwortungsvollem Datenmanagement dieser Frage annehmen und insbesondere darauf hinweisen, dass hier Diskriminierung passieren könnte.

Es besteht also die Gefahr der Diskriminierung, wenn Rohdaten unvollständig und nicht repräsentativ sind.

Wiederum: Das ist nicht der Algorithmus (das wird auch in diesem Artikel klar gesagt, den ich rechts angegeben habe), sondern es geht um die Daten, die verwendet wurden, um diesen Algorithmus zu trainieren.

Das hatten wir auch gestern Abend schon als ein Beispiel gehört: Der Algorithmus ist genauso böse oder schlecht wie die Zahl Fünf. Es sind wirklich die Daten, die die Problematik hervorrufen.

(Folie 14)

Ein weiteres Beispiel ist Überanpassung (im Englischen Overfitting), was bedeutet, dass wir zu viele erklärende Variablen in ein Modell einbauen. Das kann schnell passieren.

Ein populäres Beispiel war im Kontext von Google Flu Trends (dazu gab es auch eine Publikation in *Nature*), dass man aufgrund von Suchanfragen Grippeepidemien erkennen kann. In der Praxis hat man festgestellt, dass es nicht ganz so gut funktioniert hat. Wenn man nachguckt, was da schiefgelaufen ist, dann war ein Aspekt, dass diese Algorithmen Oberfitting betrieben haben: Da wurden zum Beispiel Suchbegriffe wie *high school basketball*, die manchmal mit Grippe zusammengefasst wurden (soll man da die Kinder hinschicken? usw.) – wenn da viel *high school basketball* war, konnte man schnell auf eine Grippeepidemie schließen. Da sind problematische Zusammenhänge durch Überanpassung entstanden.

(Folie 15)

Ein weiteres Beispiel – ein älteres, klassisches Beispiel der Datenanalyse, das sich aber in Big Data verstärken kann – ist das Simpson-Paradoxon, wo man die Bewertung einer Gruppe in der Gesamtheit anders auffasst, als wenn man diese Gruppe in Teilgruppen zerlegt und diese Teilgruppen eine eigene Bewertung haben. Konkret geht es bei diesem Beispiel um eine Diskriminierungsklage gegen die Universität von Berkeley. Man hat geguckt: Wie viele Männer wurden zugelassen, wie viele Frauen wurden zugelassen? Man hat gesagt: 44 Prozent der Männer, aber nur 35 Prozent der Frauen; das heißt: Ber-

keley diskriminiert in der Zulassung gegen Frauen.

Das war aber falsch. Der Hintergrund, warum es falsch war: Wenn man diese große Gruppe in Einzelgruppen zerlegt, Bewerbungen pro Fakultät, dann konnte man feststellen: Es gab einige Departments, da gab es nur Bewerber eines Geschlechts; bei 16 Departments gab es nur Bewerber eines Geschlechts, die erfolgreich waren. Bei den übrigen 85 Departments war es im Wesentlichen vernünftig verteilt, wobei vier bessere Erfolgsquoten bei Männern und sechs bei Frauen hatten.

Im Endeffekt, wenn man eine solide statistische Analyse mit Chi-Quadrat-Tests gemacht hat, konnte man feststellen, dass keine Diskriminierung stattfand. Denn die Bewerbungen waren abhängig von den Zulassungsdaten, und die Bewerberinnen hatten sich stärker auf Studiengänge beworben, wo die Zulassungsraten niedriger waren. Das heißt: In der Hinsicht war ein Bias vorhanden. Wenn man solche Dinge im Big-Data-Kontext zusammenfasst, kann man schnell zu solchen falschen Schlüssen kommen.

(Folie 16)

Ein weiteres Beispiel sind Scheinkorrelationen. Scheinkorrelation bedeutet, dass man zwei Größen in Beziehung setzt, wobei kein Kausalzusammenhang vorliegt, sondern noch ein Störfaktor berücksichtigt werden müsste. Es ist problematisch, wenn man dann – im sehr beliebten Schluss – von Korrelation auf Kausalität schließt.

Ein schönes Beispiel aus Wikipedia ist der Zusammenhang zwischen globaler Durchschnittstemperatur und Anzahl der Piraten, die weltweit existieren. Denn man kann klar zeigen, dass mit dem Anstieg der Durchschnittstemperatur eine Korrelation besteht, das heißt, die Anzahl der Piraten zurückging, je höher die Durchschnittstemperatur ist. Vermutlich ist Global Warming auch dafür verantwortlich, dass die Piratenzahl zurückging.

Natürlich ist das Unfug, denn in Wirklichkeit ist der Störfaktor, die Confounding Variable, hier das Datum, und natürlich ist über die Zeit die Zahl der Piraten zurückgegangen.

Ich habe hier noch eine kleine Manipulation gemacht, denn wir wissen alle: Piraterie ist in den letzten Jahren wieder ein bisschen gestiegen, aber ich habe ja auch die Zahl abgeschnitten …

(Folie 17)

Da kommen wir gleich zum nächsten Beispiel, zur visuellen Manipulation. Benjamin Disraeli sagte: „There are three kinds of lies: lies, damned lies and statistics.“ Es besteht tatsächlich eine große Gefahr für uninformierte Leser oder Konsumenten von Statistiken, dass man getäuscht wird durch visuelle Manipulation, durch die Auswahl der Achsen, wie ich die Skalen wähle, wie ich glätte.

Hier ist ein schönes Beispiel von Fox News, das zeigen sollte oder wollte, dass Obamacare ein Fehlschlag ist. Es gab ja ein gewisses Ziel von Obamacare, wie viele Leute dort teilnehmen sollten, also ein Enrollment durchführen sollten. Man sieht, dass zum 27. März 6 Millionen drin waren, dass aber eigentlich 7 Millionen drin sein sollten. Es ist klar, dass die Proportionen hier manipulativ sind.

(Folie 18)

Ein weiteres Beispiel – relativ komplex, aber mit großen Auswirkungen – sind nicht-normalverteilte Daten. Denn es ist so: In der klassischen Statistik würde man auf Bayrisch sagen: „ois schaut aus wie Gauß“. Das bedeutet, dass viele statistische Methoden darauf basieren, dass dem Ganzen normalverteilte oder normalartig verteilte Daten zugrunde liegen. Das bedeutet: Wir

können statistische Momente wie Varianz, Mittelwert etc. definieren und daraus Entscheidungsmodelle ableiten.

Die Herausforderung ist: Wenn wir keine normalartig verteilten Daten haben, dann gibt es keine statistischen Momente und diese ganzen Entscheidungskriterien sind unsinnig.

Das Interessante ist: Ein sehr lesenswertes Buch, *The Black Swan,* beschreibt, wie die Finanzkrise in den USA durch quantitative Statistik ausgelöst wurde. Denn dort wurden Entscheidungsmodelle verwendet, die auf klassischer Statistik beruhten, aber nicht berücksichtigt haben, dass die Grundlage (wie die Kreditvergabe ist, wie die Einkommenssituation der Menschen da ist) eine schiefe Verteilung war. Die Banker waren nicht böse und haben aus Gier Kredite vergeben, wie es manchmal dargestellt wird, sondern da gab es ein mathematisches Modell, das klar gesagt hat: Diese Person ist kreditwürdig. Und man hat diesem mathematischen Modell mehr oder weniger blind vertraut, und dadurch wurden viele Kredite vergeben, die nie hätten vergeben werden sollen. Eine große Herausforderung.

(Folie 19)

Ein weiteres Beispiel, das vorhin schon angesprochen wurde, sind fehlerhafte Annahmen beim maschinellen Lernen, nämlich dass zum Beispiel eine Trainingspopulation – oder auch bei der Weiterentwicklung – so repräsentativ ist, dass man damit den gewünschten Effekt erreichen kann. Das war dieser Chatbot von Microsoft, der vorhin schon angesprochen worden, Tay.ai, der durch Benutzerverhalten immer schlauer werden sollte und innerhalb eines Tages zum Nazi und Sexisten wurde, weil leider Gottes die Internet-Community – das ist natürlich auch eine gewisse Aussage –, vielleicht auch über Manipulation, diesen Chatbot mit solchen Chats gefüttert hat, dass sich dieser in diese Richtung entwickelt hat.

Wiederum kein Fehler des Algorithmus; man kann da auch sagen: Der Algorithmus oder der Chatbot hat einwandfrei funktioniert. Das Schlimme waren die Trainingsdaten, die Nutzer, wie die mit ihm interagiert hatten. Die haben ihm dieses Verhalten beigebracht, sodass verzerrte Trainingsdaten zu unerwünschten Ergebnissen führen können.

(Folie 20)

Ein weiteres Beispiel (das ist eine Arbeit aus dem Berlin Big Data Center von meinem Kollegen Klaus-Robert Müller) ist, wie maschinelle Lernverfahren fehlerhafte Schlüsse ziehen können. Denn der Lernerfolg von so einem System hängt von vielen Parametern ab. Wichtig sind die Trainingsdaten, die Lernmethode, die Features, die Konfiguration. Die Rolle der Parameter ist nicht immer direkt ersichtlich, sodass man unter Umständen zu Fehlern kommen kann.

Das ist ein Beispiel. Da war das Ziel der Lernverfahren, Pferde zu erkennen. Es gab verschiedene Verfahren, und das Verfahren, das am besten funktioniert hat – wenn man genau hinguckt, sind das Heatmaps, die versuchen zu erklären, was so ein System lernt. Dieses zunächst beste Verfahren hat in diesem roten Bereich – das war die Grundlage für die Entscheidung. Ein anderes Verfahren hat zum Beispiel Entscheidungen in dem roten Bereich und auch die gelben genommen; die grünen sind eher weniger relevant.

Man sieht: Dieses Verfahren hat den Rücken, die Stirn des Pferdes usw. als Kriterien genommen, wohingegen dieses Verfahren *diesen* Bereich hier verwendet hat. Wenn man ein bisschen genauer hinguckt: Hier steht Pferdebilder.de. Das heißt, dieses System hat erkannt, dass hier ein Text steht, und hat diesen Text gelernt.

Die Herausforderung ist: Gerade beim neuronalen Netz ist es sehr schwer, so etwas zu erklären. Es gibt inzwischen einige Arbeiten in der Wissenschaft, die versuchen, solche Heatmaps erklärbar zu machen. Das steckt noch in den Kinderschuhen. Häufig werden solche Arbeiten nicht gemacht, sondern man nimmt eine Lernmethode einfach an: Ja, hat es gelernt, passt schon. Das ist hier die große Gefahr.

(Folie 21)

Weiteres Beispiel: Datenmonopole. Datenmonopole in der Wissenschaft sind meines Erachtens eine große Herausforderung, auch im ethischen Sinne, denn es ist klar: Die Erzeugung und Speicherung von Big Data ist aufwendig. Wenn ich komplexe Experimente durchführen will oder longitudinale Studien oder was auch immer: Ich muss meine Subjekte auswählen, ich muss die Studie durchführen, Daten säubern oder ich brauche riesige Messapparate.

Dann habe ich Daten. Wer darf nun mit diesen Daten was machen? Stelle ich diese Daten zur Verfügung oder behalte ich die für mich? Denn ich will ja publizieren, ich will ja wissenschaftlichen Erfolg erreichen und meine tollen Papers schreiben. Das hat dazu geführt, dass einige Leute gesagt haben: Es gibt Parasiten, Forschungsparasiten, also Menschen, Wissenschaftler, die die Daten von anderen nehmen und daraus Ergebnisse publizieren. Das sind Parasiten. Darüber muss man diskutieren.

Auf der einen Seite kann das zu Datenmonopolen oder Oligopolen führen, auf der anderen Seite ist das aber doch der größte Fortschritt der Wissenschaft, wenn jemand diese Studie nimmt und daraus neue Erkenntnisse ableitet. Wir haben da ein Spannungsfeld zwischen dem legitimen Parasiten auf der einen Seite und auf der anderen Seite dem legitimen Interesse der Person, die diese Daten generiert hat, auch einen wissenschaftlichen Erfolg zu haben, denn diese Person braucht ja auch eine Anschlussförderung. Da muss man überlegen, wie da Belohnungen auf beiden Seiten stattfinden können.

Interessanterweise ist in dem Kontext etwas entstanden, nämlich die Parasite Awards: Die Personen, die in datenintensiver Forschung aus den Daten anderer etwas Gutes ableiten, bekommen einen Preis. Aber man muss auch in die andere Richtung gehen: Was bekommen die Leute, die die Daten generieren?

(Folie 22)

Ein letztes Beispiel, das ich immer gern anbringe, ist das Problem, dass wir von diesen Wissenschaftlern sehr viel erwarten. Wie gesagt, es gibt viele Problemstellungen im statistischen Bereich: Scheinkorrelationen, Simpson Paradoxon usw. Das heißt, ein Datenwissenschaftler muss viele Fehlerquellen und Probleme kennen.

Gleichzeitig ist es aber so: Wenn wir nach dem vierten Paradigma Wissenschaft betreiben, bedeutet das, dass wir mit diesen großen Datenmengen umgehen müssen. Das heißt, ein Data Scientist muss auch Kenntnisse im Bereich des skalierbaren Datenmanagements und tiefe informatische Kenntnisse haben, und natürlich braucht er auch Domänenwissen, das heißt, er muss über die Wissenschaftsdomäne Bescheid wissen, um zum Beispiel im Bereich der Materialforschung Dinge (thermodynamische Effekte usw.) zu verstehen.

Das heißt: Eigentlich sollte ein Data Scientist eine eierlegende Wollmilchsau sein, denn er braucht mathematisch-algorithmische Kompetenzen, informatisch-technologische Kompetenzen und zusätzlich noch Kompetenzen im Bereich der Domäne, in dem das angewendet werden soll.

(Folie 23)

Herausforderungen: Was kann in dem Kontext verantwortungsvolles Datenmanagement leisten oder was bedeutet es zunächst? Die Datenmanagement-Community hat vor ein paar Jahren begonnen, über diese Fragen zu sprechen und zu diskutieren. Es gab in diesem Kontext ein Dagstuhl-Seminar. Dagstuhl ist ein Schloss im Saarland ist, das unter anderem von der Gesellschaft für Informatik getragen wird, wo sich Informatiker treffen, um für eine Woche in Klausur über tiefe Fragen zu diskutieren. Da gab es ein Dagstuhl-Seminar von Wissenschaftlern weltweit zum Thema verantwortungsvolles Datenmanagement.

(Folie 24)

Die Grundlagen in dem Kontext kann man aus anderen Wissenschaften ableiten. Diejenigen von Ihnen aus der Biomedizin kennen wahrscheinlich den Belmont Report, eine erste Kodifizierung von Prinzipien für den Umgang mit Daten für Studien. Die drei Prinzipien, die hier als Leitideen galten, waren Respect for Persons, Beneficence und Justice.

Das Ganze hat dazu geführt, dass in den USA von den Förderinstitutionen die Common Rule eingeführt wurde, die dann von vielen National Institutes übernommen wurde: Die Aspekte, aus denen sich dann so Dinge wie *informed consent* ableiten, aber auch *minimize probabal harms* usw., waren eine Basis für die Entscheidung von Fördermitteln und Förderprojekten. Das war die Common Rule, und das Ganze wurde erweitert in einem Kontext für die IT-Wissenschaften über den Menlo Report.

Der Menlo Report wurde auch noch um eine Dimension erweitert, nämlich Respect for Law and Public Interest, die als Leitlinien gelten können.

(Folie 25)

In dem Kontext hat sich die Datenmanagement-Community zusammengesetzt und im Rahmen eines Dagstuhl-Seminars zum einen ethische und gesellschaftliche Herausforderungen definiert und sich zum anderen Gedanken gemacht, welche technischen Lösungen man anbieten kann. Denn ein wichtiger Aspekt ist: Können wir das durch Technologie unterstützen?

Ethische und gesellschaftliche Herausforderungen: Das ist zum einen Fairness. Fairness bedeutet die Abwesenheit von Diskriminierung. Wir haben schon gesehen: Durch schlechte Datenauswahl, durch verschiedene Probleme, Überrepräsentation von Dingen in den Stichproben kann man in den Lernverfahren, in den Entscheidungen diskriminierend werden. Die Frage ist: Kann man das schon in die Algorithmen einbauen? Das ist wiederum nicht gut oder böse, sondern es geht darum, dass man handwerkliche Fehler vermeidet.

Ein weiterer Aspekt ist Diversität. Das heißt, dass die Daten in der Breite genutzt werden. Ein populäres Beispiel ist beim Matchmaking – da kann man sich eine Partnerschaftsbörse vorstellen –, dass man da nicht lauter Personen mit identischem Profil sehen will, sondern dass da eine gewisse Diversität in den Ergebnissen vorhanden sein sollte.

Ein weiterer Aspekt ist Neutralität und Zugang. Ich habe gerade schon das Thema Datenmonopole, Research Parasites usw. angesprochen. Das heißt: Wie kann man sicherstellen, dass es einen fairen Zugang und Neutralität gibt?

Ein wichtiger Punkt ist Transparenz: Können wir sicherstellen, dass die Methoden, die Algorithmen, die Daten, die verwendet wurden, transparent sind?

Und letztendlich, dass die Prinzipien des Datenschutzes und der informationellen Selbstbestimmung, die hier eine große Rolle spielen, realisiert sind.

In dem Kontext ist auch zu fragen: Kann die wissenschaftliche Gemeinschaft durch technische Lösungen hierzu beitragen? Im Bereich von Testen und Verifikation der Algorithmen, um insbesondere die Eigenschaften Fairness, Diversität, Transparenz und Datenschutz sicherzustellen? Gleichzeitig die Fragen: Wie kann man es nachvollziehbar und reproduzierbar gestalten, und wie verhält es sich im Bereich Open Source und Open Data? Das können alles technische Lösungen sein, um diesen Herausforderungen zu begegnen.

(Folie 26)

In dem Kontext gab es auch Gedanken von Michael Steinmann und anderen über ein theoretisches Framework zur ethischen Reflexion von anwendungsorientierter Big-Data-Forschung. Sie unterscheiden in den Zweck (die verschiedenen Zwecke für die Datenverarbeitung), in normative Prinzipien (als Bestandteil einer normativen Ethik: Nicht-Schaden, Wohltätigkeit, Gerechtigkeit, Autonomie, Vertrauen) und natürlich: In welchem Kontext sollen die angewendet werden? Gesellschaft, Staat, Wirtschaft, Wissenschaft – was ein Framework und Leitlinien schon mitgeben können.

(Folie 27)

Nun komme ich zu meiner Konklusion.

(Folie 28)

Zunächst möchte ich die Auswirkungen auf den wissenschaftlichen Prozess betrachten. Ein wichtiger Aspekt, den Data Analytics, Big Data leisten kann und auch sollte im Bereich des Publikationsprozesses (das ist auch etwas, was Turing-Preisträger Jim Gray in dem Kontext genannt hatte), ist das Konzept von interaktiven, lebenden Publikationen, um eine Weiterentwicklung zu schaffen, damit ein kritischer Umgang oder eine kritische Reflexion mit einer Publikation stattfinden kann in Bezug auf die Vermeidung fehlerhafter Verwendung usw.

Ein weiterer Aspekt, um Nachvollziehbarkeit zu gewährleisten, ist, dass nicht nur die wissenschaftlichen Papiere veröffentlicht werden sollten, also eine Form von Erkenntnissen, sondern auch die Daten und die Software, insbesondere Open Source, um das nachvollziehbar zu machen.

Ein wichtiger Aspekt sind Dateninfrastrukturen. Da geht es um Chancengleichheit und Fairness. Insbesondere sollten diese Dateninfrastrukturen als Basistechnologie – und es ist eine Hauptaufgabe auch der Förderinstitutionen, sicherzustellen, dass solche Infrastrukturen entstehen, die diese wesentlichen Eigenschaften widerspiegeln und als Open Data, Open Source zur Verfügung stehen.

Ein wichtiger Aspekt ist die Problematik der sekundären Datenanalyse, also der Research Parasites. Dafür braucht es ein Anreiz- und Belohnungssystem für Wiederverwendung und Reproduzierbarkeit. Beispielsweise sollte die Nutzung von Daten und Software analog zu Zitationen einer Veröffentlichung behandelt werden. In dem Moment erreicht man eine Anreizstruktur, um den wissenschaftlichen Prozess voranzubringen.

Es gibt da schon Beispiele, auch in der Datenmanagement-Community. Da gibt es zwei große Konferenzen, die SIGMOD [Special Interest Group Management of Data] und die VLDB [Very Large Data Base]. Da wird Reproduktion belohnt (das stellt ja auch eine Validierung dar), indem man auf der einen Seite Papers – das macht SIGMOD – mit einem sogenannten Repeatability-Stempel versieht, dass man sagt:

Das war nachvollziehbar, was hier passiert; das haben andere auch ausprobiert. Da gibt es ein Repeatability Program Committee, das das leistet, und bei der VLDB die Experiments and Analyses Track, wo man publizieren kann, dass man Experimente zu den Methoden von anderen durchführt. Und wenn man da zu interessanten Ergebnissen kommt, ist das ein vollwertiges Paper. Manche sagen: Das ist keine richtige Wissenschaft, aber das ist wahrscheinlich schon eine richtige Wissenschaft.

Gleichzeitig gilt natürlich, dass wir für den wissenschaftlichen Prozess Ethik-Richtlinien brauchen; das ist klar und wurde auch im vorigen Vortrag schon klar. Aber noch viel wichtiger in dem Kontext erscheint es mir, nicht nur diese Richtlinien zu haben, sondern das Problembewusstsein, das viele Wissenschaftler schon haben, nach außen zu tragen. Ich glaube, wir haben auch ein Kommunikationsproblem, und diese Kommunikation des Problembewusstseins ist eine Sache.

(Folie 29)

Was ist die Rolle der Forschungsförderung?

Auf der einen Seite benötigen wir einen ethischen Kodex für die Wissenschaften. Ich würde raten, sich Gedanken zu machen und zu unterscheiden zwischen der anwendungsorientierten Forschung (wo man mit Daten umgeht, wo viele Fragen und Probleme auftreten und wo auch das Dual-Use-Problem massiv auftritt) und der Abwägung von Freiheit und Verantwortung zur Erforschung von Algorithmen und Systemforschung.

Da ist es in den meisten Fällen so, wie gesagt, ich bringe noch mal das Beispiel: Die meisten Maschinenlern-Algorithmen sind genauso böse wie die Zahl Fünf. In diesem Kontext sehe ich durchaus eine Tendenz zur Freiheit, aber natürlich im Rahmen eines ethischen Bewusstseins. Es ist sehr wichtig, dieses ethische Bewusstsein zu schaffen und zu kommunizieren, sowohl unter den Wissenschaftlern als auch nach außen, damit die Fördergeber, aber auch die Bürger das verstehen.

Wir müssen also Technologieforschung fördern. Das ist ein zweiter Aspekt, um ein verantwortungsvolles Datenmanagement zu betreiben. Da ist wirklich Forschung zu tun.

Das heißt: Welche Algorithmen, welche Methoden zum Testen, zur Verifikation und zur Sicherstellung der Eigenschaften Fairness, Transparenz, Neutralität usw.? Wie erreichen wir Nachvollziehbarkeit, Reproduzierbarkeit? Und die Unterstützung von Open Data und Open Source sowie die Bereitstellung von Dateninfrastrukturen in Bezug auf diese fünf Eigenschaften, die ich genannt hatte.

(Folie 30)

Die Rolle von Politik, Wirtschaft und Gesellschaft sehe ich so: Die Politik hat sehr geringe Chancen, bei komplexen, grenzüberschreitenden und sich schnell verändernden Fragestellungen, die wir erleben, zu regulieren. Gleichzeitig haben wir im Bereich der Datenmonopole einen gewissen Handlungsbedarf, und darüber muss man nachdenken. Da hat Politik schon eine Rolle.

Eben war die Frage: Was kann das für die Wirtschaft bedeuten? Genauso wie für die Wirtschaft brauchen wir diese Richtlinie, denn genauso wie die Wissenschaft ist die Wirtschaft anfällig für all diese Fehler und Probleme, die ich gezeigt hatte. Letztlich haben Bildung und Kommunikation eine Schlüsselrolle.

(Folie 31)

Das sind noch einmal die fünf Dimensionen von Big Data und Data Science, so wie ich sie und wir sie uns im Berlin Big Data Center ansehen.

Das Wichtige sind in der Tat Kommunikation und Bildung. Damit kann man vielen Aspekten begegnen. Danke.

Manfred Kloiber

Vielen Dank, Herr Markl. Ihre Fragen.

Hans Wernicke

Hans Wernicke, Gesellschaft Deutscher Chemiker. Passend zu Ihren Ausführungen ist gestern eine Pressemitteilung der Leibniz-Gemeinschaft gekommen, dass die Europäische Kommission eine European Open Science Cloud etablieren wird, was unterstützt wird und viele Fragen hier anspricht. Das nur als Hinweis.

Volker Markl

Ja, es gibt einige Bestrebungen in der Chemie oder in der Materialforschung mit dem NOMAD Repository usw. Dabei gibt es ein paar Aspekte, die mich nachdenklich machen, und zwar: Es reicht nicht, nur die Daten irgendwo hinzulegen, sondern man muss auch die Analysemöglichkeiten und -methoden mitgeben. Das muss eine Infrastruktur sein, die auch Datenanalyse ermöglicht und den Datenschutz in der Form gewährleistet. Da haben wir noch Bedarf, so eine Infrastruktur aufzubauen.

Momentan ist ein großer Trend – das ist in jeder Disziplin noch sehr partikulär –, dass man seine Daten einfach irgendwo hinlegt. Die große Gefahr des Datenmanagements ist: Es ist noch kein Datenmanagement, einfach die Daten rauszustellen. Man muss sicherstellen, dass es eine ganzheitliche Unterstützung dieses Datenanalyseprozesses gibt. Da sehe ich noch Probleme.

Andreas Rotor

Andreas Hotho, Universität Würzburg, ich arbeite im Bereich Data Science. Sie haben mehrfach angesprochen, dass wir eine Art Daten-Oligopol, Monopol erwarten können oder dass es passieren wird. Ich würde mal die Frage in den Raum stellen, ob das nicht schon geschehen ist, wenn man sich die großen Internetkonzerne jenseits des Teiches anguckt, wo wir im Prinzip keinen Zugriff mehr auf die Daten haben.

Es gibt noch eine Reihe weiterer Daten, aber das sind die Daten, die zu solchen Phänomenen wie Fake News usw. führen. Die Frage ist nicht nur: Wie analysiere ich die Daten?, sondern: Wie komme ich heutzutage an diesen neuen Rohstoff Daten heran?

Volker Markl

Ich bin absolut bei Ihnen. Wenn man sagt: Daten sind das neue Öl, das neue Gold, und wenn wir einen Zugang zu diesem Rohstoff haben müssen, hat das gleichzeitig einen Wert; das ist ein kritischer Kontrollpunkt, den jeder besetzen will. Das sehen wir in der Wirtschaft in vielen Bereichen. Wir sehen auch, wenn Automobilhersteller oder Hersteller von Fabrikmaschinen bei Industrie 4.0 die Daten für ihre Maschinen sammeln und kontrollieren wollen, dass da Datenmonopole oder Oligopole entstehen. Das zu durchbrechen ist meines Erachtens nur Regulierung möglich. Das ist trotzdem eine Gratwanderung.

Es gibt zwei legitime Aspekte dazu: Auf der einen Seite sind Daten ein wirtschaftliches Gut und haben einen gewissen Wert. In dem Moment will man diese Daten unter Umständen anderen nicht zur Verfügung stellen, weil man einen Nutzen davon hat; das ist das genuine Interesse eines gewinnmaximierenden Unternehmens.

Auf der anderen Seite haben wir Daten, die öffentlich erzeugt wurden, mit öffentlichen Geldern zustande gekommen sind oder generell öffentlich verfügbar sein sollten, weil sie öffentlich sind, zum Beispiel Internet. Bei diesen Daten haben wir schon eine gewisse öffentliche Aufgabe und Verantwortung, sie bereitzustellen.

Eine interessante Frage ist, gerade im Bereich des Internets an sich: Wäre es sinnvoll (gerade für Digital Humanities, aber auch andere), das Internet als Daten in einer Infrastruktur analysierbar zur Verfügung zu stellen? Ich glaube, dass das für Europa sehr wichtig wäre, um den wissenschaftlichen Anschluss nicht zu verpassen. Die USA haben das. Insbesondere China hat eine Abschottungspolitik, und wir in Europa haben es schlicht verschlafen, hier diese Möglichkeiten aufzubauen. Ich denke in der Tat, dass da ein Bedarf ist.

Das geht meines Erachtens aber nur über eine Form von politischem Eingriff. Denn die Komplexität und die Herausforderung sind hier so groß, dass eine einzelne Universität, ein einzelnes Forschungsinstitut oder was auch immer das nicht leisten kann. Auch die Markteintrittshürden sind inzwischen für Unternehmen so groß, dass ein einzelnes Unternehmen es wahrscheinlich schwer haben wird, da mit einem Google zu konkurrieren, wenn es um so etwas wie das Internet geht.

Herr Barakovic [?]

Barakovic [?] vom DFKI [Deutsche Forschungszentrum für Künstliche Intelligenz]. Ich fand das interessant. Der Vortrag zeigt für mich, dass die Frage der Verantwortung in der Informatik ganz anders gelagert ist als in den anderen Wissenschaften. Wir hatten am Anfang das Beispiel mit dem Virus. Da ist es klar: Der Virus ist böse, gefährlich. Das sind diese Dual-Use-Technologien. Bei uns in der Informatik sind das seltene Dinge, wo man sagt: Das ist gefährlich.

Das Problem ist: Die Technologien, die wir schaffen, durchdringen, verändern und bestimmen die Gesellschaft in einer ungeahnten Art und Weise, Diskriminierung und Ähnliches. Die Verantwortung ist viel weniger die Frage, ent[…] die Technologie oder nicht, sondern die Frage einer soliden Validierung, eine Veränderung – vernünftige Algorithmen und Daten, das ist nicht nur eine Frage, ist das eine gute oder schlechte Publikation, sondern ich kann nachher Millionen oder Milliarden Menschen schaden. Ich glaube, die Verantwortung ist viel mehr zu verstehen: Das, was wir tun, verändert die Welt und wir müssen sehr vorsichtig sein, was wir loslassen. Deswegen die Frage: Ist das, was wir da machen, gut oder böse? Maschinen-Learning ist genauso böse wie die Fünf; den Spruch fand ich gut.

Rolf Drechsler

Rolf Drechsler, Universität Bremen und DFKI. Wir haben bisher immer abstrakt über Daten und Algorithmen gesprochen. Hinter den Algorithmen stecken aber immer die Implementierung und die zugehörigen Hardware-Plattformen. Das müssen wir bei der Reproduzierbarkeit mit in Betracht ziehen. Wenn wir bei Publikationen, die 10, 15, 20 Jahre zurückliegen, sagen: Wir würden das gern reproduzieren, dann stoßen wir noch an ganz andere Grenzen, wenn wir diesen Systemgedanken, den Sie angesprochen haben, noch etwas weiterspinnen. Insofern ist die Frage: Ist es überhaupt realistisch machbar, dass wir die Reproduzierbarkeit und die Archivierung auf lange Zeit sichern können?

Volker Markl

Dazu gibt es Forschungsaspekte. Digital Preservation ist da ein großes Thema, schon seit Jahrzehnten. Ich denke an Arbeiten von Raymond Lorie und anderen, wo es darum ging: Kann ich durch virtuelle Maschinen die Ausführungsumgebung weiterhin sicherstellen? Ein anderer Aspekt ist, die Artefakte in einem Zustand zu speichern, der wiederverwendbar und zukunftssicher ist.

Das kann also in zwei Richtungen gehen. Digital Preservation als auch das Forschungsgebiet Data

Correction im Bereich des Datenmanagements befassen sich mit diesen Fragen. Ich bin absolut dabei: Das ist eine große Herausforderung, weil es einen Aufwand darstellt, der zunächst nicht honoriert wird.

Das Problem ist: Man braucht eine Incentive Structure, einen Anreiz: Warum soll ich das als Wissenschaftler tun? Man muss derartiges Verhalten in irgendeiner Form belohnen. Das ist auch etwas, worüber Institutionen nachdenken müssen: Wie belohnt man so ein Verhalten? Ich bin ein großer Fan von Belohnungsstrukturen gegenüber Verbotsstrukturen oder anderem Zwang, sondern um das zu belohnen, also wie wir jetzt zum Beispiel im Datenmanagement gesagt haben, mit VLDB und SIGMOD, da gibt es Belohnungen dadurch, dass über so was Publikationen entstehen können, die dann wahrscheinlich den H-Index verbessern werden usw. Da gibt es Anreize. Über solche Systeme müssen wir nachdenken.

Manfred Kloiber

Vielen Dank, Herr Markl.

... der Forschung zur IT-Sicherheit

Manfred Kloiber

Jetzt geht es weiter mit Anja Feldmann. Anja Feldmann ist bekannt als Internet-Professorin. Sie leitet die Arbeitsgruppe Internet Network Architectures an der TU Berlin und wird demnächst am Max-Planck-Institut für Informatik in Saarbrücken tätig sein. Frau Feldmann spricht über den Nutzen und die potenziellen Risiken in der IT-Sicherheitsforschung.

Anja Feldmann ML, Technische Universität Berlin / Institut für Telekommunikationssysteme

(Folie 1, 2)

Auch ich freue mich, heute da zu sein. Die Fragestellung, die ich betrachten wollte, ist mehr im Bereich der Sicherheit. Dazu sollte ich sagen, dass mein Fokus nicht die Sicherheitsforschung ist. Mein Fokus ist zu verstehen: Was tut sich im Internet? Wie verändert sich das Netzwerk? Was können wir machen, um die Sachen zu verbessern?

Das Internet ist ein komplexes System. Alle Leute interagieren miteinander, und wir kämen heute wohl nicht mehr zurecht, wenn wir kein Internet mehr hätten, sei es das Web, sei es das, was die Kinder machen, sei es die Industrie, das IoT [Internet of Things], Digitalisierung der Industrie, Digitalisierung der Gesellschaft – ich frage mich, ob das Wort Digitalisierung vielleicht das Unwort des nächsten Jahrhunderts werden wird.

(Folie 3)

Die Frage ist natürlich: Was bedeutet Sicherheit? Wenn ich in der Vorlesung zu IT-Sicherheit frage: Was ist Sicherheit, was sind die drei Haupteigenschaften?, dann erwarte ich, dass mir jeder runterbeten kann: CIA, Confidentiality, Integrity, Availabilty. Vertraulichkeit: dass meine Daten nicht irgendwo mitgelesen werden können; Integrität: dass das ankommt, was ich gesendet habe und dass das jemand überprüfen kann; und vor allen Dingen Verfügbarkeit und Erreichbarkeit.

Dummerweise vergessen die meisten Leute den letzten Punkt, die Availability. Wenn ich die nicht habe, kann ich meine Daten in die Bank einsperren und sie sind sicher – hoffentlich, bis auf Bankeinbrüche. Aber das ist nicht unser Thema heute. Das heißt: Availability ist ein sehr wichtiger Teil.

Kryptographie, das sind die Methoden zur Verschlüsselung, Algorithmen. Natürlich gibt es auch da Sicherheitslücken; wir brauchen immer neue Kryptographieverfahren. Hauptproblem ist die Frage: Welche Schlüssellänge brauche ich? Wenn ich jetzt eine Schlüssellänge von 56 habe, was ist in fünf Jahren? In fünf Jahren ist ein Schlüssel 56 vermutlich schon längst crackbar. Aber das ist eine Frage der Auswahl, der Nutzung.

Heute möchte ich mehr auf das Thema Availability eingehen. In Sachen Verfügbarkeit wird das Ganze viel schwieriger. Was habe ich an Tools zur Verfügung? Ich kann eine Firewall aufbauen, um zu sagen: Ich möchte nicht, dass da alles durchgeht, was aus dem Internet herauskommt.

Es gab mal Aussagen wie: Wenn jemand einen neuen Microsoft-PC ins Netz hängt, wird er vermutlich innerhalb von einer Stunde gehackt sein. Dagegen kann man sich mit Firewalls wehren. Aber leider müssen die konfiguriert werden; das sind Software-Systeme, die können auch gehackt werden. Da muss man aufpassen.

Dazu kommen Intrusion-Detection-Systeme. Denn ich muss analysieren, was da sonst noch ist. Das ist eine Kunst; da nutzen die Leute Big-Data-Analysen oder andere Sachen, aber was das alles macht, wie es zu konfigurieren ist – Fehlalarme so können immer mal passieren, auch mitten in der Nacht, aber wenn das zum fünften Mal passiert, kümmert sich der Systemadministrator nicht mehr.

Das ist das ganze Problem dahinter. Das heißt, die Nutzbarkeit dieser Systeme ist nicht einfach und es bräuchte viel mehr Forschung in dem Bereich, um die Tools, die wir zur Verfügung haben, auch sinnvoll einsetzen zu können.

Das Problem ist auch: Das Internet wächst, das ist ein Riesensystem. Wir brauchen also Systeme für die Sicherheit, die mit diesen großen Wolken umgehen können. Wie erreichen wir das? Wie machen wir ein System, das eigentlich für kleine Sachen gedacht ist, groß?

(Folie 4)

Apropos groß und Angriffe auf Availability: DDoS[Distributed-Denial-of-Service]-Attacken sind da, waren da und werden immer wieder da sein: „Hackers Hit Dozens of Countries“, ein DDoS Attack auf Pippa Middleton, Yahoo, KrebsOnSecurity, „National Internet Defense – More States on the Skirmish Line“, alle möglichen Attacken.

Das sind nicht nur DDoS-Attacken. DDoS gehen im Prinzip dahin, dass man sagt: Ich sende so viel Verkehr, dass der normale Verkehr nicht mehr durchkommt. Es gibt auch andere Fehlerquellen, die dafür sorgen, dass sich jemand in ein System einhackt, die ganzen Daten des Systems verschlüsselt und dann sagt: „Bitte überweise mir soundso viele Bitcoins, damit ich das Ganze eventuell (oder auch nicht) freischalte.“ Das ist die sogenannte Ransomware.

Das heißt: Sicherheit ist ein Problem.

(Folie 5)

Was ist eine Sicherheitslücke? Eine Lücke ist im Allgemeinen ein Fehler im Code, in der Umsetzung oder im Design, der zu einem Sicherheitsrisiko im Netz oder im Endgerät führen kann. Es geht hier um Bugs, und Bugs können in jedem Teil des Prozesses mit Software stattfinden, nicht nur in der Software, sondern auch in der Hardware. Das heißt: Jeder kleine Bug, der irgendwo existiert, kann ein Sicherheitsrisiko sein.

Wenn ich das zu einem Extrem nehme, müsste ich sagen: Ich muss immer bugfreie Systeme bauen. Das werden Sie nicht erreichen. Irgendwo

ist meistens doch eine Lücke. Darum muss man nicht nur die Fehlerquellen haben, sondern auch die Risikobewertung machen: Was ist die Wahrscheinlichkeit, dass etwas eintritt? Und das mit der Schadenshöhe multiplizieren.

Das ist genau die Frage. Wenn Sie ein Fahrrad irgendwo anschließend wollen: Was für ein Schloss verwenden Sie? Ist Ihr Schloss genauso schwer wie Ihr Fahrrad? Oder ist es nur ein einfaches Schloss, weil Ihr Fahrrad so alt ist?

Wie sieht das aus, wenn Sie jetzt ein Elektrofahrrad haben, das nicht nur 500 Euro kostet, sondern vielleicht 4.000 Euro? Was für ein Schloss sollte das haben? Ist das versichert? Genau solche Fragen gehen auch mit dem IT-System einher.

Das andere Problem ist in dieser Sicherheitsfrage von Computersystemen auch: Kann ich eigentlich mein Risiko schon versichern? Da gibt es bisher sehr wenige Angebote. Das ist auch eine interessante Fragestellung.

Das Problem im Internet ist: die Aussage „Die Sicherheitslücke wird niemand finden“ – vergessen Sie es. Wenn es sich um eine publizierte Sicherheitslücke handelt, wird irgendjemand in der Wolke diese mit hoher Wahrscheinlichkeit ausnutzen.

Auch Aussagen wie: „Diese Attacke ist viel zu kompliziert und wird deshalb nicht passieren“ haben sich als falsch herausgestellt.

(Folie 6)

Sehen wir uns ein paar Beispiele von Sicherheitslücken an.

Es kann Probleme mit der Krypto und der Umsetzung, der Implementierung geben. Dort hat jemand im Linuxkern einfach eine Zeile auskommentiert, und damit war SSH [Secure Shell] plötzlich kaputt, weil die Anzahl der Schlüssel, die noch zur Verfügung standen, sehr eingeschränkt war.

Buffer Overflows treten überall dort auf, wo in maschinennahen Programmiersprachen programmiert wird. Das ist so, dass ich da einen Speicher alloziere. In diesen Speicher wird irgendetwas hineingeschrieben, und wenn dort etwas Größeres hineingeschrieben wird als das, was man reinschreiben sollte, wird ein anderer Speicher überschrieben. Das kann genutzt werden, damit das Programm irgendwo anders hinspringt, und plötzlich hat jemand, der in den USA oder in Russland sitzt, Zugang zu einem Rechner in Deutschland. Das kann schnell passieren. Buffer Overflows gibt es fast überall, in jeder Software, und die Verifikationstools, die wir haben, sind leider noch nicht gut genug, dass wir all diese Sachen ausschließen können.

Cross-Site-Scripting [XSS]: Sie gehen auf irgendeine Webseite, auf der Schadcode untergebracht ist, der dann Ihren Rechner identifiziert. Das hängt zum Teil damit zusammen, dass Leute, wenn sie Webseiten aufsetzen, sagen: „Oh, die Leute sollen da irgendwelche Nachrichten hinterlassen können. Und diese speichern wir dann mal ab.“ Wenn dann nicht überprüft wird, dass da kein Skript ausgeführt wird, dann können Informationen von anderen Benutzern, die auf diese Webseite gehen, plötzlich woanders hingelangen.

Phishing: Jemand sendet Ihnen eine E-Mail und Sie drücken darauf, obwohl Sie eigentlich wissen, dass Sie es nicht tun sollten. Das ist die typische Art und Weise, wie man sich einen Virus einfängt, der sich dann weiter verbreiten kann.

Probleme in der Konfiguration, in der Wartung: Zum Beispiel die ganze Ransomware, die die Deutsche Bahn für eine gewisse Zeit lahmgelegt hatte, kam daher, weil die ihre Systeme nicht

upgedatet haben und keine Patches, die Sicherheitslücken schließen, eingeführt haben.

Jetzt ist die Frage: Wie kann ich dafür sorgen, dass die Software, die überall verbreitet wird, immer auf dem aktuellen Stand ist und alle bekannten Fehlerlücken behoben werden? Das ist nicht so einfach.

Andere Probleme, die auftreten: Die Leute denken, sie haben ihr System hinter einer Firewall und damit sollte es von außen nicht erreichbar sein. Tja, Pech gehabt: Irgendjemand hat die Firewall abgeschaltet oder irgendwo hat jemand was vergessen. Oder jemand nimmt einen Laptop, packt den ins Firmennetz und dieser Laptop hat ein Sicherheitsproblem: Damit sind Ihre Informationen im Netz.

(Folie 7)

Da kommen eine Menge an ethischen Fragen rein, wenn wir Sicherheitslücken haben: Wer darf die eigentlich ausnutzen? Wer darf bis zu welchem Grad zeigen: „Oh, wir haben hier ein Problem“?

Darf der Forscher zum Beispiel bei Amazon eine Cloud übernehmen, um zu zeigen: „Hey, Amazon, du hast da wirklich ein Problem in deiner Virtual Machine“, und damit gewisse Dienste offline stellen? Nein, darf er nicht. Aber die Frage ist: Bis zu welchem Grad muss er das zeigen können, damit das Ganze entsprechend veröffentlicht wird?

Wie sieht es aus mit den Geheimdiensten? Die haben natürlich ein Rieseninteresse daran.

Wie sieht es aus mit der Polizei? Die Polizei hat das Problem, dass die Kriminellen inzwischen auch alle Tools verwenden, von WhatsApp über verschlüsselte E-Mail und diese Geräte hier zum Kommunizieren. Die würden natürlich gern mitlesen, was denn hier ist. Nur müssen sie dazu die Verschlüsselung knacken und brauchen damit wieder eine Sicherheitslücke, um das hinzukommen.

Wie sieht es mit dem Militär aus? Darf das Militär im Krieg die Computer des anderen Militärs hacken?

Dazu ein paar Beispiele: Trump behält das Hacking Vulnerability Program, um dafür zu sorgen, dass das US Government immer gute Zero-Days hat, nämlich diese Art von Zugriffen, um andere Computer zu hacken.

Cisco bestätigt: „NSA-linked zeroday targeted its firewall for years.“ Die NSA hat gewisse Zero-Days, die gegen ihre Firewalls gehen.

„New leaks prove it: the NSA is putting us all at risk to be hacked.“ Denn sie haben Sicherheitslücken zum Teil zurückgehalten, damit sie sie selber nutzen können, um auf verschiedene Informationen zugreifen zu können.

Ist das noch ethisch? Sollten wir das zulassen? Unter welchen Randbedingungen?

(Folie 8)

Wie ist das mit Bug-Bounty-Programmen? Bug-Bounty-Programme sind Programme von Firmen, die sagen: „Hey Leute, wenn ihr irgendwo einen Fehler gefunden habt, dann meldet uns den, und wir geben euch eine gewisse Menge an Rewards.“

Diese Rewards können sein, wie mal bei Amazon, eine Kreditkarte mit einem gewissen Credit. Es kann dahin gehen, dass Yahoo T-Shirts ausgeteilt hat. Es kann aber auch so weit sein, dass es inzwischen Firmen gibt – ich habe hier von Wikipedia den entsprechenden Eintrag geholt, wonach es eine Information-Security-Firma gibt, die große Beträge zahlt dafür, dass da gewisse Zero-Day-Attacken zur Verfügung stehen. Das ist richtig Geld.

Dürfen jetzt zum Beispiel Forscher, die Sicherheitsprobleme finden, zu dieser Firma gehen und sagen: „Ich habe einen Fehler gefunden. Gebt mir eine Million dafür, dann kann ich wieder Forschung machen.“ Und damit gehen sie nicht mehr zur DFG. Ist das legal oder nicht?

Ist das ein guter Ansatz der Firmen? Denn die Firma hat dadurch natürlich den Vorteil, dass sie vielleicht keine Sicherheitsabteilung mehr braucht, denn sie kann ja nur im Erfolgsfall den freien Mitarbeitern, die sie über das Bug-Bounty-Programm bezahlt, die Probleme abkaufen. Das bedeutet aber auch, dass die Firma damit durchaus weiß, dass sie vermutlich nicht ihre ganze Software nach allen möglichen Sicherheitslücken untersucht hat und sie trotzdem ins Netz stellt und verkauft. Ist das eigentlich ethisch?

Sollen wir die Beta-Tester von aller Software im Internet sein? Eigentlich ja nicht. Das sind auch interessante Fragen.

(Folie 9)

Wo liegen die Chancen für die IT-Forschung?

Die Tatsache, dass hier Sachen fehlerhaft eingesetzt werden, ist eigentlich nicht ein Problem der Resultate der Forscher. Aber das wird immer wieder passieren. Sind wir als Hammerhersteller dafür verantwortlich, wenn sich jemand irgendwo mit dem Hammer auf den Finger haut? Eigentlich nicht.

Das ist der Grund, wo wir aufpassen müssen. Ist ein Algorithmus per se schlecht? Nein. Kann er missbraucht werden? Ja.

Das heißt, wir müssen viel mehr schulen, wie man sinnvoll mit den Tools der Informatik umgeht, um davon sinnvolle Systeme zu bauen. Gleichzeitig brauchen wir Möglichkeiten, um viel mehr der Probleme, die wir im Moment haben, zu verhindern.

Wir brauchen proaktive Verfahren, um Bugs zu verhindern. Wir brauchen eine sichere Software-Entwicklungsumgebung, Programmiersprachen ohne Buffer Overflow. Wir müssen unsere Software verifizieren können, um sicherzustellen, dass sie das tat, was sie tun soll. Wir brauchen gute und sichere Defaults. Wir müssen uns damit beschäftigen: Wie verhindere ich den Fehleinsatz von verschiedenen Systemen? Wie konfiguriere ich das System in einer Art und Weise, dass Fehler erst gar nicht auftreten?

(Folie 10)

Gleichzeitig brauchen wir reaktive Verfahren. Wir brauchen systematische Anwendungen für die automatische Verifikation von Systemen und Software. Wir müssen Sicherheitslücken finden. Dazu ist nur das Thema Fuzzing zu nennen, das viele Buffer Overflows finden kann. Wir müssen aber auch im Internet scannen, um zu sehen: Wo sind denn Systeme, die fehlkonfiguriert sind? Das heißt, wir brauchen Tools, um diese Sachen trainierbar zu finden.

Das Problem hinter diesen Tools ist, dass sie auch von den Bösen benutzt werden können. Denn die Bösen benutzen dieselben Sachen, um die Systeme zu finden, die angreifbar sind. Hier haben wir das typische Problem des Dual Use. Und natürlich benutzen die Schlechten dieselben Verfahren wie Fuzzing und andere Sachen, um Buffer Overflows zu finden. Die werden sie nur in ihrem Sinne verwenden. Das heißt, die guten Tools, die wir haben, werden auch von den Leuten ausgenutzt, die die Systeme hacken wollen. Gut und schlecht.

Es gibt den Begriff des White Hat Hackers und des Black Hat Hackers. Der White Hat Hacker nimmt sich zum Beispiel Security Audits in verschiedenen Systemen vor, um dann im Auftrag der Firma zu sagen: Ja, alles in Ordnung (oder

nicht). Die anderen – na ja, da gibt es halt den Schwarzmarkt.

(Folie 11)

Ich möchte in diesem System auf drei verschiedene Komponenten hinweisen: Wir haben auf der einen Seite die Programmierer; die erschaffen die Programme, die Anwendungen. Dann haben wir die Administratoren; die betreiben die Server und die Infrastruktur; und wir haben die Nutzer der bereitgestellten Systeme.

Wenn man sich mit Sicherheit beschäftigt, ist der klassische Ansatz zu sagen: Wir fokussieren uns darauf, dass die Programme wirklich sicher sind, denn in Sachen Nutzbarkeit fokussieren wir uns auf den Endbenutzer. Hier haben wir eine Gruppe vergessen: die Administratoren. Und darüber müssten wir uns eigentlich viel mehr Gedanken machen.

(Folie 12)

Hier ist eine schöne Darstellung, einen Cartoon, den ich im Netz gefunden habe. Data Security: „In this corner, we have firewalls, encryption, Antivirus Software, etc. And in this corner, we have Dave“ mit „Human Error“.

Wir haben viel zu wenig Möglichkeiten, die menschlichen Fehler zu verhindern.

(Folie 13)

Ich möchte etwas zur Häufigkeit von Fehlkonfigurationen sagen:

Es gibt eine Hamburger Klinik, die ihre medizinischen Daten im Netz stehen hatte, und zwar weil sie eine Backup-Datei auf einem Webserver vergessen hatte.

Das nordkoreanische Facebook benutzte „admin“ als Passwort. Damit waren die Sachen *da*.

Viele Leute hatten für lange Zeit auf ihrem Home-Router das Standard-Passwort; es wurde nicht geändert. Damit wurden diese Home-Router zu einem schönen Botnet zusammengefügt. Das wird uns mit den ganzen IoT-Geräten in Zukunft mit Sicherheit noch mehrfach passieren. Passwort ändern!

Daten des französischen Orange(O2)-Nutzers waren öffentlich über eine MongoDB erreichbar, weil die Firewall nicht da war.

Es gibt jede Menge Industrieanlagen, die ohne Authentifikation übers Internet erreichbar sind. Wir können glücklich sein, dass die Hacker das noch nicht benutzt haben.

(Folie 14)

Dazu möchte ich zwei Beispiele zeigen anhand von Key-Value Stores, die zum Teil öffentlich übers Netz erreichbar sind.

Was sind Key-Value Stores? Wir reden immer von Datenbanken, von NoSQL-Datenbanken; das sind diese Key-Value Stores. Die sind im Prinzip nichts anderes als eine große Hashtable: Ich schreibe einen Wert hinein, assoziiere ihn mit irgendwelchen Daten und kann dann über diesem Wert wieder auf die Daten zugreifen. Typische Beispiele sind Memcached, MongoDB und Redis (nicht Dedis).

Diese werden fast überall in der Cloud benutzt, weil sie wunderbare Zwischenspeicher für verschiedene Webservices und andere Sachen sind.

Das Problem ist: Es gibt keinerlei Authentifizierung oder Sicherheit, was den Zugriff zu diesen Datenbanken angeht, sondern die Annahme hinter diesen Datenbanken ist: Sie werden in einem privaten Bereich des Netzes benutzt, wo ich keine Authentifikation oder Autorisation brauche. Wenn ich diese Daten dann nicht mehr in einem abgeschlossenen System habe, kann das dazu führen, dass ich Nutzerdaten veröffentliche oder dass weitere Anwendungen darüber Angriffe machen können, weil darin systemimmanente Daten gespeichert werden.

(Folie 15)

Jetzt ist die Frage: Gibt es solche Fehlkonfigurationen? Wie finde ich die? Und was darf ich mit den gefundenen Daten machen?

(Folie 16)

Beispiel Redis-Server: Hier sehen wir, wie viele Systeme es im öffentlichen Internet gab zu dem Zeitpunkt, wo wir gescannt haben. Hier sehen wir, dass 20.000 bis 45.000 Systeme frei im Internet verfügbar sind. Nein, wir haben nicht geguckt, welche Daten darin sind; wir haben die Daten nicht extrahiert.

Wir sehen, dass es im Februar 2015 dazu eine Bekanntmachung gab. Die Anzahl der Systeme ist nicht drastisch reduziert worden, sondern eher gewachsen. Im November 2015 gab es in der Presse eine Demonstration, wie man mit öffentlichen Servern diese Systeme übernehmen kann. Es gab eine prompte Reaktion: Wir sehen, dass es praktisch reduziert wurde. Wir sehen aber auch, dass es danach wieder hochgeht.

(Folie 17)

Memcached ist ein ähnlicher Dienst. Hier war ebenfalls seit Februar 2015 bekannt, dass es da Probleme gibt. Hier sehen wir, dass sich im November das Ganze drastisch reduziert hat, hier nicht. Auf der anderen Seite sehen wir, dass es hier eine große Anzahl von Systemen gibt, die plötzlich dazukommen und wieder runtergehen.

Womit hängt das zusammen? Das hängt damit zusammen, dass die Forscher hier diese Anbieter einzeln kontaktiert haben. Manchmal ist es ein einziger Systemadministrator, der kontaktiert werden muss, der für 10.000 oder 100.000 Systeme verantwortlich ist, weil das in der Cloud produziert wird. Und wenn der das Problem fixt, geht die Anzahl der betroffenen Systeme wieder zurück.

(Folie 18)

Diese fehlkonfigurierten Systeme lassen sich überall im Netz finden (obwohl sie nicht da sein sollten), weil in der Konfiguration, in der Zusammenstellung Fehler gemacht wurden.

Nur weil man diese Informationen veröffentlicht, bedeutet das noch nicht, dass die Leute etwas tun. Administratoren haben ein kurzes Gedächtnis und sind auch nicht unbedingt die höchstqualifizierten Leute; das ist zum Teil das Problem dahinter. Sie führen Kochrezepte aus.

Da heißt: Wir müssen Tools haben, um diese Sachen zu verhindern.

(Folie 19)

Da kommen wir wieder zu ethischen Fragen: Was machen wir, wenn eine relevante Sicherheitslücke gefunden wurde? Wann muss man die Informationen an wen veröffentlichen? Wie sieht es mit den CERTs [Computer Emergency Response Team] aus? Wann darf man an die Öffentlichkeit gehen? Darf man erst dann an die Öffentlichkeit gehen, wenn die Firmen nicht reagieren? Wie sieht das Ganze aus?

Hier gibt es unterschiedliche Meinungen. Einige Sicherheitsforscher haben zum Teil versucht, die Sachen an die Firmen zu melden, und haben dann so: „Na ja, vielleicht könnte das mal interessant sein. Wir werden uns das mal ansehen.“ Dann gehen sie natürlich an die Öffentlichkeit. Aber wenn die Sachen an die Öffentlichkeit gehen, bevor die Patches deployt sind, haben wir wirkliche Sicherheitsprobleme. Wie lösen wir das?

Wie sieht das insgesamt aus für die verschiedenen Forschungscommunitys? Gibt es da schon ethische Standards? Einige Sicherheitscommunitys haben schon explizite Statements, Ethical Considerations, was Veröffentlichungen angeht:

> "If a paper relates to human subjects, analyzes data derived from human subjects, may put humans at risk or might have other ethical or legal implications, authors should disclose if an ethics review (e.g., IRB approval)",

das ist die entsprechende Institution, die jede amerikanische Uni haben muss; ob dies schon gemacht wurde und ob die Sachen hier überprüft wurden.

Für die Internet Measurement Community gilt auch: Experimente mit Benutzern oder sensitive Daten sollen die Privatsphäre respektieren. Denn diese Sachen wurden eingeführt, weil es in der Vergangenheit Papers gegeben hat, die die Privatsphäre von Leuten nicht berücksichtigt haben.

In der Measurement Community gibt es immer wieder den Ruf: „Leute, veröffentlicht eure Daten!" Das Problem mit dem Veröffentlichen der Daten ist allerdings: Diese Daten sind für spezifische Zwecke erhoben wurden. Wenn andere Leute diese Daten nehmen, machen sie Mist, weil sie die Randbedingungen nicht respektieren, unter denen die Daten erhoben wurden.

Zum anderen ist die Privatsphäre ein großes Problem. Meistens sind es die Leute, die sagen: „Veröffentlicht eure Daten", die noch nicht mal ihren eigenen Code oder Analysen veröffentlichen. Das finde ich erschreckend.

In der Community gibt es auch so etwas wie: Wie geht man um, wenn man Daten teilen will? Wie muss man sich damit auseinandersetzen? Was sind die Issues und die Etikette, die dahintersteckt? Der Mendro Report ist einer von den Bereichen, auf den man sich immer wieder stützt.

Was muss oder soll man tun, um einen Bug zu fixen? Einige Leute hatten mal die Idee: Wenn ich den Bug kenne, kann ich den ja eigentlich nutzen, um daraus einen Fix zu schreiben, der den Bug fixt. Darf man das tun?

Nein, das darf man nicht. Denn man weiß nicht, ob das nicht auf dem System, wo man es einpflegen würde, irgendwelche Nebeneffekte hätte, die zum Absturz des Systems führen würden. Und wenn das während einer Operation passiert, ist das nicht gerade lustig.

(Folie 20)

Ich könnte noch weitere Fehlkonfigurationen zeigen, aber dann kommen wir über die Zeit hinaus.

Immer wieder Problemquellen für Fehlkonfigurationen sind Protokolle. Brauchen wir einfache Protokolle oder brauchen wir komplexe Protokolle? Machen wir Security by Design oder erlauben wir es den Benutzern, Sicherheitsfeatures auszuschalten, nicht zu nutzen? Wie sieht das aus?

Die Kultur. Zu sagen: Administratoren sind die Experten; die wissen schon, was sie tun – nein. Auch Zeitdruck muss berücksichtigt werden, und es ist immer die Frage: Was wird mehr geschätzt, Sicherheit oder Feature? Dann müssen wir dahin kommen, dass Sicherheit wenigstens genauso wichtig ist wie neue Features.

(Folie 24)

Gehen wir noch mal auf die Erwartungen der Nutzer ein. Wir haben da die Frage: Wie zuverlässig oder wie verfügbar müssen die Sachen sein?

Jeder erwartet, dass sein Auto zu 100 Prozent funktioniert, wenn man da morgens einsteigt. Es bringt einen einfach von A nach B; Batterieprobleme sind inzwischen vergessen. Der Rechner, na ja … der kann mal abstürzen. Aber wie sieht das mit dem autonomen Auto aus, wo jede Menge Rechnersachen und Computer drin sind?

Wie sieht es aus mit der Lebensdauer? Ein Auto: zehn Jahre. Ein Rechner: zwei bis drei Jahre. Und das autonome Auto?

(Folie 25)

Wie sieht das eigentlich aus? Wie muss ich diese Systeme betrachten? Wie sieht die Wartbarkeit aus, wie kann ich hier die Sache weitermachen?

Dazu muss man das Ökosystem Internet, Sicherheit beobachten: Was sind die aktuellen Angriffe? Für wie viel kann ich mir den neuesten Angriff einkaufen? Da gibt es unterschiedliche Marktsegmente, und da ist es so: Die Firmen zahlen über ihr Bug-Bounty-Programm einen relativ kleinen Betrag. Wenn ich das Ganze auf dem Schwarzmarkt verkaufe, kann ich viel, viel mehr Geld verdienen. Legal oder nicht?

Die Frage ist auch: Wann und unter welchen Randbedingungen muss wer einbezogen werden? Und wie sieht es mit dem Datenschutz aus?

Damit bin ich am Ende.

Manfred Kloiber

Vielen Dank, Frau Feldmann. Mir ist aufgefallen, dass es in der deutschen Gesellschaft einen Zielkonflikt gibt, der mittlerweile offensichtlich geworden ist und der auch unter Informatikern stark diskutiert wird:

Das IT-Sicherheitsgesetz verlangt, dass Sicherheitslücken nicht offengelegt werden, sondern dass sie nur anonym gemeldet werden. Die Informatik-Community hat sich eindeutig positioniert und hat dem Staat gesagt: Das geht so nicht, ihr müsst eine Veröffentlichungspflicht machen, damit die Lücke sofort geschlossen werden kann. Der Staat hat andere Interessen. Wie wird das bei Ihnen diskutiert?

Anja Feldmann

Das ist genau das Problem: An wen soll man das veröffentlichen? Wie sieht das mit den CERTs aus? Haben die eigentlich die Möglichkeit, diese Sicherheitslücken zu schließen? Es reicht nicht, wenn man das nur zum Staat hin kommuniziert, sondern es sind ja meistens internationale Lücken, das heißt: Wer ist dafür rechtlich verantwortlich? An wen müsste man so etwas kommunizieren?

Es gibt natürlich über die CERTs die Möglichkeit, dass man die Sachen dort kommuniziert. Man sollte die Sachen an die Firmen kommunizieren, nicht nur an den Staat. Ich glaube, das ist schon die allgemeine Conclusion, wenn man fragen würde: Wie gehen wir mit einer neuen Lücke um?

Ich bin da nicht die Expertin, denn ich habe mich noch nicht mit zu vielen Bugs herumgeschlagen. Von daher würde ich erst mal meine Kollegen fragen, die entsprechende Erfahrungen haben.

Manfred Kloiber

Wie gut das klappen kann, hat man an diesen WPA[WiFi Protected Access]-Bugs gesehen. Das hat ein europäischer Wissenschaftler nach Amerika gemeldet und erst drei Tage später hat das BSI [Bundesamt für Sicherheit in der Informationstechnik] aus der Presse davon erfahren. Das hat nicht so gut geklappt.

Ninja Marnau

Ninja Marnau vom CISPA [Center for IT-Security, Privacy & Accountability] in Saarbrücken. Wir setzen uns jeden Tag mit diesen ethischen Problemen auseinander und überlegen: Inwiefern dürfen wir, wenn wir Honeypots deployen, wenn auch nur zu feingranularen Teilen, an einem DDoS-Angriff teilnehmen, um ihn zu beobachten und um herauszufinden, was für Malware darüber verteilt wird und wie die Kriminellen agieren?

Sehr schön fand ich, dass Sie gesagt haben: Wir sind nicht die Pentester des Internets. Genau das sind wir eben nicht, und ich bin froh, dass in der IT-Security Community die großen Konferenzen da tatsächlich positive Anreize setzen, nämlich

in der Form eines verpflichtenden IRB [Institutional Review Board] Approvals der Forschung und auch in der Form, dass diese Low hanging Fruit eine Vulnerability finden und dass auf den Konferenzen nicht mehr akzeptiert wird, dass die aufs Internet losgelassen werden, sondern erwartet wird, dass dazu Analysen und Fixes kommen, wie das Ganze in der Systemarchitektur in Zukunft verhindert werden kann. Das sind gute Beispiele, die auch andere Communitys aufnehmen könnten, indem sie auf den großen Konferenzen so etwas zur Verpflichtung machen.

Anja Feldmann

Dem kann ich nur zustimmen.

Ingo Dachwitz

Ingo Dachwitz, Autor bei Netzpolitik. Eine Anmerkung, weil Sie im Hinblick auf die Janusköpfigkeit oder den Zielkonflikt des staatlichen Handelns im Bereich Sicherheit vor allen Dingen auf die USA verwiesen hatten. Nur als Ergänzung der Blick auf Deutschland: So bekommen wir in Deutschland keine klare Antwort dazu, ob deutsche Behörden auch Zero-Days einkaufen. Aber klar ist, dass es einen (wahrscheinlich scheidenden) Innenminister gibt, der sagt: Es darf keine Kommunikation geben, auf die der Staat nicht auf irgendeine Weise einen Zugriff haben darf. Es ist klar, dass es staatliches Hacking gibt in Form von Staatstrojanern. Wie das ohne Zero-Days funktioniert, ist eine spannende Frage.

Es gibt neuerdings die zentrale Stelle für Informationstechnik im Sicherheitsbereich, ZITiS, unter dem Innenministerium angesiedelt, die genau dafür da ist, mit wissenschaftlichen Methoden zu erforschen, wie verschlüsselte Kommunikation gebrochen oder zumindest angeschaut werden kann. Die ist zwar bei der Bundeswehr-Uni in München angesiedelt, aber die Frage, wie man da zusammenarbeitet oder ob es eine Zusammenarbeit auch mit Nicht-Bundeswehr-Unis geben wird, wird die deutsche IT-Forschung sicherlich noch beschäftigen. Das nur, um das Bild zu ergänzen. Da brauchen wir gar nicht in die USA zu gucken.

Anja Feldmann

Mit Sicherheit, und es wird mit Sicherheit etliche Leute geben, die sagen: Mit denen werden wir nicht zusammenarbeiten, weil sie für sich ethisch beschlossen haben, das nicht zu tun. In Deutschland gibt es auch mit dem CCC [Chaos Computer Club] eine sehr lautstarke Organisation, die durchaus auf die Rechte der Benutzer und der Gesellschaft als Ganzes und auf die Veröffentlichung pocht. Auch diesen Teil der Community darf man nicht unterschätzen.

Ninja Marnau

Was unglaublich helfen würde für unseren eigenen Umgang mit dem Auffinden von Sicherheitslücken, sind deutschlandweite Standards, was Responsible Disclosure angeht, eine Einigung der deutschen Community: Wie gehen wir damit um? An wen berichten wir?, damit solche Sachen wie dass die deutschen, die europäischen CERTs nicht informiert werden, nicht passieren und damit unsere Mitarbeiter und Studenten auf einer sichereren Ebene stehen, wenn sie solche Disclosures machen. Würde sich die DFG, würde sich die Leopoldina dort engagieren und an so etwas mitarbeiten, auf so etwas hinarbeiten?

Anja Feldmann

Diese Frage sollte von den entsprechenden Vertretern hier beantwortet werden.

Frank Allgöwer

Von der DFG-Seite kann man das klar sagen: Die DFG ist keine ausführende Institution. So etwas sollte nicht von einem Forschungsförderer übernommen werden, und ich gehe davon aus, dass die Leopoldina das ähnlich sieht.

Bärbel Friedrich

Das ist eine Frage, die wir in unserem Komitee sicherlich stellen müssen. Wir sind ja hier, um diese Anregungen zu bekommen, und das wird sicherlich Gegenstand der Diskussion sein.

Anja Feldmann

Ich denke schon, dass auch die DFG in der Pflicht ist, auch für die Finanzierung dieser verschiedenen Aspekte, eventuell daran teilzunehmen, und das war die Frage. Die Frage war nicht, ob die DFG es selbst macht, sondern dazu beizutragen, dass eine solche Einigung tatsächlich passiert und dass wir da bessere Strukturen bekommen.

Das andere, was zu erwähnen ist: Wir müssen mit dem deutschen Gesetzgeber sehr aufpassen, weil der deutsche Gesetzgeber zum Beispiel im Bereich der Netzwerktools gesagt hat: All das, was dazu gebraucht werden könnte, zu hacken, darf nicht mehr weiterentwickelt werden. Das Problem ist nur, dass die Leute, die zum Beispiel Intrusion-Detection-Systeme machen, genau dieselben Methoden einsetzen, um die Verteidigung zu schaffen. Da ist der Gesetzgeber durchaus in die Pflicht zu nehmen, darüber nachzudenken: Wo sind die Grenzen? Was kann man überhaupt verbieten und verbietet man nicht zu viel?

Manfred Kloiber

Gab es da nicht schon eine Klarstellung zu dem Thema?

Anja Feldmann

Da gab es eine Klarstellung, aber das ist halt nur eine Klarstellung. Das Gesetz sagt etwas anderes.

Manfred Kloiber

Okay. Vielleicht ist auch die Gesellschaft für Informatik noch ein Ansprechpartner. Ich glaube, die arbeiten auch an Community-Standards.

Bärbel Friedrich

Selbstverständlich darf nicht der Eindruck entstehen, dass eine Akademie, auch die Leopoldina, irgendetwas verbieten kann. Wir können nur Empfehlungen aussprechen. Die gesetzlichen Regelungen müssen dann die Parlamente machen.

Manfred Kloiber

Danke für die Klarstellung. Jetzt Ihre Frage.

Felix Breining

Felix Breining, Uni Erlangen-Nürnberg. Sie hatten die Rolle von Exploits und den Exploithandel mit dieser Firma angesprochen. Da sehe ich einen Bezug zu Proliferationsbestrebungen im Bereich Atomwaffen zum Beispiel, wo der Handel mit solchen schädlichen Produkten stark reguliert wird, auch international. Was halten Sie davon, so etwas Ähnliches auch mit dem Handel von Exploits, insbesondere Zero-Days zu machen?

Anja Feldmann

Das Ganze ist nicht so einfach. Denn wir brauchen Leute, die diese Zero-Days finden. Diese Leute brauchen ein Incentive dafür, und zwar auch dafür, das Ganze nicht auf den Schwarzmarkt zu bringen, sondern auf den offenen Markt. Von daher ist es vielleicht nicht schlecht, dass es Firmen gibt, die diese Sachen aufkaufen und dafür sorgen, dass andere Firmen diese Probleme wieder fixen.

Wir haben es hier nicht nur damit zu tun, dass wir hier schlechte Sachen haben, die nicht verbreitet werden dürfen oder die nicht publiziert werden sollen, sondern diese Lücken müssen auch geschlossen werden. Dadurch ist es nicht so einfach, zu sagen: Es darf niemand damit handeln, es darf niemand die Sachen machen. Auch die Polizei braucht manchmal die Möglichkeit, Systeme zu hacken oder Zugriff darauf zu ge-

winnen. Die Polizei sollte das allerdings nur dann machen, wenn sie einen Gerichtsbeschluss dafür hat.

Das ist pro Land sehr unterschiedlich, wie das gehandhabt wird. In einigen Ländern haben wir Rechtsstaatlichkeit, in anderen Ländern nicht. Das ist gerade das Problem, wo wir dann wieder in einem ethischen Dilemma sind.

Diese Sachen müssen sich über die Zukunft sortieren. Als Techniker können wir sagen, was möglich ist. Wie dann die Gesellschaften damit umgehen, ist eine gesellschaftliche Diskussion. Die können wir als Techniker nicht vorwegnehmen, und darum sitzen wir hier zusammen. Ich glaube, das ist ein gutes Schlusswort.

Manfred Kloiber

Vielen Dank dafür. Ich darf allen drei Referenten der ersten Session für die interessanten Vorträge danken und denke, dass Sie, wenn Sie sich gestärkt haben, Lust darauf haben, die zweite Session mitzuerleben.

Session 2: Ansätze für eine wertegeleitete IT-Forschung

Manfred Kloiber

In der Session 2 werden wir uns vor allen Dingen mit ethischen Fragestellungen beschäftigen. Den ersten Vortrag werden Sie jetzt über Ethik in der Informationstechnologie von Petra Grimm hören. Frau Grimm arbeitet am Institut für Digitale Ethik an der Hochschule der Medien in Stuttgart.

Ethik in der Informationstechnologie

Petra Grimm, Hochschule der Medien Stuttgart / Institut für Digitale Ethik

(Folie 1)

Ethik in der Informationstechnologie ist mein Thema. Ich habe mich gefreut, dass schon die Vorredner und die Vorrednerin sich darauf bezogen haben. Vielleicht kann ich hier einige Ergänzungen vornehmen.

(Folie 2)

Sie haben in den Präsentationen schon eine Reihe von Werten gehört. Die Frage ist immer: Wie sieht es von gesellschaftlicher Seite aus? Technologie steht ja nicht kontextlos in der Gesellschaft. Auch die Entwicklungen in diesem Bereich sind stark durch gesellschaftliche Werteprozesse geprägt.

(Folie 3)

Vorab ein Aspekt, der versucht, das Ganze in einem größeren Maßstab zu erfassen, nämlich die Frage nach dem Wertewandel. Wertesysteme sind nicht in Stein gemeißelt. Sie variieren, abhängig von kulturellen und technologischen Entwicklungen.

Mitte der 1960er Jahre fand gerade in der westlichen Welt ein Wertewandel statt, bei dem insbesondere die sogenannten Pflicht- und Akzeptanzwerte (Fleiß, Disziplin, Pünktlichkeit etc.) zugunsten der Selbstentfaltungswerte (Selbstverwirklichung) zurücktraten. Mit der zunehmenden Ausdifferenzierung und Individualisierung, die dadurch mehr oder weniger beschleunigt wurde, wurde auch die Pluralität von Lebensstilen in unserer Gesellschaft zunehmend akzeptiert.

Seit der Jahrtausendwende kann man eine zunehmende Ökonomisierung der Wertesysteme beobachten, das heißt, auch in eigentlich nicht ökonomischen Systemen, wie zum Beispiel dem

Bildungssystem oder dem Gesundheitssystem, finden mehr und mehr ökonomische Werte Eingang. Diese ökonomischen Werte sind insbesondere Leistung, Effizienz, aber auch Quantifizierung und Pragmatismus. So werden auch an Hochschulen mehr und mehr Qualitätsmanagementprozesse eingeführt, wo es nach Kennzahlen geht, das heißt betriebswirtschaftliche Strukturen, die mittlerweile in ein Bildungssystem implementiert worden sind, was auch den Bildungsanspruch und auch die Bildungsprozesse beeinflusst.

Auf Seiten der Studierenden wissen wir, dass diese vor allem an guten Noten interessiert sind, was zu einem erheblichen Leistungsdruck führt.

(Folie 4)

Wozu brauchen wir eigentlich Werte? Wie sähe eine Welt aus ohne Werte? Ist das überhaupt vorstellbar? Ich denke nicht. Weil wir, einfach gesagt, nicht überleben könnten, wenn wir nicht mit anderen Menschen in einem sozial-kommunikativen Handeln im Austausch stünden und auch Gemeinschaften bilden. Die Fähigkeit des Homo sapiens, sich an seine Umwelt anzupassen, unterscheidet ihn noch nicht vom Tier oder von der Pflanze. Erst die Fähigkeit, auf der Grundlage von Gegebenheiten, also inneren Neigungen, Wünschen und auch Gründen für sein Handeln, aufgrund dieser Ethik zu handeln, das macht ihn, den Homo sapiens, zu einem kulturellen Wesen.

Wenn Sie sich dann überlegen, dass kleine Gemeinschaften in kleinen, lokalen Umgebungen auch möglich sind, zum Beispiel bei den Schimpansen, dann ist dem Homo sapiens aber einiges gelungen. Er hat es nämlich geschafft, über größere Distanzen, über lokale und räumliche Grenzen hinaus Menschen auf bestimmte Ideologien, Religionen und damit Wertesysteme zu verpflichten, und damit erst diese kulturellen Prozesse ermöglicht.

(Folie 5)

In der Werteforschung werden auch den Werten bestimmte Funktionen zugeschrieben. Es besteht ein Konsens darin, dass Werte die Auswahl von Handlungen bei Individuen und Gruppen steuern, dass sie zur Rechtfertigung von Handlungen, also auch als Motive dienen und dass sie letztendlich die Wahrnehmung der Welt und deren Beurteilung beeinflussen.

Das ist die Funktion.

(Folie 6)

Wir unterscheiden zwischen Funktion und Definition. Die Definition wiederum besagt, dass Werte, vereinfacht ausgedrückt, als Vorstellung, Ideen oder Ideale zu bezeichnen sind, die angeben, was wünschenswert sei.

Somit sind Werte bewusste, aber auch unbewusste Orientierungsstandards und Leitvorstellungen.

(Folie 7)

Sie haben gehört, dass ich in Leitungsgremien des Instituts für Digitale Ethik an der Hochschule der Medien tätig bin. Wir sind hier also auf dem Gebiet der digitalen Ethik.

(Folie 8)

Wenn man von Ethik spricht, ist mir wichtig, dass man diesen Begriff auch adäquat versteht. Ethik ist auf keinen Fall mit Moral gleichzusetzen, sondern zu den Aufgaben einer digitalen Ethik gehört es, die Auswirkungen der Digitalisierung auf Gesellschaft und den Einzelnen zu diagnostizieren, also Analyse zu betreiben, auch empirisch, und konsistente Begründungen für moralisches Handeln und normative Standards zu erarbeiten. Wenn man normative Standards hat (und wir haben heute schon von einigen Standards gehört), besteht die Herausforderung

auch darin, zu begründen, warum bestimmte Normen gelten sollen und andere vielleicht nicht, oder wenn man von Hierarchisierung von Werten spricht, warum eine bestimmte Hierarchie gelten soll.

Des Weiteren kann die digitale Ethik bei Werte- und Normenfragen, die mit den neuen Technologien und den daraus resultierenden sozialkommunikativen Praktiken verbunden sind, als Navigationsinstrument fungieren.

Man könnte sagen, gerade im interdisziplinären Bereich: Sie hat durchaus ein Ziel, ein praktisches Ziel: nämlich eine wertebezogene und nicht allein technisch bezogene Digitalkompetenz zu fördern.

(Folie 9)

Günter Ropohl hat ein Beispiel gegeben für eine funktionierende Technikbewertung, und zwar in Form eines Regelkreismodells. Hierbei wird ein mehrdimensionales Wertesystem von Beginn an in den Entwicklungsprozess einbezogen.

Was mir bei den Vorreden klar geworden ist: Man kann ethische Leitlinien und Standards nicht von oben über einen Prozess stülpen, sondern die Kunst in diesem gesamten Zusammenwirken besteht meines Erachtens darin, bereits zu Beginn, also in der Entwicklung, interdisziplinär zwischen Technologie und Ethik eine Multiperspektivität herzustellen. Ethische Leitlinien und Standards sind immer prozessbezogen zu erstellen und können nicht in einer Roundtable-Expertenkommission oder was auch immer parallel oder gesondert von den technologischen Fragestellungen erstellt werden, wenn nicht die Interdisziplinarität gleich zu Beginn eines technischen Prozesses oder Forschungsprozesses prozessual mit einbezogen wird, sei es in Form eines ethischen Monitorings oder in Form von Privacy oder Ethics by Design.

Auch Ropohl hat darauf hingewiesen. Er geht in seinem Modell davon aus, dass ein mehrdimensionales Wertesystem von Beginn an in den Entwicklungsprozess einbezogen werden sollte. Das Wertesystem besteht bei ihm aus Werten hinsichtlich der Funktionsfähigkeit der Technik, der Sicherheit und der Wirtschaftlichkeit auf der einen Seite, und Werten der Nachhaltigkeit in Bezug auf den Umweltschutz und den gesellschaftlichen Nutzen auf der anderen Seite.

Das wäre ein Modell, an dem man sich orientieren kann, weil es eine holistische Betrachtung als Grundlage und Orientierungsvorgabe für den gesamten Entwicklungsprozess zur Verfügung stellt.

Das Regelkreismodell steht dabei für jeden einzelnen Entwicklungsschritt im gesamten Prozess und symbolisiert die Regelung und Anpassung hinsichtlich der Istwerte hin zu den Sollwerten. Voraussetzung ist die konstante Technikbewertung und Folgenabschätzung. Ethik kann nicht erst im Nachgang wirksam werden, sondern muss von Beginn an in alle Prozesse einbezogen werden, damit sie als regulierende Größe wirksam werden kann.

(Folie 10)

Einer der zentralen Begriffe in diesem ethischen Diskurs ist der der Verantwortung. Vielleicht schauen wir uns den ein bisschen genauer an.

(Folie 11)

Der Verantwortungsbegriff hat eine prospektive und eine retrospektive Bedeutung. Auf zukünftiges Verhalten hin bedeutet Verantwortung: „P ist verantwortlich für X: P hat auf X bezogene Verpflichtungen."

In Artikel 11 der Ethischen Leitlinien der Gesellschaft für Informatik heißt es:

> „Informatikerinnen und Informatiker tragen Verantwortung für die sozialen und gesellschaftlichen Auswirkungen ihrer Arbeit; sie sollen durch ihren Einfluss

> auf die Positionierung, Vermarktung und Weiterentwicklung von Informatiksystemen zu ihrer sozial verträglichen Verwendung beitragen."

(Folie 12)

Mit retrospektiv meinen wir: „P ist verantwortlich für X", wobei X für Handlungen bzw. Handlungsfolgen steht, die wir P zurechnen. Ein Beispiel:

> „Konstrukteure von Fitness-Apps und Wearables, die Privacy by Design nicht implementieren, sind (mit-) verantwortlich dafür, dass die Privatsphäre der Nutzer verletzt wird."

(Folie 13)

Dass das nicht aus der Luft gegriffen ist, sondern empirisch nachweisbar ist, zeigt die aktuelle Studie der Verbraucherzentralen. Sie hat aufgezeigt, dass Fitness-Apps kein Konzept für Privacy by Design anwenden, mit dem man die Privatsphäre schon bei der Entwicklung eines Produkts berücksichtigen könnte. So erlaubt eine Vielzahl an Apps ein Tracking, zum Beispiel die Standortverfolgung. 16 von 19 Apps senden darüber hinaus Daten an Drittanbieter. Die überwiegende Anzahl der getesteten Fitness-Apps weist zudem ein ausgeprägtes Datensendungsverhalten aus. Dabei werden zum Teil sensible personenbezogene Informationen an die Anbieterserver übertragen.

(Folie 14)

Hier wurden die Verbraucher, also die Kunden, gefragt, und ein überwiegender Teil von ihnen befürchtet denn auch, dass sie die Kontrolle über ihre persönlichen Informationen verlieren und die Daten ohne ihre Erlaubnis weitergegeben werden.

(Folie 15)

Als Determinanten der Verantwortung gilt gemeinhin erstens Kausalität: Eine Person ist dann für die Folgen einer Handlung verantwortlich, wenn diese durch die Handlung verursacht wurden;

zweitens Wissen: Eine Person ist verantwortlich für die Handlungsfolgen, wenn diese für sie absehbar waren bzw. absehbar hätten sein müssen.

Drittens besteht Verantwortung, sofern wir handlungsmächtig sind, die Handlung also für uns überhaupt möglich ist; viertens, sofern sie freiwillig ist, und fünftens, wenn wir auch alternativ hätten handeln können.

Dass die digitale Ethik darin noch über die Ethik hinausgeht, können wir gerade an dem Verantwortungsbegriff sehen. Denn hier stellt sich gerade im Kontext von Big Data die Frage, ob wir eigentlich noch die Determinante der Handlungsmächtigkeit haben und vor allen Dingen auch das Wissen über die Handlungsfolgen: Können wir die Handlungsfolgen tatsächlich absehen und einschätzen?

Insofern müsste man sich im Bereich der digitalen Ethik vielleicht noch mal verstärkt dem Verantwortungsbegriff zuwenden.

(Folie 16)

Dies ist ein Modell von Lenk, das als klassisches Verantwortungsmodell gilt, denn hier wird differenziert

- einmal nach dem Subjekt: Wer ist verantwortlich als Subjekt?
- Wofür ist jemand verantwortlich? Für die Handlungsfolgen.
- Wovor? Das ist die Norminstanz, vielleicht auch das Gewissen oder das Berufsethos eines Forschers oder Entwicklers.
- Wem gegenüber? Nämlich dem Betroffenen.
- Und weswegen? Warum soll er überhaupt für etwas verantwortlich sein? Prosoziale Normen vielleicht, Moral Sense oder Gesetze.

Auch hier würde sich im Zuge der Diskussion um Big Data, KI, maschinelles Lernen die Frage stellen: Können wir die Subjektfrage noch ein-

deutig klären und können wir auch die Handlungsfolgen so einfach definieren?

(Folie 17)

Als besondere Herausforderungen für die Gesellschaft und den Einzelnen gelten denn auch aus ethischer Perspektive Künstliche Intelligenz und Big Data sowie die prädikative Analytik, von der wir schon vorher Beispiele gehört haben.

Hier sind zwei relativ aktuelle Papers;[2] das eine ist jetzt im September erschienen. Für Big-Data-ethische Fragen stand ich als Expertin zur Verfügung. Es zeigt sich also gerade im Kontext von autonomen Entscheidungen auf der Grundlage von KI und Big Data, inwieweit überhaupt noch Kontroll- und Steuerungsmöglichkeiten des Menschen gegeben sein werden.

Zudem stellen sich für bestimmte ethische Prinzipien, wie zum Beispiel die Verantwortung, neue Voraussetzungen. Denn Kausalität und Folgenabschätzung ist gerade bei sich selbst steuernden automatisierten Entscheidungen nicht mehr ohne Weiteres als Determinante gegeben.

(Folie 18)

Einer der wichtigsten Punkte zieht sich durch verschiedene Bereiche, sei es das autonome Fahren, sei es Internet of Things, also Internet der Dinge, soziale Medien oder wo auch immer: Wir haben es mit dem Thema der Datafizierung der Privatsphäre zu tun.

(Folie 19)

Diese Grafik zeigt, dass wir mit der Nutzung der digitalen Medien einen digitalen Fußabdruck hinterlassen, wobei wir nicht wissen, nach welchen Algorithmen die Daten ausgewertet werden, wie klassifiziert wird und welche individuellen Profile von uns erstellt werden.

Die Daten zu unserer Psychografie geben zum Beispiel Aufschluss über unsere Big Five Persönlichkeitsfaktoren, ob man emotional labil ist, gesellig, leistungsorientiert und/oder kooperativ. Zu unserer Intelligenz, Lebenszufriedenheit, zu unseren politischen und religiösen Ansichten, zu unserer sexuellen Orientierung und unserem Beruf werden Algorithmen erstellt. Wer das bei Facebook einmal selbst kontrollieren will, könnte zum Beispiel das Tool Data Selfie nutzen, um sich das plastisch vor Augen zu führen.

Bei Algorithmen geht es um die abstrakte Beschreibung eines Problems in einer Sprache, die maschinell verarbeitet werden kann und bei der zwischen der Ein- und Ausgabe eine vordefinierte endliche Zahl von Einzelschritten abgearbeitet wird. Sie dienen aber auch der Preisgestaltung beim Online-Kauf oder des Versicherungsbeitrags, der Priorisierung in der Trefferliste, der Autocomplete-Funktion bei Suchmaschinen oder der Prognose, wie wahrscheinlich die Rückzahlung der Verbindlichkeiten eines Kreditnehmers ist.

Oftmals handelt es sich hier – und damit sind wir auch auf der politischen oder der Machtebene – um proprietäre Algorithmen. Das heißt, es ist nicht vollständig transparent, welche Kriterien mit welcher Gewichtung einfließen.

(Folie 20)

Die weitaus wirkmächtigeren Folgen im Kontext dieser Datafizierung sind erstens die Klassifizierung. Das heißt, man wird als Handlungssubjekt von durch Big Data vorhergesagten Neigungen beurteilt und nicht aufgrund des tatsächlichen Verhaltens.

Zweitens Kommerzialisierung: Hier findet wieder der Ökonomisierungstrend Eingang, nämlich

[2] Entscheidungsunterstützung mit Künstlicher Intelligenz. Wirtschaftliche Bedeutung, gesellschaftliche Herausforderungen, menschliche Verantwortung. Bitkom, DFKI, 05.09.2017; Big Data – Ethische Fragen. Herausgegeben vom Vodafone Institut für Gesellschaft und Kommunikation, Oktober 2016.

private Handlungen und Äußerungen werden permanent kommerziellen Interessen unterworfen.

Drittens das Thema Überwachung. Eine umfassende, permanente Beobachtung kann Menschen dazu veranlassen, sich in ihrem Verhalten einzuschränken, zum Beispiel wenn ich mein Verhalten ändere, um nicht aufzufallen, die eigene Meinung verschweige oder den Kontakt zu Menschen unterbinde, die sich kritisch äußern. Wie das gesellschaftlich aussehen kann, können wir gerade in China mit dem Citizen Score gut beobachten.

Aus meiner Sicht auch interessant, wenn man sich empirisch die Einstellung der Nutzer anschaut: Die europäische Vodafone-Studie[3] zeigt, dass rund die Hälfte aller Befragten im Phänomen Big Data mehr Nachteile sieht, während knapp ein Drittel mehr Vorteile erkennt. 17 Prozent geben an, es nicht einschätzen zu können. Auffällig ist, weil es eine europäische Studie ist, dass insbesondere in Deutschland eine kritische Haltung der Befragten mit immerhin 62 Prozent überwiegt.

(Folie 22, 23)

Die Studie zeigt auch, dass das Vertrauen der Kunden in Banken und Kreditanbieter bezüglich der Nutzung ihrer privaten Daten eher gering ist. Noch am besten schneiden Gesundheitseinrichtungen ab, am schlechtesten die Anbieter von sozialen Netzwerken.

Im europäischen Vergleich liegen die Deutschen in der Gruppe derer, die hier relativ wenig Vertrauen haben, sei es in Bezug auf Banken oder Versicherungsunternehmen, relativ weit vorne.

(Folie 24)

Für viele, natürlich auch für die Wirtschaft, ist interessant: Wie kann man das Vertrauen der Kunden gewinnen? Das ist auch ein Anzeichen dafür, wo es im Argen liegt.

Um Vertrauen beim Verbraucher im Hinblick auf die Sammlung und Verwendung ihrer persönlichen Daten zu gewinnen, sind laut dieser Befragung drei Faktoren erfolgsversprechend.

[1] Nutzer sollten verstehen können, welche Daten von ihnen gesammelt werden und wie diese verwendet werden. Hier helfen eine einfache und klare Sprache und kurze AGB.

[2] Stichwort Transparenz: Das haben wir auch schon mal als Wert gehört, nämlich Transparenz darüber, welche Daten gesammelt werden und wie diese dann genutzt werden. Das wird in der Liste der vertrauensbildenden Maßnahmen mit 64 Prozent am zweithäufigsten genannt

[3] Die Organisationen können diese Bedürfnisse zum Beispiel auch durch die Vermeidung von Kleingedrucktem fördern. 56 Prozent sagen, dass dies das Vertrauen erhöhen würde.

(Folie 25)

Insgesamt besteht die Grundhaltung des Misstrauens. Das bezieht sich nicht nur auf Ältere, sondern – sehr überraschend – schon bei Kindern und Jugendlichen. So zeigt sich in der repräsentativen Studie von Knop et al., dass für Kinder und Jugendliche das Thema Datenpreisgabe mit an der Spitze der erlebten Risiken steht.

(Folie 26)

Ich möchte noch den Wert der Privatheit ansprechen vor dem Hintergrund: Was ist eigentlich Privatheit? Räumlich kann man das in diesem Zwiebelmodell gut versinnbildlichen. Im Innersten liegt der Bereich der Intimsphäre, zum Beispiel das Tagebuch. Die zweite Schicht ist der klassische Privatbereich, die Familie oder andere

[3] Big Data. Wann Menschen bereit sind, ihre Daten zu teilen. Herausgegeben vom Vodafone Institut für Gesellschaft und Kommunikation, Januar 2016.

intime Beziehungen, repräsentiert meist durch private Räume wie das eigene Zimmer, die eigene Wohnung oder das eigene Haus. Drumherum wäre dann das gesellschaftliche und staatliche Außen, die Öffentlichkeit.

Aber wir haben es nicht nur mit einem räumlichen Verständnis von Privatheit zu tun, sondern auch mit dem von Handlungen. Denn Handlungen können ebenfalls privat sein. Zum Beispiel ist es meine private Entscheidung, ob ich in die Kirche gehe oder welche Kleidung ich trage. Auch ein Gespräch mit einem Freund in der Öffentlichkeit ist meine Privatsache.

Ebenfalls können Informationen privat sein. Private Informationen können zum Beispiel meine politische Einstellung sein oder meine Meinung über eine Person, aber auch Daten zu meiner Gesundheit oder das Wissen darüber, mit wem ich zusammenlebe.

(Folie 27)

Wichtig ist mir: Privates ist immer kontextbezogen und als solches auch so zu definieren. Was ich meinem Banker erzähle, werde ich kaum meinem Arzt erzählen und vice versa. Nach Beate Rössler ist Privatheit zu verstehen

> „in dem Sinn, dass ich Kontrolle darüber habe, wer welchen ‚Wissenszugang' zu mir hat, also wer welche (relevanten) Daten über mich weiß; und in dem Sinn, dass ich Kontrolle darüber habe, welche Personen ‚Zugang' oder ‚Zutritt' in Form von Mitsprache- oder Eingriffsmöglichkeiten haben bei Entscheidungen, die für mich relevant sind."[4]

Daraus kann man die ethische Norm des Privatheitsschutzes ableiten, nämlich selbstbestimmt darüber entscheiden können, wer was wann und in welchem Zusammenhang über einen weiß.

Der Informationsethiker Luciano Floridi argumentiert, dass wir anstelle einer ursprünglich auf Newton und Locke zurückgehenden Sicht von Privatheit, die private Daten als ökonomischen Besitz versteht, Privatheit als konstitutiv für unsere Identität verstehen sollten. Private Daten bzw. eher Informationen besitzen wir nicht, wie wir ein Auto besitzen, sondern private Daten gehören zu uns, in unseren Körper. Privatheit ist somit Teil unserer Identität. „It's not just mine, it's me."

(Folie 28)

Die Funktion der Privatsphäre hatte bereits Alan Westin sehr gut beschrieben. Ich glaube, dass diese vier Aspekte heute immer noch gültig sind:

[1] Vor allen Dingen garantiere Privatsphäre die persönliche Autonomie, nämlich zu verhindern, von anderen manipuliert, dominiert oder bloßgestellt zu werden. Sie ermöglicht eine selbstbestimmte Lebensgestaltung und auch Experimente.

[2] Emotionaler Ausgleich: frei von sozialem Druck und gesellschaftlichen Erwartungen Stress abzubauen, die innere Ruhe zu finden und ganz man selbst zu sein. Denn der Mensch ist auf Erholungs- und Rückzugsräume angewiesen.

[3] Selbstevaluation: die Erfahrungen und Eindrücke aus dem Alltag zu reflektieren, einzuordnen und Schlüsse daraus abzuleiten. Sie ist Bedingung für eine kreative und pluralistische Gesellschaft.

[4] Geschützte Kommunikation: zu unterscheiden, wem man was sagt; sich in einem geschützten Raum mit Vertrauten auszutauschen.

Gerade diese Punkte, auch emotionaler Ausgleich und die Chance zur Selbstevaluation – durch die neuen Medien, insbesondere das Smartphone, werden sozialkommunikative Praktiken mehr und mehr zurückgedrängt.

(Folie 29)

Wichtig ist aber, dass der Wert der Privatsphäre nicht nur individuell definiert oder gesehen wird, sondern auch in einer gesamtgesellschaftlichen

[4] Beate Rössler: *Der Wert des Privaten*, 2001.

Dimension zu verorten ist. Unsere Demokratie basiert darauf, dass wir autonome Bürgerinnen und Bürger sind. Das ist ein grundlegendes Menschenbild, was wir hier als Grundlage nehmen, nämlich dass wir Entscheidungs- und Handlungsfreiheit haben. Der Schutz der Privatheit ist ein Mittel, um autonom entscheiden und handeln zu können.

Wenn nun aber ein Score anhand meiner Daten und der Freunde im Netz berechnet, welche politische Auffassung ich habe, welche psychische Disposition ich habe und ob ich zu einem Vorstellungsgespräch eingeladen werde, dann ist meine Autonomie eingeschränkt. Und meine freie Meinungsbildung ist auch eingeschränkt, wenn die Informationen und Nachrichten durch Social Bots und Algorithmen in sozialen Netzwerken manipuliert werden. So kann zum Beispiel Facebook Themen befördern oder unterdrücken.

(Folie 30)

Ethik und Recht sind sehr nah beieinander. Sie stehen in einem engen Kontext und in einem gemeinsamen Lösungsfindungsprozess für die durch die Digitalisierung begründeten Herausforderungen. Beide Perspektiven müssen miteinander verknüpft werden.

Digitale Ethik kann man als Ausgangspunkt von Digitalkompetenz verstehen, die wiederum in gesamtgesellschaftlicher Verantwortung entwickelt werden muss. Das schließt staatliche Akteure ebenso ein wie Unternehmen, Inhalteanbieter, Intermediäre und Nutzer. Kernelemente einer so orientierten Wertschöpfungskette sind Information, Transparenz, Awareness, Selbstbestimmung und Vertrauen.

(Folie 31)

Wenn das zu abstrakt klingt – ich habe hier Beispiele aus der Praxis mitgebracht.

(Folie 32, 33)

Das ist ein aktuelles Masterprojekt mit Studierenden, wo versucht wurde, die zehn ethischen Leitlinien für die Digitalisierung von Unternehmen zu entwickeln. Diese Leitlinien sollen als Wegweiser verstanden werden, der in die Nachhaltigkeitsstrategie der Unternehmen zu integrieren ist. Sie umfassen die Aspekte datenökologische Verantwortung (ein ganz wichtiger Begriff für mich), faires und gerechtes Arbeiten 4.0, Chancengerechtigkeit und Fürsorge sowie Folgenabschätzung und Nachhaltigkeit.

Es reicht aus meiner Sicht nicht, nur von Digitalkompetenz zu sprechen. Wir brauchen auch die Verantwortung der Unternehmen, auch in freiwilligen Selbstformulierungen und Regulierungsmaßnahmen, um Digitalkompetenz für den Nutzer sinnhaft einzuführen.

(Folie 34)

Ein weiteres Beispiel (auch da habe ich Ihnen sozusagen die Produkte mitgebracht) ist das Projekt „Die 10 Gebote der digitalen Ethik“. Sie sind zu verstehen als ein Ausgangspunkt für die Vermittlung von Digitalkompetenz, aber nur als Impuls. Sie fungieren gerade in Bezug auf Jugendliche als Navigationsinstrument und geben einen Impuls, um über Handlungsnormen und Wertekonflikte ins Gespräch zu kommen.

(Folie 35)

Sie wurden ebenfalls in dem Masterprojekt erstellt in Kooperation mit der Deutschen Telekom Stiftung und juuuport, einer Selbstschutzplattform von Jugendlichen für Jugendliche. Es gibt sie zum einen als Postkarte (wir haben mittlerweile an die 50.000 Exemplare nachdrucken müssen, weil Schulen und Jugendeinrichtungen das stark nachfragen) und zum anderen als kleines Booklet. Denn ich komme stark vom narrativen Anteil und glaube, dass Werte nur in narrati-

ver Form vermittelt werden können und Ideen einer narrativen Ethik zeitgemäß wären.

(Folie 36)

Die 10 Gebote sollen Jugendlichen helfen, die Herausforderungen, mit denen sie im digitalen Kosmos konfrontiert sind, zu meistern. So geht es in den ersten beiden Geboten vor allen Dingen um den Schutz der Privatsphäre und das Thema Big Data, im Weiteren aber auch um die Frage: Wie bilde ich mir eine Meinung, ohne manipuliert zu werden? Auch Werte wie Respekt und Empathie, Selbstschutz und die Befähigung, sich auch mal eine Auszeit zu nehmen, sind hier formuliert.

(Folie 37)

Das Institut für Digitale Ethik hat in unterschiedlichen Forschungsprojekten eine zentrale Steuerungsfunktion. Es ist dafür verantwortlich, dass auch gesellschaftliche und soziale Werte in technologischen Innovationen von Beginn an implementiert werden.

Ein Beispiel: Im Projekt PräDiSiKo [Präventive digitale Sicherheitskommunikation] werden präventive Konzepte in den digitalen Medien erforscht und erarbeitet. Es soll für eine verbesserte Sicherheitskommunikation von Behörden wie der Polizei, die hier Projektpartner sind, eingesetzt werden.

In einem anderen Projekt, KoFFI [Kooperative Fahrer-Fahrzeug-Interaktion], geht es um die Zukunft des automatisierten Fahrens. Zusammen mit Projektpartnern aus der Industrie wie Bosch oder Daimler, aber auch an Universitäten und Hochschulen wird an einem Konzept für ein multimodales Interface für die Mensch-Maschine-Interaktion geforscht. Wir haben hierbei die Aufgabe, rechtliche und ethische Vorgaben zu benennen, die als Orientierung für die Gestaltung dieser Mensch-Maschine-Interaktion wirksam sein sollen. Der Grundgedanke, der hier realisiert werden soll, ist das, was ich zu Beginn gesagt habe: dass nämlich bereits zu Beginn des Prozesses ein Privacy-by-Design- und auch ein umfassenderes Ethics-by-Design-Konzept einfließen soll bzw. erarbeitet wird.

Auch die Zukunft von Studierenden wird entscheidend durch die Digitalisierung verändert. Mithilfe von Big Data lassen sich ja Zukunftsprognosen erstellen. Hier ist ein Forschungsprojekt zum Thema Learning Analytics und ein weiteres, wofür wir uns gerade bewerben, im Bereich Education Analytics. Hier ist es die Aufgabe der Ethik, klare Ziele und auch Grenzen für einen humangerechten Einsatz und Umgang mit der Technik zu benennen.

(Folie 38)

Damit komme ich zum Abschluss. Ich betone einerseits den prozessualen Charakter, aber es ist auch notwendig, dass wir uns darauf verständigen, welche ethischen Prinzipien für uns relevant sind. Da würde ich nicht bei den vielleicht naheliegenden Werten anfangen, sondern da, wo wir anfangen sollten, nämlich bei der politischen Dimension.

[1] Wir leben in einer Demokratie und sollten nicht den Fehler machen, diese als selbstverständlich hinzunehmen. Unsere politische Grundordnung ist das Ergebnis und das Fundament unseres Handelns. Ein freies Handeln und eine freie Entwicklertätigkeit ist nur in demokratischen Strukturen möglich. Oberstes Prinzip sollte deshalb auch für die Technikentwicklung sein, sich an unseren demokratischen Grundwerten zu orientieren und auch den Erhalt der demokratischen Grundhaltung zu garantieren.

[2] Hierfür muss man sich seiner eigenen Verantwortung bewusst werden. Dies geschieht nur, indem man auch die Folgen seines Handelns oder von Entwicklungen mitdenkt. Dazu muss man bedenken, dass die Privatheit nicht abge-

schafft und ersetzt werden kann, sondern erhalten bleiben muss, um weiterhin freie Entscheidungen treffen zu können.

[3–5] Kontrolle ist nur möglich, wenn Prozesse nachvollziehbar und verständlich sind. Transparenz ist nicht nur wünschenswert, sondern unabdingbar für unsere Zukunft.

(Folie 39)

[6] Vertrauen verdient man sich durch sein Handeln. Enttäuschtes Vertrauen zieht schwerwiegende Konsequenzen nach sich. Die Arbeit, Vertrauen zu gewinnen und zu erhalten, ist daher für jeden Einzelnen unersetzlich.

[7] Die eigene Rolle und den eigenen Beitrag für die Gesamtsicherheit der Systeme zu bedenken ist eine Pflicht, derer sich viele nicht bewusst sein. Sicherheit kann auch durch Demut entstehen und die Einsicht, dass weniger manchmal mehr ist. Hierfür ist ein Bewusstsein zu entwickeln, das sich mit der Machtverteilung und mit den Kräfteverhältnissen beschäftigt. Wie viel Macht entsteht durch neue Strukturen und wie ist diese Macht verteilt?

[8] Man muss eine Sensibilität und Achtsamkeit für die unsichtbaren und nicht offensichtlichen Folgen der Technik und Digitalisierung gewinnen.

[9] Nötig ist ein Perspektivenwechsel, der die Realität und unsere Menschlichkeit nicht nur in Zahlen und Einsen und Nullen bemisst.

[10] Nur so lassen sich Gerechtigkeit und Chancengleichheit für eine positive Zukunft für alle Menschen verwirklichen.

Damit herzlichen Dank für Ihre Aufmerksamkeit.

Manfred Kloiber

Vielen Dank, Frau Grimm. Ich habe gerade viel über Privatheit gelernt, weil Sie so viele Aspekt der Privatheit aufgezählt haben, die mir nicht so klar waren. Auch die Verankerung der Privatheit in unserer demokratischen Gesellschaft fand ich sehr interessant. Denn daraus ergibt sich, dass Privatheit nicht nur ein individuelles Recht ist, sondern auch ein kollektives Recht, und wenn es das ist, gibt es einen Grund mehr, Privatheit zu schützen. – Ihre Fragen an Frau Grimm.

Harald Schöning

Sie haben zehn ethische Leitlinien genannt, die offensichtlich von einem Wertesystem abhängig und damit sicherlich nicht universell akzeptiert sind. Wo liegen da die Grenzen? Beispielsweise demokratische Grundordnung – wenn wir an China denken, ist die Frage: Gehört das da zum Wertesystem? Wie weit gelten die und wie geht man mit solchen ethischen Prinzipien in einer globalen und vernetzten Welt um?

Petra Grimm

Wenn ich die Diskussion zum Beispiel im Kontext des autonomen Fahrens verfolge, wo gerade auch in Hongkong Prinzipien festgeschrieben worden sind, kann man sehen, dass diese Leitlinien eigentlich schon globalen Ansprüchen gerecht werden.

Wenn Sie die demokratische Grundordnung als dies voraussetzenbar definieren, dann ist das einer der zentralen Aspekte, über die man sich auch auf globaler Ebene austauschen kann. Denn bislang habe ich noch kein besseres politisches System kennengelernt als die Demokratie. Wenn wir verhandeln müssten, ob wir für oder gegen Demokratie sind, dann verlieren wir unser europäisches Fundament, wenn wir das in Frage stellen. Darüber hinaus gibt es aber im asiatischen Bereich viele Werte, die hier durchaus im technologischen Kontext gültig sein könnten.

Gleichwohl halte ich genau die Auseinandersetzung für wichtig. Es ist ein Prinzip der Ethik,

dass man reflektiert und versucht, sich in einem Konsens darüber zu verständigen, welche Werte zu gelten haben oder zu achten sind.

Das ist ein Vorschlag, den ich erstellt habe; das können Sie nicht irgendwo nachlesen. Ich habe mir das auch überlegt in Bezug auf die heutige Veranstaltung: Was sind die wichtigsten Werte? Es müsste darum gehen, das in entsprechenden Gremien, Organisationen oder bei Forschungsprojekten zu diskutieren: Was heißt dieses eher allgemein formulierte Prinzipienwerk konkret für unser Projekt? Wo wird das virulent? Wo sind Aspekte, die für uns diskutabel sind?

Manfred Kloiber

Bei der Frage, die Herr Schöning eingebracht hat, muss man beachten, dass das eine politische Frage, eine Frage der politischen Bewertung ist. Man kann durchaus die politische Meinung haben, dass Demokratie Mist ist, auch wenn ich das nicht verstehen kann. Aber kann ich nicht von einem Forscher verlangen – und da würde ich Sie um eine Einschätzung bitten –, wenn er in einem demokratischen System lebt und da zum Beispiel die Vorzüge der Forschungsfreiheit genießt und dieses System selbst lebt, dass er zumindest den Anspruch haben sollte, es anderen Menschen zu ermöglichen, in solch einem System zu leben? Das wäre doch ehrlich, oder?

Petra Grimm

Das wäre mein Ansatz, dass man sich in seinem Beruf, in seinen Tätigkeiten darüber Gedanken macht, welche gesellschaftliche Entwicklung meine Tätigkeit hat und wie weit ich der als Einzelner, als Handelnder der Gesellschaft gegenüber eine Verantwortung trage. Es ist ja nicht nur mein eigenes Wirken für mich und meine Nächsten, sondern im Großen und Ganzen bin ich nicht davon befreit zu sagen, dass ich durch meine Tätigkeit eine Verantwortung für die Gemeinschaft und für die Gesellschaft habe.

Ich glaube, das ist auch eine Frage des Berufsethos, was man noch mal diskutieren könnte: Was ist das Berufsethos in der Informationstechnologie? Wird das eigentlich im Studium vermittelt? Wo finden diese Diskussionen statt? Wo kann man die Studierenden sich mit solchen Fragen auseinandersetzen lassen? Das wäre auch eine Frage des Curriculums: Wie implementiert man das? Da sehe ich die Wurzel dessen, wie man nach dem Studium seinen Beruf wählt und seine Tätigkeit ausübt.

Anja Feldmann

Sie haben angesprochen, dass gerade die Jugendlichen skeptisch sind, was Datenfreigabe etc. angeht. Auf der anderen Seite sehen wir in ihrem Verhalten, dass sie alle möglichen Dienste nutzen und ihre Daten in die Welt hinausposaunen, gerade mit der Selbstdarstellungsvariante. Wie passen diese beiden Sachen der Antworten und dem tatsächlichen Handeln zusammen?

Petra Grimm

Erst mal wäre ich vorsichtig zu pauschalisieren. Die Jugendlichen posaunen nicht alles raus, sondern sie nutzen bestimmte Möglichkeiten, zum Beispiel bei sozialen Medien, dass sie nur bestimmte Freunde in diese Communitys lassen, oder sie nutzen WhatsApp, weil sie denken, diese Kommunikation ist sicher.

Wir haben es hier mit zwei Aspekten zu tun, die unter dem Privacy Paradox gefasst werden: Das ist auf der einen Seite der Wunsch nach Schutz der Privatheit und auf der anderen Seite die Gefahr, sozial exkludiert zu werden, dass man also nicht mehr teilhaben kann. Dann überwiegend letztendlich der Wunsch nach Teilhabe, und in dem Moment, wo ich in sozialen Medien präsent bin, bin ich qua Struktur, qua System veranlasst, Daten von mir preiszugeben.

Dann muss man noch berücksichtigen, dass hier Bildungsunterschiede ins Gewicht fallen. Wir wissen, dass Jugendliche aus eher bildungsfernen Schichten weniger Bescheid darüber wissen, was mit diesen Daten passieren kann, als solche aus bildungsnahen Schichten.

Darum will ich sagen: Vorsicht. Es gibt durchaus unterschiedliche Jugendliche, erst mal von der Art und Weise des Umgangs mit dem Thema, aber auch in der Frage der Aufklärung, Digitalkompetenz. Da gebe ich Ihnen recht, für viele ist es noch zu abstrakt. Sie wollen sich schützen davor, dass sie von anderen angegriffen werden, aber sie haben selten im Bewusstsein, dass auch diese Unternehmen mit ihren Daten letztendlich Geld verdienen. Das ist eine Frage der werteorientierten Digitalkompetenz, die in Schulen stärker verankert werden müsste, was bislang noch nicht der Fall ist.

Anja Feldmann

Ich wollte noch an einer anderen Sache nachhaken. Sie haben gesagt: Es ist zum Teil zu verteufeln, wenn automatische Algorithmen Entscheidungen fällen. Ist es denn so viel besser, wenn individuelle nach ihren eigenen Vorlieben Entscheidungen treffen? Oder sind nicht manchmal die neutralen Entscheidungen vielleicht zu bevorzugen?

Petra Grimm

Ich weiß nicht, ob ich mich so ausgedrückt habe. Dann ist es vielleicht missverständlich gewesen. So würde ich das nicht sagen. Mir geht es eher darum, was auch im Vortrag von Herrn Markl ausgeführt wurde, auf welcher Datengrundlage diese Algorithmen gebildet wurden und inwieweit man hier Steuerungs- und Kontrollmöglichkeiten hat, um in diesen Prozess einzugreifen.

Ich würde nicht sagen, dass grundsätzlich automatisierte Entscheidungen ethisch fragwürdig sind.

Johannes Buchmann

Sie haben am Schluss die zehn Regeln genannt, und wir sprechen heute über die Verantwortung der IT-Wissenschaftler. Sie haben am Anfang gesagt: Der Vorgang, Informationsethik zu machen, ist ein Prozess. Wir haben vorhin kurz über die Frage gesprochen, ob man Regelkataloge aufstellen soll. Meine Frage: Wenn man jetzt solche Prinzipien nimmt und wenn man die umsetzen will, braucht man dafür einen Regelkatalog, wie man das machen soll? Oder muss man so lange miteinander reden, bis das eintritt? Was ist Ihre Position?

Petra Grimm

Das gehört vielleicht sogar zusammen. Denn wenn ich mich auf für jeweils bestimmte Bereiche geltende Codes of Conducts (oder was auch immer, wie man das Kind beim Namen nennen will) verständigen will, dann halte ich den Prozess, bis es dazu kommt, für den eigentlich wichtigen Part, also der Diskurs und die Reflexion darüber: Welche Prinzipien sollen für uns gelten? Wie kommen wir dahin und wie können wir das überhaupt in einem Projekt oder einem Geschäftsmodell implementieren?

Diesen Prozess halte ich persönlich für den wichtigeren Part.

Manfred Kloiber

Vielen Dank, Frau Grimm, und für die Diskussion.

Wertentscheidung in der (IT-)Forschung

Manfred Kloiber

Wir machen weiter mit Wertentscheidungen in der IT-Forschung. Darüber spricht jetzt Judith

Simon vom Fachbereich Informatik an der Universität Hamburg.

Judith Simon, Universität Hamburg / Fachbereich Informatik

(Folie 1)

Danke schön. Es ist etwas schwierig, Ihnen jetzt noch etwas Neues über Ethik zu erzählen. Ich hoffe, dass die Perspektive trotzdem nützlich sein kann.

(Folie 2)

Was ich mache, ist Folgendes: Ich werde Ihnen drei Zugänge zum Verständnis von Ethik in der Informationstechnologie eröffnen. Ich werde dies dann am Beispiel von Big Data und Künstlicher Intelligenz aufschlüsseln, weil ich dadurch argumentieren werde, dass diese drei Zugänge zwar notwendig, aber nicht hinreichend sind.

(Folie 3)

Fangen wir an mit den drei Zugängen zur Ethik in der Informationstechnologie.

(Folie 4)

Der erste ist die Ethik der Profession, das heißt die Ethik der DesignerInnen und EntwicklerInnen. Es gibt hier die Ethischen Leitlinien der deutschen Gesellschaft für Informatik; ebenso gibt es von IEEE [Institute of Electrical and Electronics Engineers] und ACM [Association for Computing Machinery] ethische Codes of Conduct, die gerade aktualisiert werden, weil viele der Ideen in den ursprünglichen Codes of Conduct im Kontext von Big Data und KI nicht mehr so ganz funktionieren.

(Folie 6)

Der zweite Blick ist die Ethik der Nutzung. Hier ist die Frage, in welcher Art und Weise die Nutzerinnen und Nutzer von Informationstechnologien ethisch handeln können, müssen oder sollen und was das heißen kann.

(Folie 7)

Fragen, die man hier stellen könnte, sind: Soll ein Individuum die Freiheit haben, rassistische Kommentare online zu posten? Darf ein Provider die Daten seiner Nutzer an Drittanbieter verkaufen? Müssen Regierungen die Daten ihrer Bürger schützen und falls ja, wie soll dies geschehen? Welche Interessen müssen hier gegebenenfalls gegeneinander abgewogen werden? Das sind Fragen der Nutzung von Informationstechnologien.

(Folie 8)

Der dritte Aspekt ist die Ethik des Designs. Hier geht es konkret um die Analyse der IT-Artefakte, weniger um den Designprozess. Natürlich führt dieser zu diesen Artefakten, aber die Analyse liegt hier in den Dingen selbst.

(Folie 9)

Hier gibt es zwei Aufgaben: die ethische Analyse von existenten IT-Artefakten und das ethische Design von neuen IT-Artefakten.

(Folie 10)

Kommen wir zur ersten Aufgabe. Hier ein Zitat von Philip Brey:

> "Computer ethics should not just study ethical issues in the use of computer technology, but also in the technology itself."
>
> "(...) computer systems and software are not morally neutral and (...) it is possible to identify tendencies in them to promote or demote particular moral values and norms."

Das wäre genau das Gegenmodell von dem, was wir vorhin hatten, mit dem Hammer, mit dem man machen kann, was man will. Sondern da wäre die Idee, dass sich die Art und Weise, in der Technologien aufgeladen sind, unterscheidet. Zum Beispiel kommen mit dem Auto bestimmte Konsequenzen, vor allem mit der massiven Nutzung von Autos. Somit gibt es bestimmte moralisch relevante Konsequenzen von Artefakt-Design. Da ist der Hammer das eine Extrem, wo

man sagen würde, der *intended use* ist ein anderer, aber er eignet sich genauso gut zum Mordwerkzeug.

Hier muss man schauen, in welcher Art und Weise und in welchem Ausmaß verschiedene Artefakte moralisch aufgeladen sind. Je verpflichtender sie sind, je stärker sie in Infrastrukturen eingebettet sind, umso wichtiger ist die Analyse dieser Artefakte.

(Folie 11)

Heute Morgen hatten wir Robotik als Beispiel. Ein klassisches Thema in der Computerethik wäre ethisch zu analysieren, welche Konsequenzen sich ergeben durch Arbeitsroboter, Kampfroboter, Pflegeroboter – alles Robotik, aber in unterschiedlichen Kontexten mit unterschiedlichen Auswirkungen, die zu berücksichtigen sind.

(Folie 12)

Was die Computerethikerin klassischerweise macht oder lange gemacht hat, ist, zu schauen, in welcher Art und Weise uns bekannte ethische Theorien (wie die Pflichtethik von Kant, utilitaristische Ethiken oder Tugendethiken) im Verständnis dieser neuen Technologien nützen, auch wenn sie in einem ganz anderen Kontext entstanden sind. Natürlich gibt es auch neue Ethiken, die andere Fragen stellen. Aber das ist der klassische Zugang gewesen.

(Folie 13)

Die zweite Frage ist hier: Wenn wir wissen, dass Technologien in gewisser Art und Weise inhärent moralisch sind, in welcher Art und Weise kann man dies beim Design neuer Technologien berücksichtigen?

(Folie 14)

Zwei Proponentinnen dieses Ansatzes möchte ich kurz vorstellen, weil ich explizit gebeten wurde, über Werte zu sprechen: Das sind Helen Nissenbaum, bekannt auch zu ihren Theorien zu Privatsphäre, und Batya Friedman.

Interessant ist: Helen Nissenbaum ist ursprünglich Philosophin und Batya Friedman ist Informatikerin. Das macht klar, dass diese Entwicklung aus beiden Feldern gemeinsam vorangetrieben wurde.

(Folie 15)

Worum geht es bei dem Forschungsfeld Values in Design? Ein Zitat der Game-Designerin Mary Flanaghan:

> "If an ideal world is one in which technologies promote not only instrumental values such as functional efficiency, safety, reliability and ease of use, but also substantive social, moral and political values to which societies and their people subscribe, then those who design systems have a responsibility to take this latter values as well as the former into consideration as they work."

Das ist die Idee von Values in Design: dass man zusätzlich zu Security und Usability (Usability war nicht immer ein Wert, sondern ist in den letzten Jahren als Wert stärker geworden) auch andere Werte, die geteilt sind, im Designprozess berücksichtigt.

(Folie 16)

Die beiden Autorinnen schlagen eine bestimmte Methodologie vor, die im Grunde genommen eine Metamethode ist, und zwar eine Methode der interdisziplinären Zusammenarbeit zwischen InformatikerInnen, SozialwissenschaftlerInnen und PhilosophInnen. Worum geht es?

(Folie 17)

In der philosophischen Phase stellt man sich, wenn man Technologien entwickelt (und das kann so etwas sein wie Software zur Simulation von Stadtentwicklung oder das Design von Browsern; Sie können in alle Richtungen denken, das ist eine Metamethode), folgende Fragen:

Welche direkten und indirekten Stakeholder werden wie vom Design betroffen? Klassischerweise denkt man in der Usability-Forschung an die Nutzer, die mit dem System interagieren, aber nicht unbedingt an die Personen, die betroffen sind, wie die Patienten. Wenn Sie Kliniksoftware entwickeln, sind es nicht nur die Administratoren, sondern auch die Schwestern und Pfleger, die Ärzte, die Patienten, deren Angehörigen. Das wären die indirekt Betroffenen von Systementscheidung.

Welche Werte sind relevant in diesem Kontext?

Welche Werte stehen im Konflikt miteinander und welche Werte und wie soll man bei Wertekonflikten verfahren, zum Beispiel im Sinne von Autonomie versus Sicherheit?

Sollen moralische Werte wie zum Beispiel das Recht auf Privatsphäre Vorrang haben vor nichtmoralischen Werten wie ästhetische Präferenzen oder Nutzerfreundlichkeit? Und wie soll man sicherstellen, dass, wenn man anders entscheidet, das System auch genutzt wird?

Das wären solche philosophisch-konzeptuellen Fragen.

(Folie 18)

Empirisch kann man, anstatt dass nur der Philosoph oder die Philosophin sich das in dem Sessel überlegt, auch die NutzerInnen fragen, was denn die Werte sind, die ihnen wichtig sind. Hier würde man fragen:

Welche Werte sind verschiedenen Stakeholdern wichtig? Wie priorisieren diese verschiedene Werte? Bei Wertkonflikten? Zeigen sich Unterschiede zwischen angeblicher und realer Relevanz verschiedener Werte, wie zum Beispiel Usability und Privatsphäreschutz? Und wie kann man damit im Kontext umgehen?

(Folie 19)

Am Ende eines Designprozesses oder im Sinne einer formativen Evaluation auch währenddessen stellt sich die Frage: In welcher Art und Weise habe ich erreicht, was ich wollte, nämlich die intendierten Werte in die Technologie eingeschrieben?

(Folie 20)

Die technische Phase steht hier nur knapp, ist aber natürlich einer der komplexesten. Denn hier geht es um die Frage: Wie kann ich diese Werte in Designspezifikationen und in die Technologie umsetzen?

Denken Sie an so etwas Banales wie ein Steuersystem. Es werden sich alle einig sein, dass Gerechtigkeit ein wichtiger Wert ist. Spätestens bei der Entscheidung, welches Steuersystem Sie haben, werden unterschiedliche Gerechtigkeitsideen zum Tragen kommen, und wenn Sie dann überlegen müssen, was genau für Steuerpolitiken Sie ins Gesetz schreiben wollen, wird es noch konkreter. Ähnlich ist der Prozess bei der Translation der abstrakten universellen Werte in die konkreten Systemspezifikationen.

(Folie 21)

Die Idee ist natürlich auch, dass die verschiedenen Phasen iterativ sind ineinanderfließen sollen.

(Folie 22)

Das wären also zusammenfassend diese drei Zugänge.

(Folie 23, 24)

Jetzt drei Vorbehalte. VW, die manipulierten Abgasmessungen, ist ein Fall, den ich nützlich finde, zum einen dafür, sich klarzumachen, dass das Artefakt und die Analyse des Artefakts oft einhergeht mit Designprozessen, und zum anderen, um sich klarzumachen, dass Entwicklung nicht im luftleeren Raum passiert, sondern in ökonomisch geprägten Kontexten, in denen na-

türlich bestimmte Incentives für verantwortungsbewusstes oder nicht verantwortungsbewusstes Handeln bestehen. Das als erstes Caveat, wenn wir über die Idee sprechen, Werte in den Designprozess einzuschreiben.

(Folie 25)

Zweitens: Wenn ich Technologien schaffe, habe ich eine intendierte Nutzung vor Augen, und dementsprechend plane ich für bestimmte Werte und setze, im Englischen würde man sagen, *affordances and limitations.* Aber natürlich können Systeme immer anderweitig genutzt werden. Hier nur ein Beispiel.

(Folie 26)

Zweites Beispiel, das auch schon erwähnt wurde. Ich habe jahrelang in der Technikfolgenabschätzung gearbeitet. Zentral ist die Frage: Wer weiß und wer entscheidet? Wer kann voraussehen, was sich entwickeln wird? Konnte man bei den ersten Autos voraussehen, welche Probleme sich ergeben würden, wenn alle Auto fahren? Das ist einmal die Frage der Omnipräsenz oder der Fiktion der Omnipräsenz und auch der Frage: Wer entscheidet in diesen Kontexten?

(Folie 27)

Was mir ganz wichtig ist (denn ich wurde gebeten, auf Dual Use einzugehen): Im Kontext von Big Data und KI ist Dual Use keine sinnvolle Metapher, weil es hier im Grunde genommen um *manifold uses* geht. Es gibt nicht die Guten und die Bösen und die Black und die White Hat Hacker. Das war bei den Hackern vielleicht noch einfacher zu zeigen. Aber diese Dichotomie ist in vielen Kontexten irreführend, wenn wir verstehen wollen, was die Konsequenzen von Technologien sind.

(Folie 28)

Das werde ich jetzt am Beispiel von KI und Big Data verdeutlichen.

(Folie 29, 30)

Wenn Sie in die Geschichte von KI zurückschauen, und ich als Philosophin fange dann bei Leibniz an, wird klar, dass die Geschichte der Künstlichen Intelligenz eine lange ist, mit Höhen und Tiefen, wo es im Laufe der Jahrzehnte immer wieder enorme Versprechungen gab, die immer wieder massiv enttäuscht wurden.

(Folie 31)

In den letzten Jahren haben wir wieder einen massiven Aufschwung der Ideen in KI. Ich beziehe mich hier nicht auf Ideen zu Singularität und menschenähnliche Intelligenz, sondern auf konkrete, anwendungsbezogene KI-Felder. Der Grund, warum es hier zu massiven Entwicklungsschüben kam, liegt im Kontext von Big Data. Durch das Vorhandenheit von massiven Daten sind viele Entwicklungen in der KI so weit vorangetrieben worden.

(Folie 32)

Das ist eine klassische Definition, die oft verwendet wird, gerade im Wirtschaftskontext von Big Data, als die vier (oder drei oder X) V's, wo gesagt wird: Es geht nicht nur um die schiere Menge an Daten [Volume], sondern um die Geschwindigkeit [Velocity] der Erhebung, der Verarbeitung, der Prognosen. Es geht um die Unterschiedlichkeit [Variety] der Datentypen, und es geht um die Unsicherheit [Veracity]. Es geht nur in einem geringen Maße um die stark kontrollierten Datenphänomene, sondern um größere Datenmengen.

(Folie 34)

Eine Definition, die ich nützlicher finde, kommt von Boyd und Crawford. Sie schreiben:

> "We define Big Data as a cultural, technological, and scholarly phenomenon that rests on the interplay of:
>
> 1) Technology: maximizing computation power and algorithmic accuracy to gather, analyze, link, and compare large data sets.

> 2) Analysis: drawing on large data sets to identify patterns in order to make economic, social, technical, and legal claims."

Hier verlassen wir den Bereich des Numerischen, des rein Quantitativen.

> "3) Mythology: the widespread belief that large data sets offer a higher form of intelligence and knowledge that can generate insights that were previously impossible, with the aura of truth, objectivity, and accuracy."

Auf diesen Punkt möchte ich ganz am Ende noch mal eingehen.

(Folie 35, 36)

Wenn wir weggehen von den Definitionen und uns anschauen: Worüber reden wir, wenn wir über Big Data reden? Das ist das Bild der Stuttgarter Künstlerin Doris Graf. Ich glaube, das ist das erste Bild, woran viele im Kontext von Big Data denken: diese etwas graue Frau, die etwas online liest, und während sie das tut, klassifiziert wird als weiblich, nicht verheiratet, Raucherin usw.

Denken Sie aber auch an Transaktionsdaten: Wann kaufen Sie was mit Ihrer Kreditkarte und bezahlen das wo? Das Stichwort Internet der Dinge fiel vorhin schon. Auch Ihr Handy ist eine massive Datenmaschine. Wenn ich weiß, wo sich Ihr Handy zu welchem Zeitpunkt befindet, weiß ich, wo Sie wohnen, wo Sie arbeiten, wie Sie vom Arbeitsplatz zum Wohnort kommen, ob Sie Kinder haben, die Sie in den Kindergarten bringen, ob Sie auffällige Angewohnheiten haben, gegebenenfalls Geliebte an bestimmten Orten, all diese Dinge sind deduzierbar mit dem Wissen um die Lokation Ihres Mobiltelefons zu bestimmten Zeitpunkten.

(Folie 37)

Denken Sie an Big Data in den Wissenschaften. Big Data ist ein Boom in verschiedenen Wissenschaftsbereichen, endlos viele Tagungen, und selbst wenn man in medizinische Daten nur reinzoomen würde, merkt man, da ist die ganze Bandbreite von genomischen Daten, Molekulardaten, Daten aus den Versuchsreihen zu Klinikdaten, Sensordaten usw. Die Bandbreite dessen, was darunterfällt, ist enorm.

(Folie 38)

Denken Sie an Open Government Data; wir hatten auch den Verweis auf Open Data. Diese Daten sind nicht notwendigerweise alle offen. Daten aus Geburtsregistern, Volkszählungen, Finanzdaten, all diese Typen von Daten.

(Folie 39)

Das Interessante im Kontext von Big Data ist aber nicht, dass diese Daten existieren, sondern dass man sie miteinander in Bezug setzen kann. Und was passiert hier?

(Folie 40)

Bestimmte Unterscheidungen, die wir als gegeben angenommen haben, werden plötzlich obsolet. Eine klassische Unterscheidung, die hinfällig geworden ist, ist die zwischen sensiblen persönlichen Daten und unverfänglichen Daten.

(Folie 41)

Ich gebe Ihnen ein Beispiel, was sicherlich vielen von Ihnen bekannt ist, was dieses aber sehr gut illustriert. Das war ein Fall, der 2012 durch die Medien ging, das TARGET-Beispiel, wo sich ein erboster Vater bei TARGET über schwangerschaftsbezogenes Werbematerialien, die sie bekommen hatten, beschwert hat, was das denn solle. Die Geschichte geht ungefähr so, dass dann jemand von TARGET eine Woche später zurückrief und einen sehr kleinlauten Vater am Telefon hat, der sich entschuldigt hat und sagte, es habe ein Missverständnis in der Familie gegeben. Die 16-jährige Tochter ist in der Tat schwanger gewesen.

(Folie 42)

Was ist hier das Problem? Was hier deutlich wird, ist die medizinische Relevanz nichtmedizinischer Daten. In diesem Fall sind es Konsumdaten gewesen, sprich das Kaufen von Folsäure oder geruchsfreier Bodylotion, die durch Verarbeitung und Nutzung im bestimmten Kontext sensible Daten wurden. Aus unverfänglichen Konsumdaten werden sensible Prognosedaten oder Prädiktionsdaten.

Diese Proxydaten sind rechtlich natürlich weniger geschützt als klassische Medizindaten.

(Folie 43)

Die zweite Unterscheidung, die wir klassisch als gegeben annehmen, ist die zwischen personenbezogenen Daten und anonymen Daten.

(Folie 44)

Warum? Durch Aggregation und Datenverarbeitung können anonyme Daten zunehmend leicht deanonymisiert werden.

(Folie 45)

Ich gebe Ihnen ein Beispiel, das in dem Kontext vielleicht ganz passend ist. Ich war lange in Österreich und hatte dort ein Forschungsprojekt, gefördert vom FWF [Fonds zur Förderung der wissenschaftlichen Forschung]. Irgendwann wurde ich gebeten, einen kurzen Fragebogen zur Zufriedenheit mit diesem Forschungsförderer auszufüllen und am Ende ein paar wenige personenbezogene Daten abzugeben: Alter, Geschlecht, Disziplin und Förderzeitraum. Ich bin mir sicher, dass ich mit diesen vier Datenpunkten in Österreich eindeutig identifizierbar gewesen bin. Je mehr Daten, umso einfacher ist die Reidentifizierung von sogenannten anonymen Daten.

(Folie 46)

Zweites Beispiel: Um diskriminieren zu können, muss ich nicht notwendigerweise persönlich identifiziert worden sein. Ein Beispiel, ebenfalls auch den Medien; es geht um Software, die verwendet wurde, um die Wahrscheinlichkeit der Rückfälligkeit von Kriminellen vorherzusagen. Dort wurde durch Reverse Engineering herausgefunden, dass diese Software systematisch Afroamerikaner schlechter bewertet hat und dementsprechend Diskriminierung auf Gruppenebene stattgefunden hat, die zwar Individuen betroffen hat, aber wo die individuelle Identifizierung nicht notwendig war.

(Folie 47)

Die Frage ist: Wer ist involviert in Big Data und wie kann man die Personen klassifizieren?

(Folie 48)

Hier ein Zitat von Manovich:

> "Specifically, people and organizations are divided into three categories: those who create data (both consciously and by leaving digital footprints), those who have the means to collect it, and those who have expertise to analyze it."

Das sind natürlich unterschiedliche Akteure. Wir alle hinterlassen Datenspuren, aber nur bestimmte Personen haben den Zugriff und die Möglichkeit, mit denen etwas anzufangen.

(Folie 49)

Wichtig ist, und das wird in diesem White House Report erwähnt:

> "But these capabilities [of number crunching], most of which are not visible or available to the average consumer, also create an asymmetry of power between those who hold the data and those who intentionally or inadvertently supply it."

Das heißt: Diese Fragen des Zugangs sind inhärente Machtfragen; das hat die Vorrednerin Frau Grimm schon betont.

(Folie 50)

Wer sammelt denn die personenbezogenen Daten? Hier kann man grob klassifizieren: Wissenschaft, Staaten, Unternehmen und auch der Nut-

zer bis zum gewissen Grad durch Self-Tracking, aber wesentlich geringer.

(Folie 51)

Die Funktionen und Implikationen von Big Data sind unterschiedlich, aber es gibt auch Querbezüge: dessen muss man sich bewusst sein.

(Folie 52)

Um den Nutzen und die Risiken von Big Data zu verstehen, müssen wir domänenspezifische Analysen betreiben.

(Folie 53)

In der Wissenschaft gibt es dazu viele Debatten. Das Sammeln von Daten ist inhärenter Bestandteil der Wissenschaften von Anfang an.

(Folie 54)

Exemplarisch ist hier der Schmetterlingsfänger, in der Mitte das Teleskop von Galilei und auf der rechten Seite Francis Galton, für die Sozialwissenschaftler unter Ihnen.

(Folie 55)

Eine der heiß diskutierten Fragen ist: In welcher Art und Weise führt Big Data zu einem Paradigmenwechsel in der Wissenschaft? Das ist hoch umstritten; dazu kann ich gerne ins Detail gehen.

(Folie 56)

Der Grund, warum ich gestern nicht da war, war eine Tagung zu Big Data in den Wissenschaften. Das sind spannende Fragen.

(Folie 57)

In den Unternehmen besteht ein großer öffentlicher Fokus auf diesen nicht mehr ganz so neuen Datensammlern.

(Folie 58)

Das Beispiel TARGET hat gezeigt, dass viele Unternehmen schon lange Daten über uns sammeln, in anderen Ausmaßen, aber dass der Blick auf die Akteure ausgeweitet gehört.

(Folie 59)

Das ist die Big Data Landscape von 2016, das ist die Backbone von Big Data, all die Unternehmen, die im Hintergrund die Infrastruktur, die Systeme und Methoden für diese Datenanalyse zur Verfügung stellen.

(Folie 60)

Letzter Punkt: Politik.

(Folie 61)

Es gibt seit ein paar Jahren unglaublich viele Whitepapers, die Big Data als das neue Öl oder was auch immer sehen.

(Folie 62)

Da ist wieder ein Bild der früheren US-Regierung, das deswegen ganz schön ist, weil es zeigt, welche Mengen an Daten in welchen Sektoren erwartet werden.

Hier wird klar: Wir reden über den Transportsektor, Energiesektor und den Medizinsektor. Die Frage ist: Wie kann man all diese Daten nutzen im Sinne eines Evidence-based Policy Making? In welcher Art und Weise kann man Daten nutzen, um basierend darauf politische Entscheidungen zu treffen?

(Folie 63)

Es gibt noch weitere Querbezüge zwischen Big Data und Politik. Über die Rolle von Social Bots im Wahlkampf wurde schon diskutiert. Wir haben Debatten über Blue- – das war wieder ein amerikanisches Beispiel, aber die Idee, in welcher Art und Weise Filterblasen dazu führen, dass Leute nur bestimmte Arten von Informationen bekommen; auch die Frage, in welchem Grad Cambridge Analytica den Wahlausgang in den USA beeinflusst haben könnte oder nicht, was schwer nachweisbar ist. Auf der einen Seite muss man sich fragen: War die Gefahr real oder auch nicht?

Das sind Themen, die man debattieren könnte, die aber nicht im Zentrum dessen liegen, was ich machen möchte.

(Folie 64)

Kommen wir zur Analyse.

(Folie 65–68)

Ein ethischer Blick auf Big Data und KI ist notwendig. Diese Fragen sind aber schon aus der philosophischen Perspektive nur dann beantwortbar, wenn man erkenntnistheoretische Fragen, Fragen nach dem Wissenspraktiken zusammendenkt mit politischen und ethischen Fragen. Auch rechtliche und ökonomische Fragen muss man von Anfang an mitdenken. Man kann sie nicht getrennt betrachten. Darauf werde ich schlaglichtartig noch einmal eingehen.

(Folie 69)

Was sind erkenntnistheoretische Fragen, die primär sind, um sich dann den ethischen Fragen zuwenden zu können?

(Folie 70)

Wenn wir uns mit Big Data und KI beschäftigen, müssen wir fragen: Wie ist es um die Qualität der Datenquellen und die Herkunft und die Kompatibilität von Daten bestellt? Wie angemessen sind die Algorithmen und Methoden? Man kann ja sagen, der Algorithmus ist so schlecht wie fünf, aber es geht trotzdem um eine Angemessenheit, um eine Passung zwischen Daten, Aufgaben und gewählten Algorithmen.

Es geht um die Qualität der Analysen und Prognosen. Natürlich: Wenn ich nicht weiß, dass eine Software gebiast ist und fehlerhaft ist, dann kann ich auch nicht nachweisen, dass da bestimmte ethische Probleme entstehen wie Diskriminierungsfälle. Das heißt, der erste Blick muss darin bestehen, zu verstehen, wie die Systeme funktionieren.

Da haben wir jetzt ein Problem. Die Überprüfung dieser Aspekte ist schwierig, aus diversen Gründen: Erstens gibt es einen Mangel an Zugang zu Daten, an Software, vor allen Dingen bei proprietären Systemen. Viele Softwares sind geschützt, und selbst wenn man die Expertise hätte, hat man keinen Zugriff und keinen Blick auf diese Dinge, um das zu prüfen.

Zweitens gibt es einen Mangel an Kompetenz und Expertise. Wie viele Leute haben die Kompetenz, das zu überprüfen? Und wenn man Ideen hat, von einem Algorithmen-TÜV, dann muss man auch fragen: Wie stattet man das aus? Wer hat die Expertise und die Kompetenz, das zu machen? Ich halte das für sinnvoll, aber dann muss man auch gucken, wie man das ausstattet.

Der dritte Punkt ist zum einen ein realer, zum anderen aber auch ein vorgeschobener Punkt: die inhärente Komplexität der Systeme und Berechnungen. Es gibt gerade im Kontext von Deep Learning viele Aspekte, die nicht verstehbar sind. Aber auch hier muss man fragen: In welcher Art und Weise reguliert man in der Form, dass man sagt: In bestimmten Kontexten müssen Systeme verstehbar sein, um für bestimmte Zwecke eingesetzt werden zu können? Es gibt auch in der Informatik Bestrebungen zu Transparenz. Welche Methoden kann es geben, um die Transparenz der Rechenschritte darzustellen?

Zu guter Letzt: Eine mediale und populärwissenschaftliche Darstellung von Big Data als neutrale Werkzeuge, die neutral entscheiden, weil sie keine menschlichen Biases enthalten, ist doppelt gefährlich, wenn man sich diese Dinge genau anschauen will.

(Folie 71)

Kommen wir zu den ethischen Fragen.

(Folie 72)

Hätten wir alle epistemologischen oder erkenntnistheoretischen Fragen geklärt, hätten wir immer noch einen ganzen Ballast an Fragen in Bezug auf das, was auch Frau Grimm erwähnt hat: Privatsphäre, Diskriminierung, Autonomie, Freiheit und Gerechtigkeit. Gerade diese beiden Beispiele – die Software zur Vorhersage und die offene Frage der Wahlbeeinflussung und Manipulation – sind Fragen, an denen diese Probleme sehr deutlich werden.

(Folie 73)

Darüber hinaus müssen wir uns die Frage stellen: Wenn wir in der Lage sind, Handlungsfähigkeit soziotechnisch zu verteilen, wo möchten wir das tun? Wo möchten wir Entscheidungen an Maschinen delegieren und damit auch Verantwortung ein Stück weit diffundieren? Und wo möchten wir das nicht?

Zwei Beispiele, in denen das sehr interessant ist: Das ist einmal die Finanztechnologie und einmal die Frage von Killer Robots. Da sind wir im klassischen Dual-Use-Bereich.

(Folie 74)

Dritte Frage: Zukunft der Arbeit und Verteilungsgerechtigkeit. Hier wird gefragt: In welcher Art und Weise brauchen wir Steuern für Roboter oder künstliche Agenten, wenn es um Fragen geht wie: Wer hat noch Arbeit in welchen Kontexten? Es hat mich gewundert, dass das im Wahlkampf so wenig eine Rolle gespielt hat.

(Folie 75)

Große Frage: Was ist denn dieses gute menschliche Leben in diesen soziotechnisch vernetzten Welten mit zunehmend intelligenten nichtmenschlichen Akteuren? Das ist die große philosophische Rahmenfrage.

(Folie 76)

Kommen wir zu den politischen Fragen.

(Folie 77)

Einerseits – und das ist eine konstruktive Wende – müssen wir uns die Frage stellen, welche Rolle KI und Big Data für Politik und Administration spielen sollen. Da sehe ich viele Möglichkeiten, vor allem auf lokaler Ebene: im Sinne von Smart-City-Kontexten, im Sinne der Verbesserung von Maintenance, wenn ich die Routen optimieren kann, in denen Mülleimer geleert werden, wenn ich optimieren kann, wenn irgendwo etwas repariert werden muss. Es gibt viele gute Einsatzfelder für KI und Big Data; es ging mir nicht darum zu sagen, dass es die nicht gibt. Man muss aber gut überlegen, in welchen Kontexten ich das delegieren und nutzen möchte und wo nicht.

(Folie 78)

Die Frage, die sich stellt, und die haben wir schon seit jeher gehabt, auch in der Frage der Expertenberatung von Politik: Welche Rolle soll Expertenwissen, Expertokratie oder Technokratie in diesem speziellen Sinne in der Politik haben?

(Folie 79)

Wenn wir uns die Frage stellen, wie KI und Big Data für Politik genutzt werden, muss man im letzten Schritt auch fragen: Welche Form von Politik bedarf es für die Regulierung von Big Data und KI? Die übergeordnete Frage ist: (Wie) Kann und soll KI und Big Data im Interesse des Gemeinwohls reguliert werden? Ich gehe jetzt nicht auf meine Definition von Gemeinwohl ein.

(Folie 80)

Man muss hier darüber nachdenken, in welcher Art und Weise es eine Kombination geben soll zwischen rechtlicher Regulierung, Selbstverpflichtung, Governance by Design (das waren die Ideen, die ich vorhin mit Values in Design vorgelegt habe. Da gibt es schon viel zu Privacy

by Design, Security by Design) und welche Rolle auch Bildung spielt.

Im Rechtlichen ist es wichtig zu sehen, dass so etwas wie die Datenschutzgrundverordnung *ein* rechtlicher Hebel ist, über den wir sprechen, aber auch so etwas wie kartellrechtliche Überlegungen, was heute Morgen schon angesprochen wurde, in welcher Art und Weise man Datenmonopole verändern muss usw.

(Folie 81)

Ich komme zu meinen Konklusionen.

(Folie 82, 83)

Ich hoffe, ich konnte Ihnen zeigen, dass diese drei Zugänge nützlich sind und dass man sie zusammendenken muss, aber dass man, wenn wir über Ethik in der Informationstechnologie reden, nicht allein auf die Nutzung, nicht allein auf die Verantwortung der Ingenieure und auf das Design gucken kann. Alle drei gehören zusammen.

(Folie 84)

Darüber hinaus müssen wir über eine dreifache Erweiterung nachdenken: einerseits eine Berücksichtigung von Artefakten und Systemen. Was meine ich damit?

(Folie 85)

Wir haben es zunehmend mit künstlichen Agenten zu tun, die bis zu einem gewissen Grad handlungsfähig sind. Deswegen müssen wir überlegen, in welcher Art und Weise wir unsere akteurs- und personenzentrierten Ethiken mit eher systemorientierten Ethiken ergänzen müssen. Da gibt es Ansätze aus der Pflanzenethik (das klingt absurd, aber ist tatsächlich sinnvoll) oder, was Frau Grimm schon meinte, Floridis Informationsethik, um zu berücksichtigen, dass diese Handlungsfähigkeit zunehmend verteilt ist.

Außerdem müssen wir überlegen, in welcher Art und Weise diese Überlegungen in ökonomische und politische Systeme eingebettet sind. Das ist gerade in den letzten Monaten, wenn nicht schon vorher, relativ deutlich geworden.

(Folie 86)

Das bringt mich zu Fragen von Macht und Verantwortung.

(Folie 87)

Hier habe ich einen Satz, der das zusammenfasst. Die Frage, die sich mir hier stellt, ist:

> „Wie viel und welche Macht und Verantwortung haben welche menschlichen, nicht-menschlichen, individuellen und kollektiven Akteure in zunehmend komplexen und dynamischen soziotechnischen Netzwerken mit verteilter Handlungsfähigkeit?“

Das ist auch ein Punkt, über den wir reden müssen: in welcher Art und Weise die Anerkennung verteilter Handlungsfähigkeit dazu führen kann, dass man Verantwortung von sich wegschiebt, oder in welcher Art und Weise wir unter dieser Bedingung neue Instrumente von lokaler Verantwortlichkeit werden institutionalisieren müssen.

(Folie 88)

Letzter Punkt: Ethik + X.

(Folie 89)

Analytisch geht es mir darum, zu sagen: Ethik muss man immer zusammendenken mit Erkenntnistheorie, politischer Theorie, Ökonomie. Das sehen sicherlich auch viele Kollegen so.

Praktisch muss man zudem Ethik komplementär denken mit politischen, rechtlichen und Bildungsinitiativen.

(Folie 90)

Mit dieser Zusammenschau möchte ich mich verabschieden und bedanke mich für Ihre Aufmerksamkeit.

Manfred Kloiber

Vielen Dank, Frau Simon. Sie haben viele neue Aspekte in die Diskussion gebracht, von daher

stellen sich auch viele Fragen, denke ich. Sie haben jetzt die Gelegenheit, Fragen zu stellen.

Wolfram Burgard

Sie haben viel über Probleme gesprochen, aber wenig über Chancen und dieses Dilemma, in dem man sich da befindet. Denn man könnte natürlich auch eine metaethische Diskussion führen und sich die Frage stellen: Wenn wir das alles verteufeln und sagen: Nein, das dürfen wir alles nicht machen, dann verlieren wir auch die Chance, vielleicht die Welt besser zu machen, im Sinne von weniger Unfallopfern oder so.

Wenn man aufgrund einer ethischen Diskussion einfach sagt: Nein, wir können oder sollten das nicht tun, und dann selbstfahrende Autos *nicht* einführt, dann könnte in 20 Jahren jemand kommen und sagen: Mit großer Wahrscheinlichkeit wäre das jetzt nicht passiert.

Judith Simon

Erstens habe ich das nicht verteufelt. Ich habe nur gesagt: Man muss bestimmte Fragen stellen, wenn man das macht, und zwar erkenntnistheoretische, ethische und politische Fragen.

Zweitens habe ich nichts zu selbstfahrenden Autos gesagt. Denn da könnte man selbst aus ethischer Perspektive gut argumentieren, dass es sinnvoll wäre, die zu haben. Nur wird es eine Zwischenphase geben, in der nicht alle Autos selbstfahrend sind. Hätten wir schon lauter selbstfahrende Autos, wäre die Kosten-Nutzen-Rechnung via Utilitarismus sehr einfach: weniger Unfälle, mehr Sicherheit. Das Thema habe ich aber nicht einmal angeschnitten.

Ich glaube, es gibt viele und große Chancen. Wir müssen uns nur gut überlegen, in welchen Kontexten wir das einsetzen wollen. Es gibt viele Bereiche, gerade im Sinne von Energieeffizienz, Verbesserung der Stadt-Infrastruktur, wo man das gut einsetzen kann. Man muss es nur klug machen und man muss es gut machen, und deswegen müssen solche Fragen gestellt werden. Aber es ging mir beim besten Willen nicht darum, zu sagen, dass wir das nicht machen sollen.

Ich kann noch einen Schritt weitergehen: Ich war im Frühjahr auf dem Panel mit einem Vertreter der Digitalisierungsagentur für Dänemark, die die Digitalisierung in Dänemark vorantreiben. Er meinte: Wir wissen, dass Kinder, die im Grundschulalter viel Karies haben, eine hohe Wahrscheinlichkeit haben, später straffällig zu sagen. Wir haben es erkenntnistheoretisch alle verstanden: Das ist keine Kausalität, sondern es gibt eine gemeinsame Variable. Die gemeinsame Variable ist vielleicht Armut oder Vernachlässigung; das haben wir verstanden.

Dann kommt aber die ethische Frage, nämlich: Was mache ich jetzt mit dieser Information? Darf ich darauf handeln? Muss ich darauf handeln? Also die ethische Frage, die sich anschließt: Wenn die Daten erst mal da sind, habe ich gegebenenfalls eine normative Verpflichtung, auf Basis dieser Daten tätig zu werden. All diese Fragen stellen sich.

Mir ging es nicht darum, das zu verteufeln. Mir ging es eher darum, Fragen zu stellen: Wenn ja, wie?

Wolfram Burgard

Da könnte man trotzdem die Frage stellen: Warum soll man eine Robotersteuer erheben und warum erhebt man nicht eine Steuer auf die Heizung, weil die Leute, wenn sie in geheizten Arbeitsbedingungen sind, weniger krank werden als andere? Oder warum erhebt man nicht eine Steuer auf Hämmer? Weil Hämmer deutlich effizienter sind, als wenn man die Nägel mit der bloßen Hand reinschlägt.

Judith Simon

Das hat damit zu tun, dass man darauf Steuern erhebt, was die Arbeitsbedingungen und die Verteilung von Arbeit verändern wird. Ich glaube, dass durch die zunehmende Automatisierung in der Arbeitswelt viele Leute arbeitslos werden. Und wenn Unternehmen Gewinne einfahren, wenn sie weniger Arbeitnehmer haben und dementsprechend mehr automatisieren, könnte man das durch steuerliche Veränderungen geltend machen. Ich finde das keine unplausible Überlegung.

[Zuruf, unverständlich]

Es gibt eine Korrelation zwischen der …

[Zuruf, unverständlich]

… über die letzten hundert Jahre.

Wolfram Burgard

… wenn wir über die hundert Jahre deutliche Automation haben, müsste man ja sagen, heute sind viel mehr Menschen arbeitslos sind als damals.

Judith Simon

Gut, wir können natürlich arbeitssoziologisch weit zurückgehen und dann gucken: Was passiert in dem Moment, wo Automatisierung schon durch Fließbänder stattgefunden hat? Viele Formen der technologischen Entwicklung haben zu massiven Umwälzungen in der Anzahl der Arbeitnehmer geführt. Es gibt viele plausible Prognosen, dass die Zunahme der Nutzung von Drohnen für die Auslieferung von Gütern bestimmte Gruppen von Arbeitnehmern arbeitslos machen wird. Da muss man nicht weit vorausdenken.

Ich weiß nicht, ob wir da hundert Jahre zurückblicken müssen oder ob wir nicht relativ sinnvoll prognostizieren können: Bestimmte Aufgaben werden zunehmend automatisiert. De facto werden dann bestimmte Leute, die jetzt diese Jobs haben, arbeitslos, und dann zu sagen, dass man so etwas gegebenenfalls in der Steuerpolitik implementiert – der Vorschlag kam nicht von mir, sondern von Bill Gates, aber ich glaube, man kann das zumindest überdenken.

Herr NN

Viel von der Diskussion erinnert mich an die Zeit, wo IT in die Steuerung von Maschinen, von Luftfahrzeugen, von Autos usw. eingeführt wurde, diese ganze X-by-Wire-Technologie. Da wurde auch gesagt: Darf man das? Wer hat da die Verantwortung? Was automatisiert man und was automatisiert man nicht?

Was unterscheidet die heutige Diskussion von der damaligen Diskussion? Oder gibt es da Parallelen, was kann man da vielleicht lernen? Oder machen wir die gleiche Diskussion noch einmal neu durch?

Judith Simon

Ich glaube, es gibt parallele Diskussionen. Und es gibt zwei Komponenten, die man unterscheiden muss. Wenn ich entscheide, was soll ich delegieren und was nicht?, muss man zwei Dinge trennen. Das eine ist: Ist es funktional besser, wenn ich delegiere? Wer trifft die besseren Entscheidungen? Das ist auch die Frage Pilot versus System, was landet es besser? Soll ich nicht bestimmte Entscheidungen gerade von Menschen weglassen? Da ging es vorhin schon um die Frage: Sind nicht manchmal die Maschinen weniger gebiast als die Menschen? Da muss man genau hingucken: Reden wir über *cognitive biases* oder über gesellschaftliche? Das ist ein Riesenfeld.

Ein zweiter Punkt ist eine moralische Frage, ob wir bestimmte Entscheidungen aus moralischen Gründen an Maschinen delegieren wollen. Gerade bei diesen Kampagnen gegen Killerroboter und selbsttötende Maschinen ist nicht nur die

Frage: Wer entscheidet besser?, sondern: Wollen wir die Entscheidung über das Töten, diese Art der Entscheidung an Maschinen delegieren? Das ist natürlich ein sehr spezieller Fall, aber ich glaube, in dem Fall ist es massiv zu überlegen.

Als Fußnote: Man hat da teilweise Sekundäreffekte, an die man gar nicht denkt. Ich saß vor einer Weile in den USA auf einem Podium, wo jemand über Drohnen sprach. Dann stand ein Mitglied des Militärs auf, hat einen sehr emotionalen Redebeitrag gehalten und meinte: Die Drohnen im Afghanistan-Einsatz waren für die Truppen am Boden eine massive Belastung, weil ihnen nicht mehr vertraut wurde und weil sich so auch viel Zorn aufgestaut hatte gegen diese über den Dörfern kreisenden Drohnen, die irgendwann zuschlagen, auf die man aber nicht eins zu eins reagieren kann, sodass es dann zu negativen Effekten gegenüber den Truppen am Boden gab. Das sind Dinge, über die man oft nicht nachdenkt. Deswegen: Einerseits gibt es Komplementarität und Kontinuität von alten Debatten, aber je nach Kontext kommen neue Fragen dazu.

Herr NN

Mich würde interessieren, wie stabil Ethik und Moral sind. Das klingt polemisch, aber schauen wir uns einfach mal so Sachen wie die Vorfälle in Silvester an, wo die Polizei zu spät auf dem Kölner Bahnhof war, oder gar nicht da war.

Davor war es ein absolutes Unding, dass die Polizei Online-Streamings von sozialen Netzwerken macht. Kurz danach wurde der Polizei vorgeworfen, warum sie das nicht macht. Das wäre doch eine offensichtliche Datenquelle und das müsste man doch überwachen.

Wir haben in Frankreich gesehen, dass nach den Terroranschlägen in rasender Geschwindigkeit Gesetze geändert wurden, um viel stärkere Überwachungen durchzuführen.

Von daher würde es mich interessieren, wie die Ethik mit so etwas umgeht. Denn die Technologie kann gegebenenfalls durch Parametrisierung oder Scharfschalten von Systemen ziemlich schnell reagieren. Aber das ist offensichtlich nicht die einzige Antwort.

Judith Simon

Eine Antwort wäre erst einmal zu sagen: Ethik würde untersuchen und versuchen zu verstehen, wie es zu so einem Wertewandel kommt oder wie es durch bestimmte Anlässe gegebenenfalls zu einer unterschiedlichen Gewichtung von Werten kommt. Das wäre kein Ethikwandel, sondern eine Umwandlung von Werten durch bestimmte äußere Einflüsse.

Ich weiß nicht, inwiefern das ein Problem der Ethik ist oder nicht vielmehr ein Problem der öffentlichen Wahrnehmung und gegebenenfalls auch – das ist meine These – irrationaler Reaktionen, wo die Hoffnung auf Lösungen liegt, die vielleicht nicht gegeben ist. Aber das ist eine andere Note.

Die zweite Frage, die daran anknüpft, ist: Wenn wir wissen, dass Technologien, wenn sie da sind, für diese oder jene Zwecke genutzt werden können, dann müsste man sich vielleicht noch stärker fragen, in welcher Art und Weise man welche Art von Daten erhebt.

Jenseits von dem Beispiel des Kölner Bahnhofs haben sich viele Befragungen unter Amerikanern, wie stark sie vertrauen, stark gewandelt in dem Moment, wo nicht mehr Obama, sondern Trump an der Regierung ist. Da ist tatsächlich nicht nur die Frage: Wie ändern sich Werte?, sondern wie ändert sich auch die Wahrnehmung von Gefahren unter gleich bleibender technologischer Bedingung? Das ist ein bisschen um die Ecke geantwortet, aber ich hoffe, es ist trotzdem angekommen.

Manfred Kloiber

Noch weitere Fragen? Das ist nicht der Fall. Herzlichen Dank, Frau Simon.

Podiumsdiskussion: Freiheit und Verantwortung in den IT-Wissenschaften – Wie gehen Forschende, die Politik und die Gesellschaft damit um?

Manfred Kloiber

Wir kommen jetzt zum letzten inhaltlichen Teil des heutigen Tages, nämlich zu unserer Podiumsdiskussion über das Thema Freiheit und Verantwortung in der IT-Forschung. Wie gehen Forschende, die Politik und die Gesellschaft damit um?

Im Moment sind vier von sechs Sesseln besetzt. Einer ist für mich, aber der sechste ist für Sie. Wir haben uns überlegt, dass wir die Diskussion nicht in klassischer Weise für Beteiligung öffnen, dass wir also erst mal diskutieren und Sie erst am Ende mit diskutieren können, sondern Sie können jederzeit mitdiskutieren. Wer eine Frage stellen will, kommt nach vorn, setzt sich dahin, nimmt sich das Mikrofon und ich sorge dafür, dass Sie Ihre Frage loswerden können.

Kommen Sie und setzen Sie sich einfach hin. Das ist unproblematisch und eine gute Form der Beteiligung, damit das nicht so die starren Fronten sind.

Steigen wir ein in die Diskussion. Ich darf Ihnen die Teilnehmer unserer Diskussionsrunde vorstellen. Zu meiner Linken Ingo Dachwitz, Redakteur bei Netzpolitik.org in Berlin. Über Netzpolitik.org muss man in der IT-Szene nicht mehr viel sagen; in den letzten Jahren hat sich dieses Bloggerforum als netzpolitische Größe etabliert und meldet sich regelmäßig zu allen Themen, die mit Moral, Ethik und Bürgerrechten im Netz zu tun haben. Herr Dachwitz ist einer davon, der diese Themen aufgreift und als Redakteur bearbeitet.

Neben Herrn Dachwitz sitzt Thomas Lengauer. Er ist noch Direktor des Max-Planck-Institutes für Informatik in Saarbrücken; Frau Feldmann wird Ihnen nachfolgen und Sie werden sich dann anders wissenschaftlich betätigen, davon gehe ich jedenfalls aus. Herr Lengauer ist sicherlich vielen bekannt als einer der Bioinformatiker in Deutschland, die die Szene hier maßgeblich mit aufgebaut haben.

Neben Herrn Lengauer ist Wolf-Dieter Lukas. Er ist Leiter der Abteilung „Schlüsseltechnologien – Forschung für Innovationen“ beim Bundesministerium für Bildung und Forschung in Bonn, in dieser Eigenschaft stark mit IT befasst und derjenige, der darüber wacht, dass bestimmte moralische, wahrscheinlich mehr politische Kategorien eine Rolle bei der Forschungsförderung spielen.

Neben Herrn Lukas haben wir Harald Schöning. Er ist Vice President Research (das lasse ich unübersetzt) bei der Software AG in Darmstadt. Die Software AG ist ein großes IT-Unternehmen und stark unterwegs zum Beispiel beim Thema Big Data; dazu wird er sicherlich einiges sagen können.

Steigen wir ein. Wir haben ziemlich viel Input bekommen. Dabei wurde mir klar: Wertefragen spielen eine große Rolle. Das haben wir relativ abstrakt diskutiert. Ich frage mich angesichts der relativ schwachen eindeutigen Positionierung: Für welche Werte treten wir eigentlich ein? Welche Werte sind für uns relevant? Welche Werte verfolgen wir tatsächlich in der Forschung? Was sind bei Ihnen konkret in der Arbeit Werte, die Sie auf Papier schreiben könnten, wo Sie sagen würden: Das sind die Werte, an denen ich mich orientiere?

Erst mal aus der Außenperspektive. Herr Dachwitz, erkennen Sie einen Wertekanon, von dem Sie sagen würden, daran orientiert sich die deutsche IT-Forschung und vielleicht auch die deutsche IT-Industrie?

Ingo Dachwitz, netzpolitik.org

Nein, das könnte ich nicht. Unser Fokus bei netzpolitik.org ist die politische Regulierung. Da kommen die IT-Wissenschaften immer mal wieder vor. Von daher nehmen Sie es mir nicht übel, dass ich als jemand, der nicht so stark mit den IT-Wissenschaften befasst ist, das so nicht sagen könnte. Ich habe mich in der gedanklichen Vorbereitung ein bisschen danach gefragt – Informatik und IT sind ja relativ junge Wissenschaften – und würde die Frage deshalb am liebsten weitergeben an diejenigen, die stärker damit befasst sind.

Die Frage war: Ist die IT-Wissenschaft und ist Informatik in Deutschland eine Wissenschaft, die sich im Dienst der Öffentlichkeit versteht? Ist das ein Leitbild? Das war meine Frage, auf die ich keine Antwort habe.

Manfred Kloiber

Ich lasse das erst einmal offen. Welche Werte stehen oder standen bei Ihnen, Herr Lengauer, auf dem Zettel, wo Sie gesagt haben: Das ist etwas, woran ich mich vielleicht sogar fast automatisch orientiere, wenn ich über bestimmte Fachprobleme nachdenke?

Thomas Lengauer ML, Max-Planck-Institut für Informatik, Saarbrücken

Ich habe ja mehrere Leben hinter mir: Ich habe angefangen als Theoretiker und beschäftigte mich damals mit der Komplexität von Berechnungen. Damals wurde ich getrieben durch Neugier und dem Wunsch nach Erkenntnisgewinn.

Dann habe ich zehn Jahre lang Methoden und Software für den Entwurf von Schaltkreisen entwickelt. Da war der Motor, ich sag's mal ganz deutlich: Technologie-Happiness. Ich fand das einfach extrem spannend. Gesellschaftliche Dinge haben keine große Rolle gespielt, ich war ein junger Mensch. Ich glaube aber auch, dass generell in dem Gebiet damals gesellschaftliche Dinge nicht so eine große Rolle gespielt haben.

Dann bin ich Anfang der Neunzigerjahre Bioinformatiker geworden. Bioinformatik heißt Bioinformatik, weil sie Informatik für die Biologie ist. Das heißt, ein Bioinformatiker nimmt eigentlich die Werte der Biologie und der Biomedizin an. Das sind bei uns hauptsächlich Werte – wir sind sehr menschenorientiert: medizinisch, Heilen von Krankheiten, Patientenwohl, diese Dinge. Da war es relativ einfach und unkontrovers.

Manfred Kloiber

Das heißt, in der Phase, in der Sie jetzt arbeiten, steht die Humanität ganz klar auf Ihrem Zettel?

Thomas Lengauer

Genau. Und ich ziehe eine Menge Inspiration aus den Ähnlichkeiten und auch Unterschieden des Wertekanons und der Probleme in der Biologie und in der IT. Wenn man beide in Bezug setzt, lernt man eine Menge: ich persönlich, aber auch wir als Community, auch der Ethikrat, die DFG oder die Leopoldina. Denn unsere Auseinandersetzung mit diesen Fragen in der Biologie ist deutlich älter als in der IT. Da haben wir schon eine Menge Erfahrung, und da können wir uns fragen: Was können wir davon übertragen oder was geht gar nicht? Da sehe ich eine Menge Ähnlichkeiten, aber auch eine Reihe von Unterschieden.

In der Biologie gibt es externe Werte und Ziele. Die mögen manchmal nur vorgeschoben sein, aber die werden propagiert: Ernährung der Weltbevölkerung, Ausmerzung von Krankheiten und von Plagen. Es ist sicher so, dass das proximale

Ziel in vielen Fällen Profitgenerierung ist und dass die anderen Dinge in einigen Fällen nur als Aushängeschild genutzt werden. Aber wir haben uns immer an der Existenz dieser Ziele orientiert, und je klarer die waren, desto mehr hat uns das interessiert. Dann sind wir nicht so sehr in die Agrartechnologie gegangen, sondern eher in die Medizin, obwohl die Medizin sehr schwer ist. Der Mensch hat ein unaufgeräumtes Genom und die Möglichkeiten, am Menschen zu experimentieren, sind sehr eingeschränkt.

Diese externen Ziele sehe ich in der IT nicht. Ich sehe in der IT nur die proximalen, nächsten Ziele: Gewinnmaximierung, neue Businessmodelle. Technologie-Happiness ist immer noch meiner Ansicht nach ein massiver Treiber unter den Innovatoren. Das Wort disruptiv wird als Idol eingesetzt. *dis* ist ein negatives Präfix, und *rompere* heißt zerreißen; eigentlich ist das Wort disruptiv ein durch und durch negatives Wort.

Man darf sich auch die Frage stellen, ob disruptive Innovation nun gerade das ist, was wir brauchen. Aber es wird so verwendet, es wird auf breiter Front umgedeutet vor dem Paradigma, das im letzten Vortrag genannt wurde, und wird jetzt als Ideal hingestellt. Damit habe ich ein bisschen Probleme.

Manfred Kloiber

Herr Schöning, wie ist das in der Industrieforschung in einem IT-Unternehmen. Sind die Ziele, die Herr Lengauer gerade so provokativ aufgezählt hat, die Werte, die Sie treiben?

Harald Schöning, software AG

Das kann man so nicht sagen. Disruption ist ja kein Wert, sondern ein Phänomen, das wir beobachten.

Thomas Lengauer

Ein Prozess.

Harald Schöning

Ja, das ist erst mal nichts, was man per se aus irgendwelchen theoretischen Überlegungen anstrebt, sondern das passiert halt. Unser Ziel – und das Ziel vieler Unternehmen – ist es, das verträglich zu gestalten, verträglich auch für die deutsche Wirtschaft beispielsweise. Es ist nicht so, dass Disruption als solches der Wert ist, sondern das ist die Randbedingung, unter der man agieren muss.

In der industriellen Forschung haben wir keinen unabhängigen Ethikrat oder so etwas. Wir haben aber einen Code of Conduct in der Firma und ein Ethical Board, und wir haben auch die ethischen Rahmenbedingungen, die uns die EU oder auch der Bund bei Fördermaßnahmen vorgibt; dazu machen wir uns viele Gedanken.

Letztlich sind auch die Fördermaßnahmen an irgendwelchen Zielen orientiert, ob das jetzt ökonomische Ziele sind, ökologische oder gesellschaftlich wünschenswerte Ziele. Zu den Förderprogrammen kann Herr Lukas sicher mehr sagen. Die fallen nicht vom Himmel, sondern haben auch, sagen wir mal, gesellschaftliche Ziele und wollen in irgendeiner Form die Welt verbessern, um es mal ganz allgemein zu sagen. Da kann die Ernährung der Weltbevölkerung durchaus eines dieser Ziele sein, was man IT-seitig verfolgt. Also ich würde nicht sagen, dass es diese Ziele nicht gibt. Die werden vielleicht genauso ernst oder weniger ernst genommen wie in der Bioforschung oder Medizin.

Manfred Kloiber

Ich habe im Vortrag von Frau Grimm ein Plädoyer zum Beispiel auch dafür gehört, dass man die Stärkung oder das Wohl der demokratischen Gesellschaft durchaus als Wert auch für die IT-Forschung ansehen könnte. Herr Lukas, ist das etwas, wo Sie als Forschungsförderer, als politische Institution sagen würden: Ja, das muss auf

jeden Fall sein und wir achten darauf, dass die demokratische Grundordnung damit befördert wird? Oder zumindest ihr kein Schaden zugefügt wird?

Wolf-Dieter Lukas, Bundesministerium für Bildung und Forschung

Zu den Werten würde ich zwei Perspektiven einnehmen. Die erste Perspektive ist meine Rolle als Ministerialbeamter. Wir haben es als Beamte leicht. Das Erste: Wir sind alle vereidigt auf die Verfassung, Artikel 1, die Menschenwürde ist ableitbar daraus, die informationelle Selbstbestimmung. Dies ist nicht verhandelbar und nicht diskutierbar; darauf haben wir einen Eid geschworen. Der ist auch nicht veränderbar.

Damit ist klar: Wenn ich das jetzt auf IT beziehe, rede ich über informationelle Selbstbestimmung. Da geht es am Ende nur noch um die Frage: Wie kann ich das verwirklichen? Wir reden ja über Werte, und Werte helfen einem nicht, wenn ich nicht am Ende einen Prozess habe, die Werte zu verwirklichen, sodass sie eine Wirkung in einer Gesellschaft haben. Da gibt es verschiedene Werte, die ich jedes Mal – so ist auch unsere Verfassung aufgebaut – abwägen muss.

Interessant ist übrigens: In unserer Verfassung steht *nicht* drin, dass die Erhaltung der Bundesrepublik Deutschland das oberste Ziel ist. Das wird zwar unterstellt, weil man sagt, man muss ja die Verfassung schützen – der Schutz der Verfassung ist der Staat, also muss der erhalten werden. Aber wenn Sie die Verfassung lesen, sind die alle wertebezogen. Das finde ich toll. In dem Sinne ist es leicht, einen Eid zu schwören auf so eine Verfassung.

Jetzt ist unsere Aufgabe, zu sehen: Wie können wir diese kodifizierten Werte umsetzen? Das ist die eine. Sie haben Ziele genannt; das sehe ich auf einer anderen Ebene. Wir müssen natürlich sehen: Was sind die Bedarfe einer Gesellschaft? Wo haben wir auch Schutzfunktionen? Dies müssen wir immer wieder in Beziehung stellen. Denn Politik heißt: die Lebensbedingungen der Menschen zu verbessern. Das ist das Ziel. Da ist das Thema: Auf welcher Basis? Welche Werte haben eine Basis? Aber am Ende geht es um ganz alltägliche Probleme: Die müssen essen, die müssen trinken, und wir müssen die Demokratie, unsere Grundordnung, erhalten, die wiederum die sozialen Verfassungswerte schützt und umsetzen hilft.

Ich will aber noch eine andere Perspektive einnehmen. Ich bin auch Honorarprofessor an der Technischen Universität Berlin. Bei der Antrittsvorlesung habe ich gesagt: Ich bin als Beamter verpflichtet, die Wahrheit zu sagen. Ich brauche nicht immer die ganze Wahrheit sagen; man kann mir sagen: „Das sagst du nicht." Aber ein Beamter darf nicht lügen. Andere dürfen es, Politiker dürfen es, Beamte dürfen es nicht. Ein Politiker darf mir sagen: „Das darfst du nicht sagen." Dann sage ich: „Okay, das sag ich nicht." Aber er kann mich nicht zwingen zu lügen.

Jetzt komme ich zur Wissenschaft. Wenn ich Honorarprofessor bin, schulde ich mehr, und zwar die ganze Wahrheit. Ich schulde auch, dass ich die Gedanken offenbare, die ich mir mache, die Spekulationen, die ich im Kopf habe.

Wenn ich jetzt eine Technik habe und sage: Ist die nützlich oder nicht nützlich? Wenn man mich als Beamter fragt, sage ich: „Weiß ich nicht, kann ich nicht, krieg ich nicht zu Ende gedacht." Denn ich kann nicht einen Haken dran machen: ja oder nein. Das kann wahrscheinlich keiner.

Wenn ich aber den anderen Hut aufhabe, kann ich sagen: „Ich denke; ich könnte; in der Historie hat gezeigt und vielleicht und so." Ich kann spekulieren. Und wenn ich diese ganze Wahrheit (auch das, was ich mir auch denke, einschließlich der Spekulation, einschließlich dessen, wo

ich sage: Da kann ich irren) nicht offenbare, können wir über die Frage: Ist diese Technologie nützlich, nicht nützlich; wo ist sie nützlich; wo ist sie nicht nützlich? nicht diskutieren. Denn wenn ich einen Hammer habe (das hat vorhin jemand gesagt), weiß ich nicht, was man alles damit machen kann. Und ohne die Fantasie einzubeziehen kann ich es nicht machen. Ich kann nur sagen: Wofür ist der Hammer zugelassen?

Wenn wir jetzt für jedes Instrument, jedes Programm eine Zulassung haben, dann weiß ich: Das ist nur dafür zugelassen. Aber die Dinge sind erst mal für alles zugelassen. Das bedeutet: Ich schulde eigentlich (übrigens am Ende bei der Beratung auch meiner Ministerin) die gesamte Wahrheit, auch das Spekulieren. Ich muss sagen: „Das könnte, das hätte." Das finde ich wichtig in der Diskussion.

Aber ich möchte zu Herrn Lengauer eine Bemerkung machen. Wir wollen ja diskutieren und widersprechen. Ich kann Ihnen bei der Disruption dummerweise nicht widersprechen. Disruption heißt Innovation, um vorhandene Geschäftsmodelle zu zerstören. Ich finde es bemerkenswert – ich war in Österreich und anderen Ländern, alle sagen jetzt: „Wir brauchen disruptive Innovation." Einige sagen: „Wir brauchen Revolution." Ich finde es großartig, dass Politiker jetzt Revolution wollen, das wollten sie früher nie!

[Lachen]

Und jetzt wollen sie Disruption. An der Stelle lacht man, denn man muss ja auch den Politiker sehen und verstehen. Denn was wir gut können, ist: diese leisen Schritte, gucken, beobachten, einen Schritt nach dem anderen, unsere Geschäftsmodelle retten ins nächste Jahrzehnt, und immer gehen wir vorsichtig vor. Sie wissen ja: Wer den deutschen Datenschutz beherrscht, kann eigentlich jeden Datenschutz in der Welt beherrschen, weil die Deutschen da besonders vorsichtig sind. Das finde ich eigentlich ganz gut.

Nun gibt es andere Gesellschaften, die auch erhebliche Probleme damit haben, die ein Geschäftsmodell nicht mehr verteidigen, sondern aufgeben, und dann sagen: Das ist halt ein anderes. Das heißt, wir sehen Industrien, die sterben, in anderen Regionen, und jetzt sagen wir: Ja, das, was die neu aufbauen, hätten wir auch gerne. Deshalb das Disruptive.

Und nun haben Sie ein Problem. Wir fördern als Staat überwiegend den Erhalt dessen, was wir uns erarbeitet haben, nicht nur wirtschaftlich, sondern auch Werte etc.; Datenschutz gehört auch dazu. Und andere probieren aus und sagen: „Können wir nicht das eine oder andere weglassen?" In Klammern: ein anderes Geschäftsmodell.

Ich behaupte: Auch da ist der Weg des Abwägens. Wir hätten uns nicht entwickelt, wenn wir nicht etwas riskiert hätten. Aber die Frage der Bewertung ist immer wieder – der Wertekanon, den wir haben, zwingt uns zu einer langsameren, bedächtigeren Bewegung, und wir müssen jetzt – diese Disruptionsdiskussion gefällt mir gar nicht. Aber ich glaube auch eines: Innovation heißt: Ich muss die, die im Markt sind, die, die etwas haben, angreifen; ich muss Alternativen vorschlagen. Den Jungen, den Neuen muss man Raum geben, aber sie müssen sich am Ende auch den gesellschaftlichen Regeln und damit den Werten unterstellen. Und dann kann man gern über Disruption reden, aber nicht über Disruption von Werten.

Manfred Kloiber

Das Problematische an der Disruptionsdiskussion ist eigentlich die Aggressivität, die teilweise hinter den Geschäftsmodellen, aber auch in dem Begriff selbst steckt.

Herr Dachwitz, Sie haben eben gesagt, dass Sie sich als derjenige, der die IT-Szene beobachtet, wünschen, dass man sich stärker die Frage stellt: Was ist eigentlich gesellschaftlich nützlich? Ich kann mir vorstellen, dass man, wenn man dann über disruptive Geschäftsmodelle redet, leicht sagt: Das meiste davon kann man unter dem Aspekt eigentlich in die Tonne klopfen.

Ingo Dachwitz

Das ist definitiv so. Was ich am Begriff Disruption gut finde, ist, dass er halbwegs ehrlich ist, ehrlicher als das Gerede von der Revolution des Technischen, denn mit der Revolution geht auch immer eine Neuordnung der sozialen Verhältnisse einher. Das ist bislang zumindest nicht sichtbar gewesen, weder durch Facebook noch durch das iPhone. Da ist Disruption vielleicht der ehrlichere Begriff, auch wenn es als Ideal nicht das Richtige ist.

Ich finde es nur schwierig, nur auf der abstrakten Ebene darüber zu sprechen …

[Zuruf, unverständlich]

Genau, ich würde Sie direkt ansprechen, Herr Lukas. Wenn Sie von der informationellen Selbstbestimmung als Wert sprechen und von der Möglichkeit – der Staat oder die Regierung hat ja gewisse Einflussmöglichkeiten, zum Beispiel die Förderlinien aufzusetzen. Wir vermissen in Deutschland eine Förderlinie, die explizit dafür da ist, den Datenschutz durch Technik (Privacy by Design und Privacy by Default) in der Praxis zu fördern bzw. die Förderung auszuweiten. Da geht es um Innovation, Datenschutz durch Technik, die nicht disruptiv ist in dem Sinne, dass sie andere Sachen verdrängt, sondern die Werte verteidigen oder erhalten soll.

Wolf-Dieter Lukas

Erstens: Wir fördern dieses, und ich mache da denen richtig Druck, übrigens auch auf die Wissenschaft. Sie kommt übrigens dem Druck gerne nach, weil sie kreativ sein muss. Aber ich sage häufig und sage es auch hier wieder, es gibt einige, die sagen: „Der Datenschutz ist so kompliziert“, dann sage ich: „Moment mal. Mit euren IT-Systemen wollt ihr die Probleme der Welt lösen. Ihr schafft alles. Ihr wollt die Ernährungsfrage lösen, ihr wollt es mit der Energie lösen – aber nur den Datenschutz, den bekommt ihr nicht hin?“ Das ist doch nur ein Regelsystem. Und was IT kann, sind Regelsysteme.

Unsere Förderlinie ist: Wir wünschen uns von der Wissenschaft Projekte – und wir haben auch welche (einige im Saal arbeiten daran) –, die durch Technik, durch Lösungen, den Datenschutz, die Information und Selbstbestimmung realisieren. Das ist es. Wenn es um Privacy geht, ist das genau die Zielrichtung, die Sie genannt haben. Die ist mir relativ klar.

Das hören übrigens einige nicht so gerne, weil sie sich lieber über die Datenschutzregeln beschweren. Ich sage auch jedes Mal meiner Ministerin – die sagt es auch immer: „Wieso können die das nicht lösen?“ Es gibt Grenzen, und manchmal kann man durch Technik nicht alles lösen. Aber solche Lösungen brauchen wir.

Wo vermissen Sie es? Denn ich kenne Projekte, die wir konkret …

Ingo Dachwitz

Genau, es gibt bestimmt Projekte, aber die Bundesregierung oder Politik fördert ja auch Start-ups im Bereich Wirtschaftsförderung. Das ist nun nicht Ihr Haus, von daher …

Wolf-Dieter Lukas

Es könnte unser Haus sein, ja.

Ingo Dachwitz

Oder ist es vielleicht. Aber ich wüsste nicht, dass das eine Bedingung wäre für Start-ups, dass sie

Privacy by Design und Privacy by Default, die von der Datenschutzgrundverordnung vorgeschrieben sind, realisieren müssen, um eine Wirtschaftsförderung zu bekommen.

Harald Schöning

Jetzt muss ich aus Sicht der Wirtschaft aber mal etwas sagen. Das kann ja nicht sein. Sie können ja nicht, egal, was das Start-up machen will, sagen: „Ihr kriegt die Förderung nur, wenn ihr euch auch mit diesem Thema befasst."

Ingo Dachwitz

Da, wo es Sinn macht, natürlich.

Harald Schöning

Ja, aber auch für Start-ups gelten die gesetzlichen Regelungen, und man muss ein Start-up nicht zwingen, in einem Bereich innovativ zu sein, der nicht der Kernbereich des Start-ups ist. Dann macht man es gleich kaputt. Aus meiner Sicht reicht es …

Ingo Dachwitz

… ab Mai 2018, wenn die Datenschutzgrundverordnung gilt, Privacy by Design und by Default umsetzen müssen. Das ist …

Harald Schöning

Ich sage ja, die gesetzlichen Regelungen müssen eingehalten werden. Aber darüber hinaus kann ich doch von einem Start-up, das sich mit etwas ganz anderem befasst, nicht erwarten, dass es darauf noch investiert. Das geht übers Ziel hinaus.

Manfred Kloiber

Ich finde das auch ein bisschen weitgehend, zu verlangen, dass es alles von sich aus können und berücksichtigen muss. Ich würde eher dazu tendieren, zu sagen: Es muss auf jeden Fall verhindert werden, dass irgendetwas kannibalisiert wird von den gesellschaftlichen Werten, die wir aufgestellt haben. Dazu gehört der Datenschutz, der steht in der Verfassung. Sie haben darauf hingewiesen, Herr Lukas …

Wolf-Dieter Lukas

Der Datenschutz nicht, das haben Gerichte so abgeleitet.

Manfred Kloiber

Das Recht auf informationelle Selbstbestimmung, und da muss man schon sehen: Da sind Sie ständig im Verfassungskonflikt, Herr Lukas, wenn Sie Big-Data- oder Smart-Data-Projekte entscheiden. Das kannibalisiert ja alles.

Wolf-Dieter Lukas

Ja, das ist richtig. Ich will noch mal die Brücke zwischen Ihrer Frage und …

Manfred Kloiber

Ja, erzählen Sie uns etwas über diese Gewissenskonflikte.

Wolf-Dieter Lukas

Wir haben ja, wir fördern nicht nur IT-Sicherheit, sondern auch zivile Sicherheit. Da nützen alle Technologien und bestimmte – auch Sicherheitsprobleme sind noch zu lösen. Da geht es am Ende um Mustererkennung und Ähnliches, also kritische Fragen, wo es auch um eine Grenzziehung geht: Wo darf der Staat eingreifen? In bestimmte Dinge darf er eingreifen, und zwar wenn ein bestimmter Verdacht, eine Auffälligkeit da ist. Dann kann er eingreifen, Aufzeichnungen machen; das ist alles kodifiziert.

Sie haben recht: Ich gebe zu, dass ich häufiger – ich bekomme übrigens von jedem Projekt, was meine Abteilung umsetzt (da wird viel Geld umgesetzt, ein paar Projekte auch im höheren dreistelligen Millionenbetrag), Steckbriefe. Die sehe ich mir schon an, und es gibt häufig Lösungen, die sich im ersten Moment technisch sehr interessant anhören und vielleicht auch einen Nutzen für eine kleine Klientel geben, die aber

am Ende nicht konform sind mit dem, wie wir uns Gesellschaft vorstellen. Da ist es schon so, dass ich dann draufschreibe „Nein“, weil die Zielrichtung falsch ist.

Ich möchte noch etwas zu diesem Start-up sagen. Ich glaube, da sind wir einer Meinung. Eines ist klar: Wenn wir Projekte fördern, gehen wir davon aus und schauen uns auch an, dass das im Rahmen der gesetzlichen Regelungen passiert und dass Datenschutz da auch ein Thema ist.

Wenn wir aber eine ganz andere Maßnahme im […] wo wir sagen, dass wir Start-ups mal eine Chance geben, sich zu gründen, sich zu entwickeln, dann müssen sie sich an alle gesetzlichen Bedingungen und Regeln halten. Aber wir können nicht in ihren Weg, den sie suchen, und wie viel sie sich mit der Frage beschäftigen, auch noch hineinreden.

Ich glaube, was man auch – da ist übrigens unsere Verfassung wieder auch toll: Es gibt nichts, was am Ende – unsere Verfassung ist, Grenzen der Freiheit, verschiedene Freiheiten stoßen aneinander und da gibt es auch Grenzen. Man kann also nicht eine Regel nehmen und sagen: Diese eine Regel muss alles andere überlappen, sondern da muss es auch Freiheiten des Handelns geben; da bin ich Ihrer Meinung. Vielleicht haben Sie es auch gar nicht so scharf gemeint.

Thomas Lengauer

Ihre Frage ist ein gutes Beispiel dafür. Ich will wieder mal den Vergleich zwischen Biologie und IT machen, wie wenig wir noch verstehen in dem, was wir eigentlich tun mit der IT: In der Biologie gibt es Freisetzungsexperimente. Die Freisetzungsexperimente sind mit einem hohen Respekt verbunden, und man muss durch viele Vorprüfungen gehen, um ein solches Experiment zu bekommen mit den besten Ideen. Vor einem Monat hat in unserer Leopoldina-Jahresversammlung jemand gesprochen, der ein Gene-Drive in Moskitos reinsetzen will, um Malaria auszumerzen. Das führt zu einer genetischen Kettenreaktion, die dann die Vektoren, die Moskitos, in den Stand versetzt, dass sie das Pathogen nicht mehr unterstützen können. Klingt super, gleichzeitig haben die Leute einen hohen Respekt vor den möglichen unbeabsichtigten Auswirkungen und es wird lange brauchen, bis so etwas genehmigt und durchgeführt wird. Und es gibt noch immer ein Restrisiko.

Ich behaupte mal: Die Einführung von Smartphones in den Markt war ein Freisetzungsexperiment. Die Einführung von Sensoren, dieses ganze Internet of Things, ist ein fantastisches Freisetzungsexperiment mit entsprechend umwälzenden Konsequenzen, die wir nicht verstehen. Wir haben keine Regelungsmöglichkeit und wir haben auch richtig Angst vor möglichen unbeabsichtigten Auswirkungen. Aber wir werden mit den Konsequenzen leben müssen.

Meiner Ansicht nach ist das eine Inspiration, um in dem Bereich zu mehr Verständnis zu kommen, zu mehr Prädiktivität, aber auch zu mehr Schutzmechanismen. In den Empfehlungen, die hoffentlich aus unserer Big-Data-AG einmal herauskommen, wenn diese Empfehlungen fertig sind, irgendwann in ein paar Monaten, werden solche Sandboxes drinstehen, indem man geschützte IT-Räume hat, in denen man Dinge gründlich testen kann, bevor man sie freisetzt. Das ist eine Sache, die …

Ingo Dachwitz

Das ist aber nur bedingt übertragbar, oder? Denn Innovation entsteht ja erst in Interaktionen, indem Leute Technik in den Alltag einsetzen.

Manfred Kloiber

Ich wollte da mit einem konkreten Beispiel nachhaken. Wir haben heute von diesem Social Bot von Microsoft gehört, der auf einmal anfing,

rechtsradikale Sprüche abzulassen, weil er das im Netz gelernt hat. Das war die Erklärung, die ich hier von den KI-Experten gehört habe. Hätte man es verantwortlicherweise bei Microsoft so organisieren müssen, dass man Technologien der Technikfolgenabschätzung auch auf die IT anwendet, dass man bei Microsoft sagt: Jetzt müssen wir das Netzwerk erst mal anlernen wie in der Schule, dass Rassismus, Extremismus, Nationalsozialismus usw. alles vom Teufel ist, damit das Netzwerk das weiß, bevor es weitermacht?

Ingo Dachwitz

Ich finde das ein spannendes Beispiel und Experiment, weil es deutlich widerspiegelt, was passiert, wenn man einen einseitigen IT-Begriff hat, der sich nur auf das Technische bezieht. Ich glaube zum Beispiel nicht, dass Gesellschafts-, Kommunikationswissenschaftler mit in der Konzeption einbezogen waren. Wenn das von vornherein mitgedacht und wirklich interdisziplinär gedacht worden wäre, dann wäre man eher darauf gekommen, dass genau solche Wege für so ein Experiment möglich sind.

Von daher – ich bin heute auch ab und zu mal ins Überlegen gekommen, wenn davon die Rede war, was eigentlich IT oder Technik ist. Wenn es um IT oder IT-Wissenschaften geht, denken wir meistens nur im technischen Sinne. Die Veranstaltung heute ist ein glänzendes Beispiel dafür, wie es interdisziplinär geht. Gleichzeitig – ich weiß nicht mehr, wer es war – zeigte jemand vorhin die Kompetenzen, die ein IT-Wissenschaftler oder Data Scientist haben muss. Ich bekomme sie nicht mehr genau zusammen, aber das waren nur technische bzw. datenwissenschaftliche Kompetenzen. Da fehlt die ethische Kompetenz, gesellschaftliche Reflexion usw., das spielte in dem Verständnis davon, was der Techniker für Kompetenzen haben muss, keine Rolle.

Manfred Kloiber

Gut, dass das nicht leicht ist, liegt auf der Hand. Herr Schöning, an diesen Beispielen und das, was Herr Lengauer eben kritisiert hat, dass da viel passiert, ohne dass sich jemand vorher Gedanken macht, also es wird einfach gemacht …

Thomas Lengauer

Ich habe es nicht kritisiert, ich will nur sagen: Wir sind nicht in der Lage, die Konsequenzen abzuschätzen.

Manfred Kloiber

Sie haben festgestellt, dass es oft so ist, und die Kritik, die auch Herr Dachwitz gerade daran geäußert hat – wie sieht das bei Ihnen im Unternehmen aus? Was sind für Sie relevante Kriterien, wenn Sie bestimmte Technologien entwickeln wollen? Machen Sie sich solche Überlegungen, die weitergehend sind als das, ob Sie Ihr geschäftliches Ziel damit erreichen können?

Harald Schöning

Wahrscheinlich nur sehr eingeschränkt. Zum einen produzieren wir als Unternehmen Basistechnologie, also den Hammer, wenn man die Analogie überträgt, und nicht die Endapplikation. Aber wir machen auch mit Kunden deren Lösungen. Und da gibt es schon Grenzfälle, wo man sich fragt: Will man das? Denn in Ländern, die nicht der EU-Datenschutzgrundverordnung unterliegen, gibt es halt Anwendungen, die nach unserem Datenschutzverständnis nicht ganz in Ordnung sind.

Die Frage stellt man sich schon. Aber wir sind ein globales Unternehmen, und der Wert Datenschutz ist eben kein global akzeptierter. Wenn man ein globales Unternehmen ist, muss man sich auf Werte verständigen, die im ganzen Unternehmen gelten. Die gibt es, die sind aufgeschrieben. Die Privacy gehört aber nicht dazu. Letztlich hat jeder bei uns die Freiheit zu sagen:

„Nein, in so einem Projekt mache ich nicht mit.“ Aber als Firma haben wir Grenzfälle, die nicht unbedingt dem deutschen Wertekanon entsprechen.

Manfred Kloiber

Aber da ist ja schon mal ein Stück Klarheit, dass Sie das aufgeschrieben haben und dass man weiß, dass zum Beispiel Privacy kein im Unternehmen anerkannter Wert ist, den man verfolgen muss.

Harald Schöning

Es steht keine Negativliste drin, aber es steht nicht in der Positivliste.

Manfred Kloiber

Ja gut, aber die Interpretationsfreiheit habe ich mir genommen. [Lachen]

Frau Friedrich, wunderbar, dass Sie mich unterstützen.

Bärbel Friedrich

Ich weiß nicht, ob ich Sie unterstütze, aber DFG und Leopoldina haben eingeladen, um diesen Bereich der IT-Wissenschaften kennenzulernen, ob wir ein ähnliches Prinzip einsetzen können, was Sie bei den Biowissenschaften gelobt haben. Ob das nun so funktioniert und ob wir damit zufrieden sind – aber immerhin haben wir Erfahrungen, es gibt Ansätze. Jetzt höre ich, Herr Lengauer, dass Sie pessimistisch sind, dass wir in diesem Bereich, wo wir doch mit viel Optimismus rangegangen sind, das ethische Bewusstsein schärfen können. Ist das wirklich so abwegig, dieser Gedanke?

Thomas Lengauer

Ich glaube, ich werde missverstanden. Ich bin nicht pessimistisch, sondern ich mache lediglich eine Standortbestimmung. Ich schaue mir diese zwei Bereiche, Lebenswissenschaften und IT, an und stelle fest: In dem einen Bereich sind wir mit unseren Konturen viel weiter als in dem anderen. Das können Sie auch als Inspiration verstehen, in dem anderen Bereich Schritte zu unternehmen, die uns in diese Situation bringen. Der andere Bereich, IT, wird ungleich schwerer sein aufgrund der Dinge, die Sie nennen: dass wir die Prozesse, die wir durch die Technologie in Gang setzen, nicht verstehen und dass unsere Prädiktionsfähigkeit da gering ist. Aber man kann es ja versuchen.

Ich glaube aber nicht, dass wir ähnliche ethische Konturen in der IT bekommen werden, wie wir sie in der Biologie haben, ohne dass wir versuchen, diesen Weg zu beschreiten. Wir brauchen externe Ziele, wir brauchen irgendeinen Richtwert: Wo will ich hin mit der Technologie?

Ja, meiner Ansicht nach ist es hauptsächlich Kommerzialisierung, sind es neue Businessmodelle, wirtschaftlicher Wettbewerb zwischen Regionen. Man kann zum Beispiel nicht behaupten, dass wir die Technologie einsetzen, um die Demokratie zu stärken. Ich bin der Meinung, dass die neue Technologie eher eine Herausforderung für die Demokratie ist und nicht a priori eine Unterstützung. Wir laufen dann den Effekten, die die Technologie-Ausbringung nach sich zieht, hinterher und versuchen zu retten, was zu retten ist.

Harald Schöning

Aber das ist doch in der Agrartechnologie nicht anders. Da ist vieles von Unternehmen auf den Markt gebracht worden, was große Eingriffe und gesellschaftliche Auswirkungen hat, ohne dass dem große wissenschaftliche oder ethische Diskussionen vorangegangen sind.

Thomas Lengauer

Ja, aber ist das toll?

Harald Schöning

Nein, das ist nicht toll, aber ich sage nur: Es ist nicht so, dass es in der IT ganz anders und viel schlimmer ist als anderswo.

Thomas Lengauer

Ich beschuldige niemanden, ich will nur eine Standortbestimmung. Wir müssen uns doch irgendwann mal bewusst werden, wie wenig wir verstehen von dem, was wir da lostreten.

Harald Schöning

D'accord.

Thomas Lengauer

Sonst kommen wir nie dazu, das zu verbessern, das Verständnis. Das ist das Einzige, was ich will, mehr nicht.

Manfred Kloiber

Ist uns das nicht klar geworden? Dass in der IT vieles passiert, weil vieles einfach gemacht wird, ohne darüber nachzudenken, oder gemacht wird, weil es halt möglich ist?

Ich sehe das nicht so pessimistisch. Sie machen ja keine Wertung, sondern beschreiben nur. Ich sehe das nicht so pessimistisch, dass es keine Leute gibt, die anfangen darüber nachzudenken und Konsequenzen daraus ziehen. Ich habe zum Beispiel erlebt, dass mittlerweile viele Forscher sagen: Das Internet ist ein völlig anderes Ding geworden als das, was wir erhofft haben, im gesellschaftlichen Kontext. Also es gibt auch Überlegungen.

Thomas Lengauer

Ich fühle mich durch Ihre Bemerkung bestätigt.

Wolf-Dieter Lukas

Drei Bemerkungen. Ich habe mit vielen Wissenschaftlern im IT-Bereich zu tun, und ich hoffe, ich habe mit den Besten zu tun. Ich glaube, es sind die Besten, und die sind sehr reflektiert und sind sich dieser Sache bewusst.

Man muss auch sehen, dass sie an etwas arbeiten, was Riesenpotenzial hat. Wir beschäftigen uns mit Informationen. Wenn wir eine Gesellschaft gestalten wollen, wenn wir mit Fragen der Energie umgehen wollen und mit Fragen wie: Wie lenke ich Verkehr? Wie kann eine Gesellschaft sich selbst steuern?, dann ist die Frage, wie wir mit Informationen umgehen, unerlässlich. Information und Kommunikation sind die Grundlagen, um Gesellschaft zu gestalten.

Aber jetzt kommt's: Weil es so wichtig ist, ist das ein Bereich, mit dem wir sehr sensitiv, sehr vorsichtig umgehen müssen.

Der erste Punkt ist: Ich glaube, den Wissenschaftlern ist es bewusst, dass – wir reden doch über Verantwortung, und die wesentliche Frage ist, ob die Wissenschaftler, die in Deutschland an diesem Problem arbeiten, die auch in diesem Raum sitzen, dieser Verantwortung ausreichend nachkommen. Das ist das Thema. Ich würde sagen: Das tun sie.

Jetzt haben sie aber nicht Verantwortung für das System, was weltweit geschaffen wird. Das ist ein Problem. Wir haben ein Problem, dass bestimmte Produkte von den Menschen genutzt werden, übrigens freiwillig, für die sie nichts oder nur sehr wenig zahlen, oder sie zahlen mit ihren Daten, wo wir wissen, dass die Geschäftsbedingungen nicht mit unserem deutschen Standard – dass sie rechtswidrig sind oder nicht rechtskompatibel sind. Sie werden genutzt und bringen in Zukunft sicher Probleme für die Menschen, die sie nutzen, mit sich.

Die erste Pflicht, die wir alles Wissenschaft und natürlich auch als Staat haben, ist, die Menschen darüber aufzuklären, zu sehen, wo die Probleme sind. Ich kenne nur eine Projekt[…] hat mir ge-

fallen. Ich weiß nicht, von wem sie war, das habe ich vergessen. Vielleicht sogar von – nein, ein Kollege von Ihnen, der hat gesagt: Kann ich nicht ein IT-System schaffen, das mich in Privacy-Dingen berät? Nicht technisch berät, sondern sagt: „Wenn du diese Daten herausgibst und gleichzeitig auf bestimmten Plattformen bist (Big-Data-Ansatz), dann könnte diese Information an diese Personengruppe gelangen. Willst du das oder willst du es nicht?“

Das finde ich einen hochinteressanten Forschungsansatz. Eines der drei Kompetenzzentren für IT-Sicherheit beschäftigt sich mit der Frage: Kann ich nicht ein Beratungssystem haben, nicht eines, das sagt: „Du musst die und die Einstellung wählen“, sondern: „Kann ich dir die Auswirkungen sichtbar machen als Nutzer, wie weit die Informationen fließen, wenn andere Big Data nutzen?“

Das finde ich eine super Fragestellung. Wissenschaftlich kompliziert, weil man die Methoden, die man kontrollieren will, Big-Data-Methoden, darauf ansetzen muss, auch Simulationen. Aber das ist etwas, womit sich zum Beispiel die IT-Sicherheitszentren beschäftigen. Ich finde, das ist genauso eine Hilfestellung, auch für die Fachleute, denn nicht jeder Fachmann in der IT, der Informatiker, überschaut die gesamte Big-Data-Ausführung und die Frage der Künstlichen Intelligenz.

Zweiter Punkt: Ich erlebe es immer wieder, dass Wissenschaftler, auch anerkannte, große Wissenschaftler, das Wort Künstliche Intelligenz in den Mund nehmen und dann eher im Feuilletonstil erzählen, dass jetzt unsere Intelligenz in Gefahr ist und die Maschinen uns ablösen usw. Auch Ihnen fallen sicher einige große Namen ein, auch von Leuten, die sehr bekannt sind, auch Physiker, die in Großbritannien sind, an renommierten Universitäten. Das ist hoch spannend, toll fürs Feuilleton und Weltuntergangsstimmung. Aber sie lenken ab von den Problemen, die gerade geschildert wurden, die ganz real sind.

Ich habe keine Angst vor lernenden Systemen, weil ich weiß, wie fehlerhaft und wie beschränkt sie zurzeit sind. Aber weil sie fehlerhaft und beschränkt sind, müssen wir diese Grenzen kennen. Computer, also lernende Systeme sind für mich eher wie Kinder, diese Kinderschuhe, die können Go spielen und verbrauchen da ein paar tausend Watt. Wir machen das mit 30 Watt – und wenn ich dem Ding ein Schachbrett hinstellen würde, müsste es wieder ewig lernen.

Aber die Frage ist: Wir müssen lernen, *wie* sie lernen, und dann werden wir bei lernenden Systemen feststellen, wie sie zu völligen – in Klammern: Wir wissen häufig nicht, *was* sie gelernt haben. Wenn Sie ein kleines Kind haben, sagen: Das ist ein Apfel, und irgendwann kann es zeichnen, dann malt es etwas, Sie gucken drauf und sagen: „Ja, das ist ein Apfel.“

Wenn ein System gelernt hat, Bilder zu erkennen, kann es sein, dass es gar nicht gelernt hat, das Pferd zu erkennen, sondern es kann nur unten ein Copyright erkannt haben und merkt am Copyright plötzlich: Ach, das muss ein Pferd sein. Da gibt es schöne Experimente, wo ein Pferd mit 100 Prozent erkannt wird und alle anderen Tiere nur mit 80 Prozent.

Anderes Beispiel: ein Übersetzungssystem, das als ersten Schritt erkennen soll, welche Sprache gesprochen wird; das ist ja wichtig bei Übersetzungen. Da kam ein junger Student oder Studentin zum Professor und sagte: „Das System ist toll. Es erkennt zu 100 Prozent die Sprache.“ Sagt der Professor: „Dann ist ein Fehler drin, da ist ein Problem.“ Schon mal gut, wir haben kluge Leute!

Die zweite Frage war: „Sag mal, in welcher Zeit erkennt das System die Sprache?“ Dann sagt er oder sie: „Unter einer Sekunde. Ganz schnell.“ – „Aha, das ist das zweite Problem, was du hast. Das kann auch nicht sein. Guck noch mal genauer hin.“

Dann kam der Student oder die Studentin und sagte: „Ja, bevor die Konversation anfängt.“ Dann sagt er: „Jetzt hast du aber ein Riesenproblem.“

Und was war? Das lernende System hat gesehen (es war eine Videoschaltung): amerikanische Klimaanlage, deutsche Klimaanlage. Das eine klappert, das andere nicht (ich sag jetzt nicht, welches), und dann hat der Computer sofort gewusst, welche Sprache.

Zu sehen, dass da Muster erkannt werden, worauf wir gar nicht achten, die wir nicht wahrnehmen würden, wird zum Footprint für die Sache. Und wie mache ich das? Mein System hat etwas gelernt und ich weiß es nicht. Bei einem Kind würde ich sagen: „Mal mal, erzähl mal, woran hast du es erkannt?“

Sie merken: viele Forschungsaufgaben. Was mich umtreibt: Ich glaube, dass da ein riesiges Potenzial in diesem System ist, aber die, die es anwenden und darüber reden, sollten wissen, in welchem Stadium das ist und wo die Grenzen sind. Wir brauchen Aufklärung. Bei Ihnen ist das klar, Sie sind im IT-Unternehmen und Sie verstehen etwas davon. Aber ich möchte auch, dass die anderen, die jetzt sagen: Wir müssen uns in das Deep Learning hineinbegeben, dass die Vorstände auch wissen, was das ist und worauf sie sich da einlassen.

Ich rede auch mit Leuten über autonomes Fahren. Da gibt es ja kluge Leute, die sagen: Moment mal, ich kann doch nicht jedes Auto selbst lernen lassen (in sicherheitsrelevanten Fragen) und mal fahren lassen, sondern ich müsste doch eigentlich das System lernen lassen, und dann müsste jedes Auto gleich sein und das Gelernte anwenden. Aber ich kann doch nicht – jedes Auto ist individuell. Weiß der Teufel, was das eine Auto gelernt hat! Woran erkennt es Fußgänger? Vielleicht ganz anders als das andere System.

Die Frage ist, dass man diese Grenzen der Technologie erkennt. Dann kann man nämlich an den Grenzen und Gefahren auch Lösungen machen, als dass wir eine Diskussion haben, die feuilletonartig ist. Es ist Aufgabe von Wissenschaft, den Anwendern von IT – und das sind alle Branchen und auch Politik – deutlicher klarzumachen, wo Grenzen, wo Chancen und wo Risiken sind.

Diese Debatte […] in der Gesellschaft, da muss Wissenschaft ran, und da müssen die Leute, und ich weiß, dass das immer heißt: Jetzt kommt der wieder und redet wieder so negativ. Machen Sie das nicht so. Das machen Sie nicht. Jetzt sehe ich immer die an, die es sich nicht so leicht machen. Die anderen sind ja draußen, die sind heute nicht hier.

Viele machen es sich so leicht, weil sie sagen: „Da bekomme ich einen Auftrag, da kann ich irgendeinem Unternehmen ein neues System aufsetzen; da freuen die sich.“ Diese klare Aufgabe, zu zeigen, wo die Grenzen dieser Technologie und wo die Risiken sind, das ist Aufgabe von Wissenschaft und auch von denen, die mit der Wirtschaft arbeiten. Ich sehe weniger die Gefahr bei den IT-Unternehmen, sondern bei denen, die Dinge herstellen, die unmittelbar beim Konsumenten ankommen, und das sind die Großen, die das Geschäft machen. Bei denen muss man diese Aufklärungsarbeit täglich leisten, damit sie ihre Systeme technisch nicht überschätzen.

[gleichzeitig, unverständlich]

Ingo Dachwitz

Facebook und Google sagen von sich, sie machen die Welt besser. Das ist deren Ziel, also was sagen Sie?

Wolf-Dieter Lukas

Diese Aussage haben schon viele in der Weltgeschichte gemacht. Jetzt können Sie sagen: Es gibt ein paar, die uns gefallen; ein paar haben uns nicht gefallen. Ich werde keine Vergleiche machen und will die beiden Firmen nicht werten und Ähnliches. Diese Debatte führe ich häufiger auch in Kalifornien; es ist eine Debatte, die den Glauben hat, dass mit der IT alle Probleme gelöst werden. Das kann sogar sein, aber die andere Fragestellung, dass es auch viele Probleme bringt, wird gar nicht betrachtet.

IT ist für mich kein Heilsbringer, sondern eine Methode, mit der wir sicher viele Probleme lösen können und bei der, wenn wir es richtig machen, möglichst wenige dadurch entstehen. Es kommt auf den Weg an. Die Sache selbst ist nicht positiv oder negativ. Das Potenzial ist riesig, aber wir müssen das, was der Gesellschaft nützlich ist – und das ist Aufgabe von Wissenschaft, Politik, Wirtschaft – immer wieder den Filter draufsetzen und richtig abbiegen. Manchmal muss man einen kleinen Weg gehen und auch einen Schritt zurück. Man darf sich auch mal irren.

Manfred Kloiber

Wir haben einen Gast in unserer Runde, bitte schön.

Andreas Raabe

Andreas Raabe von der DFG-Geschäftsstelle. Wir haben heute viel über die Verantwortung der IT-Wissenschaften und der Politik gehört. Herr Lukas und Herr Lengauer, mich würde interessieren, wie Sie die Rolle des interdisziplinären Diskurses hier sehen, über die Bedeutung der Bioinformatik hinaus, und welche anderen Fächer da insbesondere eine Rolle spielen könnten, sollten und wie da die Beteiligung sein könnte.

Thomas Lengauer

Ein interdisziplinärer Diskurs ist das A und O dabei. Wir haben sie heute eigentlich alle hier: Soziologie, Philosophie, Psychologie, Politik, Jura – wie bitte? – Theologie wäre mir jetzt nicht in den Sinn gekommen, aber das nehme ich gern dazu. Wir brauchen sie alle, denn wir wollen das Zusammenspiel zwischen der Technik und der Gesellschaft verstehen, und da spielt alles eine Rolle.

Wir hatte im Juli eine Leopoldina-Tagung mit dem Titel: „Die Digitalisierung und ihre Auswirkungen auf Mensch und Gesellschaft“. Da sind wir auf die kognitiven Konsequenzen, die IT-Assistenz auf das Individuum und Gruppen hat, eingegangen: Wie prägt sie meine Weltsicht? Wie moduliert sie meine Entscheidungen? Auch der Vertrauensbegriff wurde angesprochen: Kann man Algorithmen vertrauen? Wir haben den ganzen Tag darüber gesprochen, wie die Dynamik der Meinungsbildung und Entscheidungsfindung in Gruppen durch IT-Unterstützung beeinflusst wird. Da waren alle Disziplinen, die ich eben genannt habe, mit dabei. Auf der Ebene und nicht kleiner kann diese Diskussion geführt werden.

Harald Schöning

Da muss ich einhaken. Es ist ja schön, dass die Diskussion in diesen Zirkeln geführt wird, aber strahlt das in die Gesellschaft aus? Ich würde mir wünschen, dass man diese Themen mehr in der Öffentlichkeit diskutiert und nicht nur unter Wissenschaftlern.

Wolf-Dieter Lukas

Darf ich ein Beispiel dazu bringen? Zwei Aussagen: Die erste Aussage ist: Wir bauen eine Platt-

form lernende Systeme auf – da wird es Arbeitsgruppenleiter geben zum Thema Recht, Ethik und IT-Sicherheit. Aber wir haben gesagt, ihr drei setzt euch erst mal zusammen. Was wir nicht wollen (das ist uns schon ein paar Mal passiert), ist, dass es eine Versäulung gibt, denn Recht ist etwas, was sich auf die technischen Möglichkeiten und auf die Werte, die wir umsetzen wollen, beziehen muss. Das heißt, ich habe gesagt: Erst mal trefft ihr euch und betrachtet das zusammen.

In Klammern: Die fanden das auch gut und wären wahrscheinlich auch allein auf die Idee gekommen. Aber Sie wissen ja, manchmal ist da so eine Separation.

Aber jetzt: Eine Dame, die auch in der Leitung ist, ist Frau Ammich Quinn, ich kannte sie aus Tübingen, die sich mit Ethik beschäftigt. Ja, genau, sie ist Theologin. In dem Sinne haben wir die richtige Frau, und deswegen will ich Ihre Frage beantworten.

Was wir nicht brauchen, sind Leute, die miteinander Diskurs führen und dann nicht rausgehen. Die Frau ist hingegangen, in der Sicherheitsforschung, da haben wir ja solche Fragen. Da war die Frage: Wie machen wir das mit den Bodyscannern? Die Nacktscanner kennen Sie ja noch, nicht? Dann haben wir gesagt: Die Politik hat entschieden, ein Herr Schäuble und Frau Schavan haben gesagt: Wir wollen keine Nacktscanner, wir wollen, dass kein Mensch sich die Bilder anschaut. Liebe Leute, Industrie, wenn ihr was liefert, muss es Daumen hoch und Daumen runter sein. Das soll die Maschine machen, und wenn der Daumen runter ist, dann muss der Mensch das machen, dann muss man sehen: Wie gehe ich mit dem Fall um? Dann sind wir wieder im normalen Polizeirecht etc., aber die Frage ist: Die Maschine soll nicht Bilder zeigen und Leute sollen sich nicht die Menschen anschauen.

So, und dann hat Frau Ammicht Quinn – und das fand ich toll – ein Unternehmen, das so etwas entwickelt hat, beraten und hat gesagt: „Geht, geht nicht. Geht, geht nicht. Da habt ihr Probleme.“ Die Firma hat sich so bedankt und hat gesagt: Wir hätten tausend Fehler gemacht und hätten endlos Probleme gehabt. Übrigens: Die Scanner von dieser Firma stehen jetzt an den Flughäfen und werden gegen andere ausgetauscht.

Sie hat sie in vielen Dingen beraten, auch das Verfahren, wenn Sie das durchlesen, Freiwilligkeit, auch die Frage: Wie steht man da? Können auch Behinderte mit hinein? Auch das Thema Mann–Frau war so ein Thema. Da gibt es übrigens einen Knopf; wenn er es nicht weiß, schreibt er: neutral, weiß nicht.

Sie hat sie also in vielen Dingen beraten, und das erwarte ich auch von Wissenschaft, wenn ich etwas weiß, dass ich dann auf die Wirtschaft zugehe und denen ins Gewissen rede. Die lassen sich da nämlich ganz gern ins Gewissen reden, denn manchmal ist dann das Produkt besser, weil es von der Gesellschaft angenommen wird. Das ist eine Holschuld bei Ihnen, aber auch eine Bringschuld von der Wissenschaft.

Ich habe jetzt ein Beispiel genommen, was mit IT viel zu tun hat. Es war Mustererkennung, und am Ende war die Software entscheidend und nicht die Sensoren.

Thomas Lengauer

Sie haben gesagt, das sollten Wissenschaftler nicht nur unter sich machen. Die Tagung war nicht für Wissenschaftler. Es waren 200 Leute in dem Raum, aus der Wirtschaft, aus der Politik, Studenten, sogar Bürger, ohne irgendwelche Affiliation. Die Tagung war in Deutsch, bis auf einen Vortrag oder zwei. Die Vorträge sind alle im Internet, Sie können sie sich ansehen.

Wo wir noch ein bisschen schwach auf der Brust sind, das ist die Hit Rate für die Leopoldina-Website; die könnten wir noch ein bisschen hochdrehen. Wenn die alle kennen, können sich viele Leute das ansehen.

Bärbel Friedrich

Professor Schöning, Sie repräsentieren ein Software-Unternehmen. Wären Sie auch ein Ansprechpartner für unsere Aktion? Denn wir haben erst die Universitäten angesprochen, die Großforschungseinrichtungen, und wir diskutieren in unserem Ausschuss, ob wir nicht auch die Industrie ansprechen sollten, um in diesen Zirkeln zu diskutieren.

Harald Schöning

Oh, da wäre nicht nur ich interessiert, sondern sicher auch viele Kollegen, die ich aus der Industrie kenne.

Ingo Dachwitz

Ich kann das schwer greifen, aber mein Gefühl wäre, bei all dem warmen Regen, der jetzt auf die IT-Wissenschaft fällt, noch mal ein bisschen Wasser in den Wein schütten zu wollen, weil die Disparität zwischen der Verantwortung, die wir haben, und der Praxis sowohl in der universitären Ausbildung als auch der Forschung doch riesengroß ist. Wenn man allgemein darüber spricht, über die Verantwortung, dann stimmt das alles. Aber ich kenne keine Informatik- oder IT-Studenten, die in ihrem Studium damit konfrontiert werden, wie ihre Arbeit später tatsächlich wirkt oder die das überhaupt auseinandersetzen müssen. Wir haben von Frau Simon gehört, wie wichtig es ist, ethische Fragen schon im Designprozess zu implementieren. Werden solche Konzepte an den Universitäten in der IT-Wissenschaft gelehrt? Ich glaube das nicht.

Ein weiterer Punkt: Wir haben hier mehrfach die Ökonomisierung des Wissenschaftsbetriebes angesprochen. Auch das ist wieder eine Frage der Förderung. Kaum eine Wissenschaft ist so auf Drittmittelförderung und Partnerschaften mit wirtschaftlichen Partnern angewiesen wie die IT-Wissenschaft. Rückbau des akademischen Mittelbaus usw., das sind alles Themen, die eine Rolle spielen müssten, wenn wir über die ethische Verantwortung sprechen.

Manfred Kloiber

Ich glaube, Herr Lengauer, die Frage war an Sie gerichtet. Sie haben eben beschrieben, dass in der IT ethische Fragen oft wenig Einfluss haben. Ist es so, dass in der Institution Universität, Hochschule da der erste Schritt gemacht wurde und jetzt zumindest rudimentär die Studenten ausgebildet werden, diese Fragen mitzudenken?

Thomas Lengauer

Ich bin leider nicht sicher. Aber ich glaube, bei uns an der Uni des Saarlandes gibt es so eine Vorlesung, es gibt auch gute Internetangebote und einen sehr guten Vorlesungszyklus aus Harvard, der bei uns propagiert wird.

Ich bin wirklich nicht sicher. Denn ich bin Bioinformatiker, wir haben unser eigenes Curriculum. Aber ich glaube, zumindest in Saarbrücken gibt es so etwas, wohl mehr auf dem Wahlpflichtfachniveau, aber es ist definitiv ausbaufähig. Für die hundert Universitäten in Deutschland kann ich natürlich nicht sprechen.

Aber so etwas wäre auch ein Ausfluss aus Akademie-Tätigkeit, da eine entsprechende Kommunikationsinitiative zu machen und das Bewusstsein der Leute zu wecken.

Manfred Kloiber

Herr Lukas, wäre es nicht auch für die Forschungseinrichtungen, die in diesem Bereich unterwegs sind, wo viel Drittmittelforschung und viel Forschung unmittelbar für die Industrie passiert, viel stärker als in anderen Bereichen – dass

man als ersten Schritt verlangt, dass diese Institutionen, die Forscher, wenn sie nicht sagen können, was sie machen und was sie lassen, zumindest ihre tatsächliche Motivation offenlegen und sagen: „Okay, das sind die Werte, auf die ich achten werde“, so etwas wie ein Code of Conduct für jede Institution geschaffen wird, damit man weiß, woran man ist?

Wolf-Dieter Lukas

Das stelle ich mir so nicht vor. Denn zwei Drittel der Forschungsmittel sind Mittel der Wirtschaft, wo die Wirtschaft selbst forscht. Dann gibt es das andere Drittel, wo es öffentliche Mittel gibt. Dazu gibt es die DFG, die Mittel ausgibt. Wir geben direkte Projektfördermittel und wir fördern Institutionen.

Da, wo wir direkt Geld geben, wenn wir Projekte bewilligen, bin ich zu jeder Frage des Abwägens nicht nur willens, sondern auch verpflichtet. Wir sind ein Tendenzbetrieb, so wie die katholische Kirche und andere. Wir haben eine Tendenz, wenn wir etwas tun. Aber die meisten, großen Mittel sind institutionelle Mittel. Und da sollte sich Wissenschaft selbst organisieren. Ich bin nicht dafür, dass der Staat es tut, sondern dass sie sich organisieren und nicht nur innerhalb der Fakultät, sondern zwischen den Fakultäten darüber beraten und diskutieren, was sie tun. Diese Reflexion muss Wissenschaft selbst machen.

Ich sage noch mal: Freiheit und Verantwortung. Ich möchte, dass die Wissenschaft frei ist und dass sie ihre Verantwortung wahrnimmt.

Noch zwei Bemerkungen zu der Verantwortung, denn es hieß immer die Verantwortung des einzelnen Wissenschaftlers. Erstens: Der einzelne Wissenschaftler ist frei. Zweitens: Wissenschaft muss sich – und tut es auch – organisieren in Akademien und anderes und muss dort Regeln aufstellen, so wie man das auch tut. Was ist ein guter Kaufmann, was ist ein guter Wissenschaftler? Was sind die Werte, auf denen wir uns basieren?

Zwei Bemerkungen: Erstens kann Nichtstun auch das Falsche sein, also nach dem Motto: Ich bewege mich nicht, also bin ich richtig. Nein, völlig falsch. Das Nichtstun kann unmoralisch sein. So nach dem Motto: Ich mache nichts, ich greife nicht ein.

Der zweite Punkt ist nach dem Motto: Ich bin der Wissenschaftler und ich habe abzuwägen – das sehe ich so nicht. In einer Demokratie muss ich mich den anderen stellen, der Gesellschaft. Das kann die Fakultät sein, das kann die Universität sein, das kann die Gemeinschaft einer Akademie sein, das kann auch mal das Parlament sein.

Es gibt viele, die immer sagen: Der Einzelne ist verantwortlich. Klar, wenn wir einen Staat haben, der nicht mehr funktioniert, wenn wir eine Diktatur oder Ähnliches haben, dann ist es so, dass am Ende das Individuum alleine ist und entscheiden muss. Ich glaube, dass wir diese Gesellschaft nicht haben.

Deshalb zwei Dinge: Ich erwarte, dass sie auch etwas wagen und sagen: Wir tun es, auch wenn wir Risiken eingehen. Aber dass sie immer wieder im Konzert der Wissenschaften miteinander diskutieren und sich selber beobachten, und dass der Staat nur da eingreift – erstens muss er selbst richtig handeln. Sie müssen mich daran messen, wo wir direkt Geld ausgeben, aber wenn wir Ihnen institutionelle Förderung geben, dann müssen Sie gemessen werden von Ihren Wissenschaftskollegen, und zwar aller Fakultäten an der Universität oder einer Forschungseinrichtung. So nach dem Motto: der Staat als Oberaufseher, das möchte ich überhaupt nicht. Der Staat muss aber helfen, dass diese Strukturen entstehen. Mit „Staat“ meine ich nicht nur den Bund, sondern die Länder müssen helfen, die Strukturen zu

schaffen, aber am Ende muss es Wissenschaft selbst tun. Nur es darf nicht immer so sein, dass man sagt: Wir verändern nichts und wir entscheiden nichts. Das Nichtstun kann der völlig falsche Weg sein.

Manfred Kloiber

Das war fast schon ein Schlusswort. Ich denke, was heute klargeworden ist und auch die Veranstaltung und die Aktivitäten von DFG und Leopoldina beweisen es: Der Weg der Selbstreflexion und des Drübernachdenkens ist beschritten. Da ist allerdings noch vieles zu tun, viele Fragen sind noch unklar. Das hat Herr Lengauer mehrfach beschrieben. Dafür ist die Diskussion unter den Wissenschaftlern interdisziplinär der richtige Weg. Heute war so ein Tag, wo wir das getan haben.

Ich danke Ihnen recht herzlich für die Diskussion, ich danke Ihnen fürs Zuhören und Durchhalten. Als Belohnung gibt es jetzt von der TU Darmstadt einen kleinen Umtrunk, zu dem Sie alle herzlich eingeladen sind. Herzlichen Dank.