H 7625

# FIfF-Kommunikation

Zeitschrift für Informatik und Gesellschaft

35. Jahrgang 2018 Einzelpreis: 7 EUR **3/2018 – September 2018**

## Informatik und Gesellschaft


## Staatstrojaner

ISSN 0938-3476

• 40 Jahre IuG Bremen • BigBrotherAwards 2018 • Netzpolitik.org •

FIfF Kommunikation

Zeitschrift für Informatik und Gesellschaft



# Inhalt

Ausgabe 3/2018

**Titelbild:** Die Prozession des Trojanischen Pferdes nach Troja, Detail, Giovanni Domenico Tiepolo, 18. Jahrhundert
*https://de.wikipedia.org/wiki/Danaergeschenk#/media/File:The_Procession_of_the_Trojan_Horse_in_Troy_by_Giovanni_Domenico_Tiepolo.jpg*
Urheber: Giovanni Domenico Tiepolo

# Editorial

Wir leben in politisch bewegten Zeiten. Rechtspopulisten sind auch in Deutschland im Aufwind, nachdem sie in anderen europäischen Ländern bereits an der Regierung beteiligt sind. Und es tobt ein Kampf um die Deutungshoheit: Gerade haben wir die Ausschreitungen rechtsgerichteter Demonstranten in Chemnitz erlebt. Der Präsident des Verfassungsschutzes bezweifelt öffentlich – im Gegensatz zu vielen Medien –, dass es zu den berichteten Hetzjagden auf Migranten gekommen ist, und stellt sich damit offen gegen die Bundeskanzlerin. Es mag schwer sein, die tatsächlichen Geschehnisse in Chemnitz aus der Ferne im Detail zu beurteilen – es wäre aber – nicht zuletzt angesichts der Ereignisse um die Terrorgruppe *Nationalsozialistischer Untergrund* (NSU) – nicht das erste Mal, dass der Verfassungsschutz den rechten politischen Flügel vernachlässigt und verharmlost.

Gleichzeitig werden in vielen Bundesländern gerade die Polizeigesetze novelliert – hin zu Elementen eines autoritären Präventionsstaats. Unklar ist, ob hier versucht wird, den Rechtspopulisten durch eine besonders repressive Politik den Wind aus den Segeln zu nehmen. Erfreulich, dass so viele Menschen wie schon lange nicht mehr für den Erhalt der Grundrechte auf die Straße gehen. Doch auch hier geht es letztlich um die Deutungshoheit: Während die verantwortlichen PolitikerInnen erklären, die neuen Befugnisse für die Polizei seien angemessen und notwendig, halten JuristInnen bürgerrechtlicher Organisationen sie für verfassungswidrig.

Die Polizeigesetze sind damit auch Thema in dieser Ausgabe der *FIfF-Kommunikation*. Nachdem sich in der letzten Ausgabe Dagmar Boedicker das bayerische Polizei-Aufgabengesetz vorgenommen hatte, befassen sich *Anja Heinrich* und *Stefan Hügel* in dieser Ausgabe ausführlich mit den Risiken und der technischen und rechtlichen Bewertung der Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung mit besonderem Augenmerk auf das niedersächsische Gesetz über die öffentliche Sicherheit und Ordnung.

Doch es gibt auch andere Themen, denen wir unsere Aufmerksamkeit widmen müssen. *Hans-Jörg Kreowski* befasst sich in seinem Beitrag mit autonomen Systemen. Er geht der Frage nach, „… was es mit der Autonomie in technischen Systemen auf sich hat, worum es dabei überhaupt geht, wo die Schwierigkeiten liegen, wo die Gefahren dieser Entwicklung lauern und ob technische Autonomie schon richtig verstanden und durchdacht ist." Er ist dabei skeptisch: „Was man aber nicht versteht, lässt sich auch nicht nachbauen".

*Wolfgang Hofkirchner* – von dem weiter unten noch die Rede sein wird – skizziert eine Informatik für eine globale nachhaltige Informationsgesellschaft. Er stellt fest, „… dass Information die Voraussetzung dafür darstellt, dass die gestiegene Komplexität der Interaktion der voneinander abhängig gewordenen sozialen Systeme in Sicht genommen und wieder in den Griff bekommen werden kann." Dafür schlägt er vor, die Informatik so zu gestalten, „… dass Anwendungen die Generierung solcher Information (Wissen, Weisheit) erleichtern und befördern, die für die Transformation gebraucht wird."

Ausgehend von der Studie einer Unternehmensberatung, die Empfehlungen für die Förderung von KI-Start-Ups formuliert, setzt sich *Christoph Marischka* mit der *Cyber-Valley-Initiative* in Stuttgart und Tübingen und deren militärischen Verbindungen auseinander. Er kritisiert dabei unter anderem „eine Wissenschaftskommunikation, die die Öffentlichkeit für dumm verkauft."

Am 26. August 2018 verstarb Jürgen Friedrich, der an der Universität Bremen die Professur für Informatik und Gesellschaft inne hatte und langjähriges FIfF-Mitglied war. Aus diesem traurigen Anlass zeichnet *Ralf E. Streibl* die Geschichte des Fachgebiets an der Universität Bremen nach. Wir verbinden das mit einem Nachruf, den *Wolfgang Coy* verfasst hat.

*Wolfgang Coy* ist auch die Retrospektive in dieser Ausgabe gewidmet: *Weder vollständig noch widerspruchsfrei*.

Auch in diesem Heft sind einige Beiträge enthalten, die wir der Kooperation mit *netzpolitik.org* verdanken: *Constanze Kurz* interviewt den Rechtsanwalt Ulrich Schellenberg zur Überwachung am Bahnhof Berlin Südkreuz, *Wiebke Denkena* befasst sich mit dem Tracking anhand von Touch-Gesten, *Alexander Fanta* und *Constanze Kurz* nehmen sich die KI-Strategie der Bundesregierung vor, *Julia Krüger* betrachtet Algorithmen und Künstliche Intelligenz und die Defizite der öffentlichen Debatte, *Felix Sühlmann-Faul* behandelt die Folgen unserer Liebe zu Smartphones und *Tomas Rudl* die Zerstörung unserer Demokratie durch unregulierte soziale Netzwerke, wie sie ein Ausschuss des britischen Parlaments in einem Bericht festgestellt hat.

Am 20. April 2018 wurden in Bielefeld die BigBrotherAwards vergeben – diesmal im Bielefelder Stadttheater. Wir berichten wie immer ausführlich davon und drucken die Laudationes zu Smart Cities von *Rena Tangens*, für die Cevisio GmbH und ihre Quartiermanagement-Software für Flüchtlingsunterkünfte von *Thilo Weichert* und für die hessischen Landtagsfraktionen von CDU und Bündnis90/Die Grünen für das Verfassungsschutzgesetz und die Novellierung des hessischen Polizeigesetzes von *Rolf Gössner*.

Bekanntlich hat das FIfF einen Beirat gebildet, in den wir Persönlichkeiten einladen, die das Fachgebiet *Informatik und Gesellschaft* prägen und dort im Sinne des FIfF wirken. Wir freuen uns sehr, dass Professor Dr. Wolfgang Hofkirchner (Wien) und Professor Dr. Jochen Koubek (Bayreuth) unsere Einladung in den Beirat angenommen haben. Mit Wolfgang Hofkirchner besteht seit einiger Zeit eine Kooperation im Umfeld der International Society for the Study of Information (IS4SI) und dem Arbeitskreis Emergente Systeme, Information und Gesellschaft der Leibniz-Sozietät, Jochen Koubek hat bei seiner Mitarbeit in der Jury des Weizenbaum-Studienpreises wichtige Impulse gegeben.

Wir wünschen unseren Leserinnen und Lesern eine interessante und anregende Lektüre – und viele neue Erkenntnisse und Einsichten.

*Stefan Hügel*
*für die Redaktion*

# Chemnitz und anderswo


Liebe Leserinnen und Leser, liebe Mitglieder des FIfF,

immer häufiger machten Anfang der 1990er Jahre Übergriffe auf Asylsuchende Schlagzeilen. Hoyerswerda, Mölln, Rostock-Lichtenhagen, später Solingen, wurden zu deren Symbolen. Doch statt einer Solidarisierung mit Menschen, die in Deutschland Schutz vor politischer Verfolgung suchten, verstärkte sich in breiten Schichten die ausländerfeindliche Stimmung. Auch in sonst seriösen Publikationen war von einer „Asylantenflut" die Rede.

Am 26. Mai 1993 konnten die rechtsradikalen Gewalttäter die Früchte ihrer Aktivtäten ernten: Es stand eine Änderung des Grundgesetzes auf der Tagesordnung des Deutschen Bundestages. Das bisher uneingeschränkte Grundrecht auf Asyl wich einer erheblich eingeschränkten Fassung. Auch wenn es vielleicht nicht beabsichtigt war: Durch die Änderung des Grundgesetzes hatte man Nazis und Rassisten signalisiert, dass sich ausländerfeindliche Gewalt politisch auszahlt.

Liest man heute das Plenarprotokoll[1] der damaligen Sitzung, findet man bekannte Muster. Rechte Gewalttaten waren die Begründung, die Rechte der Opfer weiter zu beschneiden. Nicht die Morde an ausländischen Mitbürgerinnen und Mitbürgern waren das Problem, vielmehr wurden die Proteste gegen die Grundgesetzänderung in Bonn während der Sitzung des Bundestags als „Anschlag auf die Demokratie" bezeichnet.

Viele Jahre später, 2015. Eine große Zahl von Flüchtlingen kommt in die Europäische Union. Bundeskanzlerin Angela Merkel ist überzeugt: Unser Land ist stark genug, um diesen Menschen Schutz zu bieten – „Wir schaffen das." Obwohl sie in der Folge wohl für die restriktivste Ausländerpolitik in der bundesdeutschen Geschichte verantwortlich ist – eine Ausländerpolitik, die nicht einmal davor zurückschreckt, Menschen in Kriegsgebiete wie Afghanistan abzuschieben – wird sie aufgrund dieses einen Satzes massiv von Rechtspopulisten angefeindet. Die AfD, die als neoliberale, europakritische Partei gestartet war, entwickelt sich zur rechtspopulistischen Partei, wird in Teilen offen rechtsradikal. Gleichzeitig verroht die öffentliche Debatte zunehmend: Zu Tausenden ertrinken fliehende Menschen im Mittelmeer,[2] und in Deutschland diskutieren wir darüber, ob es richtig ist, ihnen zu helfen – oder nicht[3]. Mutige Menschen, die den Fliehenden das Leben retten wollen, werden als „Schlepper" vor Gericht gestellt.[4]

Gleichzeitig kippt die politische Debatte nach rechts. Auch Mitglieder von politisch liberalen Parteien verharmlosen rechte Positionen; rechts und links werden gleichgesetzt; wird von rechter Gewalt berichtet, folgt reflexartig der Hinweis, dass es schließlich auch linke Gewalt gebe – angesichts von Szenen, in denen Menschen durch Chemnitz gejagt werden.[5] Sebastian Czaja, Berliner Politiker der FDP, schreibt: „Antifaschisten sind auch Faschisten"[6] – ein Satz, der angesichts von WiderstandskämpferInnen in Nazi-Deutschland, die für ihren Mut mit dem Leben bezahlen mussten (nicht nur) seinem früheren Geschichtslehrer Tränen in die Augen treiben müsste. Bei „linken" Demonstrationen ist die Polizei ausgerüstet, als ziehe sie in einen Bürgerkrieg[7], geht es um „rechte" Demonstranten, wirkt sie plötzlich merkwürdig hilflos. Und die Verantwortlichen rechtfertigen diese politische Schlagseite. Das seien „ganz normale BürgerInnen" sagen sie – was sofort empört zurückgewiesen wird. Aber vielleicht ist genau das das Problem: Vielleicht sind es einfach „ganz normale BürgerInnen" – so wie 1933 auch.[8]

Manche behaupten, wir befänden uns heute bereits wieder in einer Situation wie 1930. Die NSDAP erreichte – nachdem sie bei den Reichstagswahlen 1928 auf 2,6 % abgestürzt war – bei Landtagswahlen 1929-1930 wieder über 10 %, überdurchschnittliche 14,4 % in Sachsen.[9] Was würde denn ein Szenario bedeuten, bei dem wir 1930 auf das aktuelle Jahr 2018 projizieren?

Es würde bedeuten: in drei Jahren (2021) übernähme eine rechtspopulistische oder rechtsradikale Partei die Macht – möglicherweise gefördert durch die gemäßigten Parteien, die sich davon erhoffen, dass die Rechtspopulisten dadurch eingebunden und ruhiggestellt werden[10]. Statt Olympischer Spiele wie 1936 in Berlin, hat Deutschland gute Chancen, 2024 die Fußball-Europameisterschaft auszurichten – diese Veranstaltung könnte genutzt werden, Propaganda zu betreiben und Deutschland in einem *guten* Licht erscheinen zu lassen. 2027 käme es dann zu einem Krieg, der bis 2033 andauert und mit dem Zusammenbruch Deutschlands endet. Nach Besatzungszeit und Staatsneugründung könnten wir – falls wir es überlebt haben – von heute an in 20 Jahren wieder mit einem demokratischen Staatswesen rechnen. Wie alt werdet Ihr in 20 Jahren sein?

Ein solches Szenario sei kompletter Blödsinn, mögen jetzt manche Leserinnen und Leser denken. Wirklich? Was hätten die Menschen 1930 auf so eine Hypothese geantwortet?

Die Sommerzeit wird jetzt wohl wieder abgeschafft. 1989 erschien ein Buch des Psychologen Dietrich Dörner[11], in dem dieser das Verhalten von Menschen in komplexen Situationen untersuchte. Eine Kernaussage, die mir im Gedächtnis haften geblieben ist: Menschen, die mit der Komplexität einer Aufgabe völlig überfordert sind, konzentrieren sich auf überschaubare Dinge, die sie zu lösen imstande sind. Auch wenn um sie herum alles zusammenbricht: Sie lösen dann akribisch genau dieses Problem.

Und was[12] hat das jetzt mit der Sommerzeit zu tun?

Mit FIfFigen Grüßen

*Stefan Hügel*

## Anmerkungen

1 http://dip21.bundestag.de/dip21/btp/12/12160.pdf
2 https://de.wikipedia.org/wiki/Flüchtlingskrise_in_Europa_ab_2015
3 https://www.zeit.de/2018/29/seenotrettung-fluechtlinge-privat-mittelmeer-pro-contra
4 http://www.spiegel.de/politik/ausland/griechenland-fluechtlingshelferin-von-der-heldin-zur-verdaechtigen-a-1225920.html, https://www.zeit.de/politik/ausland/2018-07/illegale-migration-italien-seenotrettung-ngos-unterstuetzung-verdacht, https://www.zeit.de/gesellschaft/zeitgeschehen/2018-07/rettungsschiff-lifeline-kapitaen-claus-peter-reisch-kaution-malta
5 Irritationen löste der Präsident des Bundesverfassungsschutzes, Hans-Georg Maaßen, aus, als er behauptete, die Medienberichte über Hetzjagden in Chemnitz seien falsch. Kommentatoren (http://www.tagesschau.de/kommentar/maassen-chemnitz-107.html) sehen ihn deswegen als „Kronzeugen der AfD". Bereits zuvor war Maaßen durch AfD-Nähe aufgefallen (http://www.spiegel.de/politik/deutschland/afd-und-verfassungsschutz-innenministerium-bestaetigt-treffen-von-maassen-mit-petry-a-1222668.html). Spekulationen gehen dahin, dass Maaßen auf Anweisung von Bundesheimatminister Seehofer gehandelt habe (http://www.spiegel.de/politik/deutschland/hans-georg-maassen-hat-horst-seehofer-ihn-zum-bild-interview-gedraengt-a-1227156.html)
6 https://twitter.com/SebCzaja/status/1034374729493356544
7 https://twitter.com/RaulZelik/status/1034359973822820352
8 Vgl. z. B. Goldhagen DJ (1996) Hitlers willige Vollstrecker. Ganz gewöhnliche Deutsche und der Holocaust. Berlin: Siedler-Verlag oder https://daserste.ndr.de/panorama/archiv/2001/Holocaust-Die-Luege-von-ahnungslosen-Deutschen,erste7664.html
9 https://de.wikipedia.org/wiki/Nationalsozialistische_Deutsche_Arbeiterpartei
10 https://de.wikipedia.org/wiki/Franz_von_Papen
11 Dörner D (1989) Die Logik des Mißlingens: Strategisches Denken in komplexen Situationen. Reinbek bei Hamburg: Rowohlt.
12 EU-Kommission will Zeitumstellung abschaffen, https://www.zeit.de/wissen/gesundheit/2018-08/eu-kommissionspraesident-will-zeitumstellung-abschaffen; „Man muss ständig nerven, dann klappt es irgendwann", https://www.zeit.de/politik/deutschland/2018-08/zeitumstellung-herbert-reul-eu-parlament-abgeordneter-abschaffung; Angela Merkel befürwortet Abschaffung der Zeitumstellung, https://www.zeit.de/politik/deutschland/2018-08/sommerzeit-abschaffung-zeitumstellung-angela-merkel-zustimmung

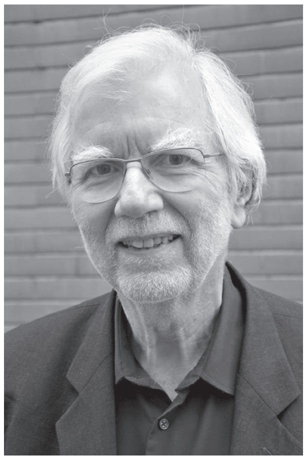


**Wolfgang Coy**

# Trauer um Jürgen Friedrich

## * 1942 † 2018

Jürgen Friedrich ist tot.



Der ehemalige Professor der Universität Bremen baute im Fachbereich Mathematik/Informatik das Lehr- und Forschungsgebiet *Informatik und Gesellschaft* in den achtziger Jahren des vergangenen Jahrhunderts auf. Seine 1986 besetzte universitäre Professur war die erste in diesem Bereich der deutschsprachigen Informatik. Zuvor hatte er von 1976 an eine einschlägige Forschungsgruppe an der Universität Dortmund als eigenständiger wissenschaftlicher Mitarbeiter betreut.

Nach dem Studium der Nachrichtentechnik und Technischen Informatik an der RWTH Aachen studierte Jürgen Friedrich Sozialwissenschaften und Ökonomie an der Freien Universität Berlin und promovierte dort 1979 mit dem Thema *Soziologie und Kybernetik*, womit sich seine Arbeitsinteressen von der Technik zu ihren gesellschaftlichen Wirkungen und Folgen verschoben. Ein Schwerpunkt seiner Interessen lag auf der Veränderung der Arbeitssituationen unter dem Einfluss digitaler Technologie, insbesondere auf den Anforderungen an konkrete Arbeitsplätze, soweit diese durch die Rechentechnik und Datenverarbeitung verändert oder gar aufgelöst wurden (*Computergestützte Gruppenarbeit* CSCW).

Im Fortgang seiner Arbeit war er Gründungsmitglied des Technologiezentrums Informatik (TZI) der Universität Bremen, dessen späterer Sprecher er vorübergehend wurde. 1997 wurde er zum Vorsitzenden der Gründungskommission für den hochschulübergreifenden internationalen Studiengang Digitale Medien bestimmt. Von 2001 bis 2012 war er Mitglied im Vorstand des *Zentrums für Multimedia in der Lehre* der Universität Bremen.

Nach dem Ende seiner Lehrtätigkeit in Bremen hielt er Vorlesungen in China – ab 2004 als Gastprofessor an der Technischen Universität Guangdong und seit 2017 auch als Gastprofessor an der Tongji-Universität in Shanghai.

Prof. Dr. Friedrich war treibende Kraft und einer der vier Herausgeber des ersten deutschsprachigen Lehrbuchs *Informatik und Gesellschaft* (1995).

Jürgen Friedrich starb am 26. August 2018 an den Folgen eines häuslichen Unfalls.

# ~ Bits & Bäume ~

## Die Konferenz für Digitalisierung und Nachhaltigkeit
## 17.–18. November 2018

**Ort: Technische Universität Berlin, Straße des 17. Juni 135, 10623 Berlin**

Wir bringen Communities zusammen!

In den letzten Jahrzehnten sind gesellschaftsverändernde Bewegungen gewachsen, die ihrer jeweils eigenen Utopie folgen: Sie kämpfen dafür, die Natur und unsere Lebensgrundlagen zu erhalten, für faire Arbeitsbedingungen ohne Ausbeutung, für eine Eindämmung der Macht von Konzernen und gegen die Zerstörung des Planeten. Sie setzen sich ein für demokratische Teilhabe, für nachhaltige Produktions- und Konsumweisen, für gerechten Handel zwischen globalem Süden und Norden und für verbindliche Regeln für die Wirtschaft im Sinne dieser Ziele. Andere Communities arbeiten konkret daran, die Digitalisierung so zu gestalten, dass Bürgerrechte, Schutz der Privatsphäre, Datenschutz, Souveränität und Demokratie für eine offene Gesellschaft gewahrt sind. Sie stehen auf für einen freien Zugang zum Wissen der Mächtigen, für eine Kultur des Miteinander-Teilens, für eine überwachungsfreie digitale Welt, für flache Hierarchien, globale Vernetzung und Dezentralität, für Selbstbestimmung und Menschenrechte angesichts eines Zeitalters der Künstlichen Intelligenz und der Übermacht globaler Internet-Monopole.

Bislang agieren diese Bewegungen der Umwelt-AktivistInnen und digitalen MenschenrechtlerInnen oft nebeneinander. Sie bieten Lösungsansätze und Ideen für ihre jeweils eigenen Themen, die inzwischen nicht nur Politik, Zivilgesellschaft, Wirtschaft, sondern sogar fast jeden Haushalt erreicht haben. Beide wollen die Welt verstehen, aber vor allem aktiv gestalten. Sie sehen, dass wesentliche Veränderungen für ein *gutes Leben* sowie eine gerechte und zukunftsfähige Gesellschaft nötig sind. Doch eine ökologische, soziale und ökonomische Nachhaltigkeit kann nur gemeinsam gelingen – dafür müssen diese Communities zusammenkommen, voneinander lernen, die Gemeinsamkeiten ihrer Utopien erkennen und diese mit neuer Wucht umsetzen!

Wie also kann die Digitalisierung eine Transformation hin zu einer nachhaltigen Gesellschaft unterstützen? Wie kann Nachhaltigkeitsdenken die Techie-Szene inspirieren, so dass die Digitalisierung langfristig Bürgerrechte und individuelle Freiheiten garantiert? Wie können beispielsweise erneuerbarer Strom und intelligente Netze mit vereintem Wissen weiterentwickelt werden? Welche Rolle spielen die drei Facetten der Nachhaltigkeit für stabile Tech-Communities? Welche ökologischen Chancen stecken in digitalen Anwendungen etwa für Klima- und Ressourcenschutz? Welche Arten von Digitalisierung stehen diesen Zielen entgegen oder sind sogar grob kontraproduktiv? Wie kann die digitale Gesellschaft demokratisch und gerecht gestaltet und zugleich darauf ausgerichtet sein, auf friedvolle Weise die Grundlagen unseres Lebens auf diesem Planeten zu bewahren?

Unter diesen Leitfragen steht *Bits & Bäume* als eine offene Vernetzungskonferenz – für neue Perspektiven auf eine Digitalisierung mit Nachhaltigkeit! Wir wollen gegenseitigen Austausch, wir brauchen aktive Vernetzung.

Dafür wollen wir

- unterschiedliche Szenen, Akteure und Organisationen in die Diskussion bringen,
- Schnittstellen zwischen Nachhaltigkeitsthemen und einer umsichtigen Digitalisierung herausarbeiten,
- visionäre Lösungen finden und mit gemeinsamer Vehemenz umsetzen.

Neben Vorträgen wird es Raum geben für Diskussionsrunden sowie für die Planung von Projekten und Kampagnen, die die unterschiedlichen Communities verbinden: Hands-on-Workshops, Aktivisten-Infotische, Sofas oder Hackathons. *Bits & Bäume* soll politisieren und den Auftakt geben für gemeinsame Positionen zu einer nachhaltigen Digitalisierung und wider demokratiefeindliche Trends. Zwei Konferenztage geben Anstoß für intensiven Austausch und politische Aktivitäten. Neben Akteuren aus zivilgesellschaftlichen Organisationen richten wir uns auch ausdrücklich an die interessierte Öffentlichkeit.

*Bits & Bäume* wird organisiert von:

- Bund für Umwelt und Naturschutz Deutschland (BUND)
- Brot für die Welt
- Chaos Computer Club (CCC)
- Deutscher Naturschutz Ring (DNR)
- Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF)
- Germanwatch
- Institut für ökologische Wirtschaftsforschung (iöw)
- Konzeptwerk Neue Ökonomie
- Open Knowledge Foundation Deutschland (OKF)
- PowerShift
- Technische Universität Berlin, Fachgebiet Sozial-ökologische Transformation (TU-Berlin)

Medienpartner:

- Netzpolitik.org

Die Veranstaltungsplanung und -organisation wird Nachhaltigkeitskriterien entsprechen: Wir achten bei der Nutzung und Bereitstellung digitaler und analoger Infrastrukturen auf Ressourcenschonung, Datenschutz und Gemeinwohlorientierung gleichermaßen und stellen unsere Erfahrungen und Materialien offen zur Verfügung.

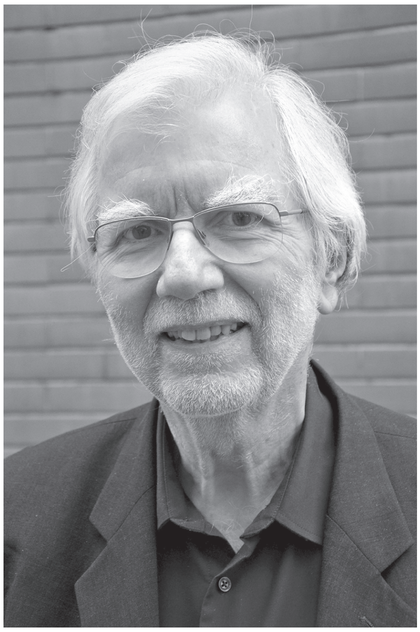
**Ralf E. Streibl**

# »Informatik und Gesellschaft« an der Universität Bremen

## Schlaglichter auf eine 40-jährige Geschichte

*Diesen Beitrag widme ich in großer Dankbarkeit Prof. Dr. Jürgen Friedrich, der mich vor über 25 Jahren an die Universität Bremen holte. Neben fachlichen Impulsen und Anregungen gab er mir dort von Anfang an die Möglichkeit und vor allem auch die Freiheit, mich auf eigenen Wegen und Schwerpunkten weiterzuentwickeln. Sein stetiges Hinterfragen, seine Lust am Streitgespräch, seine Offenheit, seine Ruhe und sein Humor waren mir Hilfe, Anregung und Vorbild.*

*Ralf E. Streibl*



**Jürgen Friedrich (1942–2018)**

Der Informatikstudiengang an der Universität Bremen wird in diesem Herbst 40 Jahre alt. Einst eingeführt als Diplom-Studiengang, existiert er heute als Bachelor- und Masterstudiengang. Im Laufe der Jahre gab es diverse Veränderungen der Struktur und der Prüfungsordnung, konstant ist jedoch eine Besonderheit dieses Studiengangs: Von der Gründung an bis heute ist in diesem Studiengang das Fachgebiet *Informatik und Gesellschaft* als fester Teil des Studiums verankert, nicht zuletzt verortet durch eine zum Pflichtanteil des Studiums gehörende Veranstaltung.

In Betrachtung von Vergangenheit und Gegenwart der Idee und des Fachgebietes *Informatik und Gesellschaft* an der Universität Bremen soll ein Einblick in die Hintergründe und Bedeutung, die Entwicklung sowie das jetzige Verständnis dieses Fachgebiets versucht werden.[1]

### Experiment Universität Bremen

Dem offiziellen Gründungdatum der Universität Bremen, 14. Oktober 1971, gingen lange Diskussionen voraus. Die erste Idee einer Universitätsgründung datiert bereits auf das Jahr 1947, wurde aber zunächst nicht weiter verfolgt. Vor dem Hintergrund steigender Studierendenzahlen empfahl der Wissenschaftsrat im Jahr 1959 die Neugründung von Universitäten und empfahl u. a. auch Bremen als möglichen Standort. 1961 fasste die Bremische Bürgerschaft einen Grundsatzbeschluss zur Errichtung einer Universität.

Beflügelt durch die allgemeine gesellschaftliche Stimmung Ende der 60er Jahre wurde das sogenannte *Bremer Modell* entwickelt, welches durch Kooperation und Transparenz charakterisiert sein sollte und eine sich ihrer gesellschaftlichen Funktion und Verantwortung bewusste Organisation zum Ziel hatte. Im *Bremer Modell* wird *„die Universität in der Gesellschaft als Stätte kritischer Bewusstseinsbildung gegenüber gesellschaftlichen, politischen und ökonomischen Prozessen, als Stätte wechselseitiger Beeinflussung aller gesellschaftlichen Gruppen, als Zentrum geistiger Ausstrahlung für alle Bildungsbemühungen"* verstanden (Bürgermeister Hans Koschnick 1970, zit. n. Meier-Hüsing 2011, S. 25).

In der Konkretisierung dieser Ziele wurden Anstrengungen unternommen, andere Formen von Studium und Prüfungen zu realisieren (u. a. durch fächerübergreifende integrierte Eingangsphasen, das Projektstudium, studienbegleitende Leistungsnachweise anstelle von Klausuren und mündlichen Prüfungen) sowie andere universitäre Entscheidungsstrukturen zu etablieren (Drittelparität zwischen HochschullehrerInnen, DienstleisterInnen und Studierenden – bald wieder abgeschafft in Folge des Hochschulrahmengesetzes des Bundes). Frieder Nake – seit 1972 Hochschullehrer an der Universität Bremen, zunächst im Studiengang Elektrotechnik/Kybernetik, später in der Informatik – bezeichnete jüngst die Universität Bremen als *„Experiment einer unwahrscheinlichen Universität"* (Weisser & Nake 2018) und resümiert: *„Eine Großtat, die einmalig war und sich nicht wiederholte, wenngleich der Ruf der Bremer Gründung in akademische Kreise hinein ausstrahlte. Der Ruf strahlte begeisternd für die einen, zu verwerfen für andere"*.[2]

Ein zentrales Element des *Bremer Modells* war es, *„Ausbildung und Forschung enger mit gesellschaftlichen Bezügen zu verknüpfen, ohne dabei wissenschaftliche Standards aus dem Auge zu verlieren"*, betont der ehemalige Rektor Alexander Wittkowski in einer Rückschau auf die ersten 10 Jahre der Universität (Universität Bremen 1981, S. 2). Diese Auseinandersetzung mit gesellschaftlich relevanten Fragen und Themen spiegelte sich dementsprechend in der Planung der Studiengänge wider.

## Bremen 1978: Gründung des Informatik-Studiengangs

Informatik an sich ist eine vergleichsweise junge Wissenschaft. Nachdem politisch zunächst vor allem Technologieförderung im Fokus war, richtete sich ab Ende der 60er Jahre vor dem Hintergrund fehlender Fachkräfte die Aufmerksamkeit verstärkt auf die Ausbildung. Das *Bundesministerium für wissenschaftliche Forschung* konstituierte 1968 einen Ausschuss, der ein Konzept zur Einführung von Informatik-Studiengängen erarbeiten sollte. Mit dem *Überregionalen Forschungsprogramm Informatik* förderten Bund und Länder anschließend den Aufbau der Informatikforschung und -lehre an deutschen Hochschulen.[3]

Während bundesweit vor allem Perspektiven des technischen und wissenschaftlichen Fortschritts sowie Anforderungen aus Industrie und Wirtschaft die Debatten um die Gestaltung neu entstehender Informatik-Studiengänge prägten, wurden in Bremen schon bei den Vorplanungen andere Sichtweisen einbezogen:

> *„Bei einer Wissenschaft wie der Informatik, die getragen wird von der derzeit höchsten Entwicklungsstufe der Technologie, ist die Gefahr besonders groß, in Faszination vor der Maschinerie erstarrend stromlinienförmig technokratische Studiengänge zu konzipieren. Das kann nicht Absicht eines Studiengangs an der Universität Bremen sein"* (aus dem ersten Konzeptpapier der 1971 innerhalb der von Planungskommission Naturwissenschaften ins Leben gerufenen Unterkommission Informatik (UKI); zit. n. Robben 2013).[4]

Diese Unterkommission legte im April 1973 ihren Bericht vor, auf dessen Grundlage der Akademische Senat der Universität Bremen am 2. Mai 1973 die Einrichtung eines Informatik-Studienganges beschloss und zur weiteren Vorbereitung eine eigene Planungskommission Informatik (PKI) bildete, in der mehrere Jahre lang um Inhalte und Konzeptionen gerungen wurde. Bereits bevor dann im Juli 1979 der Abschlussbericht dieser Planungskommission in seiner Endfassung vorlag, wurde zum Wintersemester 1978/79 der Studienbetrieb des Diplomstudiengangs Informatik an der Universität Bremen eröffnet.

Im Vorwort des Berichts wird die mangelnde Anwendungsorientierung bisheriger Informatikstudiengänge kritisiert:

> *„Obwohl die Informatik einen Großteil ihrer Probleme aus Anwendungsbereichen bezieht, werden die Anwendungen als neben der Beschäftigung mit der ‚eigentlichen' Informatik laufende Aufgaben betrachtet"* (PKI 1979, S. 1).

Als Grundzüge des Bremer Informatikstudiums hebt der Bericht insb. den Bezug des Studiums auf gesellschaftliche Anwendungsbereiche, das Projektstudium und die Integration rechtswissenschaftlicher Gebiete des Datenschutzes und des Rationalisierungsschutzes hervor.

Volker Claus, als Professor an der Universität Dortmund damals einer von mehreren externen Gutachtern im Prozess der Einrichtung des neuen Bremer Studiengangs, berichtete später von der massiven Kritik und den Widerständen, welche die Ideen und Konzepte der Planungskommission von außen erfuhren, u. a. seitens des Fakultätentages und des Fachausschusses Ausbildung der Gesellschaft für Informatik. Im Schwerpunkt der an anderen Orten bereits bestehenden Studiengänge wurden gesellschaftliche Aspekte und Rahmenbedingungen von Informatikanwendungen ausgeklammert und bewusst der Berufsphase überlassen. In der Rückschau resümiert Claus (1988, S. 10): *„Man muss es als positiv einstufen, dass die Bremer diese zum Teil herbe Kritik konstruktiv in den Studiengang einarbeiteten, ohne dabei den integrierten Anwendungsbezug, die gesellschaftlichen Auswirkungen und das Projektstudium, also das Bremische des neuen Studiengangs, aufzugeben."*[5]

> *„Ziel der Ausbildung im Rahmen der Berufspraxisanalyse ist die Vermittlung derjenigen gesellschaftswissenschaftlichen Kompetenzen, die erforderlich sind, um die Möglichkeiten und Grenzen des EDV-Einsatzes im allgemeinen beurteilen zu können und die gesellschaftlichen Bedingungen der Berufspraxis des Informatikers wissenschaftlich analysieren zu können. Dazu ist in der ersten Studienphase eine Grundlage zu vermitteln, die die Aufarbeitung der ökonomischen, sozialwissenschaftlichen und rechtswissenschaftlichen Behandlungen der Probleme der Rationalisierung und Betriebs- bzw. Arbeitsplatzveränderungen ermöglicht. Insbesondere sind die informationsrechtlichen Probleme des Datenschutzes und die arbeitsrechtlichen Probleme des Rationalisierungsschutzes zu berücksichtigen. (…)"*
>
> Auszug aus der Beschreibung der 1. Studienphase des Informatik-Studiums im „Vorläufigen Studienführer Informatik, WS 78/79" – Fassung vom 6.9.1978
> *Universitätsarchiv Bremen: BUA 2AD_Nr. 3683 Studienführer Informatik*

## Informatik und Gesellschaft in Bremen: Die Idee

Das Studium wurde von der Planungskommission in die drei Dimensionen *Fachsystematik, Anwendungsbezug* sowie *Berufspraxisanalyse des Diplominformatikers*[6] *einschließlich ihrer gesellschaftswissenschaftlichen Grundlagen* gegliedert (PKI 1979, S. 20ff), wobei als übergreifender Rahmen *das „Ziel der Lösung der Probleme in den gesellschaftlichen Anwendungsbereichen"* und eine *„gesellschaftlich nützliche Arbeit des Informatikers"* benannt werden. Die sogenannte *Berufspraxisanalyse* beinhaltet die *„Vermittlung derjenigen gesellschaftswissenschaftlichen Kompetenzen, die erforderlich sind, um die Möglichkeiten und Grenzen des EDV-Einsatzes im allgemeinen beurteilen zu können und die gesellschaftlichen Bedingungen der Berufspraxis des Informatikers wissenschaftlich analysieren zu können"*. Gemeint ist damit insb. die Auseinandersetzung mit ökonomischen, sozialwissenschaftlichen und rechtlichen Aspekten in Zusammenhang mit dem Einsatz informationstechnischer Systeme. In der von der Planungskommission beschlossenen Prüfungsordnung des Studiengangs Informatik (PKI 1979, S. 171) werden als problemorientierte Grundlagen der Berufspraxisanalyse aufgelistet:

- Gesellschaftliche Funktion von Informationsverarbeitungstechnologie
- Gesellschaftliche Funktion der Arbeit

- Arbeitsbedingungen, soziale Lage und politisches Verhalten der technischen Intelligenz, insbesondere des Informatikers

- Entwicklungstendenzen auf dem EDV-Markt und auf dem Markt der EDV-Fachkräfte

- Soziale Folgen und soziale Kontrolle der Automation (Rationalisierungsschutz)

- Informationsrecht (Datenschutz)

An der Universität Bremen gab es schon vor dem Start des Informatik-Studiengangs im Studiengang *Elektrotechnik/Kybernetik* Lehrveranstaltungen, die ähnliche Bezüge erkennen ließen, beispielsweise *Einführung in die Berufspraxis von Ingenieuren: Zum Verhältnis von Arbeitsorganisation und Technologie* (Hans-Dieter Hellige und Wilfried Müller), *Datenschutz* (Frieder Nake), *Soziale Lage und politisches Bewusstsein von Ingenieuren* (Hans-Dieter Hellige). Im neuen Informatikstudiengang wurden anfangs manche Veranstaltungen zu gesellschaftlichen Implikationen und Rahmenbedingungen der Informationstechnik und der Informatik von Lehrbeauftragten durchgeführt, die beispielsweise aus dem „Informatik-Seminar" am Fachbereich Informatik der TU-Berlin oder dem „Bereich Informatik und Gesellschaft" am Fachbereich Informatik der Universität Dortmund bereits Erfahrungen mit Kursen zu gesellschaftlichen Fragestellungen mitbrachten.[7] In den 80er-Jahren wurden die zentralen Lehrveranstaltungen zu *Informatik und Gesellschaft* dann vor allem von den Hochschullehrern Klaus Haefner, Wilhelm Steinmüller und Jürgen Friedrich sowie von den Lehrbeauftragten Ulrich Briefs und Alfred Büllesbach durchgeführt.

## Bremen 1988: Die ersten 10 Jahre

Die von Anfang an gedachte und geforderte Integration von Anwendungen und Auswirkungen der Informationstechnik in den Studiengang spiegelte sich gleich in einer ganzen Reihe spezifischer Lehrveranstaltungen wider. Jürgen Friedrich, der 1986 nach Bremen auf die erste Professur für Informatik und Gesellschaft im deutschsprachigen Raum berufen worden war (Coy 2018)[8], stellte in seinem Beitrag zum 10-jährigen Jubiläum der Bremer Informatik dar, dass seit Gründung des Studiengangs neben den Fachinhalten der Kerninformatik spezifische Grundlagenveranstaltungen zu *Informatik und Gesellschaft* im Grundstudium verankert sind, um *„einen Fundus an Basiswissen zu schaffen"*. Die damalige „Säule" *Informatik und Gesellschaft*, bestehend aus drei Lehrveranstaltungen, beschrieb er folgendermaßen:

> *„In der Einführungsveranstaltung werden neben den philosophischen, erkenntnistheoretischen und historischen Bezügen der Informatik vor allem deren ökonomische und gesellschaftliche Einordnung behandelt. Darüber hinaus werden die Anwendungen und Auswirkungen der Informations- und Kommunikationstechnologien in verschiedenen gesellschaftlichen Bereichen (z. B. Betrieb/Verwaltung, Staat/Bürger, Freizeit, internationale Beziehungen, Militär usw.) analysiert und aus der Sicht unterschiedlicher Interessen bewertet. Schließlich werden einführende Überlegungen zur Vermeidung negativer Wirkungen (z. B. Datenschutz) bzw. zur Gestaltung menschengerechter Systeme (z. B. Software-Ergonomie) dargestellt. In zwei weiteren Veranstaltungen (2. und 3. Semester) werden zwei der Themen schwerpunktmäßig vertieft, einerseits das Thema Rationalisierungsschutz und menschengerechte Arbeitsgestaltung an computergestützten Systemen und zum anderen das Thema Persönlichkeitsgefährdung und Datenschutz"* (Friedrich 1988, S. 44).

Neben diesen spezifischen Veranstaltungen zu *Informatik und Gesellschaft* beinhaltete das Bremer Konzept der Angewandten Informatik – wie schon in der Planung angedacht – auch in anderen Kursen enge Bezüge zwischen Fachinhalten und Kontext.

Studiengang Informatik　　　　Seite 1

| 1) Veranstaltungs kennziffer (VAK) | 2) Veranstaltungsform | 3) Titel der Veranstaltung (mit Kurzbeschreibung) | 4) Veranstalter | 5) Schwerpunkt und/oder Schulfach/ Lernbereich/berufl. Fachrichtung | 5a) Studiengebiet | 6) Eignung für Semesterstufen | 7) Eignung für Schulstufe | 8) Semester wochenstunden | 9) Termin | 10) Raum |
|---|---|---|---|---|---|---|---|---|---|---|
| 4901 | K | Hilfsmittel zur formalen Beschreibung informationsverarbeitender Syteme A | N.N.,N.N. | D | | A | | 3 | wird noch mitgeteilt | |
| 4902 | K | Hilfsmittel zur formalen Beschreibung informationsverarbeitender Systeme B | N.N.,N.N. | D | | A | | 3 | | |
| 4903 | K | Aufbau und Wirkungsweise von Rechenanlagen | N.N.,N.N. | D | | A | | 2 | | |
| 4904 | PL | Programmierlabor A | N.N.,N.N.,N.N. | D | | A | | 3 | | |
| 4905 | S | Informationsverarbeitende Systeme A | N.N.,N.N.,N.N. | D | | A | | 3 | | |
| 4906 | K | Gesellschaftliche Funktion der Arbeit | N.N.,N.N. | D | | A | | 3 | | |
| 4907 | K | Mikroökonomie als schwerpunktorientierte Grundlage der Berufspraxisanalyse für den Schwerpunkt Transport und Wertverkehr | N.N.,N.N. | D | | A | | 2 | | |

*Das erste Veranstaltungsverzeichnis des Bremer Informatik-Studiengangs (Winter-Semester 1978/79) enthielt u. a. den Kurs „Gesellschaftliche Funktion von Arbeit" – wie alle Informatik-Veranstaltungen zum Zeitpunkt der Drucklegung noch ohne genaue Angaben zu Lehrenden, Termin und Raum*

Im Hauptstudium nach dem Vordiplom setzte sich die Integration von *Informatik und Gesellschaft* in der Angewandten Informatik fort, zum einen gestützt durch die Bereitschaft vieler Lehrender, Bezüge des Gebiets *Informatik und Gesellschaft* aufzunehmen, und zum anderen befördert durch das Projektstudium. Klaus-Peter Löhr, von 1978 bis zu seinem Wechsel 1985 an die FU Berlin Informatik-Hochschullehrer an der Universität Bremen, schreibt rückblickend:

> *„Das Projekt kann man, wenn man will, als rein technikbezogenes, didaktisches Bonbon konzipieren (was immerhin schon eine gute Sache ist). Die gesellschaftsbezogenen Veranstaltungen legen aber nahe, auch im Projekt nach Anwendungen und Auswirkungen zu fragen. Damit gewinnt der Studiengang ein Potential, das weit über die Vermittlung einer guten individuellen Fachqualifikation hinausgeht. Wer es nicht schon selbst gemerkt hat, der erfährt in den gesellschaftsbezogenen Veranstaltungen, dass die Informationstechnik reich an gesellschaftlichem Sprengstoff ist, aber arm an kompetenten Fachleuten, die sich darüber Gedanken machen. Es liegt auf der Hand, dass wir Informatiker/innen brauchen, die über den Tellerrand ihrer rein technischen Kompetenz hinausblicken können, die Folgen ihres Handelns verstehen und dafür Verantwortung übernehmen können"* (Löhr 1988, S. 19).

Neben dem Projekt und integrierten Anteilen gab es zusätzlich im Hauptstudium wechselnde Wahlangebote zu spezifischen Einzelthemen von Informatik und Gesellschaft sowie regelmäßig ein Seminar Berufspraxis der Informatiker/innen, welches alle Studierenden des Hauptstudiums besuchen sollten, um sich schon während des Studiums anhand von Fallstudien, Firmenbesuchen etc. mit qualifikatorischen und persönlichen Anforderungen unterschiedlicher Tätigkeitsfelder der beruflichen Praxis auseinanderzusetzen, ebenso wie mit Fragen von Arbeitsbedingungen und Interessenvertretung (vgl. Friedrich 1988, S. 45).

> *„Es kann ja nicht Aufgabe einer Universität sein, künftigen Studenten einfach einen Katalog von ‚Fertigkeiten' anzubieten, aus dem sie sich etwas aussuchen. (…) Dann würde die Universität den Studenten als eine Art Einkaufskorb ansehen, in den die Waren des intellektuellen Warenlagers der Universität gepackt werden sollen. Mit anderen Worten, sie würden den Studenten völlig richtig als ein dem Computer ziemlich ähnliches Objekt ansehen, dessen Speichereinheiten nach immer neuen ‚Daten' hungern."*
>
> Joseph Weizenbaum (1978, S. 363)

## Blick ins Bücherregal: Suche und Strukturierungsversuche

In den 90er-Jahren wurde verstärkt vielerorts um ein tiefergehendes Verständnis von *Informatik und Gesellschaft* gerungen, was sich in Tagungen und Publikationen aus dieser Zeit widerspiegelt. Häufig waren daran auch Personen aus dem Kontext der Bremer Informatik beteiligt, was widerspiegelt, dass gerade auch an der Universität Bremen selbst die Beschäftigung mit diesen Themen intensiv weiterging. Ohne Anspruch auf Vollständigkeit seien hier einige Beispiele herausgegriffen:

1992 entstand vor dem Hintergrund einer Tagung des *Fachbereichs Informatik und Gesellschaft der GI* in Freiburg der Sammelband *Informatik cui bono?* (Langenheder, Müller, Schinzel 1992). Schon im Vorwort wird darin programmatisch formuliert, dass *"die Entwicklung und der Einsatz von Technik dem sozialen und kulturellen Fortschritt dienen"* und *„nicht nur an Kriterien wie Erkenntnisgewinn und Verwertungslogik, sondern auch an den Grundsätzen der Erhaltung und Entfaltung"* orientiert sein solle. Das Tagungsmotto aufgreifend stellt Frieder Nake im seinem Beitrag klar, dass die Frage „Wem zum Nutzen?" in den 70er-Jahren als Klassenfrage aufgefasst und beantwortet worden wäre, da Computer in kritischer Betrachtungsweise als Mittel der Rationalisierung in der Hand von Staat und Kapital angesehen wurden (Nake 1992b, S. 29f). Jedoch habe sich diese Sicht in der ersten Hälfte der 80er-Jahre geändert – Nake verweist hier auch auf den Schwenk in der Haltung von Gewerkschaften zur Technikentwicklung: Die Frage der aktiven und sozialverträglichen Gestaltung von Technik – auch in der Informatik – trat verstärkt in den Vordergrund. Gestaltung in diesem Sinne beschränkt sich – wie Arno Rolf (1992) im gleichen Band hervorhebt – jedoch nicht auf das Herstellen eines Technikkonzeptes, sondern benötigt als Grundlage das Erkennen und Verstehen gesellschaftlicher Zusammenhänge. Jürgen Friedrich beschreibt unter den Titel „Informatik und Gesellschaft in der Hochschullehre", dass sich das lange Zeit vorherrschende Selbstverständnis von Informatik als rein technische Disziplin langsam ändere. Er verweist in seinem Beitrag zu dem Band darauf, dass es *„an mindestens sechs universitären Informatikstudiengängen eigene Lehrkräfte für Informatik und Gesellschaft und an mindestens ebenso vielen weiteren Universitäten mehr oder weniger regelmäßige Lehrveranstaltungen zu diesem Thema"* gebe (Friedrich 1992, S. 259). Er charakterisiert Informatiktheorien, -methoden und -systeme als Verkörperung vergegenständlichter Optionen der Technikentwicklung und fordert:

> *„Informatik und Gesellschaft soll bei den Studierenden das Denken in alternativen Entwürfen fördern, die Einsicht in die Multiperspektivität informationstechnischer Entwicklungslinien. Erkennen der Optionen, die in der Informationstechnik enthalten sind, und Reflektion der mit ihnen verbundenen Leitbilder sind nicht Selbstzweck, sondern Voraussetzung für die Entwicklung von Gestaltungskompetenz bei den Studierenden"* (Friedrich 1992, S. 261).

Eine stark interdisziplinär geprägte Herangehensweise sei hierfür notwendig. Sie fordere den Studierenden ab, sich auf *„unbekanntes Terrain"* zu begeben und sich mit fremden Wissenschaftssprachen und Methoden auseinanderzusetzen.

Der als Professor für Rechts- und Verwaltungsinformatik (mit Schwerpunkt Datenschutz) an der Universität Bremen tätige Jurist Wilhelm Steinmüller[9] unternahm in seinem über viele Jahre gewachsenen Hauptwerk *Informationstechnologie und Gesellschaft* (Steinmüller 1993) den Versuch einer systematischen Einführung in die Angewandte Informatik. Ausgehend von einer wissenschaftstheoretischen Betrachtung der Informatik erfolgt im weiten Verlauf des Buches eine Auseinandersetzung mit Informationssystemen und den aus ihnen resultierenden Folgen. Darauf aufbauend beschäftigt sich auch Steinmüller dann mit Fragen einer verantwortlichen und sozialen Gestaltung solcher Systeme.

1995 erschien – ebenfalls von langer Hand vorbereitet – das Lehrbuch *Informatik und Gesellschaft* (Friedrich, Herrmann, Peschek, Rolf 1995), mit welchem der Versuch unternommen werden sollte, eine möglichst ganzheitliche, umfassende und zugleich vielschichtige Betrachtung dieses Gebiets vorzunehmen. Hierzu sollten die jeweiligen Perspektiven vieler verschiedener beteiligten Autorinnen und Autoren beitragen. In dem Band finden sich neben übergreifenden Erörterungen z. B. zu Selbstverständnis und Sichtweisen der Informatik, Ethik und Informatik, Professionalisierungsprozessen und Berufspraxis diverse Beiträge in denen der Technikeinsatz in verschiedenen Bereichen exemplarisch dargestellt und diskutiert wird. Es ist die Crux derartiger Vorhaben, dass sie bereits kurz nach Erscheinen teilweise veraltet erscheinen. Viele der Beispiele beziehen sich auf die damalige Zeit und Technik. Doch teilweise können sie – aufgrund des systematischen Vorgehens und transparenten Aufbaus – heute als historischer Bezug sowie als Vergleichsmaterial bei der Auseinandersetzung mit verwandten Themen dienen.

> *„Bei-bringen kann ich ihnen [den Studierenden] nur das, worüber ich verfüge. Aufnehmen, erwerben können es die Studierenden nur selbst. Ich kann, was ich mir angeeignet habe, was ich erfahren habe, vor ihnen ausbreiten. Ich kann dazu beitragen, die Bedingungen zu verbessern, unter denen sie das Ausgebreitete aufnehmen können. Ich kann also erzählen und zeigen und kann ihnen das Zuhören und Fragen angenehm machen. Wir können beginnen, gemeinsam tätig zu werden. Da lernen wir dann schon, in unseren unterschiedlichen Rollen, voneinander."*
>
> Frieder Nake (1992b, S. 38) in einer „Schlussbemerkung für Lehrende", mit der er seinen Beitrag in dem Band „Informatik cui bono?" enden läßt

Weitere thematisch bedeutsame Buchveröffentlichungen in dieser Zeit wurden angestoßen durch Diskussionen und Zusammenkünfte in Zusammenhang mit dem Arbeitskreis *Theorie der Informatik* in der Gesellschaft für Informatik. So beschäftigte sich der Sammelband *Sichtweisen der Informatik* (Coy, Nake, Pflüger, Rolf, Seetzen, Siefkes, Stransfeld 1992) allgemein sowie bezogen auf Arbeitswelt und Kultur mit dem Selbstverständnis der Informatik, einer „Disziplin im Umbruch" (so beschreibt Wolfgang Coy[10] in seinem einleitenden Beitrag den Zustand; Coy 1992). Intensiv werden in anderen Beiträgen Fragen von Ethik und Verantwortung der und in der Informatik angesprochen, parallel zu den Debatten und Prozessen, die 1994 zur erstmaligen Verabschiedung von *Ethischen Leitlinien* der Gesellschaft für Informatik mündeten.[11] In einem vier Jahre später erschienenen Sammelband *Schnittstellen* (Schinzel 1996) finden sich neben grundsätzlichen Reflexionen zum Verhältnis von Informatik und Gesellschaft (insb. Coy 1996) und zur Technikfolgenabschätzung in und für die Informatik diverse weitere Betrachtungen und Positionierungen – beispielsweise zum „Weg in die Informationsgesellschaft" (angesichts der zunehmenden Vernetzung).

1999 erschienen im Rahmen eines Projekts „Entwicklung" und Erprobung eines Fernstudienangebots zum Themenbereich ‚Informatik und Gesellschaft'" die *Tübinger Studientexte Informatik und Gesellschaft*. Die neun von verschiedenen Autorinnen und Autoren verfassten Themenhefte greifen wesentliche Aspekte des Gebiets jeweils in einführender Weise auf. Das Fehlen einer abschließenden Theorie und Systematik von *Informatik und Gesellschaft* wird hier nicht als Schwäche verstanden. Die Autorinnen und Autoren laden dazu ein, neue und vielleicht ungewohnte Perspektiven einzunehmen und sich anhand von Materialien, Fallbeispielen und Fragen in einem lebendigen Prozess mit *Informatik und Gesellschaft* sowohl in Hinblick auf eine Tätigkeit in der Praxis als auch als generellen Erkenntnisgewinn zu beschäftigen (vgl. Klischewski 1999).

Auf den Vorwurf des Fehlens einer einheitlichen wissenschaftlichen Begründung für das Fachgebiet reagierten Christian Fuchs und Wolfgang Hofkirchner 2003 mit ihrem *Studienbuch Informatik und Gesellschaft*, welches in einem kleineren ersten Teil exemplarische Beispiele unserer „informationsgesellschaftlichen Realität" skizziert, um in einem zweiten Teil theoretische Betrachtungen von für das Fachgebiet relevanten Begrifflichkeiten vorzunehmen sowie diese anschließend in größere Zusammenhänge zu stellen und zu diskutieren.

Das *Forum Informatikerinnen und Informatiker für Frieden und gesellschaftliche Verantwortung (FIfF)*, 1984 vorrangig als gesellschaftliche Plattform gegründet, um einen Ort zu haben, um die das eigene Fach betreffenden gesellschaftlichen und politischen Debatten führen zu können und sich gemeinsam einzumischen, hat in den darauf folgenden Jahrzehnten bis heute in spannender Weise den Spagat gemeistert, sein gesellschaftspolitisches Selbstverständnis im Verbund mit anderen zivilgesellschaftlichen Organisationen und Akteuren beizubehalten und gleichzeitig konstant die fachliche und fachwissenschaftliche Auseinandersetzung zu *Informatik und Gesellschaft* zu begleiten und aktiv zu fördern (vgl. rückblickend Streibl 2014). Neben regelmäßigen Fachtagungen (#FIfF-Kon) geschieht dies insb. durch die inzwischen im 35. Jahrgang erscheinende Zeitschrift *FIfF Kommunikation* sowie durch Buchpublikationen und durch die Vergabe eines Studienpreises für Abschlussarbeiten im Themenfeld *Informatik und Gesellschaft*.[12]

Als anregendes Beispiel internationaler Literatur, soll abschließend noch *A Gift of Fire* (Baase 1997) erwähnt, werden, eine Ende der 90er Jahre erstmals erschienene Umschau über soziale, ethische und rechtliche Aspekte der Informatik, die in den Folgejahren – anders als die deutschsprachige Literatur zum Thema – immer wieder aktualisiert und erneuert wurde, und inzwischen in 5. Auflage vorliegt (Baase & Henry 2018).

## Aufschwung oder Auflösung? IuG nach der Jahrtausendwende

Im Laufe der Jahre waren an einer ganzen Reihe von Hochschulen Professuren eingerichtet worden, die – unter unterschiedlichen Bezeichnungen – deutliche Schwerpunkte im Bereich *Informatik und Gesellschaft* aufwiesen. Eine Schwerpunktredaktion der Zeitschrift *FIfF Kommunikation* des *Forums Informatikerinnen und Informatiker für Frieden und gesellschaftliche Verantwortung* bat daraufhin 2001 diesen Personenkreis, für ein Schwerpunktheft *Informatik und Gesellschaft als akademische Disziplin* ihre Sicht auf *Informatik und Gesellschaft* in Beiträgen zu skizzieren (Engbring & Streibl 2001). Herausgekommen ist eine Artikelsammlung, in der jenseits aller Unterschiede in der strukturellen Einbindung an den jeweiligen Hochschulen und auch jenseits verschiedener inhaltlicher Schwerpunktsetzungen die Bedeutsamkeit einer festen Einbindung dieses Gebietes in der Informatiklehre deutlich wird. In der Zusammenschau der Beiträge werden unterschiedliche Sichtweisen auf das eigene Fachgebiet sichtbar und Fragen aufgeworfen, u. a.: In welchem Verhältnis stehen „Kritik“ und „Gestaltung“? Welcher „Kitt“ kann die „IuG-Community“ zusammenhalten? Macht eine stärkere Integration in die Kerninformatik eigene Lehrveranstaltungen zu *Informatik und Gesellschaft* obsolet? Kann solch eine Integration überhaupt gelingen, oder fehlt es dort ab einer gewissen Stelle dann an kritischer Distanz? Wie gestaltet sich das Verhältnis von *Informatik und Gesellschaft* als akademisches Fachgebiet zu gesellschaftspolitischen Aktivitäten und Entwicklungen? Wie kann und soll man mit Widersprüchlichkeiten des eigenen Fachgebiets umgehen?

> *„Angesichts der spezialisierten technischen und theoretischen Fachgebiete, die sich bislang in der Informatik entwickelt haben, ist es nun endlich an der Zeit, in allen Informatikfachbereichen ‚Informatik und Gesellschaft' als selbständige Lehre und Forschung zu verankern.“*
>
> Wolfgang Coy (2001, S. 47)

Besonders herausgreifen aus den Artikeln dieses Schwerpunktheftes möchte ich an dieser Stelle den Beitrag *Weder vollständig noch widerspruchsfrei* von Wolfgang Coy, in welchem ich viele Verbindungen zu meinen eigenen, in langjähriger Lehrpraxis gewachsenen Erfahrungen und zu meinem persönlichen Verständnis von Lehre in *Informatik und Gesellschaft* wiedererkenne. Coy versteht *Informatik und Gesellschaft* als den „natürlichen Ort“, an welchem die Informatik als Technik im Kontext und „als Ganzes“ reflektiert werden kann. Folgerichtig vertritt er entschieden die Forderung, *Informatik und Gesellschaft* in allen Informatikfachbereichen als selbständige Lehre und Forschung zu verankern. Bezugnehmend auf gelegentlich geäußerte Vorstellungen, *Informatik und Gesellschaft* werde als eigenständiges Fach überflüssig, wenn nur alle anderen Vorlesungen und Seminare diese Aspekte hinreichend berücksichtigten, präzisiert er:

> *„Um den reichhaltigen Kontext moderner Informatiksysteme angemessen zu vermitteln, muss die Lehre in Informatik und Gesellschaft so vielfältige Inhalte wie Informationsrecht, (alte und neue) Ökonomie oder Arbeits- und Berufswelt der Informatik ansprechen und gegebenenfalls vertiefen. Darüber hinaus muss Informatik und Gesellschaft die geistigen und kulturellen Grundlagen des Faches vermitteln und nicht zuletzt soll die Fähigkeit zur Bewertung sozio-kultureller Prozesse geweckt werden – von der berufsspezifischen Ethik bis zu den historischen und politischen Aspekten der Globalisierung und Informationsgesellschaft. So begrüßenswert es ist, wenn solche Themen an der richtigen Stelle im fachlichen Kontext an- und ausgesprochen werden, so scheint es mir doch unerlässlich, diese Themenkomplexe auch im eigenen Kontext und mit der eigenen Logik, eben in einem eigenen Fach Informatik und Gesellschaft, zu präsentieren und zu diskutieren“* (Coy 2001, S. 47).

Leider zeigten die folgenden Jahre vielerorts eher gegenläufige Entwicklungen. Nach und nach wurden freiwerdende Professuren im Bereich *Informatik und Gesellschaft* nicht wiederbesetzt oder ihre Schwerpunkte wurden deutlich verändert. Die Gründe mögen dabei durchaus unterschiedlicher Natur sein. Eine gerade im Rückblick sehr spannende Beobachtung in diesem Zusammenhang hat Jörg Pflüger unter dem Titel „*Was machen wir, wenn wir gewonnen haben sollten?“* formuliert: In der Anfangszeit von *Informatik und Gesellschaft* standen gesellschaftspolitische Perspektiven im Mittelpunkt einer kritischen Auseinandersetzung der Computertechnologie im Mittelpunkt. Während sich die daraus abgeleitete Forderung nach Gestaltung einer den Menschen nicht ersetzenden, sondern unterstützenden Technologie überraschend schnell verbreitete, gerieten die übergreifenden Leitlinien aus dem Blick. Anschaulich beschreibt Pflüger eine Situation auf einem Workshop:

> *„Die jüngeren Teilnehmer konnten mit dem Slogan „Humanisierung der Arbeitswelt“ überhaupt nichts mehr anfangen und brachten keinerlei Verständnis für den Wunsch der älteren nach einem vereinheitlichenden Gestaltungskriterium auf. Für sie geht es ausschließlich um konkrete Probleme des menschengerechten Designs bei unterschiedlichen Anwendungen, die jeweils für sich beantwortet werden können und müssen“* (Pflüger 2001, S. 16).

Weitere Diversifizierung der gesellschaftlichen Bezüge der Informatik ergab sich aus den rapide wachsenden soziokulturellen Bezügen der Technik infolge vielfältiger medialer Anwendungen und zunehmender Vernetzung. Diese Entwicklung kann durchaus positive Effekte für den Lehr- und Lernkontext haben: Manche würde sich deswegen von sich aus mit Themen aus *Informatik und Gesellschaft* befassen. Pflüger schreibt von „offenen Türen“, die sich vor diesem Hintergrund in Wissenschaft und bei Studierenden, die mit dem Internet aufgewachsen sind, für derartige Fragen ergeben. Im Bild bleibend merkt er jedoch an, dass „offene Türen“ auch „ins Leere“ führen können:

> *„Nach meiner Erfahrung sind viele Studierende (wie Lehrende) allzeit bereit, einen Gesellschaftsbezug zu konzedieren, wollen aber ansonsten ihre technische Ruhe haben und sich einer Auseinandersetzung entziehen“* (S. 17).

Als Schluss aus diesen Entwicklungen relativiert Pflüger für die Gestaltung eigenständiger Lehrveranstaltungen zu *Informatik und Gesellschaft* den Anspruch einer top down systematisierten, von einem vereinheitlichenden Prinzip ausgehenden Überblicksvorlesung. Für ihn steht im Vordergrund zunächst das Ziel, den angehenden Informatikerinnen und Informatikern ein Bewusstsein für den Kontext und die Ambivalenzen ihrer Technik, für (auch nicht-intendierte) Wirkungen und für ihre jeweiligen Handlungsmöglichkeiten und die Verantwortung bei der Gestaltung von Informationstechnologie zu vermitteln.

## IuG in Bremen: Vom Diplom zum Bachelor

Für geraume Zeit bestand im Bremer Diplomstudiengang Informatik eine eigene Säule *Informatik und Gesellschaft*, bestehend aus drei Veranstaltungen, die Studierende üblicherweise in den ersten drei Semestern besuchten. Im Zuge der Überarbeitung der Diplomprüfungsordnung 1993 reduzierte sich der Umfang: Nunmehr war noch eine einführende Veranstaltung *Anwendung und Auswirkungen der Informatik* im 1. Semester sowie eine Vorlesung mit Übung *Informatik und Gesellschaft* (üblicherweise im 3. Semester) als Pflichtanteil des Studium verankert. Diese Veranstaltungen wurden dann im wesentlichen von Jürgen Friedrich, Herbert Kubicek und Karl-Heinz-Rödiger (und anfangs auch noch Wilhelm Steinmüller) gehalten, im Übungsbetrieb unterstützt von Wissenschaftlichen MitarbeiterInnen.

Nicht im Pflichtbereich, aber durchaus im Sinne der ursprünglichen Planungen des Studiengangs dem Bereich *Informatik und Gesellschaft* zuzurechnend, wurden regelmäßig *Seminare zur Berufsorientierung* (später *Berufsbild der Informatik*) angeboten, früher oft von Ulrich Briefs, ab Ende der 90er-Jahre von Susanne Maaß.[13]

Inhalte und didaktische Konzepte von Lehrveranstaltungen unterliegen Wandlungen: Begleitet von kritischer Selbstreflexion wurde auch an der Universität Bremen experimentiert und es wurden didaktische Konzepte überprüft und verändert. Beispielsweise wurde Mitte der 90er-Jahre zeitweise der Versuch unternommen, die einführende Veranstaltung *Anwendungen und Auswirkungen der Informatik* (AAI) als computerunterstütztes Planspiel durchzuführen. Inhaltlich stand dabei eine Fallstudie zum Thema „Hafeninformatik" (mit für Bremen naheliegendem Regionalbezug) im Mittelpunkt – an diesem Beispiel sollten sowohl gleichermaßen Veränderungsprozesse aufgrund technischer Entwicklungen und Veränderungen als auch Auswirkungen und Folgen thematisiert und erlebbar gemacht werden. Verschiedene Interessenlagen und Perspektiven sollten in einem diskursiven Lernprozess transparenter werden. Die Erfahrung zeigte jedoch, dass das für Erstsemester-Studierende anspruchsvolle Thema und die Sensibilisierung für die Vielschichtigkeit des Szenarios aufgrund der damals eher rigiden technischen Realisierung der Interaktionsformen zu sehr in den Hintergrund geriet, weshalb in der Folge von diesem Vorgehen wieder abgesehen wurde.

Ein Phänomen, welches ebenfalls einen Anteil am Scheitern des AAI-Lehrexperiments hatte, war ein sich verstärkt zeigendes, verändertes Studierverhalten: Die Kurse *Anwendungen und Auswirkungen der Informatik* sowie *Informatik und Gesellschaft* waren damals – wie viele andere Veranstaltungen im Fach Informatik – konzipiert als Vorlesungen mit begleitendem Übungsbetrieb (der in mehreren kleineren Gruppen durchgeführt wurde). In den Veranstaltungen der Kerninformatik ist für die Studierenden der Zusammenhang zwischen Vorlesung und Übung üblicherweise klar ersichtlich und kurzfristig erlebbar, wenn jede Woche in der Übung die für den Scheinerwerb zu lösenden Aufgaben mit ihrem direkten Bezug auf die Inhalte der Vorlesung behandelt werden. In *Informatik und Gesellschaft* war jedoch der Übungsbetrieb anders und für die Informatik-Studierenden eher ungewohnt aufgebaut: Er hatte eher den Charakter geistes- oder sozialwissenschaftlicher Seminare mit Referaten zu spezifischen Themen an den einzelnen Terminen. Die dazu gehörige Vorlesung behandelte im Verlauf des Semesters den größeren Themenbereich grundlegend und systematisch-analytisch. Der Zusammenhang mit den auf den ersten Blick nicht direkt auf den Vorlesungsstoff der jeweiligen Woche bezogenen

*Joseph Weizenbaum erhält 1998 die Ehrendoktorwürde der Universität Bremen, (links der damalige Konrektor Wilfried Müller, rechts Hans-Jörg Kreowski) – Foto: Universität Bremen*

Referaten erschloss sich manchen Studierenden nicht schnell genug – und wenn diese für sich die Entscheidung getroffen hatten, dass der Vorlesungsbesuch zum Bestehen der Veranstaltung nicht unbedingt erforderlich sei, dann war damit natürlich auch die Chance vergeben, zu einem späteren Zeitpunkt zu einer anderen Erkenntnis zu gelangen. Unabhängig von der Person, die jeweils die Vorlesung hielt reproduzierte sich bei einer signifikanten Zahl von Studierenden das unbefriedigende Bild einer faktischen Reduktion von *Informatik und Gesellschaft* nur auf den Übungsbetrieb und dort insb. auf den eigenen Vortrag. Diese Situation rief dringend nach Veränderung.

Der Bologna-Prozess mit der Einführung gestufter Studiengänge brachte 2002/2003 auch in Bremen eine Reform des Informatik-Studiengangs mit sich, allerdings mit einer Besonderheit: das Fach beschloss, den Diplom-Studiengang zunächst parallel zum neuen Bachelor-/Masterstudiengang Informatik zu erhalten.[14] Um den Studierenden problemlose Wechsel zwischen Diplom- und Bachelor-Studiengang zu ermöglichen, wurde die Prüfungsordnung des Diplomstudiengangs überarbeitet, so dass in beiden Studiengängen im wesentlichen die gleichen Veranstaltungen vorgesehen waren. Die frühere Säule *Informatik und Gesellschaft* reduzierte sich im Rahmen dieser Reform auf eine nunmehr einzige spezifische Lehrveranstaltung im Umfang von drei SWS, die üblicherweise im dritten oder vierten Semester besucht wird. Da ergänzend zur Präsenzlehre umfangreiche semesterbegleitende Zusatzarbeiten der Studierenden ein wesentlicher konzeptioneller Teil dieser Veranstaltung sind, entspricht sie bei der Zumessung von 6 ECTS-Punkten in etwa dem Gewicht einer typischen zweistündigen Vorlesung mit begleitender Übung. Um einen didaktisch sinnvollen Rahmen für intensive Diskussion und aktive Beteiligung der Studierenden zu bieten, wird die Veranstaltung in Seminargröße durchgeführt, was angesichts der Studierendenzahlen bedeutet, dass jedes Semester mehrere solcher Seminare angeboten werden. Beginnend mit der Neukonzeption der Veranstaltung 2003 werden diese in aller Regel vom Autor dieses Artikels betreut (einzelne Seminare wurden in der Vergangenheit nach dem gleichen Konzept von Jürgen Friedrich sowie Susanne Maaß, Carola Schirmer und Maike Hecht[15] durchgeführt). Zentrale Elemente der heutigen Form dieser Lehrveranstaltung sollen nun im folgenden Abschnitt kurz skizziert werden.

forum

## Bremen 2018: Die heutige Konzeption des Seminars *Informatik und Gesellschaft*

All die im Laufe der Jahre entwickelten, an verschiedenen Stellen erprobten, in der Literatur formulierten und diskutierten Ziele von *Informatik und Gesellschaft* zu erreichen, würde eine einzelne Lehrveranstaltung zwangsläufig überfordern. Angesichts der Fülle potentieller Inhalte und Herangehensweisen einerseits und des begrenzten Zeitvolumens andererseits, wurde bei der Neukonzeption des Seminars entschieden, die inhaltlich den Stoff systematisierende, aber schlecht besuchte Vorlesung aufzugeben. Anstelle dessen trat ein Seminarkonzept in dem einige zentrale, übergreifende Kerninhalte im engeren Sinne „vermittelt" werden. Zusätzlich wird in dem Seminar die intensive eigene Beschäftigung der Studierenden mit exemplarischen Inhalten gefordert und gefördert – in unterschiedlichen sozialen Kontexten. Auf diese Weise erfolgt für alle Studierenden eine Hinführung an die Thematik, Sichtweisen und Herangehensweisen von *Informatik und Gesellschaft*. Gleichzeitig bietet das offene Seminarkonzept dieser letzten im Studienplan des Bremer Informatikstudiums verbliebenen spezifische Veranstaltung *Informatik und Gesellschaft*[16] Studierenden je nach Motivation, Interessenlage und Engagement vielfältige Vertiefungsmöglichkeiten. Zentrales Mittel hierfür sind sachlich orientierte Diskurse mit Argumentationen, die auf nachvollziehbaren Fakten oder Aussagen basieren, dazu wird die Fähigkeit weiterentwickelt, sich in andere Rollen und Situationen hineinzudenken und einen Sachverhalt aus unterschiedliche Perspektiven wahrzunehmen und einzuschätzen.

> *„Qualitätsvolle Forschung ist m.E. nur noch möglich, wenn bei ihrer Planung und Durchführung die gesellschaftliche Verantwortung beständig mitreflektiert wird. Entsprechende umfassendere Verstehens-, Wissensgenerierungs- und Urteilsbildungsprozesse über disziplinäre Traditionen und Blickwinkel hinaus sind an den Hochschulen immer noch die Ausnahme, jedenfalls nicht die Regel. Ich habe nur dann Hoffnung, dass dies doch noch in der Forschungspraxis ankommt, wenn sich bereits die Studierenden mit dieser Herausforderung vertraut machen können, dürfen und müssen."*
>
> Wolfgang Liebert (2011, S. 27f)

Es ist dem Fach immanent, dass es neben der Analyse von Wirkungszusammenhängen sowie Handlungs- und Gestaltungsoptionen in den Betrachtungen regelmäßig auch um individuelle und gesellschaftliche Werte und ethische Fragen geht.[17] Die Suche nach Entscheidungsgrundlagen, das Ringen um eigene Antworten sowie der kontroverse und konstruktive Austausch können über das Fachliche hinaus zur persönlichen Entwicklung beitragen. Es ist daher wesentlicher Teil der Veranstaltungskonzeption, kommunikative Räume zu schaffen, in denen eigene Gedanken und Bewertungen in Beziehung zum selbst recherchiertem bzw. von anderen vorgetragenem Material gesetzt, hinterfragt und im Diskurs mit anderen reflektiert werden. Dies passiert in den Referat- oder Projektgruppen oft schon während ihrer jeweiligen Vorbereitung sowie regelmäßig in den Seminarsitzungen. Der Lehrende ist dort – neben der Vermittlung ergänzender Inhalte – vor allem in einer Moderatorfunktion tätig. Er unterstützt das Herausarbeiten unterschiedlicher Perspektiven oder Konfliktlinien. Die Praxis zeigt, dass es für die Anregung von Diskussionen im Seminar hilfreich ist, möglichst konkrete Beispiele aus der Forschung oder konkrete Fallstudien oder Szenarien als Grundlage heranzuziehen (vgl. hierzu auch Weber-Wulff, Class, Coy, Kurz & Zellhöfer 2009). Der Lehrende versucht durch Aufwerfen und Präzisieren von Fragen Vergleiche sowie die Betrachtung größerer Zusammenhänge anzuregen. Um an dieser Stelle vielleicht die Terminologie des seinerzeit von Arno Rolf (2008) vorgeschlagenen heuristischen Rahmenkonzepts aufzugreifen: In diesem Sinne wird versucht, strukturierend zu unterstützen, dass die jeweiligen Themen auf unterschiedlichen Ebenen (soziotechnische Perspektive, Mikrokontext, Makrokontext)[18] erörtert und diskutiert werden.

### Übergreifende Lernziele:

Auf einer abstrakten Ebene steht bei der Veranstaltung vor allem ein Ziel im Vordergrund: ein erweitertes Verständnis der Idee sowie der Herangehens- und Betrachtungsweise von *Informatik und Gesellschaft*. Die Annäherung erfolgt in Auseinandersetzung mit dem dialektischen Verhältnis von *Technik* und *Gesellschaft* (und damit in Abgrenzung zu rein technikdeterministischen oder sozialkonstruktivistischen Perspektiven; vgl. Fuchs & Hofkirchner 2003, S. 233ff). Die genauere Betrachtung von Wechselwirkungen zwischen Technik und Gesellschaft erlaubt eine weitergehende Auseinandersetzung sowohl mit Technikgenese als auch mit Technikfolgen. Dies kann und soll (ganz im Sinne von Liebert 2009) insbesondere auch Fragen umfassen nach der Intention und dem Zweck von Technikeinsatz und Technikentwicklung, nach wissenschaftlich-technischen Potentialen, nach normativen Rand- und Vorbedingungen, nach intendierten Folgen, wie auch nach nicht-intendierten Wirkungen. Darauf aufbauend können Risiken abgeschätzt und Gestaltungsperspektiven entwickelt werden. Unreflektiertem Technikoptimismus oder Technikpessimismus wird die differenzierte Betrachtung von Ambivalenz in Forschung und Technologie gegenübergestellt. Grundlegende Fragen zu Verantwortung in Wissenschaft und Gesellschaft knüpfen daran an – insb. natürlich auch Aspekte der professionellen Verantwortung von Informatikerinnen und Informatikern.

Im Sinne einer Kompetenzorientierung ist entscheidend, was die Studierenden[19] am Ende „können" und nicht, was „in der Lehrveranstaltung behandelt" wird. Betrachtet man unterschiedliche Ebenen des Lernens, so steht so bei dieser Veranstaltung nicht eine abfragbare *Reproduktion* von Wissen und Kenntnissen im Vordergrund (obgleich sicherlich auch auf dieser Ebene das ein oder andere vermittelt und gelernt wird), sondern eher eine *Reorganisation* des eigenen Verständnisses von Informatik und deren gesellschaftlicher Bezüge. Dies berührt nicht nur das eigene Fachgebiet, sondern mag auch Folgen für das eigene Selbstverständnis haben, da in der Veranstaltung an vielen Stellen Bezüge zu persönlichen und gesellschaftlichen Werten hergestellt werden. Auf der *Transferebene* besteht das Ziel, dass die Studierenden in der Lage sind, entsprechende Kenntnisse, Betrachtungs- und Herangehensweisen wertebasiert auch auf andere Kontexte zu übertragen. Eher handlungsorientiert und im Sinne selbständigen *Problemlösens* können – so die Hoffnung und das Ziel – die Studierenden die vielfältigen Ansatzpunkte für eine differenzierte, multiperspektivische und werte-reflektierende Betrachtung von Sachverhalten, Szenarien und größeren Zusammenhängen konstruktiv auch in anderen Kontexten nutzen, z. B. in den eher fachorientierten Bereichen des Studiums sowie in der (späteren) Berufstätigkeit.

Inhaltlich ist die aktuelle Konzeption des Seminars *Informatik und Gesellschaft* an der Universität Bremen darauf ausgerichtet, *allen* Informatikstudierenden exemplarisch Einblicke in gesellschaftliche und individuellen Wirkungen, Relevanz, Rahmenbedingungen und Gestaltungsoptionen des Einsatzes von Informations- und Kommunikationstechnik bzw. digitaler Medien in verschiedenen Arbeits- und Lebensbereichen zu ermöglichen. Die Betrachtung erfolgt dabei unter Einbeziehung verschiedener Blickwinkel und Disziplinen und beinhaltet gleichermaßen Elemente von Analyse und Bewertung. Abhängig vom jeweiligen Teilthema werden ggf. auch alternative Gestaltungsoptionen und Handlungsspielräume erörtert. Die konkrete Gestaltung der Lehrveranstaltung erlaubt Studierenden entsprechend ihrer Vorkenntnisse und Interessen die Wahl von Themen und Übernahme von Aufgaben unterschiedlicher Komplexität.[20] Die Intensität der inhaltlichen und zeitlichen Auseinandersetzung mit den gewählten Themen (jenseits notwendiger Grundanforderungen) bestimmen die Studierenden dabei individuell. Von den anderen Teilnehmerinnen und Teilnehmern ihres Seminars erhalten sie hinsichtlich ihrer eigenen Präsentationen konstruktiv-kritisches Feedback. In semesterbegleitenden Projekten können interessierte Studierende im Sinne forschenden Lernens eigene Herangehensweisen an Themen entwickeln und erproben. Die Veranstaltung lässt insgesamt ein hohes Mal an individuellen Gestaltungsmöglichkeiten für die Studierenden zu, um der Heterogenität der Teilnehmerinnen und Teilnehmer, ihren jeweiligen Lernvoraussetzungen und ihrer Motivationen gerecht zu werden. [21]

### Die einzelnen Elemente der Veranstaltung:

Im Zentrum der Seminare *Informatik und Gesellschaft* stehen Referate, welche die Studierenden in Gruppen bis zu drei Personen erarbeiten und vortragen. Im Vergleich zu den Anfängen des Studiengangs sind inhaltlich aufgrund des technischen und des gesellschaftlichen Wandels über die Jahre viele neue und aktuelle Anwendungsfelder und Themen für *Informatik und Gesellschaft* hinzugekommen, andere sind in den Hintergrund getreten und manche thematische Gewichtungen haben sich verschoben. Es hat sich bewährt, den Studierenden bei der Wahl der von ihnen aktiv zu bearbeitenden Inhalte große Freiheit zu lassen – an die Stelle von Vorgaben tritt Beratung. Die Themen der Referate schlagen die Studierenden selbst vor.[22] Diese entwickeln und konkretisieren sie anschließend iterativ im Gespräch mit dem Lehrenden[23] und unterstützt durch eine Literaturrecherche.[24] In der Regel verläuft dabei der Weg von einem eher diffusen Interesse an einem größeren Themenbereich hin zur Formulierung handhabbarer kleiner Themenstellungen, die exemplarisch vertieft betrachtet werden können.[25] Referat und Diskussion (und ggf. von anderen Studierenden erhaltene inhaltliche Rückmeldungen) sind Ausgangspunkt für eine schriftliche Ausarbeitung zu diesem Thema.

In dem gemeinsamen Prozess der Themenfindung und Festlegung wird sichergestellt, dass innerhalb eines jeden der Seminare hinreichend unterschiedliche Themen bearbeitet werden. Es ist hier nicht der Ort, im Detail auf häufiger gewählte Themenblöcke oder typische Fragestellungen einzugehen, nur soviel sei gesagt: Die solcherart entstehende theoretische und praktische Vielfalt der Themen darf nicht mit Beliebigkeit verwechselt werden. Regelmäßig zeigt sich, dass viele Grundfragen, Grundprobleme und Grundkonflikte in nahezu jedem Seminar durch studentische Themenvorschläge in verschiedener Weise präsent sind und damit an passender Stelle inhaltlich aufgegriffen und bearbeitet werden können. Gegebenenfalls werden fehlende oder grundlegende Aspekte im Laufe der Veranstaltung an der ein oder anderen Stelle durch den Lehrenden ergänzend eingebracht.

> *„Bei der Forderung, die Auseinandersetzung um die gesellschaftliche Wirkung auch innerhalb der Fachwissenschaft zu führen, ist allerdings zu beachten, dass das keine neutrale oder wertfreie Position ist. Eine demokratische Gesellschaft ist im Gegenteil die Voraussetzung für einen verantwortungsbewussten Diskurs innerhalb von Wissenschaft und Technik, und in einer demokratischen Gesellschaft müssen Wissenschaft und Technik im Dienst der Menschen und des Gemeinwesens stehen.“*
>
> Hans-Jörg Kreowski (2008, S. 32)

Unabhängig von und zusätzlich zu den Referaten kann – als Element integrierten forschenden Lernens – eine zusätzliche inhaltliche Auseinandersetzung mit einem Teilthema aus *Informatik und Gesellschaft* in Form eines kleinen semesterbegleitenden Projekts erfolgen, in dem eine Gruppe von Studierenden sich einer sie interessierenden Fragestellung widmet und diese selbständig bearbeitet. Die untersuchte Fragestellung soll sich dabei hinreichend vom Thema des eigenen Referats unterscheiden. Methodisch kann ein Projekt wahlweise recherchebasiert oder empirisch angegangen werden. Der Lehrende steht während des Planungs- und Durchführungsprozesses bei Bedarf unterstützend zur Verfügung. Die Projektergebnisse der einzelnen Gruppen werden am Ende des Semesters in größerer Runde präsentiert – oftmals als Poster, wie man es von Tagungen kennt (andere Präsentationsformen sind willkommen, so gab es in der Vergangenheit beispielsweise Präsentationen als Kurzfilm oder als Audio-Feature mit Interviewausschnitten). Die projektorientierte Form des Vorgehens beinhaltet viele Freiheitsgrade, die motivierten Studierenden ermöglichen, in kleinen Erkundungsstudien eigenständig selbst gewählten Fragestellungen nachzugehen. Die Erfahrungen bei Planung und Durchführung solcher Projekte (incl. ggf. erlebter Schwierigkeiten) führt in der Folge häufig zu einem besseren und kritischeren Umgang mit forschungsbasierter wissenschaftlicher Literatur.

Studierende, die kein Projekt machen möchten, können alternativ den Vortragenden mehrerer Referatsgruppen jeweils ein ausführliches schriftliches Feedback zukommen lassen – auf diese Weise setzen sie sich jenseits ihres eigenen Referats vertieft mit weiteren IuG-Themen (hier den Inhalten der jeweiligen Vorträge) auseinander. Beide Alternativen – Projekt und Feedbacks – finden jedes Semester Zuspruch, was belegt, dass auch diese Wahlmöglichkeit der Heterogenität der Teilnehmerinnen und Teilnehmer entgegenkommt.

Wenngleich aus den oben geschilderten Gründen die Veranstaltung *Informatik und Gesellschaft* in der jetzigen Konzeption keine durchgängige Vorlesung beinhaltet, so gibt es im Laufe des Semesters doch einige Termine (Plenum), zu denen die Teilnehmerinnen und Teilnehmer aller IuG-Seminare des Semesters zusammenkommen. Neben organisatorischen Aspekten dienen diese Termine vor allem der Vermittlung wesentlicher Hintergründe und Herangehensweisen von *Informatik und Gesellschaft*. Dies kann – aufgrund der knappen Zeit – nur in eingeschränkter Weise erfolgen, hat sich jedoch als sehr wichtiger Faktor im Hinblick auf die Qualität der späteren studentischen Seminarbeiträge herausgestellt.



Das Plenum der Veranstaltung bietet zudem die Möglichkeit, Gäste in die Veranstaltung einzuladen, welche an jeweils einem Termin die Teilnehmerinnen und Teilnehmer aller IuG-Seminare des Semesters erreichen. Mit gewisser Regelmäßigkeit besucht beispielsweise die Landesbeauftragte für Datenschutz und Informationsfreiheit des Landes Bremen, Imke Sommer, die Veranstaltung und stellt in einem Vortrag die Grundlagen ihrer Arbeit verknüpft mit aktuellen Beispielen und aktuellen politischen Diskussionen dar. Aspekte des Einsatzes von Informatikanwendungen im Kontext von Betrieben und Organisationen sowie diesbezügliche Grundlagen zur Mitbestimmung werden in manchen Semestern von Peter Ansorge (BIFA)[26] vor dem Hintergrund langjähriger Erfahrung in der Beratung von Betriebs- und Personalräten im Plenum anschaulich und praxisnah vermittelt. Bis zur Auflösung der Arbeitsgruppe „Soziotechnische Systemgestaltung + Gender" hatte regelhaft mehrere Jahre lang Carola Schirmer im Plenum das Themenfeld „Informatik und Gender" in Gastvorträgen beleuchtet. Andere und weitere Gastvorträge sind denkbar und werden jeweils nach Möglichkeit und Interessenlage eingebunden.

Das Seminar *Informatik und Gesellschaft* dient darüber hinaus als Plattform, um interessierten Studierenden weitergehende thematisch dazu in Beziehung stehende Angebote zu machen.[27]

In den Seminardiskussionen finden neben „klassischen" Themen auch zeit- oder manchmal sogar tagespolitische Entwicklungen und Strömungen Eingang – oft von Studierenden selbst aktiv eingebracht. Derartige Bezüge zu Geschehnissen oder Entwicklungen im Umfeld der eigenen Lebenswelt erhöhen bei manchen Seminarteilnehmern erkennbar die Motivation, sich aktiv in Diskussionen einzubringen. Daneben ist jedoch auch der Blick in die Vergangenheit häufig in den Seminaren präsent und hilfreich. Arno Rolf bezeichnet dies als *Ergänzung der Fachdisziplin um eine temporale Perspektive* (Rolf 2008). Er verweist darauf, dass in der Betrachtung früherer Diskurse und Entscheidungen ein großes Potential für das Verständnis von Entwicklungspfaden und Handlungsoptionen liegen kann. In diesem Sinne werden die Studierenden in der aktuellen Lehrveranstaltung vom Lehrenden unterstützt und ermutigt, von den selbst gewählten, oft aktuellen Themen Bezüge und Vergleiche zu früheren Entwicklungen und Diskursen herzustellen. Auf diesem Weg gelingt es manchmal leichter, eine für die analytische Reflexion hilfreiche Distanz zum Gegenstand herzustellen.

Wesentlich für die vielschichtige Annäherung an die jeweiligen Themen ist – wie bereits erwähnt – der multidisziplinäre Charakter der Veranstaltung. Es spiegelt sich u. a. wider in der Einbeziehung von Quellenmaterial und Gedankengut unterschiedlicher Fachdisziplinen (abhängig vom gewählten Thema). Ich verwende hier bewusst den vergleichsweise schwachen Begriff der Multidisziplinarität, obgleich in manchen Situationen durchaus auch echt interdisziplinäre Ansätze im Sinne eines aktiven Zusammenführens verschiedener Disziplinen zu erkennen sind. Besonders kommt dies zum Tragen, wenn Studierende anderer Studiengänge am Seminar teilnehmen und gemeinsam mit Informatikstudierenden gemischte Arbeitsgruppen bilden – die *Informatik und Gesellschaft*-Seminare sind (im Rahmen der kapazitären Möglichkeiten) grundsätzlich für Studierende aller Fächer geöffnet.

## 40 Jahre *Informatik und Gesellschaft* in Bremen

Wie bereits zu Beginn dieses Beitrags erwähnt: Wenn im Herbst 2018 der Bremer Informatik-Studiengang sein 40-jähriges Bestehen verzeichnet, so gilt das Gleiche für das Fachgebiet *Informatik und Gesellschaft* in diesem Studiengang. Ein Grund zum Feiern?

Das Konzept der Bremer Informatik war schon bei Gründung des Studiengangs auf einen breiten Ansatz der Integration von Anwendungen und Rahmenbedingungen in die Fachlehre ausgelegt. Von Anfang an bestand dabei Klarheit, dass hierzu – ebenso wie in den fachlichen Inhalten der Kerninformatik – die Vermittlung von Grundlagen und Betrachtungsweisen in einem eigenen Fach notwendige Voraussetzung ist. In diesem Sinne wurde bei Gründung des Studiengangs die Säule *Informatik und Gesellschaft* im Pflichtprogramm der Studienstruktur verankert.

- 1993 wurden diese Säule von einem sich über drei Semester erstreckenden Veranstaltungszyklus auf zwei Veranstaltungen reduziert – das Fachgebiet selbst ist fester Teil des Studienplans geblieben.


**Ralf E. Streibl**

Ralf E. Streibl arbeitet seit März 1993 am Fachbereich Mathematik/Informatik an der Universität Bremen, anfänglich in der Arbeitsgruppe von Jürgen Friedrich. Heute ist er dort selbständig in der Lehre tätig und insb. verantwortlich für die Lehre in *Informatik und Gesellschaft*. Seit 2009 ist er außerdem Mitglied im Personalrat der Universität Bremen.

Sein Studium verbrachte er überwiegend an der Universität Erlangen-Nürnberg, wo er Lehrveranstaltungen in Psychologie, Informatik und vielen anderen Fächern besuchte und als Diplom-Psychologe abschloss. Er ist Mitglied im Beirat des FIfF.

- 2002 erfolgte im Zuge der Studienreform bei Einführung des Bachelor-Studienganges eine weitere Reduktion auf jetzt eine Veranstaltung, das heutige Seminar *Informatik und Gesellschaft* – das Fachgebiet selbst ist fester Teil des Studienplans geblieben.

- Die für das Fach im Hochschullehrertableau vorgesehene Professur für Informatik und Gesellschaft wurde nach dem altersbedingten Ausscheiden von Jürgen Friedrich im Jahr 2007 nicht wieder besetzt – das Fachgebiet selbst ist fester Teil des Studienplans geblieben.

Informations- und Kommunikationstechnik und digitale Medien sind heutzutage in allen Arbeits- und Lebensbereichen verbreitet. Versteckte Leitbilder, Metaphern und Werte sind Teil des Alltags in einer „Informationsgesellschaft" und auch Teil eines jeglichen Informatik-Studiums. Lehrveranstaltungen in *Informatik und Gesellschaft* sind ein geeigneter Ort, dies zu erkennen und ggf. zu hinterfragen, befand Jürgen Friedrich (1992). Auch heute hat sich daran nichts geändert: Die Veranstaltung *Informatik und Gesellschaft* im Bremer Informatik-Studiengang war und ist seit 40 Jahren ein wichtiger Ort der Reflexion und des Innehaltens. Inhaltlich, didaktisch und methodisch als Seminar neu konzipiert und stetig weiter entwickelt ist die Veranstaltung aktuell und gegenwärtig – und gleichzeitig vielfältig verwurzelt und verbunden mit der langjährigen Geschichte des Fachgebiets *Informatik und Gesellschaft* in Bremen und anderswo.

Kein Fazit.
Es geht weiter!

## Referenzen


Arbeitskreis Informatik und Verantwortung (2003): Ethische Leitlinien der GI – Entwurf des Arbeitskreises "Verantwortung". In: Informatik-Spektrum, 26 (6), S. 418-422.

Baase, S. (1997): A Gift of Fire. Social, Legal, and Ethical Issues in Computing. Upper Saddle River: Prentice-Hall.

Baase, S.; Henry, T.M. (2018). A Gift of Fire. Social, Legal, and Ethical Issues for Computing Technology. 5th Edition. Upper Saddle River: Prentice-Hall.

Claus, V. (1988): Informatik in Bremen und anderswo. Festvortrag zum zehnjährigen Bestehen des Studiengangs Informatik an der Universität Bremen. In: 10 Jahre Informatik an der Universität Bremen (Sammlung von Reden und Schriften). Bremen. Universität, S. 5-15.

Coy, W. (1992): Informatik – Eine Disziplin im Umbruch. In: Coy, W.; Nake, F.; Pflüger, J.-M.; Rolf, A.; Seetzen, J.; Siefkes, D.; Stransfeld, R. (Hrsg.): Sichtweisen der Informatik. Braunschweig: Vieweg, S. 1-15.

Coy, W. (1996): Was ist, was kann, was soll „Informatik und Gesellschaft"? In: Schinzel, B. (Hrsg.) (1996): Schnittstellen. Zum Verhältnis von Informatik und Gesellschaft. Braunschweig: Vieweg, S. 17-27.

Coy, W. (2001): Weder vollständig noch widerspruchsfrei. In: FIfF Kommunikation, 18 (4), S. 45-48 – als „Retrospektive" nachgedruckt auf den Seiten 20 bis 22 der hier vorliegenden Ausgabe 3/18 der FIfF-Kommunikation.

Coy, W. (2018): Nachruf auf Jürgen Friedrich. Berlin, 28.8.2018 (versandt über den Newsletter „Informatik und Gesellschaft" – abgedruckt auf Seite 5 der hier vorliegenden Ausgabe 3/18 der FIfF Kommunikation).

Coy, W.; Nake, F.; Pflüger, J.-M.; Rolf, A.; Seetzen, J.; Siefkes, D.; Stransfeld, R. (Hrsg.) (1992): Sichtweisen der Informatik. Braunschweig: Vieweg.

Engbring, D.; Streibl, R.E. (2001): Informatik und Gesellschaft als akademische Disziplin. (Editorial zum gleichnamigen Schwerpunktheft). In: FIfF Kommunikation, 18 (4), S. 3-4.

Friedrich, J. (1988): Informatik und Gesellschaft – eine Bremer Besonderheit. In: 10 Jahre Informatik an der Universität Bremen (Sammlung von Reden und Schriften). Bremen. Universität, S. 43-45.

Friedrich, J. (2001): Informatik und Gesellschaft. Aufstieg, Stagnation und Zukunft einer Disziplin. In: FIfF Kommunikation, 18 (4), S. 59-61.

Friedrich, J.; Herrmann, Th.; Peschek, M.; Rolf, A. (Hrsg.) (1995): Informatik und Gesellschaft. Heidelberg: Spektrum.

Fuchs, Ch.; Hofkirchner, W. (2003): Studienbuch Informatik und Gesellschaft. Norderstedt: Books on demand.

GI – Gesellschaft für Informatik (2018): Unsere ethischen Leitlinien. Bonn: GI. https://gi.de/fileadmin/GI/Allgemein/PDF/GI_Leitlinien_DIN_lang.pdf (Abruf 10.09.2018).

Griesche, H.-D. (1972): Die Bremer Hochschulreform und die Presse. Eine Analyse der Berichterstattung 1970/1971. Bremen: Schünemann.

Klischewski, R. (1999): Informatik und Gesellschaft – eine Einführung (Themenheft im Rahmen der Tübinger Studientexte Informatik und Gesellschaft, hrsg. von D. Krause und H. Klaeren). Universität Tübingen.

Kreowski, H.-J. (2008): Braucht die Informatik eine kritische Auseinandersetzung mit ihren Folgen? In: Kreowski, H.-J. (Hrsg.): Informatik und Gesellschaft. Verflechtungen und Perspektiven. Berlin: Lit, S. 29-35.

Langenheder, W.; Müller, G.; Schinzel, B. (Hrsg.) (1992): Informatik cui bono? Berlin: Springer.

Liebert, W. (2009): Umgang mit Dual-Use von Technologien und Ambivalenz in der Forschung. In: Albrecht, S.; Bieber, H.-J.; Braun, R.; Croll, P.; Ehringhaus, H.; Finckh, M.; Graßl, H.; von Weizsäcker, E.U. (Hrsg.): Wissenschaft – Verantwortung – Frieden: 50 Jahre VDW. Berlin: Berliner Wissenschafts-Verlag, S. 445-450.

Liebert, W. (2011): Wissenschaft und gesellschaftliche Verantwortung. In: Eger, M.; Gondani, B.; Kröger, R. (Hrsg.:): Verantwortungsvolle Hochschuldidaktik. Berlin: Lit, S. 15-33.

Löhr, K.-P. (1988): Eine spezifisch bremische Informatik? Rückschau auf das erste Jahrzehnt eines neuen Studiengangs. In: 10 Jahre Informatik an der Universität Bremen (Sammlung von Reden und Schriften). Bremen. Universität, S. 16-19.

Meier-Hüsing, P. (2011): Universität Bremen. 40 Jahre in Bewegung. Bremen: Edition Temmen.

Meyer-Degenhardt, K. (1988): Beratungsstelle für Informationstechnik (BIFA) als Beitrag zum Wissenschaftstransfer für Arbeitnehmer. In: 10 Jahre Informatik an der Universität Bremen (Sammlung von Reden und Schriften). Bremen. Universität, S. 54-55.

Nake, F. (1992a): Informatik und die Maschinisierung von Kopfarbeit. In: Coy, W.; Nake, F.; Pflüger, J.-M.; Rolf, A.; Seetzen, J.; Siefkes, D.; Stransfeld, R. (Hrsg.): Sichtweisen der Informatik. Braunschweig: Vieweg, S. 181-201

Nake, F. (1992b): In unbekanntem Land. Vom Einlassen des Informatikers auf alltägliche Situationen. In: Langenheder, W.; Müller, G.; Schinzel, B. (Hrsg.): Informatik cui bono? Berlin: Springer, S. 29-39.

Ott, K.; Busse, J. (1999): Ethik in der Informatik. (Themenheft im Rahmen der Tübinger Studientexte Informatik und Gesellschaft, hrsg. von D. Krause und H. Klaeren). Universität Tübingen.

Pflüger, J. (2001): Was machen wir, wenn wir gewonnen haben sollten? In: FIfF Kommunikation, 18 (4), S. 16-18.

Pieper, Ch. (2009): Hochschulinformatik in der Bundesrepublik und der DDR bis 1989/1990. Stuttgart: Franz Steiner.

PKI (1979): Bericht der Planungskommission Informatik über die Planung eines Studienganges Informatik an der Universität Bremen. Bremen: Universität.

Robben, B. (2013): Projektstudium in Bremen. (K)Eine Erfolgsgeschichte. In: Huber, L.; Kröger, M.; Schelhowe, H. (Hrsg.): Forschendes Lernen als Profilmerkmal einer Universität. Beispiele aus der Universität Bremen. Bielefeld: UVW, S. 37-55.

Rödiger, K.-H.; Wilhelm, R. (1996): Zu den Ethischen Leitlinien der Gesellschaft für Informatik. In: Informatik-Sprektrum, 19 (2), S. 79-86.

Rolf, A. (1992): Informatik als Gestaltungswissenschaft – Bausteine für einen Sichtwechsel. In: Langenheder, W.; Müller, G.; Schinzel, B. (Hrsg.): Informatik cui bono? Berlin: Springer, S. 40-48.

Rolf, A. (2008): Mikropolis 2010. Menschen, Computer, Internet in der globalen Gesellschaft. Marburg: Metropolis.

Schefe, P. (2001): Ohnmacht der Ethik? Über professionelle Ethik als Immunisierungsstrategie. In: Informatik-Spektrum, 24 (3), S. 154-162.

Schinzel, B. (Hrsg.) (1996): Schnittstellen. Zum Verhältnis von Informatik und Gesellschaft. Braunschweig: Vieweg.

Steinmüller, W. (1993): Informationstechnologie und Gesellschaft. Einführung in die Angewandte Informatik. Darmstadt: Wissenschaftliche Buchgemeinschaft.

Streibl, R.E. (2014): warnen und mahnen. diskutieren und begleiten. vorausschauen und fordern. 30 Jahre FIfF. In: FIfF Kommunikation, 31 (4), S. 35-39.

Universität Bremen (1981): Universität Bremen 1971–1981. Entwicklung – Planung – Aufgaben. Bremen: Universität.

Universität Bremen (1992): 20 Jahre Universität Bremen. Zwischenbilanz: Rückblick und Perspektiven. Bremen: Universität.

Weber-Wulff, D.; Class, Ch.; Coy, W.; Kurz, C.; Zellhöfer, D. (2009): Gewissensbisse. Ethische Probleme der Informatik. Biometrie – Datenschutz – geistiges Eigentum. Bielefeld: transcript.

Weichert, Th. (2013): Nachruf auf den Datenschutzpionier Wilhelm Steinmüller. In: vorgänge Nr. 201/202 (1/2-2013), S. 169-171.

Weisser, M.; Nake, F. (2018): Michael Weisser im Gespräch mit Prof. Dr. Frieder Nake über Algorithmische Revolution, Digitale Kultur, Ästhetik, Computer, Kunst. [eBook] WhitePaperCollection 24. München: BookRix GmbH.

Weizenbaum, J. (1978): Die Macht der Computer und die Ohnmacht der Vernunft. Frankfurt: Suhrkamp. [engl. Originalausgabe 1976]

Wolff, M. (2011): Von Marx zu Darwin. Universität Bremen – eine Zeitreise. DVD (98min). Bremen: Edition Temmen.

*sowie Veranstaltungsverzeichnisse, Personen- und Einrichtungsverzeichnisse der Universität Bremen.*



*Beim Universitätsarchiv Bremen bedanke ich mich für die freundliche Unterstützung, bei Frieder Nake für hilfreiche Anmerkungen zur frühen Bremer Geschichte.*

## Anmerkungen:

1 *Dies kann im Rahmen solch eines Artikels naturgemäß nicht mit dem Anspruch auf Vollständigkeit geschehen.*

2 *Hier ist nicht der Ort, um die weiteren politischen Debatten und Verwerfungen von der Gründungszeit bis heute nachzuzeichnen. Vgl. hierzu u. a. Meier-Hüsing (2011), Wolff (2011), Universität Bremen (1981; 1992), Griesche (1974).*

3 *Die Vorgeschichte der Entwicklung der Informatik an den Hochschulen wird ausführlich beschrieben bei Pieper (2009).*

4 *Die UKI sollte prüfen, ob ein Studiengang Informatik an der Universität Bremen sinnvoll und notwendig sei. Im Zuge dieses Prozesses wurde die These von der Maschinisierung der Kopfarbeit entwickelt (vgl. inhaltlich hierzu den späteren Aufsatz von Nake 1992a).*

5 *Zur Geschichte des Projektstudiums an der Universität Bremen, der besonderen Umsetzung im Fach Informatik als viersemestriges Projekt im Hauptstudium des Diplomstudiengangs sowie zu weiteren Entwicklungen bis hin zum Bologna-Prozess (mit dann zwei kleineren Projektanteilen im Bachelor und im Master-Studiengang) liefert ein Aufsatz von Robben (2013) wertvolle Hintergründe und Gedanken.*

6 *Gendersensitive Formulierungen waren auch an der Universität Bremen damals noch nicht die Regel.*

7 *Das Informatik-Seminar an der TU Berlin beschäftigte sich ab 1970 mit Fragen gesellschaftlicher Bedingungen und Auswirkungen der Informatik und kann als eine Keimzelle von Informatik und Gesellschaft in Deutschland angesehen werden (Friedrich 2001, S. 59). An der Universität Dortmund etablierte sich Mitte der 70er Jahre ein Bereich Informatik und Gesellschaft, der ab 1976 von Jürgen Friedrich als eigenständigem wissenschaftlichem Mitarbeiter betreut wurde (Coy 2018).*

8 *Die genaue Denomination der Stelle lautete damals „Gesellschaftliche Entwicklungsbedingungen und Auswirkungen moderner Informationstechnologien“ und wurde später in „Informatik und Gesellschaft“ geändert.*

9 *Wilhelm Steinmüller, einer der Pioniere des Datenschutzes, wurde 1982 an die Universität Bremen berufen. Er gilt als Mitbegründer des Konzepts der informationellen Selbstbestimmung, welches dem Bundesverfassungsgericht in seinem „Volkszählungs-Urteil“ als Grundlage für die Formulierung des „Datenschutz-Grundrechts“ diente (vgl. Weichert 2013).*

10 *Bevor er an die Humboldt-Universität nach Berlin berufen wurde, war Wolfgang Coy von 1979 bis 1996 Hochschullehrer in der Informatik an der Universität Bremen.*

11 *Die Ethischen Leitlinien der GI wurden 2003 und zuletzt 2018 überarbeitet. Eine Betrachtung der Entwicklungsgeschichte und Unterschiede der Fassungen würde an dieser Stelle den Rahmen sprengen (Rödiger & Wilhelm 1996; Schefe 2001; Arbeitskreis Informatik und Verantwortung 2003; GI 2018)*

12 *Die Vergabe eines Studienpreises wurde von der Mitgliederversammlung des FIfF beschlossen – auch als Reaktion auf die Nicht-Wiederbesetzung vakant gewordener „Informatik und Gesellschaft“-Professuren. In der Ausschreibung für das Jahr 2018 heißt es: „Das FIfF stiftet den Weizenbaum-Studienpreis in Erinnerung an den Wissenschaftler und Informatik-Pionier Professor Dr. Joseph Weizenbaum in Würdigung seiner Verdienste um einen kritischen Blick auf die Informatik“. Eingereicht werden können Qualifikationsarbeiten (Bachelor-, Master-, Diplomarbeiten oder Dissertationen), die in den letzten zwei Jahren vor Nominierungsschluss abgeschlossen wurden. Die Idee hinter dem Preis: „Studierende sowie Wissenschaftlerinnen und Wissenschaftler in der Qualifikationsphase sollen hiermit zu fundierten und differenzierten Auseinandersetzungen mit Fragen aus dem Gebiet Informatik und Gesellschaft ermutigt werden.“ – Quelle: https://www.fiff.de/studienpreis (Abruf 11.9.2018)*

13 Susanne Maaß wurde 1998 auf eine Professur an der Universität Bremen berufen, die teilweise in der Informatik und teilweise im Zentrum Gender Studies angesiedelt war.

14 Das Fach Informatik war eines der ersten, die an der Universität einen Bachelor-Studiengang einführten, es schloss den Diplomstudiengang aber erst viele Jahre später (auf politischen Druck hin). Die sich durch das parallele Angebot beider Studiengänge ergebende Flexibilität, sich ggf. später im Studium für die jeweils andere Abschlussform entscheiden zu können, ohne dass es dadurch zu Studienzeitverlängerung kommen musste, wurde von den Studierenden begrüßt und in der Praxis durch Wechsel in beiden Richtungen genutzt.

15 Maike Hecht und Carola Schirmer waren zu dieser Zeit Mitarbeiterinnen in der Arbeitsgruppe „Soziotechnische Systemgestaltung + Gender", die von Susanne Maaß geleitet wurde.

16 Natürlich gibt es weiterhin auch andere Lehrveranstaltungen, in den Aspekte, Sichtweisen und Themen aus Informatik und Gesellschaft aufgegriffen werden – der Hauptfokus dieser Lehrveranstaltungen liegt dabei naturgemäß jeweils in der Vermittlung ihrer Fachinhalte.

17 Die Spanne reicht hier von der konkreten Bezugnahme auf Ethiktheorien (vgl. z. B. Ott & Busse 1999) bis hin zum allgemeineren Verständnis eines „Orientierungswissens" sensu Mittelstraß als notwendige Ergänzung des Fach- bzw. Verfügungswissens (vgl. Rolf 2008).

18 Rolf (2008) geht dabei u. a. auf die Notwendigkeit eines Verständnisses der Prozesse Dekontextualisierung und Rekontextualisierung ein. In diesem Sinne ist im Seminar beispielsweise die Frage nach den einem konkreten System zugrundliegenden Modellen und deren Passung oft hilfreich und anregend für die Diskussion.

19 Zu den „Studierenden" gehört in diesem Sinne auch der Lehrende selbst, da der Prozess des Lernens und der eigenen Weiterentwicklung nicht bei einem Ziel endet, sondern gerade bei einer Veranstaltungskonzeption wie dieser im Diskurs mit den Studierenden, in aktiver Auseinandersetzung mit den Inhalten sowie im Hinterfragen eigener Überzeugungen unablässig weitergeht.

20 Der Lehrende ist hierbei neben seiner Fachlichkeit vor allem in der Rolle als Begleiter individueller Lernprozesse gefragt. Er kann hinsichtlich der Schwierigkeit der selbst gewählten Aufgaben und Themenstellungen Einschätzungen geben und – wenn gewünscht – den Gruppen im Kontext ihrer Referatvorbereitung und Projektarbeiten als Reflektor dienen. Studierende und Lehrende gestalten im Idealfall aktiv einen von Wertschätzung, Transparenz und Authentizität charakterisierten Prozess des gemeinsamen Lernens und der Entwicklung. Dazu gehört selbstverständlich auch, sich eigener Unzulänglichkeiten bewusst zu sein, das eigene Lehr-Handeln in kritischer Selbstreflexion zu begleiten und die Konzeption der Veranstaltung aufbauend auf den Erfahrungen stetig weiterzuentwickeln.

21 An dieser Stelle wird darauf verzichtet, ausführlicher auf integrierten außerfachlichen Lernziele der Veranstaltung Informatik und Gesellschaft einzugehen, die insb. den sogenannten „soft skills" zuzurechnen sind.

22 Studierende, die sich bei der Themenfindung unsicher fühlen, werden in der entsprechenden Seminarsitzung teilweise von den Ideen anderer inspiriert und mitgerissen. Auf diese Weise finden sich in der Sitzung öfters Referatsarbeitsgruppen anhand ihrer thematischen Interessen zusammen (und nicht nur aufgrund vorheriger Bekanntschaft). Mit Blick auf die Heterogenität der Teilnehmenden, hält der Lehrende für Unentschlossene als Anregung eine Übersicht über einige typische Themengebiete aus „Informatik und Gesellschaft" bereit.

23 Da seit einiger Zeit alle IuG-Seminare vom Autor dieses Artikels betreut werden, wird an dieser Stelle ausschließlich die maskuline Form verwendet.

24 Regelmäßig ist in der Phase der Themenfestlegung die für das Fach Informatik zuständige Fachreferentin der Staats- und Universitätsbibliothek zu Gast in der Veranstaltung, informiert die Studierende über erweiterte Möglichkeiten der Suche nach wissenschaftlichen Quellen in spezifischen Fachdatenbanken und unterstützt und unterstützt die Referatgruppen auf Wunsch individuell bei ihrer gezielten Recherche.

25 Die Erfahrung zeigt, dass bei zu großen Themenstellungen eher „an der Oberfläche gekratzt" wird, während Studierende, wenn sie parallel zur Ihren Recherchen dann ein möglichst konkretes und überschaubares Thema formulieren, dieses dann in der Regel deutlich fundierter angehen. Die Diskussionen während und nach den Referaten erweitern das Thema üblicherweise – auch mit Blick auf Vergleichbares oder Verallgemeinerbarkeiten.

26 Die BIFA (das Kürzel stand ursprünglich für „Beratungsstelle für Informationstechnikfolgen und -Alternativen") wurde 1984 im Fachbereich Mathematik und Informatik der Universität Bremen als Pilotprojekt gegründet und 1986 verstetigt (vgl. Meyer-Degenhardt 1988). Sie leistet bis heute einen wichtigen Beitrag zum Wissenschaftstransfer für Arbeitnehmervertretungen, als fachlich fundierte Grundlage zur Wahrnehmung ihrer bestehenden Beteiligungsrechte.

27 Entsprechende Angebote waren u. a. Exkursionen zum Computermuseum HNF in Paderborn, gemeinsame Theaterbesuche (beispielsweise 1984 von George Orwell), Ansehen und Diskussion thematisch interessanter Filme, Hinweise auf interessante zivilgesellschaftliche Veranstaltungen, Fachtagungen, aktuelle Ereignisse, Literatur etc.



Wolfgang Coy

# Weder vollständig noch widerspruchsfrei



Informatik ist eine technische Wissenschaft. Das ist eine banale Erkenntnis, die dennoch viel Widerspruch erfahren hat.[1] Rechnerbau und Softwareentwicklung, die gewachsenen Kernbereiche der Informatik, kommen aus einer konstruktiven technischen Praxis, nämlich einerseits dem Präzisionshandwerk des Instrumentenbaus und andererseits aus der Mathematik, vor allem der Numerik. Die faszinierende Leistung der Pioniere der Informatik bestand darin, eine mathematisch-logische Basis der maschinellen Rechenkunst zu schaffen. Alan Turing und John von Neumann haben diese Fundierung frühzeitig erkannt, aber auch Konrad Zuse hat sich fortwährend mit der mathematisch-logischen Basis befasst. Logik, Daten und Algorithmen – das sind die drei formalen Bauelemente der Informatik. Deren Umsetzung in rechnende Maschinen, die Kopplung mit digitalisierten Signalen und die globale Vernetzung haben die moderne Informatik geformt.

Bau und Programmierung von Rechenanlagen haben eine eigentümliche Form der Kommunikation geschaffen, nämlich die Notwendigkeit, eine vom Computer zu bearbeitenden Aufgabe in kontextfreier, strikt kalkülhafter Weise zu formulieren, eben: zu programmieren. Dies war vergleichsweise einfach, als die Computer noch Rechner waren: Numerische Berechnungen sind naheliegender Weise algorithmisch und als Programme notierbar. Je mehr aber die Informatik in die technische, industrielle und gesellschaftliche Praxis vordringt, um so unschärfer werden Aufgabenstellungen und um so bedeutender wird der jeweilige Kontext. Diese Kontexte treten in vielfältiger Form auf, die die Auswahl der anwendbaren Programmverfahren einschränken. So mögen je nach Aufgabe unterschiedliche Anforderungen an die Präzision einer Rechnung oder Reaktionsgeschwindigkeit eines Programms gestellt werden. Banken haben z. B. bestimmte Rundungsregeln, die am besten durch BCD-Arithmetik (statt binärer Arithmetik) abgebildet werden. Realzeitsysteme, wie beispielsweise ABS-Steuerungen im Auto, geben bestimmte maximale Reaktionszeiten für die Berechnung vor. Am restriktivsten aber mögen die rechtlichen, politischen und vor allem ökonomischen Zwänge wirken, die im jeweiligen Anwendungskontext vorgegeben sind. Kurz gesagt: Reale Aufgaben der Informatik entstehen im Kontext, werden im Kontext geformt und hängen vom Kontext ab.

Die informatische Lehre hat sich lange auf die Vermittlung von kalkülhaftem Wissen und kalkülhaften Fertigkeiten konzentriert und die realen Kontextbeschränkungen weitgehend ignoriert – mit zwei wichtigen, freilich innertechnischen Ausnahmen: Rechengeschwindigkeiten und Speicherbedarf. Das entsprach den unmittelbaren technischen Gegebenheiten – alle Computer sind bis auf den heutigen Tag zu langsam und stellen zu wenig Speicher zur Verfügung. Nicht nur die Konstrukteure und Programmierer, sondern auch die Theoretischen Informatiker haben diesem Problemkreis deshalb besondere Aufmerksamkeit gewidmet: In der Komplexitätstheorie wird unterhalb der harten Schranke der Berechenbarkeit vor allem das Laufzeitverhalten und der Platzbedarf von Algorithmen untersucht. Die allgemeineren Kontexte der informatischen Anwendungen werden in Lehre und Forschung meist weniger aufmerksam verfolgt – wenn überhaupt. Nach wie vor bilden Regelhaftigkeit, Explizitheit, Korrektheit, Vollständigkeit oder Entscheidbarkeit die Leitlinien informatischer Ausbildung. In der Informatik werden in erfolgreicher Tradition einzelne Aspekte der beruflichen und wissenschaftlichen Anforderungen gelehrt, es mangelt aber an der Integration zu einem reflektierenden Ganzen. Dies ist um so bedauerlicher, als die Informatik sich in ihrem Objektbezug regelmäßig gehäutet hat – von den Rechenautomaten über die Minis, Workstations und PCs zu den vernetzten Medienmaschinen, die uns heute zur Verfügung stehen.[2] Das Fach Informatik bleibt aber in der technischen (oder theoretischen) Ausbildung stecken und ignoriert die Anwendungen und Kontexte weitgehend; es wird nicht zur Wissenschaft, denn auch hier gilt: „Das Wahre ist das Ganze."[3]

In der industriellen Praxis bleibt dies nicht unbeobachtet, und so mehren sich seit über einem Jahrzehnt die Stimmen, die neben den formalen Qualifikationen in der Ausbildung die sogenannten *soft skills* einfordern. Obwohl dies eine eher unscharfe Beschreibung erkennbarer Ausbildungsdefizite ist, werden vor allem fehlende Anwendungsorientierung, unterentwickelte kommunikative Kompetenz, mangelnde soziale Kompetenz und unzureichende Einübung zur Teamarbeit in der Informatiklehre eingeklagt.[4] Das sind nun Anforderungen, die nicht additiv, durch Hinzufügen weiterer Wissensbestände, zu beheben sind, sondern hier werden Fertigkeiten erwartet, die über das Faktenwissen und isolierte technische Kenntnisse und Praktiken hinausgehen.

Während über die Analyse des Mangels eine zunehmende Einigkeit besteht, gibt es keine Übereinkunft zu deren Beseitigung. Fraglos jedoch muss die in ihrer Weise erfolgreiche formale technische Lehre der Informatik um Ausbildungselemente erweitert werden, die diese *soft skills* vermitteln. In besonderer Weise scheint das Gebiet *Informatik und Gesellschaft* dafür geeignet zu sein, da die Analyse des Kontextes der Informatik den Ausgangspunkt solcher Forschung und Lehre bildet. Die Minimalforderung eines zeitgemäßen Updates der Informatiklehre ist deshalb, endlich an allen Informatikfakultäten und Fachbereichen ein solches Fach als selbstständige Einheit einzuführen.

## Was soll nun in einem solchen Fach *Informatik und Gesellschaft* vermittelt werden?

Angesichts der Lernziele der gewachsenen Ausbildung in Informatik muss *Informatik und Gesellschaft* in gewisser Weise komplementär arbeiten. Wir haben auf die Vermittlung der *soft skills* hingewiesen. Zwei weitere Aufgaben scheinen mir hinzuzukommen, die über diese berufsqualifizierenden Anforderungen hinausgehen. Das ist zum einen die Reflexion der Informatik als Ganzem, in dem sich die Teile der gesamten zu einem umfassenden (eben „gesellschaftlichen") Kontext verbinden lassen.

Zum anderen gilt es, kritische Urteilskraft zu entwickeln, nämlich die Befähigung, im konkreten Kontext potentielle und reale

Konflikte oder Widersprüche zur erkennen, zu analysieren und Werturteile zu treffen. Dies kollidiert vordergründig mit der großen und erfolgreichen mathematischen Tradition der Informatik, die in ihren Kalkülen ja aus guten Gründen jeden logischen Widerspruch verbannt. Konflikte und Widersprüche im Alltag, außerhalb der formalen Kalküle, sind aber der Stoff, aus dem der Fortschritt wächst, sie sind die Basis des „Werdens", wie Hegel es ausdrückt. Widersprüche sind eben auch die Ausgangslage der Konkurrenz, der Triebkraft des wirtschaftlichen Werdens ebenso wie des wissenschaftlichen oder technischen Fortschrittes. Dies verlangt sowohl die Fähigkeit, komplexe Systeme aus technischer Sicht zu beurteilen wie aus nicht-technischer Sicht. Im Konkreten sind dies Befähigungen, die auch in den Teilgebieten der Informatik gelehrt und gelernt werden müssen, *Informatik und Gesellschaft* ist aber der „natürliche Ort", wo die Informatik als Technik im Kontext und als „Ganzes" reflektiert werden kann.

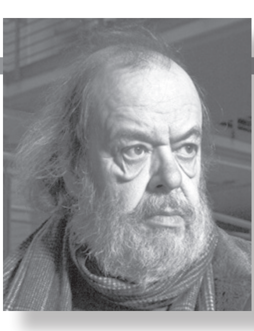
Angesichts der spezialisierten technischen und theoretischen Fachgebiete, die sich bislang in der Informatik entwickelt haben, ist es nun endlich an der Zeit, in allen Informatikfachbereichen *Informatik und Gesellschaft* als selbstständige Lehre und Forschung zu verankern. Dies ist eine notwendige Forderung, sie reicht aber nicht aus. Sicher gehören Anwendungsorientierung und die damit verbundenen kontextbewussten *soft skills* in alle Lehrfächer praxisbezogener Informatik, denn nur so können sie zur selbstverständlichen beruflichen Qualifikation werden. Doch die gelegentlich geäußerte Vorstellung, *Informatik und Gesellschaft* werde als eigenständiges Fach überflüssig, wenn nur alle anderen Vorlesungen und Seminare diese Aspekte hinreichend berücksichtigten, schießt über das Ziel hinaus. So verständlich dieser Wunsch nach einem ganzheitlichen Unterricht klingt, so geht er doch am Zwang zur Arbeitsteiligkeit vorbei, der aus der Komplexität der Probleme erwachsen ist. Um den reichhaltigen Kontext moderner Informatiksysteme angemessen zu vermitteln, muss die Lehre in *Informatik und Gesellschaft* so vielfältige Inhalte wie Informationsrecht, (alte und neue) Ökonomie oder Arbeits- und Berufswelt der Informatik ansprechen und gegebenenfalls vertiefen. Darüber hinaus muss *Informatik und Gesellschaft* die geistigen und kulturellen Grundlagen des Faches vermitteln und nicht zuletzt sollen die Fähigkeit zur Bewertung sozio-kultureller Prozesse geweckt werden – von der berufsspezifischen Ethik bis zu den historischen und politischen Aspekten der Globalisierung und Informationsgesellschaft. So begrüßenswert es ist, wenn solche Themen an der richtigen Stelle im fachlichen Kontext an- und ausgesprochen werden, so scheint es mir doch unerlässlich, diese Themenkomplexe auch im eigenen Kontext und mit der eigenen Logik, eben in einem eigenen Fach *Informatik und Gesellschaft,* zu präsentieren und zu diskutieren. Diese Komplexität zeigt, dass die Informatik eine Technikwissenschaft neuen Typs ist, die sich aus einer erfolgreichen Praxis zu einer reflektierenden Wissenschaft mausert.

## In welchen Formen soll *Informatik und Gesellschaft* gelehrt und gelernt werden?

Das Fach befindet sich in der Konkurrenz mit anderen Informatikfächern und muss zuvorderst die Anforderungen der jeweiligen Studien- und Prüfungsordnungen erfüllen. Das wird im Regelfall bedeuten, dass die üblichen Vermittlungsformen der Vorlesung, der Übung und des Seminar gewählt werden müssen. Den Besonderheiten des Faches werden diese Formen freilich nicht im gleichen Maße gerecht, wie es bei den anderen Fachgebieten der Informatik der Fall sein mag. *Informatik und Gesellschaft* ist in wesentlich stärkerem Maße diskursiv angelegt als es die reine Wissensvermittlung oder Einübung von Praktiken verlangt. Deshalb müssen Diskussionen in Übungen und Seminaren helfen, Kritikfähigkeit und Urteilskraft zu stärken.[5]

Es ist für viele Studierende (und Lehrende) in der Informatik ungewohnt, über Themen zu reden, die keinen *one best way* als „Lösung" kennen. Um sich mit solchen Themen auseinanderzusetzen, die ja im ökonomischen, rechtlichen und politischen Alltag andauernd auftreten, ist es wichtig, Themen zu bestimmen, die aktuell sind und die eine nachvollziehbare Verbindung zur Informatik besitzen. Nur so kann das im Studium erworbene informatische Fachwissen integriert werden in ein angemessenes reflektiertes Urteil, dass dann im konkreten Fall bei den Studierenden (wie bei den Lehrenden) unterschiedlich ausfallen mag. Hier kann kommunikative Kompetenz (und Toleranz) praktisch geübt werden.

Zur Stärkung kommunikativer Kompetenz und der Urteilskraft ist es sicher hilfreich, gelegentliche methodische Anleihen bei anderen Wissenschaften zu machen. Wir erleben ja seit 25 Jahren, dass sich die früher so geschlossene Welt industrieller Datenverarbeitung zur Büro- und Spielemaschine PC erweitert hat. Dieser Prozess ist in den letzten zehn Jahren mit dem Internet noch weiter beschleunigt worden und so bietet das Netz dem Bereich *Informatik und Gesellschaft* ein globales soziales und kulturelles Labor in Realzeit an. Die umfassende und rasant aufblühende Ausprägung Digitaler Medien belegt mehr als irgendeine andere Entwicklung die unmittelbare Kopplung von Informatik und Gesellschaft, Informatik und Kultur. Das Fach hätte sich kein spannenderes Szenario ausmalen können – wir sollten dieses Labor also umfassend nutzen. So mag hilfreich sein, quasi-ethnographische Erkundungen vorzunehmen, um reale Fragestellungen zu untersuchen. Der gezielte Einsatz des WorldWideWeb ist hier ebenso [zu nennen] wie die Expertenbefragung oder auch einmal die Umfrage unter Betroffenen. Solche Verfahren werden



**Wolfgang Coy**

**Wolfgang Coy** ist Informatiker und gestaltete den Fachbereich Informatik und Gesellschaft in Deutschland wesentlich mit. Er leitete die Forschungsgruppe *Informatik in Bildung und Gesellschaft* an der Humboldt-Universität zu Berlin und arbeitet aktuell im Interdisziplinären Labor *Bild – Wissen – Gestaltung.*
Er ist Mitglied im Beirat des FIfF. 2018 wurde ihm die Weizenbaum-Medaille verliehen.

zur äußerst wirkungsvollen Ergänzung zur Literaturrecherche. Zu den besonderen Herausforderungen in der Lehre gehört der Umgang mit Konfliktstoffen. Von den Juristen haben wir übernommen, in den Übungen aktuelle Kontroversen der Informationstechnik in einer Art öffentlicher Verhandlung in Proponenten-und Opponentenrollen zu vertreten. Das ist für Studierende und Lehrende ungewohnt, aber es ist ein gutes Training zum Präsentieren, Zuhören und Urteilen. Auch die Vorlesung muss ihren Charakter unter den nichttechnischen Inhalten des Fachs ändern. Die Aufgabe, in den Veranstaltungen für *Informatik und Gesellschaft* Kontexte zu vermitteln, mag Lehrende dazu bringen, ihre Kenntnisse und Erfahrungen nicht nur in einer streng systematischen Form anzubieten, sondern die Vorlesung auch dazu zu nutzen, eine Fragestellung in Form einer „Geschichte" zu erzählen. Wir haben damit gute Erfahrungen gemacht.

Fraglos können solche didaktischen Ansätze auch wesentliche Elemente eines Projektstudiums werden, wie es erfolgreich an einigen Hochschulen seit langem Teil der Ausbildung ist. Gerade die Möglichkeit, einen Themenbereich unter unterschiedlichen Aspekten zu behandeln, fordert dazu heraus, ein aktuelles Informatikthema auch unter Aspekten von *Informatik und Gesellschaft* zu behandeln – sinnvollerweise in Kooperation mit Kollegen aus dem Kernbereich der Informatik. Insgesamt bietet die Lehre in *Informatik und Gesellschaft* stärker als andere Fachgebiete Anlässe, mit neuen Lehr- und Lernformen zu experimentieren. Wir sollten das nutzen.

Bei aller Aufgeschlossenheit bleibt freilich als notwendige Einsicht: Das Ganze kann nicht gelehrt (oder gelernt) werden, aber wir können viel mehr als nichts lernen (und lehren). Das „Wahre" kann nur bruchstückhaft aus seinen Teilen heraus thematisiert werden. Doch die formale Logik lehrt uns: Solange Lehre „korrekt" bleibt, wird sie niemals vollständig sein. Wo sie aber lebendig ist, wird sie Widerspruch ernten. Wie immer wir die Lehre gestalten, es gilt unvermeidlich: *Weder vollständig noch widerspruchsfrei!*

---

*Quelle: Coy, W. (2001): Weder vollständig noch widerspruchsfrei. In: FIfF Kommunikation,18 (4), S. 45-48. Wir danken dem Autor für die freundliche Genehmigung zum Wiederabdruck.*

## Anmerkungen

1 *Vgl. Wolfgang Coy, Was ist Informatik? Eine kurze Geschichte der Informatik in Deutschland, in Jörg Desel (Hrsg.), Das ist Informatik, Berlin-Heidelberg-New York: Springer 2001.*

2 *Ich habe diesen Prozess u. a. in „Automat-Werkzeug-Medium", Informatik Spektrum 18:1 (1995) und in „Bildschirmmedium Internet? Ein Blick in die Turingsche Galaxis", in H. Schanze & P. Ludes (Hrsg.) Qualitative Perspektiven des Medienwandels, Opladen: Westdeutscher Verlag 1997 ausführlicher dargestellt.*

3 *Hegel fährt ja nach seinem berühmten Satz in der Einleitung zur Phänomenologie des Geistes fort mit: „Das Ganze aber ist nur das durch seine Entwicklung sich vollendende Wesen". Nun ist nicht mit einer Vollendung der Informatik zu rechnen, aber ein gewisse Entwicklung ist sehr wohl erkennbar.*

4 *Vgl. Empfehlung der Gesellschaft der Informatik e. V. zur Stärkung der Anwendungsorientierung in Diplom-Studiengängen der Informatik an Universitäten, Informatik Spektrum 22(6), 1999. Gezielt betonen dies auch die „Ethischen Leitlinien" der Gesellschaft für Informatik von 1993, denen die Mitgliedern mit sehr großer Mehrheit zugestimmt haben (Arbeitskreis Informatik und Verantwortung (Hrsg.), Ethische Leitlinien der Gesellschaft für Informatik, Informatik-Spektrum 16, 1993).*

5 *Damit soll die Wichtigkeit diskursiver Aneignungsweisen in den Kernfächern der Informatik keineswegs geschmälert werden. Ein oder zwei Seminare im ganzen Studium, die dann noch auf einen Vortrag mit Nachfragen reduziert werden, sind einfach zu wenig!*

**Aufruf zur Einreichung von Beiträgen / Call for Papers**

Der Schwerpunkt von Ausgabe 4/2018 der *FIfF-Kommunikation* steht unter dem Motto

## Alter(n)sgerechte Informatik

Schwerpunktredaktion: Eberhard Zehendner, Stefanie Jäckel, Henning Lübbecke

Das Thema ordnet sich ein in den umfassenden Bereich einer Teilhabe aller Menschen an den Errungenschaften der Informatik. Der bewusst mehrdeutige Titel soll Spielraum in folgender Hinsicht lassen:

„Altersgerecht" bedeutet, für ein bestimmtes Lebensalter geeignet. Häufig wird dies auf ein höheres oder sogar sehr hohes Alter bezogen, andererseits auch auf Kinder bzw. Jugendliche. Wie können Informatikprodukte oder -dienstleistungen so gestaltet werden, dass sie den Lebenswelten einer bestimmten Altersgruppe möglichst gut entsprechen?

Als „alternsgerecht" sollen im Kontext des Schwerpunkts Informatikprodukte oder -dienstleistungen angesehen werden, die sich den Bedürfnissen und Wünschen sowie den Fähigkeiten und Einschränkungen der sie nutzenden Menschen in Bezug zu ihrem Alter anpassen oder zumindest anpassen lassen. Ziel ist eine bruchlose Weiternutzung der gewohnten Hardware-, Software- und Dienste-Umgebung unter sich verändernden Bedingungen, wie sie für fortschreitendes Alter typisch sind.

Einreichung kompletter Manuskripte bis zum **22. Oktober 2018** an nez@uni-jena.de (Eberhard Zehendner)

Zur besseren Planung der Ausgabe wird um eine zeitnahe Vorankündung von Titel und Inhaltsbeschreibung gebeten.





**Hans-Jörg Kreowski**

# Autonomie in technischen Systemen

*Dieser Artikel ist ein Nachdruck aus der Internetzeitschrift* Leibniz Online 32 *vom 16. März 2018. Es handelt sich um die schriftliche Ausarbeitung eines Vortrags, der schon einige Zeit zurückliegt. Er wurde im Rahmen einer Veranstaltung der Leibniz-Sozietät der Wissenschaften zu Berlin am 10. Dezember 2015 gehalten, auf der der Arbeitskreis* Emergente Systeme, Information und Gesellschaft *vorgestellt wurde.*

## 1 Einleitung

In technisch orientierten Wissenschaftsbereichen wie der Künstlichen Intelligenz, Robotik, Logistik und Produktionstechnik wird seit über 20 Jahren mit wachsender Intensität zum Thema Autonomie geforscht und entwickelt. Roboter sollen gebaut werden, die kochen, jonglieren, tanzen oder Kranke und Hilfsbedürftige betreuen können. Selbstfahrende Fahrzeuge sollen demnächst fahrerlos den Straßenverkehr bewältigen. Maschinen sollen unter dem Motto *Industrie 4.0* eigenständig und miteinander Produktionsaufgaben planen und ausführen. Im Rahmen der Robocup-Wettkampfserie treten Roboterteams in verschiedenen Disziplinen gegeneinander an. Fernziel ist, den menschlichen Fußballweltmeister zu schlagen. Das ist nur eine kleine Auswahl technischer Systeme, die in der einen oder andern Form autonom arbeiten. Sie befinden und bewegen sich in einer sich verändernden und nicht vollständig bekannten Umgebung, in der sie ihre Aufgaben einzeln oder in Gemeinschaft erledigen sollen. Sie müssen dafür ihre Umgebung erfassen und interpretieren, Schlüsse ziehen, planen, Entscheidungen treffen und möglichst optimal handeln. Dabei ist häufig vorgesehen, dass sie sich durch Lernen verbessern. Als Vorbilder werden meist Menschen propagiert mit ihren Denk-, Handlungs-, Problemlösungs-, Kommunikations- und Lernfähigkeiten. Eine sehr große Zahl von Wissenschaftlerinnen und Wissenschaftlern arbeiten weltweit an der Lösung von Problemen, die mit der Entwicklung autonomer technischer Systeme verbunden sind. Das liegt sicher auch daran, dass es sich um äußerst interessante wissenschaftliche Herausforderungen handelt. Ein weiterer entscheidender Faktor ist aber auch, dass für die Forschung und Entwicklung auf diesem Gebiet gigantische staatliche Fördermittel zur Verfügung gestellt werden. Allerdings muss man trotz des hohen Aufwands und vieler beachtlicher Einzelerfolge konstatieren, dass der Stand der Kunst noch recht bescheiden ist. Zum Beispiel können Roboter jonglieren und halbwegs sich so bewegen, dass man von Tanzen sprechen kann. Beim Fußballspielen sind schon so immense Aufgaben zu bewältigen, dass das Spiel der Roboter noch lange nicht die Kreisklasse erreicht. Nicht viel anders sieht es beim Kochen und bei Pflegeaufgaben aus. Das selbstfahrende Auto ist trotz aller Erfolgsmeldungen noch in einem experimentellen Anfangsstadium. Es wird noch viele Entwicklungsmilliarden verschlingen; und es ist keineswegs schon sicher, dass die eingesetzten Steuergelder gut angelegt sind. Das ist nicht verwunderlich, denn der Fortschritt in der Wissenschaft ist eine Schnecke. Ein anderer Grund aber könnte sein, dass Autonomie vielleicht überhaupt gar nicht richtig verstanden und durchschaut ist. In diesem Essay möchte ich deshalb der Frage nachgehen, was es mit der Autonomie in technischen Systemen auf sich hat, worum es dabei überhaupt geht, wo die Schwierigkeiten liegen, wo die Gefahren dieser Entwicklung lauern und ob technische Autonomie schon richtig verstanden und durchdacht ist.

## 2 Was ist Autonomie?

In der Kantschen Philosophie als prominentes Beispiel birgt Autonomie die Möglichkeit und Aufgabe des Menschen, sich selbst als freiheits- und vernunftfähiges Wesen zu bestimmen und entsprechend aus Freiheit nach dem kategorischen Imperativ zu handeln: „Handle nur nach derjenigen Maxime, durch die du zugleich wollen kannst, dass sie ein allgemeines Gesetz werde." (Grundlegung zur Metaphysik der Sitten, Akademie-Ausgabe Kant Werke IV, Walter de Gruyter 1968, S. 421). Viele andere Philosophen formulieren das ähnlich. Auch die Autonomiebegriffe in Psychologie und Pädagogik sind von dieser Art. In der Politik bezeichnet man Staaten oder Gebiete als autonom, wenn sie eine eigene Gesetzgebung, Exekutive und Rechtsprechung haben. In der Biologie wird neben Menschen auch Tieren vielfach Autonomie zugesprochen, wobei die Mechanismen, die Autonomie bewirken und ausmachen, weitgehend ungeklärt sind. In der Technik erhalten Roboter, Prozesse und Systeme das Attribut autonom, wobei die Mechanismen, auf denen die Autonomie beruht, meist computergestützt sind. Sie werden von Menschen gemacht im Rahmen des algorithmisch Möglichen. Die Autonomiebegriffe in den Geistes- und Sozialwissenschaften werden, wenn ich das richtig sehe, weitgehend ignoriert. Die Autonomie biologischer Systeme wird dagegen gern und oft als Vorbild genannt. Die Analogie ist allerdings eher oberflächlich und vage, weil zwar gewisse Phänomene ähnlich sein mögen, die für Autonomie verantwortlichen Mechanismen von biologischen und technischen Systemen jedoch möglicherweise wenig bis gar nichts miteinander zu tun haben, ihre Beziehung zueinander jedenfalls unverstanden ist.

schwerpunkt

## 3 Mehr zum Konzept autonomer technischer Systeme

Ein typisches Beispiel, was unter autonomen technischen Systemen verstanden wird, findet man im Vorwort der Publikation des Bundesministeriums für Wirtschaft und Technologie 2013:

> *„Autonomik – Autonome Systeme und simulationsbasierte Systeme für den Mittelstand ist ein Technologieprogramm des Bundesministeriums für Wirtschaft und Technologie. Bei AUTONOMIK geht es um zukunftsweisende Ansätze für die Entwicklung einer neuen Generation von intelligenten Werkzeugen und Systemen, die eigenständig in der Lage sind, sich via Internet zu vernetzen, Situationen zu erkennen, sich wechselnden Einsatzbedingungen anzupassen und mit Nutzern zu interagieren. Insgesamt haben sich 14 Projektverbünde, u. a. zu fahrerlosen Transportsystemen, robotischen Assistenten, autonomen Logistikprozessen und Klinikanwendungen für eine Förderung durch das BMWi qualifiziert. Die Projekte haben eine Laufzeit von durchschnittlich drei Jahren. Rund 100 Unternehmen und wissenschaftliche Einrichtungen wirken an den Vorhaben mit. Das Projektbudget beträgt zusammen ca. 110 Mio. Euro. …“*

Ebenfalls typisch an diesem Beispiel ist, dass Entwicklungen in diesem Bereich in enger Verflechtung von Politik, Wirtschaft und Wissenschaft vorangetrieben werden.

Ganz ähnliche Betrachtungen werden im Kontext eines anderen Anwendungsfelds angestellt. In der 60-seitigen Einleitung des 320-seitigen NATO-Sammelbands zu autonomen Systemen beschreiben die beiden Herausgeber Williams und Scharre (2015) Herausforderungen und Möglichkeiten autonomer Waffen, wobei sie ausführlich auf die Charakterisierung autonomer Systeme allgemein eingehen. Sie definieren autonome Systeme als Systeme, die auf der Basis integrierter Sensorik, Analytik, Kommunikationsmöglichkeit, Planung und Entscheidung agieren, um vorgegebene Ziele zu erreichen. Spezielles Charakteristikum autonomer Systeme ist, dass sie das in sich ändernder Umgebung mit potentiellem Nichtdeterminismus tun. In jeder gegebenen Situation kann es mehrere Handlungsoptionen geben, aus denen ausgewählt werden muss. Diese informelle Beschreibung ist repräsentativ für die ausufernde Literatur zu Autonomie technischer Systeme (vgl. z. B. Siegwart et al. 2011 und Thrun et al. 2005).

Ein drittes Beispiel mag das abrunden, von dem ich aus eigener Anschauung berichten kann. An der Universität Bremen wurde von 2004 bis 2011 der Sonderforschungsbereich SFB 637 *Selbststeuerung logistischer Prozesse – Ein Paradigmenwechsel und seine Grenzen* mit dem englischen Titel *Autonomous Cooperating Logistic Processes – A Paradigm Shift and its Limitations* durchgeführt (siehe dazu Hülsmann et al. 2011 und Hülsmann und Windt 2007). Das Projekt hatte als Leitgedanken:

> *„Autonome Kontrolle beschreibt dezentrale Entscheidungsprozesse in heterarchischen Strukturen. Vorausgesetzt werden interagierende Elemente in nichtdeterministischen Systemen mit der Fähigkeit und Möglichkeit, eigene Entscheidungen zu treffen.“*

Über die vorige Definition hinaus, aber wie bereits im Zusammenhang mit dem AUTONOMIK-Projektverbund angesprochen, wird hier also darauf hingewiesen, dass eine Form autonomer Kontrolle erforderlich ist, wenn mehrere Systemeinheiten ohne zentrale Instanz interagieren und dabei Entscheidungen treffen müssen, welche Aktionen jeweils ausgeführt werden sollen.

## 4 Modellierung autonomer technischer Systeme

Die wissenschaftliche Auseinandersetzung mit technischer Autonomie bleibt nicht bei einer informellen Umschreibung stehen, sondern es wurden in den letzten zwei Jahrzehnten eine Reihe formaler und semiformaler Ansätze für die Modellierung und Realisierung autonomer technischer Prozesse und Systeme entwickelt. Neben diversen Netzvarianten sind Multiagentensysteme (siehe z. B. Wooldridge 2002) und Schwarmintelligenz (siehe z. B. Banobeau et al. 1999, Engelbrecht 2006, Kennedy und Eberhart 2001) prominente Beispiele. Das Angebot bei Multiagentensystemen reicht von Plattformen, die in JAVA programmiert sind und die Kommunikation und Ausführung von sogenannten Agenten für bestimmte Anwendungen unterstützen, bis zu rein logischen Formalisierungen, bei denen abstrakte Agenten in einer abstrakten Umgebung simultan agieren. Ein einzelner Agent kann dabei lokal seine Umgebung erfassen und verändern. Durch eine große Zahl von Axiomen werden das Verhalten und die Interaktion der Agenten eingegrenzt. Bei den verschiedenen Ausformungen von Schwarmintelligenz werden meist Schwärme in der Natur als Vorbild herangezogen wie Ameisenkolonien, Bienenvölker, Fischschulen, Vogelschwärme oder Zellstrukturen. Die Mitglieder eines Schwarms befinden sich in einer gemeinsamen Umgebung oder einem Suchraum, was ein Graph sein kann oder ein euklidischer Raum. Sie agieren simultan in Abhängigkeit von oft quantitativen Informationen in ihrer nahen Umgebung nach bestimmten Regeln. Ist die Umgebung ein euklidischer Raum, dann bewegen sich die Schwarmmitglieder mit gewisser Geschwindigkeit in gewisser Richtung. Ist sie ein Graph, dann bewegen sich die Schwarmmitglieder längs der Kanten oder kommunizieren darüber. Die mathematischen Beschreibungen sind teils lückenhaft und werden erst durch eine Implementierung vervollständigt.

Im Rahmen des oben genannten Sonderforschungsbereichs hat meine Forschungsgruppe einen eigenen Ansatz zur Formalisierung autonomer Prozesse entwickelt (siehe z. B. Dashkovskiy et al. 2010, Hölscher et al. 2009, Kreowski et al. 2011). Den syntaktischen Kern bilden Gemeinschaften autonomer Einheiten. Eine solche Gemeinschaft besteht aus einer initialen Umgebung, einer Menge autonomer Einheiten, einer Kooperationsbedingung und einem Ziel. Eine autonome Einheit verfügt über eine Regelmenge zur lokalen Veränderung der Umgebung und über eine Kontrollbedingung zur Regulierung der Regelanwendungen. Semantisch werden Prozesse definiert, die mit der initialen Umgebung beginnen und in denen jede Einheit ihre Regeln anwendet unter Beachtung der Bedingungen, bis das Ziel erreicht ist. Die Umgebungen sind Graphen, die Regeln transformieren diese Graphen, die Bedingungen und das Ziel sind logische Formeln. Je nach Kooperationsbedingung arbeiten die Einheiten sequentiell, parallel oder nebenläufig. Kooperationsbedingung und die Kontrollbedingungen können darüber hinaus Reihenfolgen, Prioritäten und Kontextvorschriften für die Regelanwendungen vorschreiben. Autonomie bedeutet in diesem Zusammenhang, dass jede Einheit ihre Regeln anwenden kann, wenn sie anwendbar sind, ohne dass die anderen Einheiten darauf direkten Einfluss haben. Ein indirekter Einfluss kann allerdings dadurch entstehen, dass die anderen Einheiten die Umgebung ändern, was die Anwendbarkeit von Regeln beeinflusst.

Zusammenfassend lässt sich festhalten, dass autonome technische Systeme oder Prozesse programmiert oder mathematisch, logisch und/oder regelbasiert modelliert sind. Die Programmsysteme unterscheiden sich von traditionellen Programmen allerdings dadurch, dass sie aus mehreren Komponenten bestehen können, die unabhängig voneinander ausgeführt werden und asynchron miteinander kommunizieren. Den mathematischen Modellen ist gemeinsam, dass sich autonome Komponenten in einer Umgebung nach bestimmten vorgegebenen Regeln in Abhängigkeit vom Zustand ihrer nahen Umgebung beziehungsweise dessen Bewertung bewegen oder sie verändern. Manchmal „lernen" die Komponenten, indem sie ihre Regeln und die Erfassung ihrer Umgebung verändern, wenn das nach vorgegeben Kriterien erfolgversprechender scheint.

Autonomie in technischen Systemen ist heute immer von Menschen gemacht und daran wird sich vorläufig nichts ändern. Es handelt sich also nicht um Autonomie im Sinne von Philosophie und Biologie, sondern um Artefakte, um eine Analogiebildung, ähnlich wie künstliche Intelligenz nicht mit menschlicher Intelligenz vergleichbar ist und maschinelles Lernen mit dem Lernen von Lebewesen wenig bis gar nichts zu tun hat. Autonome technische Systeme haben kein Bewusstsein, sind nicht vernunftbegabt, können nicht denken. Das „Kind" braucht einen Namen. Im technisch-wissenschaftlichen Bereich bedient man dabei gern bekannter Begriffe, wenn ihre eigentliche Bedeutung gewisse Ähnlichkeiten mit dem neu Benannten aufweist. Von technischer, künstlicher, maschineller Autonomie zu sprechen, ist also durchaus nachvollziehbar, aber darf nicht mit dem ursprünglichen Autonomiebegriff verwechselt werden. Wenn dieser Unterschied nicht beachtet oder sogar bewusst vertuscht wird, ist das Irreführung. Leider passiert das im Zusammenhang mit technischer Autonomie häufig – teils unbedacht, teils absichtsvoll.

Aber die Modellierung autonomer technischer Systeme krankt nicht nur hinsichtlich der mangelnden Begriffsschärfe. Sondern auch konzeptionelle Probleme werden oft nicht ausreichend bedacht oder manchmal sogar völlig ignoriert. So sind bekanntermaßen fast alle Planungs- und Optimierungsprobleme (wie Tourenplanung, Zielsuche, Clusterung, Lagerhaltung, Scheduling u. v. a. m.) und damit viele Aufgaben, die ein autonomes System zu erfüllen hat, NP-schwer, d. h. alle heute bekannten exakten Lösungen sind im schlechtesten Fall mindestens exponentiell. Sie funktionieren also nur für kleine Instanzen und brauchen in vielen Fällen mehr Zeit, als verfügbar ist. Da diese Problematik in vielen praktischen Anwendungen informationsverarbeitender Systeme auftritt, werden seit Jahrzehnten Auswege gesucht und beschritten. Drei typische Vorgehensweisen dafür sind:

1. Man hofft, dass der schlechteste Fall nicht oft eintrifft (z. B. bei Expertensystemen, SAT-Solver, Model Checker);

2. man bricht die Berechnung ab, wenn es zu lange dauert, und probiert etwas anderes;

3. man setzt sogenannte Heuristiken ein, insbesondere prozedurales Lernen, die schnelle Ausführbarkeit garantieren, aber in der Regel falsche Ergebnisse liefern mit meist unbekannter Abweichung von einer richtigen Lösung.

Das ist alles nicht gangbar, wenn man sich Fehler nicht leisten kann oder will. Autonome technische Systeme, die gemäß ihrer Programmierung eigenständig planen und entscheiden, geraten damit fast unumgänglich in die Falle der NP-Schwierigkeit. Ihr Einsatz in kritischen Anwendungen ist also äußerst gefährlich. Können beispielsweise selbstfahrende Autos, die ja sehr bald eingeführt werden sollen, die Straßenverkehrsordnung kennen und korrekt anwenden? Ist die Straßenverkehrsordnung überhaupt berechenbar? Und wenn JA, ist ihre programmierte Ausführung schnell und zuverlässig genug? Können autonome Vehikel verschmutzte, verdeckte oder verbogene Verkehrszeichen erkennen? Wie reagieren sie in Situationen, in denen menschliche Fahrerinnen und Fahrer intuitiv, spontan und antizipierend handeln? Wer wird verantwortlich gemacht, wenn autonome Fahrzeuge Sach- oder Personenschäden verursachen? Soweit ich das übersehe, sind alle diese Fragen und viele weitere weitgehend ungeklärt.

## 5 Autonome Waffen

Ein besonderes Anwendungsfeld, bei dem die Problematik technischer Autonomie besonders deutlich wird, ist die Entwicklung autonomer Waffen. Das Department of Defense der USA (2014) plant, einen erheblichen Teil der Bewaffnung auf unbemannte Vehikel in der Luft, am Boden und zu Wasser umzustellen. Laut der *Unmanned Systems Integrated Roadmap*, die auf 160 Seiten den Zeitraum von 2013 bis 2038 fortschreibt, ist ein wesentliches Forschungsthema und Entwicklungsziel für die


**Hans-Jörg Kreowski**

**Hans-Jörg Kreowski** ist Professor (i. R.) für *Theoretische Informatik* an der Universität Bremen und Vorstandsmitglied des *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung*. Neben seinen fachlichen Schwerpunkten hat er seit vielen Jahren auch immer wieder zur unheilvollen Verflechtung von Informatik und Rüstung in Wort und Schrift Stellung genommen.

nahe Zukunft mit höchster Priorität die Einführung autonomer Waffen. Als Motiv wird angegeben, die Personalkosten senken zu wollen, weil unbemannte, aber nicht autonome Waffensysteme zwar weniger Kosten verursachen als bemannte Systeme, aber immer noch eine große Zahl betreuender Personen benötigen.



Autonomie bedeutet dabei, dass die Systeme selbst die Signifikanz der gesammelten Informationen erkennen und eigenständig über weitere Aktionen (einschließlich Waffengebrauch und Tötung von Menschen) entscheiden, ohne dass Menschen direkt eingreifen. Die Entscheidung über Leben und Tod wird autonomen Maschinen überlassen. Ist das verantwortbar? Darf das sein? Ist das ethisch vertretbar? Können Maschinen das? Können Maschinen beispielsweise das Kriegsvölkerrecht beachten?

Arkin (2009) argumentiert, dass Maschinenethik nicht nur möglich, sondern wünschenswert sei. Denn Roboter geraten nicht in Panik; sie können Befehle ohne Angst und ohne Rücksicht auf die Reaktionen der Vorgesetzten beurteilen und gegebenenfalls verweigern. Ein künstliches Gewissen ist machbar. Ich setze ein NEIN dagegen. Ein autonomes Waffensystem führt programmierte Entscheidungs- und Planungsalgorithmen aus mit den oben geschilderten und heute noch völlig ungelösten Problemen hinsichtlich Effizienz und Korrektheit. Das „autonome" Töten wird programmiert, so dass der Eingriff der Menschen nur verschoben ist. Die Entscheidung über Leben und Tod fällt also nicht erst beim Einsatz der Waffen auf dem Schlachtfeld, sondern bei deren Entwicklung. Und neben allen anderen Problemen, die daraus erwachsen, lässt sich konstatieren, dass sich das Kriegsvölkerrecht wohl kaum programmieren lässt. Denn schon unter Juristinnen und Juristen gibt es viele verschiedene Auffassungen, wie einzelne Bestimmungen zu interpretieren sind (siehe dazu die ausführlichen Auseinandersetzungen mit den rechtlichen Rahmenbedingen in Schmitt 2013 und 2017 sowie Williams und Scharre 2015). Wie sollen da Waffenschmiede berechenbare und korrekte Lösungen in ihre Programme einbauen.

Der Zweifel an der Sinnhaftigkeit autonomer Waffen ist keineswegs nur auf eine kleine Schar von Bedenkenträgerinnen und Bedenkenträger beschränkt. So gibt es ausgehend von der *IJCAI-Konferenz im Juli 2015* einen weltweiten Aufruf zum Bann autonomer Waffen: *Autonomous Weapons: an Open Letter from AI & Robotics Researchers* (siehe *https://futureoflife.org/open-letter-autonomous-weapons/*). Mit Stand von Ende 2017 gibt es mehr als 20.000 Unterschriften davon über 3.500 von AI/Robotik-Fachleuten. Erwähnenswert sind auch die Aktivitäten des International Committee for Robot Arms Control (ICRAC, siehe *https://icrac.net*). Schließlich gibt es auch auf hoher politischer Ebene Initiativen zum Verbot oder zumindest zur Regulierung tödlicher autonomer Waffen. So finden im Rahmen der Vereinten Nationen seit 2014 jährliche Treffen von Regierungsfachleuten zu diesem Thema statt.

## 6 Statt eines Fazits

Autonomes Denken und Handeln gehören zu der breiten Palette geistiger und emotionaler Fähigkeiten, über die Menschen verfügen. Das umfasst Klugheit wie Dummheit, Indeenreichtum wie Planlosigkeit, rationales Entscheidungsvermögen wie Torheit, Lernen wie Vergessen, Mitgefühl wie Abneigung, Toleranz wie Vorurteile, Bescheidenheit wie Hochmut, Liebe wie Hass. Es ist weitgehend unbestritten, dass es sich dabei um Leistungen des Gehirns handelt. Was aber nach meinem Wissen noch ziemlich unklar ist, wie sie im Einzelnen im Gehirn zustande kommen und wie sie zusammenhängen. Es ist klar, dass im Gehirn chemische und physikalische Prozesse ablaufen und dass genetische Veranlagungen eine Rolle spielen. Aber wie ein einzelner Gedanke – ob schlau oder töricht – entsteht, ist vorläufig ein Rätsel. Ich vermute, dass die Wissenschaft noch sehr lange brauchen wird, um es zu entschlüsseln. Daran werden auch die rund 1,2 Millarden Euro nicht viel ändern, die die Europäische Union über einen Zeitraum von zehn Jahren für das *Human Brain Project* (siehe *https://www.humanbrainproject.eu/en/*) ausgibt. Ziel ist, das Gehirn besser zu verstehen und die Erkenntnisse in Informatik und Medizin anzuwenden. Ganz ähnliche Projekte laufen auch in den USA mit noch mehr Geld und in China.

Was man aber nicht versteht, lässt sich auch nicht nachbauen. Eine technische Realisierung von Autonomie oder anderen intellektuellen und emotionalen Fähigkeiten kann also heutzutage nur ein Artefakt sein, das vielleicht gewisse Ähnlichkeiten mit seinem natürlichen Vorbild hat. Die Technikgläubigen argumentieren gern, dass die Natur ja auch diese Fähigkeiten hervorgebracht hat, warum soll es dann nicht auch technisch gehen. Das mag sein, aber deshalb weiß man noch lange nicht, wie.

## Referenzen


Ron C. Arkin: Governing Lethal Behavior in Autonomous Systems. Chapman and Hall, Taylor and Francis Group, Boca Raton, FL, 2009.

Eric Bonabeau, Marco Dorigo, Guy Theraulaz: Swarm Intelligence: From Natural to Artificial Systems. Oxford University Press, 1999.

Bundesministerium für Wirtschaft und Technologie (BMWi) Öffentlichkeitsarbeit (Hg.): Autonomik – Autonome und simulationsbasierte Systeme für den Mittelstand: Die Projekte, Band 1, 2013.

Sergey Dashkovskiy, Hans-Jörg Kreowski, Sabine Kuske, Andrii Mironchenko, Lars Naujuk, Caroline von Totth: Production Networks as Communities of Autonomous Units and Their Stability. International Electronic Journal of Pure and Applied Mathematics 2:17-42, 2010.

Department of Defense: Unmanned Systems Integrated Roadmap, FY 2013-2038. Washington, 2014.

Andries P. Engelbrecht: Fundamentals of Computational Swarm Intelligence. John Wiley & Sons, 2006.

Karsten Hölscher, Hans-Jörg Kreowski, Sabine Kuske: Autonomous Units to Model Interacting Sequential and Parallel Processes. Fundamenta Informaticae 92:233-257, 2009.

Michael Hülsmann, Bernd Scholz-Reiter, Katja Windt (Eds.): Autonomous Cooperation and Control in Logistics, Contributions and Limitations – Theoretical and Practical Perspectives, Springer, 2011.

Michael Hülsmann, Katja Windt (Eds.): Understanding Autonomous Cooperation and Control in Logistics – The Impact on Management, Information and Communication and Material Flow. Springer, 2007.

James Kennedy, Russell C. Eberhart: Swarm Intelligence. Evolutionary Computation Series, Morgan Kaufman, San Francisco, 2001.

Hans-Jörg Kreowski, Sabine Kuske, Caroline von Totth: Modeling Production Networks with Discrete Processes by Means of Communities of Autonomous Units. Logistics Research 3:159-175, 2011.

Michael N. Schmitt (Ed.): Tallinn Manual 2.0 on the International Law

Applicable to Cyber Operations. Cambridge University Press, 2013 (2nd edition 2017).
Roland Siegwart, Illah Reza Nourbakhsh, Davide Scaramuzz: *Introduction to* Autonomous *Mobile Robots*. 2. Auflage. The Mit Press, 2011.
Sebastian Thrun, Wolfram Burgard, Dieter Fox: *Probabilistic Robotics (Intelligent Robotics and Autonomous Agents)*. The Mit Press, 2005.
Andrew P. Williams, Paul D. Scharre (Eds.): Autonomous systems: Issues for defence policymakers. North Atlantic Treaty Organization. Headquarters Supreme Allied Commander Transformation. Capability, Engineering and Innovation, Norfolk, VA, 2015.
Michael Wooldridge: Introduction to Multi Agent Systems. John Wiley and Sons, Chichester, 2002.



**Wolfgang Hofkirchner**

# Eine Informatik für eine globale nachhaltige Informationsgesellschaft[1]

*Die weltgeschichtliche Situation der Menschheit lässt sich aus einer systemtheoretischen Perspektive als Krise interpretieren, in der das Risiko des Zusammenbruchs der Zivilisation mit der Chance auf den Durchbruch zu einer Transformation in Richtung einer dauerhaften und lebenswerten Gesellschaft einhergeht. Wenn wir danach fragen, welche Rolle der Information in diesem Transformationsprozess zukommen müsste, dann ist die Antwort darauf die, dass Information die Voraussetzung dafür darstellt, dass die gestiegene Komplexität der Interaktion der voneinander abhängig gewordenen sozialen Systeme in Sicht genommen und wieder in den Griff bekommen werden kann. Die Informatik müsste demnach so gestaltet werden, dass Anwendungen die Generierung solcher Information (Wissen, Weisheit) erleichtern und befördern, die für die Transformation gebraucht wird.*

## 1. Emergente Systeme: Die Große Bifurkation

Im Zuge ihrer Evolution bewegen sich Systeme auf Trajektorien, die Bifurkationen beinhalten. Bifurkationen kommen mit einer Vielzahl möglicher zukünftiger Trajektorien einher. Es kann der Fall eintreten, dass Systeme nicht in der Lage sind, Devolution, also ihre „Abwicklung", einen Pfad, der zum Zusammenbruch des Systems führt, abzuwenden. Es kann aber auch vorkommen – und das war der Fall bei allen Systemen, die wir gegenwärtig beobachten können –, dass sie den Durchbruch auf eine höhere Komplexitätsstufe, zu einem höheren Organisationsgrad, zu einer Trajektorie schaffen, die im Rahmen einer Mega-Evolution die Fortsetzung ihrer Entwicklung erlaubt, die auf der bisherigen Trajektorie, auf der sie sich in einem Gleichgewichtszustand befunden haben, nicht mehr möglich ist. Zunehmende Fluktuationen, Abweichungen von diesem Gleichgewichtszustand, verweisen auf ein Manko in ihrer Organisation, in der Meisterung der Komplexität, und sind Anzeichen für das Erreichen von Unterbrechungen der „normalen" Evolution.

Wichtig ist, festzuhalten, dass der Übergang des Systems auf eine neue Trajektorie zwar objektiv möglich, aber im Einzelnen nicht notwendig bestimmt, sondern kontingent ist, also emergiert, und die Evolution keinen a priori gegebenen Pfaden folgt.

Soziale Systeme bilden keine Ausnahme. Die gesellschaftliche Entwicklung heute zeigt Krisen zwischen supranationalen Gebilden, nationalstaatlich verfassten Gesellschaften und als Teilstaaten verfassten Gemeinwesen, in allen gesellschaftlichen Subsystemen, ihren kulturellen, politischen, wirtschaftlichen, ökologischen und technologischen Subsystemen, Krisen, die zustande kommen durch Mängel in der Organisierung des Gemeinwohls und sich zu globalen Problemen ausgewachsen haben, die alle betreffen und nur mehr von allen gemeinsam gelöst werden können. Der Umkipppunkt erfordert die Transition in einen anderen Zustand. Entweder scheitern die immer stärker voneinander abhängig gewordenen sozialen Systeme an einer Neuordnung ihrer Beziehungen, die dem Komplexitätsgrad der Probleme gerecht wird, die sie selber hervorgerufen haben, weil die bisherige Ordnung ihrer eigenen Angelegenheiten nicht mehr im Stande ist, als Muster für eine über ihre Systeme hinaus verallgemeinerte gerechte Teilhabe aller am allgemeinen Gut weltweit zu dienen, und schlittern auf Abwegen der endgültigen Desintegration und des Auseinanderbrechens der menschlichen Zivilisation zu, oder sie einigen sich auf den Weg in ihre Integration in eine globale nachhaltige Informationsgesellschaft. Dies wäre ein Wandel sondergleichen. Es liegt an den sozialen Systemen samt ihren sozialen Akteuren, die Wahl zu treffen. Das ist die Große Bifurkation.

Die Vision einer globalen nachhaltigen Informationsgesellschaft zeichnet sich durch drei Imperative aus – einen, der die Orientierung am Ganzen betrifft, einen, der die Organisationsstrukturen betrifft, und einen, der die Fähigkeit zur Widerspiegelung betrifft.

### 1.1 Ganzheitlichkeit: Der globale Imperativ

Die Evolution komplexer Systeme kann dazu führen, dass ursprünglich unabhängige Systeme voneinander abhängig werden, sie als Ko-Systeme miteinander kooperieren und sich letztlich als Elemente eines von ihnen geschaffenen Meta- oder Suprasystems in dieses integrieren. Dies ist der Weg der Steigerung der Komplexität. Ein neues System entsteht und mit ihm Hierarchie, indem das integrierende System die anderen einbettet.

Die heutige gesellschaftliche Entwicklung steht an diesem Punkt: Die Gliederungen der Menschheit können nicht überleben und kein gutes Leben führen, solange nicht alle von ihnen im Sinne einer echten Weltgesellschaft gesteuert werden. Das ist der Imperativ, der auf Globalität drängt.

Nach dem Nomadentum der Horden von Jägern und Sammlerinnen bis zum Beginn der neolithischen Revolution entwickelten sich auf Grund der Sesshaftigkeit immer größere Agglomerationen, die einem Territorialprinzip folgten, welches heute wiederum durch neue Migrationen und gefördert von den neuen Informations- und Kommunikationstechnologien in eine Dialektik von Globalem und Lokalem – Glokalität – in einem Weltsystem aufgehoben werden könnte.

### 1.2 Organisiertheit: Der Imperativ der Nachhaltigkeit

Sobald die neue Struktur, die organisatorischen Beziehungen des Meta-/Suprasystems, das nun ein System causa sui darstellt, in Kraft tritt und als Formursache den Aktionsspielraum der Agenten, der neuen Elemente, im Falle des Meta-/Suprasystems der zu Ko-Systemen gewordenen ursprünglichen Systeme, formt, d. h. beschränkt, aber gleichzeitig neue Aktionen, Interaktionen und Ko-Aktionen ermöglicht, die Synergie hervorbringen, kann der Verbund der Systeme eine stabile Entwicklung einleiten, eine, die Synergieeffekte garantiert, eine, die Einheit durch Vielfalt verwirklicht, d. h. so viel Integration wie nötig und so viel Differenzierung wie möglich.

Stabilität heißt bei sozialen Systemen Nachhaltigkeit. Heute geht es darum, dass die Weltgesellschaft und ihre Teile nicht gesteuert werden können, solange nicht die bestehenden anthropogenen Dysfunktionen im Funktionieren der sozialen Systeme behandelt werden und etwaigen weiteren vorgebeugt wird. Das ist der Imperativ der Nachhaltigkeit.

Auch hier lässt sich ein Dreischritt ins Treffen führen. In den Urgesellschaften herrschte eine weitgehend undifferenzierte Gemeinschaft, in der die einzelnen Mitglieder Projektionen des mystisch verstandenen „Wir" waren. Die Urgesellschaften wurden von produzierenden Gesellschaften abgelöst, die Mehrwert erzeugten, welcher durch private Aneignung Klassenspaltungen, Ausbeutung und Unterdrückung erlaubte, so dass eine Diversität von Identitäten entstand, die einander entweder antagonistisch gegenüberstehen, d. h. in Konflikte eingebunden sind, in denen der Vorteil der einen auf Kosten der anderen geht, oder agonistisch miteinander wetteifern, d. h. Konflikte austragen, in welchen die Gegensätze koexistieren, miteinander kompossibel sind. Heute wäre es an der Zeit, eine Synergie der Unterschiede, eine *unitas multiplex*, zu etablieren, in der die Vielfalt sich gegenseitig stützt, in einer Komposition aller Unterschiede – eine weise Gesellschaft, wie das vor 20 Jahren die Europäische Kommission sich vorzustellen getraute.

### 1.3 Widerspiegelungsfähigkeit: der informationelle Imperativ

Wenn die Komplexität der Herausforderungen an ein System die Komplexität des Systems selber übersteigt, dann ist die Komplexitätserhöhung des Systems das Mittel der Wahl. Diese Komplexitätserhöhung des selbstorganisierenden Systems geschieht durch Generierung entsprechender Information durch das System selber. Intelligenz ist dann die Fähigkeit des Systems, diejenige Information zu generieren, die beiträgt, das Problem zu lösen, das die Performance des Systems oder dessen Aufrechterhaltung beeinträchtigt. Kollektive Intelligenz emergiert jeweils auf einer Ebene höher als die Ebene, auf der die einzelnen Intelligenzen von Ko-Systemen angesiedelt sind, und kann die letzteren übertreffen.

Kollektive Intelligenz ist heute auf der Ebene der gesamtgesellschaftlichen Entwicklung das, was erheischt wird. Den anthropogenen Dysfunktionen kann nicht gegengesteuert, die sozialen Systeme können nicht auf einen nachhaltigen Pfad gebracht werden, solange nicht die dazu notwendigen Informationen (Daten, Wissen, Weisheit) generiert werden, solange nicht eine am guten Leben und Überleben der Menschheit ausgerichtete Bewusstheit erarbeitet wird, und solange nicht die Informations- und Kommunikationstechnologien diese Prozesse unterstützen, statt sie im Interesse der Aufrechterhaltung des status quo zu hintertreiben. Das ist der informationelle Imperativ im Zeitalter der Informationsgesellschaft.

Dieser Imperativ legt einen möglichen dritten Sprung der Menschwerdung nahe. Einen ersten Sprung von unseren tierischen Vorfahren zum *homo sapiens* als *animal sociale* bildete der zum Frühmenschen. Dieser Frühmensch war fähig, bei direkt miteinander verbundenen Akteuren gemeinsame Intentionen zu erzeugen, gemeinsame Ziele, gemeinsame Aufmerksamkeit in der gemeinsamen Handlung, was gesellschaftliche Faktoren in die biologische Evolution einführte. Ein zweiter Sprung der Anthroposoziogenese führte zwar zu einer kollektiven Intentionalität in der gesellschaftlichen Gruppe, als die gesellschaftliche Entwicklung die biologische der Frühmenschen zu dominieren begann. Aber die kollektive Intentionalität wurde zur instrumentellen Vernunft pervertiert, in der *homo idioticus* für seine privaten Zwecke andere Mitglieder der Gesellschaft instrumentalisiert und seine eigene Handlungsfähigkeit dadurch beschränkt, dass er die anderen in der Arbeit für das Gemeinwohl und in dessen Nutznießung nicht als gleichwertig erachtet. Das Entstehen meta-reflexiver Akteure, deren Wissen und Gewissen die Sorge um das allgemeine Gute rehabilitieren und zu verallgemeinerten Handlungen auf unserem Planeten befähigen, würde die Menschwerdung zu einem echten *homo socialis* „vervollkommnen".

## 2. Information: kooperative, kommunikative und kognitive Herausforderungen heute

Wenn wir danach fragen, welche Rolle der Information in diesem Transformationsprozess zukommen müsste, dann ist die Antwort darauf die, dass Information die Voraussetzung dafür darstellt, dass die gestiegene Komplexität der Interaktion der voneinander abhängig gewordenen sozialen Systeme in Sicht genommen und wieder in den Griff bekommen werden kann.

Information kommt in allen selbstorganisierenden Systemen in drei Varianten vor: Systeme erkennen andere Systeme in ihrer Umwelt (kognitive Variante), als kognitive Systeme koppeln sie sich mit Ko-Systemen (kommunikative Variante), und als kommunikative Systeme verschränken sie sich miteinander über die organisatorischen Beziehungen des Meta-/Suprasystems, an dem sie teilhaben (kooperative Variante).

Soziale Systeme zeigen soziales Informationsgeschehen: Die soziale Kognition befähigt Akteure zur Reflexion ihres Selbst im Gesamtzusammenhang, die soziale Kommunikation zur Reflexion der Intention der anderen und die soziale Kooperation zur Reflexion der geteilten Intention im sozialen System, in das sie eingebettet sind.

Soziale Kognition ist konzeptuell, das heißt, sie verläuft über die Bildung von Begriffen, die verallgemeinern – sie sind damit inhärent emergente Produkte, weil sie über das in der Erfahrung Gegebene hinausgehen. Soziale Kommunikation ist konsilient, das heißt, sie verläuft über die Abstimmung der eingebrachten Standpunkte, in der über die Nützlichkeit und Wahrheitstreue der kognitiven Informationen befunden wird – ebenfalls ein emergenter Prozess, bei dem nicht festgelegt ist, was herauskommt. Soziale Kooperation ist kollektiv intentional, das heißt, sie verläuft über die auf der Basis der kommunikativen Informationen erreichte Übereinstimmung bei der Zielsetzung, der Analyse des Hier und Jetzt als Ausgangspunkt und der Planung von Maßnahmen zur Verwirklichung der Ziele – diese Entscheidungsfindung und -umsetzung ist wiederum emergent, da im Detail unvorhersehbar und nicht bestimmt. Die sozialen Informationstypen bilden eine Hierarchie: Die kooperative Information hat in sozialen Systemen eine konsensuale Funktion (sie regelt die Bestimmung der gemeinsamen Vorhaben), die kommunikative eine kollaborative (sie regelt das Zusammenwirken für die Umsetzung der gemeinsam bestimmten Vorhaben) und die kognitive eine koordinative (sie regelt das Verstehen des Zusammenwirkens für die Umsetzung der gemeinsam bestimmten Vorhaben).

Im Zeitalter der globalen Probleme ist die Informationsgesellschaft herausgefordert, die Funktionsweisen der Varianten der sozialen Information auf eine bestimmte Art zu verändern und mit neuem Inhalt zu füllen, und das ist möglich. Die konsensuale, kollektive Objektivität der Kooperation kann und muss auf das Überleben der Menschheit und am guten Leben orientiert werden; es geht um die Veränderung der Verhältnisse, die die Herstellung und Verteilung des allgemeinen Guts betreffen. Die kollaborative, konsiliente Intersubjektivität der Kommunikation kann und muss die gesamte Menschheit einbeziehen; es geht um eine globale Konversation, die keinen Akteur ausschließt. Die koordinative, konzeptuelle Subjektivität der Kognition kann und muss die eigene Handlungsfähigkeit global erweitern; es geht darum, die Restriktionen auf die eigenen Interessen hinter sich zu lassen und zu erkennen, dass die Verfolgung legitimer Eigeninteressen die Förderung des planetaren Allgemeinwohls voraussetzt.

## 3. Gesellschaft: Herausforderungen an die Informatik

Die Informatik müsste demnach so gestaltet werden, dass Anwendungen die Generierung solcher Information (Daten, Wissen, Weisheit) erleichtern und befördern, die für die Transformation gebraucht wird.

Die Informations- und Kommunikationstechnologien befördern nicht automatisch eine Qualität der sozialen Informationsprozesse, die der Herausforderung durch die globalen Probleme gerecht wird. Sie sind vielmehr auch Teil des Problems.

Denn die Informatisierung – der Prozess der Verbreitung der Techniken, die die Gesellschaft immer empfänglicher für Information machen – ist ambivalent. Sie bereitet nicht nur den Boden für informiertes Welt-Netzbürgertum, sondern konfrontiert uns auch im Bereich der Kultur mit Informationsflut und Gehirnwäsche, im Bereich der Politik mit der Verletzung des informationellen Selbstbestimmungsrechts durch Überwachung oder Informationskriege, im Bereich der Wirtschaft mit der Proprietarisierung intellektueller Güter und Dienste durch Kommodifizierung und Kommerzialisierung, im Bereich der Umwelt mit computergestützter Übernutzung und Verschmutzung der äußeren wie der inneren Natur und nicht zuletzt im Bereich der Technik selber mit der durch die Computerisierung gesteigerten Verletzlichkeit der Informationsgesellschaft. Der Informatisierung wohnt ein Potenzial zur Verminderung von Reibungsverlusten im Funktionieren der Herstellung und Nutzung der Synergieeffekte der Commons inne. Andererseits kann sie aber auch Zwecken dienen, die der Wiedergewinnung der Commons zuwiderlaufen: Sie kann bestehende Ungleichheiten quantitativ verstärken oder qualitativ neue Ungleichheiten erzeugen. Dies ist empirisch vorfindliche Realität.

Da Informatisierung beides kann und auch tut, bedürfen die Informations- und Kommunikationstechnologien einer bewussten Gestaltung, so dass sie die Problemlösungsfähigkeit der (Welt-)Gesellschaft in einem Ausmaß steigern, welches die Dysfunktionalitäten, die mit den gesellschaftlichen Verhältnissen einhergehen (können), erfolgreich unterhalb der Schwelle der Selbstgefährdung der sozialen Systeme hält. Diese Aufgabe der Informatisierung – die technische Unterstützung derjenigen sozialen Informationsprozesse, die dazu beitragen, dass der Komplexitätsgrad der sozialen Systeme so weit erhöht wird, dass ein nachhaltiger Pfad der gesellschaftlichen Entwicklung eingeschlagen werden kann – mag „Informationalisierung" genannt werden. Informatisierung ist kein Selbstzweck, sondern kann und muss der Informationalisierung dienen. Die Informatisierung muss zum Werkzeug der Informationalisierung gemacht werden.

Aus diesem Grund ist die Informations- und Computerethik ein Muss für die Informatik. Eine globale nachhaltige Informationsgesellschaft braucht eine verantwortungsbewusste Informatik. Eine verantwortungsbewusste Informatik muss die Informations- und Kommunikationstechnologien ethisch reflektiert gestalten. Technik muss einen Sinn machen, der erstens darin besteht, dass Technikfolgenabschätzung und Technikgestaltung

**Wolfgang Hofkirchner**

Prof. Dr. **Wolfgang Hofkirchner**, Technische Universität Wien, Fakultät für Informatik, Institut für Gestaltungs und Wirkungsforschung, Argentinierstraße 8, 1040 Wien; sowie Bertalanffy Center for the Study of Systems Science, Paulanergasse 13/5, 1040 Wien, Österreich, *wolfgang.hofkirchner@tuwien.ac.at* und *wolfgang.hofkirchner@bcsss.org*

den erwarteten und tatsächlichen Nutzen der Technik im Hinblick auf die soziale Nützlichkeit einer steten Überprüfung unterzieht. Diese Überprüfung darf nicht nur die Zweckmäßigkeit der Technik für die Erfüllung des sozialen Zwecks befragen, sondern muss auch den Zweck selber hinterfragen. Dieser Zweck kann im Zeitalter der globalen Probleme nur in der Erlangung, im Ausbau, in der Aufrechterhaltung und im verbesserten Einsatz der Verfügungsgewalt über das weltweite Gemeingut der Gesellschaften seine Rechtfertigung finden. Zweitens besteht der Sinn der Technik darin, dass die von der Technik Betroffenen an diesem Prozess der Technikfolgenabschätzung und Technikgestaltung teilhaben können und ermächtigt werden, durch die Gestaltung der Technik die gesellschaftliche Entwicklung mit Bewusstheit zu gestalten.

Eine ethikbasierte Informatik unterscheidet sich vom *Business as usual*, wo keine mögliche Anwendung, kein Gegenstandsbereich und keine Methode ausgeschlossen werden, solange sie Profit versprechen, darin, dass sie, unter Einbeziehung der Betroffenen, zur Entwicklung technischer Lösungen für die Wiedergewinnung der Commons und die Fortsetzung der Zivilisation auf der Grundlage von Erkenntnissen über diejenigen Faktoren in Technik, Umwelt, Wirtschaft, Politik oder Kultur, die solche Lösungen anregen oder hemmen, durch eine auf die Ziele abgestimmte und den Gegenstandsbereich transdisziplinär umfassende Methodik beiträgt. Das ist eine Informatik für eine globale nachhaltige Informationsgesellschaft.

Als vertiefende Literatur dazu siehe: Hofkirchner, W. (2017). Information for a Global Sustainable Information Society. In: Ders., Burgin, M. (Eds.), The Future Information Society: Social and Technological Problems, New Jersey u. a.: World Scientific, S. 11-33.

*Quelle: Leibniz Online 32, https://leibnizsozietaet.de/internetzeitschrift-leibniz-online-nr-32-2018/.*
*Wir danken dem Autor für die Genehmigung zum Nachdruck.*

## Anmerkungen

1 *Vortrag auf dem Kolloquium „Emergente Systeme. Information und Gesellschaft" am 10.12.2015 Veröffentlicht: 16.03.2018*

**Christoph Marischka**

# Cyber Valley: Ein *Ökosystem* für *disruptive Technologien*

*Erstaunlich häufig ist im Zusammenhang mit Künstlicher Intelligenz (KI) gegenwärtig von einer* kritischen Masse *die Rede. Im Mai 2018 veröffentlichte das Beratungsunternehmen Roland Berger eine vielzitierte Studie*[1] *über Start-up-Unternehmen im Bereich der KI, die als wesentliches Ergebnis formulierte, dass bislang kein europäischer Staat „im globalen Vergleich eine kritische Masse an KI-Start-ups" erreiche. Auf dieser Grundlage formuliert die Studie Empfehlungen, um auf europäischer Ebene „ein starkes Ökosystem für diese jungen Unternehmen aufzubauen".*[2]

Bereits zuvor haben EntwicklerInnen immer wieder von einer *kritischen Masse* an Daten und Rechenleistung gesprochen, die sprunghafte Fortschritte insbesondere beim Maschinellen Lernen erwarten lasse. Wer von einer kritischen Masse spricht, sollte eigentlich damit rechnen, Assoziationen an eine Explosion oder gar die Atombombe zu wecken. So warnt etwa der Journalist und ehemalige Tagesthemen-Redaktionsleiter Jay Tuck: „Wenn Künstliche Intelligenz eine kritische Masse erreicht und in der Lage ist, eigene Software in hoher Geschwindigkeit zu schreiben, wird sie sich explosionsartig vermehren".[3] Entsprechende Assoziationen können auch daher rühren, dass die KI-Forschung gegenwärtig häufig als *disruptive Technologie* beschrieben wird, im Sinne der Etymologie also eine zerstörerische Technologie. Weiteres Unbehagen kann die Argumentation hervorrufen, mit der die Notwendigkeit einer intensivierten KI-Forschung in Deutschland und Europa wieder und wieder begründet wird. Dabei handelt es sich letztlich um eine geopolitische Begründung: „Die Entwicklung sollte nicht den Amerikanern und Chinesen überlassen werden", zitiert etwa das Schwäbische Tagblatt indirekt Tamara Almeyda vom Max-Planck-Institut für Intelligente Systeme in Tübingen.[4] Martin Stratmann, Präsident der Max-Planck-Gesellschaft, argumentierte gegenüber dem Deutschlandfunk ganz ähnlich: „[W]ir reden auch von großen Forschungsräumen, die untereinander in Konkurrenz stehen. Das sind im Wesentlichen die USA, Asien und Europa, und unsere Heimat ist Europa. Wir müssen also dafür sorgen, dass Europa stark bleibt, stark wird".[5]

Während man das noch für reinen Standortnationalismus halten könnte, diskutieren außen- und sicherheitspolitische Zirkel die Notwendigkeit von KI-Forschung ganz offen auch unter militärischen Gesichtspunkten. Die Ausgabe Juli/August 2018 der IP („Internationale Politik" – nach eigenen Angaben „Deutschlands führende außenpolitische Zeitschrift") war dem Schwerpunktthema „Künstliche Intelligenz" gewidmet. „Künstliche Intelligenz wird die Weltpolitik durcheinanderwirbeln", lautet gleich der Untertitel des ersten Beitrags, in dem es weiter heißt: „Ein Land, das diese Entwicklung zu ignorieren versucht, wird an Relevanz verlieren". Bislang laufe Deutschland „den Entwicklungen hinterher." Im direkt an diesen Beitrag anschließenden Interview mit Karin Suder – bis vor kurzem Staatssekretärin im Bundesverteidigungsministerium und dort u. a. mit dem Aufbau des Kommandos Cyber- und Informationsraum beschäftigt – äußert diese sich noch deutlicher: „KI ist zentraler Bestandteil des ‚digitalen Gefechtsfelds' oder, ein bisschen drastischer formuliert, KI kann eine ‚Waffe' sein … [W]er es schafft, die beste KI zu entwickeln, hat wiederum einen Verteidigungs- oder gar Angriffsvorteil … Wer bessere Informationen hat, wem es gelingt, all diese Informationen zusammenzufügen, der gewinnt".[6]

## Der Weg zur Weltspitze

Während die beteiligten WissenschaftlerInnen die Relevanz ihres Themas v. a. mit dem internationalen Wettbewerb unterstreichen, geht also die außen- und sicherheitspolitische Szene längst von einem Wettrüsten aus. Die aktuelle Bundesregierung hat sich hierfür bereits im Koalitionsvertrag in Stellung gebracht. Darin wird das Ziel ausgegeben, „Deutschland zu einem weltweit führenden Standort bei der Erforschung von künstlicher Intelligenz [zu] machen" und gemeinsam mit Frankreich als „Innovationsmotor" in diesem Bereich zu wirken.

Der Plan für den Weg an die Weltspitze ist bereits im Koalitionsvertrag angedeutet: Umfangreiche Forschungsförderung, der Aufbau eines „Nationalen Forschungskonsortiums für künstliche Intelligenz und maschinelles Lernen", eines deutsch-französischen „Zentrums für künstliche Intelligenz" sowie allgemein der Ausbau von „Forschungscamps". Zugleich gelte es, die „direkte Forschungsförderung des Bundes stärker auf den Wissens- und Technologietransfer in die Wirtschaft aus[zu]richten" und einen „schnellere[n] Transfer von Forschungsergebnissen in marktfähige Produkte" zu ermöglichen. Hierzu will man „rechtliche Barrieren für Wissenschaftskooperationen abbauen". Dass die Bundesregierung dabei nicht nur den Wettbewerb, sondern auch das Wettrüsten im Auge hat, deutet nicht nur die starke Ausrichtung auf deutsch-französische Zusammenarbeit an, die Parallelen zur politisch gewollten Fusion der Rüstungssektoren beider Länder aufweist, sondern wird auch im Bezug auf die sogenannte *Sicherheitsforschung* deutlich. Hier heißt es explizit: „Wissenschaft, Wirtschaft, Sicherheitsbehörden und Einsatzkräfte sollen zusammenarbeiten". Zumindest eines der im Kapitel „Digitalisierung" angesprochenen „neue[n] Instrumente zur Förderung von Sprunginnovationen und des Wissenstransfers in die Wirtschaft" wird letztlich im Kapitel „Für eine modern ausgerüstete Bundeswehr" ausbuchstabiert: „Zur Sicherstellung technologischer Innovationsführerschaft werden wir unter Federführung des Bundesministeriums der Verteidigung und des Bundesministeriums des Innern eine ‚Agentur für Disruptive Innovationen in der Cybersicherheit und Schlüsseltechnologien' (ADIC) sowie einen IT-Sicherheitsfonds zum Schutz sicherheitsrelevanter Schlüsseltechnologien einrichten". Denn „Chancen und Risiken der Digitalisierung sind auch für die Bundeswehr das entscheidende Zukunftsthema".[7]

Kurz gesagt besteht das Rezept soweit aus mehr Geld und mehr Vernetzung bzw. Clustering. Das ist nicht besonders neu: Gerade die nationalen und EU-europäischen Sicherheitsforschungsprogramme zielten bereits auf die enge und durch die Forschungsförderung forcierte Zusammenarbeit zwischen Hochschulen und wissenschaftlichen Instituten, (häufig in der Rüstung aktiven) Unternehmen und AnwenderInnen (insbesondere Behörden und Organisationen mit Sicherheitsaufgaben) ab. Dies führte zu einer starken Ausrichtung der wissenschaftlichen *Forschung* auf von den Sicherheitsbehörden definierte Szenarien (etwa der Terrorismusbekämpfung und der Migrationskontrolle) und eine schnelle Umsetzung wissenschaftlicher Erkenntnisse in die Praxis. Während hierbei jedoch auf industrieller Seite v. a. auf die bekannten großen Player der Sicherheits- und Rüstungsindustrie gesetzt wurde, gelten nun Start-up-Unternehmen als Schlüssel zu einer schnellen Implementierung und Kommerzialisierung. Entsprechend soll, ganz im Sinne der Studie von Roland Berger, ein *Ökosystem* für solche Unternehmen geschaffen werden. Die mit dieser Geschäftsform assoziierten hohen privaten Gewinne sollen zugleich Deutschlands Position im vielfach proklamierten „Kampf um die besten Köpfe" und seinen Ruf als Forschungsstandort verbessern. Im Koalitionsvertrag heißt es entsprechend, man wolle „Start-ups und Gründungen aus der Forschung" fördern und hierzu u. a. den „Zugang zu der Forschungsförderung für Start-ups" deutlich erleichtern.[8]

## Vorbild Cyber Valley

Was die Bundesregierung in ihrem Koalitionspapier und insbesondere das Beratungsunternehmen Roland Berger ausbuchstabieren, wurde bereits zuvor mit der sogenannten Cyber-Valley-Initiative in Stuttgart und Tübingen umgesetzt. Auch hier ist immer wieder von einem Ökosystem, der schnellen Umsetzung in marktfähige Produkte und der zentrale Rolle von Start-ups hierbei die Rede. So heißt es aktuell auf der Startseite der Initiative:

> *„Mit einem neuen Modell der Zusammenarbeit zwischen Wissenschaft und Wirtschaft wird Cyber Valley ein befruchtendes Ökosystem für den Technologietransfer im Bereich der Künstlichen Intelligenz schaffen. Denn bei der Entwicklung intelligenter Systeme ist der Weg von der Grundlagenforschung bis zur Kommerzialisierung oft sehr kurz: Start-ups, die im Umfeld der Forschung entstehen, sind Motoren dieser Entwicklung. Cyber Valley bildet durch eine enge Verzahnung von Wissenschaft und Wirtschaft die ideale Umgebung zur Förderung von Start-ups".*[9]

Die Max-Planck-Gesellschaft schrieb bereits in ihrer Pressemitteilung zur Gründung der Initiative im Dezember 2016:

> *„Das Cyber Valley soll ... nicht nur ein internationales Zentrum für Forschung an Intelligenten Systemen sein, sondern auch Unternehmensgründungen in diesem Bereich fördern, um von der Grundlagenforschung möglichst rasch zu marktfähigen Anwendungen zu kommen".*[10]

**Christoph Marischka**

**Christoph Marischka** ist Politikwissenschaftler, Mitglied im Vorstand der *Informationsstelle Militarisierung* und lebt in Tübingen. Seine Themenschwerpunkte sind u. a. Dual-Use- und Sicherheitsforschung, Drohnen und Aufklärungstechnologie.

Beteiligt an dem Projekt sind das Land Baden-Württemberg, die Universitäten Stuttgart und Tübingen, die Max-Planck-Gesellschaft sowie die Unternehmen Amazon, BMW, Daimler, Porsche, Bosch, ZF Friedrichshafen sowie IAV Automotive Engineering. Das Land Baden-Württemberg hat 50 Mio. Euro Unterstützung in den ersten Jahren zugesagt, eine vergleichbare Summe will die Industrie beisteuern. Gemeinsam finanzieren Land und Industrie zunächst neun Forschungsgruppen und mehrere Professuren; die Universitäten wollen ihrerseits *Brückenprofessuren* zu den Max-Planck-Instituten einrichten. Politik und Wirtschaft greifen damit tief in die Ausrichtung von Forschung und Lehre ein. In einem zweiten Ausbauschritt will die Landesregierung „ein gemeinsames Neubauvorhaben als physisches Zentrum von Cyber Valley unterstützen".[11] Zuvor wurde bereits der Neubau des Max-Planck-Institutes für Intelligente Systeme in Tübingen mit 41 Mio. vom Land unterstützt. Amazon wird noch in diesem Jahr mit dem Bau eines Entwicklungszentrums für Künstliche Intelligenz, eines „Büro- und Laborgebäudes für rund 200 Mitarbeiter" beginnen. Das Unternehmen bekundete „das starke Interesse, das Gebäude in unmittelbarer räumlicher Nähe zu den Max-Planck-Instituten zu erstellen"[12] und bekam entsprechend einen Bauplatz direkt neben der *Oberen Viehweide* zugewiesen, die bislang das Gravitationszentrum des Cyber Valley darstellt und wo bereits kräftig gebaut wird. Allein hier wird von 3.500 neuen Arbeitsplätzen ausgegangen. Weitere Flächen sind für die drei dort bereits ansässigen Max-Planck-Institute (MPI für biologische Kybernetik, MPI für Intelligente Systeme und MPI für Entwicklungsbiologie), das Cyber Valley und die Universität Tübingen vorgesehen. Räumlichkeiten für Start-up-Unternehmen werden von der Universität und der *Technologieförderung Reutlingen-Tübingen* vermittelt, einer Tochtergesellschaft der Städte Tübingen und Reutlingen, die gemeinsam mit der L-Bank den *Technologiepark Reutlingen Tübingen* (TTR) mit je einem Standort in beiden Städten betreibt. Im Idealfall sollen sich hier neu gegründete Unternehmen zunächst in angemieteten Räumen ausprobieren und im Erfolgsfall in räumlicher Nähe anschließend selbst Gebäude errichten können. Als Erfolgsmodell gilt dabei die CureVac AG, ein Unternehmen der Biotechnologie, das 2000 aus einer Arbeitsgruppe der Universität heraus gegründet wurde, sich 2003 im Technologiepark ansiedelte und dort seit 2016 neue Gebäude auf etwa 1,5 ha Fläche baut, die hierfür zum Teil von der Stadt Tübingen an „eine noch zu gründende Objektgesellschaft der Fa. Reisch" veräußert[13] und damit privatisiert wird.

## Schnittstellen zum Militär

Gemeinsam mit der Europäischen Weltraumagentur ESA weihte der TTR im April 2018 an seinem Reutlinger Standort (gut 10km entfernt von der Oberen Viehweide) ein *Business Incubation Centre* (BIC) ein, das als „Nährboden für Gründerideen" wirken und „jungen Startups bei der Verwirklichung innovativer Geschäftsideen im Bereich Weltraumtechnologie, Materialforschung, Navigations- oder auch Kommunikationstechnik helfen" soll. Das Landesministerium für Wirtschaft, Arbeit und Wohnungsbau fördert das BIC mit 750.000 Euro. Geplant ist, „ausgewählten Startups" Räume zur Verfügung zu stellen sowie „eine Starthilfe von insgesamt 50.000 Euro" wobei je 25.000 vom Land und der ESA bzw. dem Deutschen Zentrum Luft- und Raumfahrt (DLR) bereitgestellt werden.[14] Am BIC beteiligt sind neben der TTR GmbH, der ESA und dem DLR u. a. Bosch und Airbus Defence & Space. Das DLR ist eine der tragenden Säulen der deutschen Rüstungsforschung und betreibt gemeinsam mit Airbus Defence & Space die Aufklärungs- und Kommunikationssatelliten der Bundeswehr. Airbus stellt darüber hinaus nicht nur den Militärtransporter A400M und verschiedene Kampfhubschrauber her, sondern kümmert sich u. a. um den Betrieb der bislang größten Drohnen der Bundeswehr, die das Unternehmen vor Ort (z. B. in Afghanistan) wartet. Airbus ist damit nicht nur eines der größten Rüstungsunternehmen weltweit, sondern in Teilen bis zur Ununterscheidbarkeit mit der Bundeswehr verschmolzen. Dasselbe gilt für das DLR, das u. a. die Bodenstationen der Kommunikationssatelliten der Bundeswehr betreibt und hierfür zivile MitarbeiterInnen einstellt, die dann ausschließlich für die Aufrechterhaltung der militärischen Kommunikation zuständig sind.

Damit hat sich die eng mit der Bundeswehr verwobene Rüstungsindustrie vor Ort eine Schnittstelle geschaffen, um die Start-up-Szene zu beobachten und deren Produkte auf militärische Nutzung zu analysieren und gegebenenfalls auszurichten. Im entfernten Berlin hat das Verteidigungsministerium selbst eine entsprechende Institution geschaffen und damit ebenfalls die Relevanz der Start-Up-Szene für die schnelle Umsetzung von Forschung in die militärische Praxis unterstrichen. Der *Cyber Innovation Hub* (CIH), der im April 2018 seine Büros in Berlin-Moabit eröffnete, soll nach eignen Angaben eine „Schnittstelle zwischen Startup-Szene und Bundeswehr" darstellen:

> *„Er hat den Auftrag, digitale Innovationen innerhalb der Bundeswehr voranzutreiben. Der Hub identifiziert innovative Technologien in der internationalen Startup-Szene und entwickelt und validiert diese für die Bundeswehr. Ein besonderer Fokus liegt dabei auf disruptiven Technologien aus den Bereichen Cyber/Informationstechnik und digitalen Produkten und Services".*[15]

Ein explizites Ziel des Cyber Valley besteht auch darin, Tübingen und das Neckartal zum deutschlandweit wichtigsten Forschungsstandort der KI aufzuwerten und die Ansiedelung und Gründung weiterer Unternehmen zu induzieren. Dabei zeigt sich bereits jenseits der Initiative, dass viele IT-Unternehmen in der Rüstung aktiv sind und als Dienstleister des Militärs zumindest ausprobiert werden. Ein etwas älteres Beispiel hierfür ist die Reutlinger Eyevis GmbH, die als Kunden ihres *Control Room Manager* u. a. die NATO, die Bundeswehr und die Armeen Frankreichs, der USA und Abu Dhabis nennt.[16] Auch das

*Baustelle Obere Viehweide – Quelle: IMI*

Tübinger Start-up Syss, das nahe der Tübinger Innenstadt kürzlich einen großen Neubau errichtet hat und auf Penetrationstests spezialisiert ist, zählt die Bundeswehr zu seinen Referenzen. Mit der Übernahme des Tübinger Start-Up-Unternehmens Science & Computing hat sich auch Atos einen Standort in Tübingen erschlossen, ein Unternehmen, das teils in der Rüstung tätig ist und u. a. Grenzüberwachungssysteme und automatisierte Checkpoints konzipiert, die Personen und Objekte auf der Basis von Mustererkennung eigenständig detektieren und gegebenenfalls als *Bedrohung* oder *Ziel* klassifizieren.[17] Auch das oben erwähnte Bio-Tech-Unternehmen CureVac wurde im Rahmen von zwei Projekten der DARPA (der Forschungsagentur des Pentagon) mit über 30 Mio. US$ finanziert.[18]


*Reutlinger Standort des Technologieparks – Quelle: IMI*

## Unbehagen in der Gesellschaft

Dass auch jenseits eines ohnehin angespannten Wohnungsmarktes, massiver Bautätigkeiten und steigenden Baukosten die Idee, Tübingen und die gesamte Region in ein *Ökosystem* für *disruptive Innovationen* zu verwandeln, in der Bevölkerung Unbehagen auslöst, sollte nicht weiter erstaunen. Tatsächlich geht das neue *Ökosystem* bereits jetzt (zumindest zeitlich) mit der Zerstörung bestehender Ökosysteme einher, indem Flächen versiegelt und Naherholungsgebiete in Baugebiete für Laborgebäude umgewidmet werden. Dass die Besetzung von Lehrstühlen nun von Großkonzernen mitbestimmt wird, löst auch bei den Studierenden Empörung aus. Eine (zumindest zeitgleiche) wachsende Präsenz rüstungsrelevanter und im *Grenzschutz* aktiver Unternehmen und die Ansiedelung des Amazon-Konzerns, der für die Vernichtung arbeitsrechtlicher und Datenschutz-Standards berüchtigt ist, tun hierzu ihr Übriges. Eine Rolle bei diesem Unbehagen spielt in Hinblick auf die Forschungsschwerpunkte *maschinelles Sehen* und *maschinelles Lernen* womöglich auch das neue Baden-Württembergische Polizeigesetz, das erstmals den Einsatz *intelligenter Videoüberwachung* ermöglicht, die gegenwärtig in einem Pilotprojekt am Mannheimer Hauptbahnhof erprobt wird. Implementiert wird das Projekt vom Fraunhofer Institut für Optronik, Systemtechnik und Bilderkennung (IOSB), das auf Betreiben des Verteidigungsministeriums aus der Fusion eines militärischen und eines zivilen Instituts hervorging mit dem expliziten Ziel, durch eine verstärkte Zusammenarbeit mit der Wirtschaft und der zivilen Wissenschaft die Innovationszyklen zu verkürzen und militärische Techniken der Muster- und Zielerkennung auch in der *zivilen Sicherheit* zur Anwendung zu bringen.[19]

Über diese lokalen bis regionalen Faktoren des Unbehagens hinaus spielt natürlich auch der globale Diskurs um *Künstliche Intelligenz* eine Rolle. Weltweit äußern KI-ForscherInnen eine wachsende Kritik an der militärischen Indienstnahme ihrer Arbeit, wobei die thematische Engführung auf letztinstanzliche Tötungsentscheidungen auch die Funktion eines Feigenblattes einnehmen kann. Der weltweit sicherlich bekannteste Physiker, Stephen Hawking, warnte kurz vor seinem Tod, KI könnte zum „schlimmsten Ereignis in der Geschichte der Zivilisation" werden. Der ebenfalls kürzlich verstorbene Herausgeber der FAZ warnte vor einem „Technologischen Totalitarismus" und die Mathematikerin und frühere Hedge-Fonds-Managerin Cathy O'Neil beschreibt in ihrem Buch „Weapons of Math Destruction", wie bereits jetzt Existenzen durch Algorithmen sozial, finanziell und auch physisch vernichtet werden.

Insofern böte das im Entstehen begriffene Projekt Cyber Valley auch das Potenzial für eine konkrete Auseinandersetzung um die Frage, welche Formen der KI-Forschung überhaupt wünschenswert und unter welchen Produktionsbedingungen diese zu erreichen wären. Mit der Beteiligung von Amazon, der deutschen Automobilindustrie und an der Rüstung beteiligten Firmen wurde diese Diskussion jedoch umgangen und der als Wesensmerkmal des Cyber Valley angestrebte schnelle Transfer der Grundlagenforschung in die kommerzielle, ggf. auch militärische Nutzung zielt implizit auf die Umgehung gesellschaftlicher Diskussion und Technikfolgenabschätzung.

Entsprechend hat ein kleines, aus der Friedensbewegung, der „*Linken*" und der Studierendenschaft zusammengesetztes Bündnis am 6. Juli 2018 zu einer Kundgebung *Cyber Valley: Gegen den Ausverkauf der Stadt, der Universität und des Wissens* aufgerufen. Zu den Forderungen des Bündnisses gehörte: „Eine Offenlegung aller Pläne und Strukturen des Cyber Valley", „Keine Zusammenarbeit mit Militär und Rüstung" und „Keine öffentliche Unterstützung für Projekte, die die schnelle Umsetzung neuer Technologien in die Praxis ohne öffentliche Diskussion und Technikfolgenabschätzung zum Ziel haben".[20]

## Eine Wissenschaftkommunikation, die die Öffentlichkeit für dumm verkauft

Zum Unbehagen im Vorfeld der Kundgebung mag auch noch beigetragen haben, dass die Berichterstattung in der Lokalpresse über das Cyber Valley zuvor von den Sprechblasen der Beteiligten und einer professionellen und unehrlichen Wissenschafts-PR bestimmt war. Unter dem Titel *Auf dem Weg zur Weltspitze der Künstlichen Intelligenz* durften die Wissenschaftsministerin des Landes, der Rektor der Universität und ein Sprecher des Cyber Valley Relevanz und Strahlkraft des Projekts im Schwäbischen Tagblatt beschreiben bzw. simulieren:

> *„Erfolgreiche Forscher aus aller Welt sammeln sich im Cyber Valley um das Max-Planck-Institut … ‚Die Wissenschaftler kommen von den besten Universitäten und Forschungseinrichtungen der Welt', ‚werden in einem hoch selektiven Auswahlverfahren aus aller Welt rekrutiert', ‚sind die meist umkämpften Köpfe weltweit, und diese Spitzenkräfte wollen mit den Besten zusammenarbeiten' … ‚Das Cyber Valley findet national und international zunehmend Beachtung'".*

In einem anderen Beitrag der Zeitung fasste der Vize-Präsident der Max-Planck-Gesellschaft das vermeintliche Ziel der Initiative so zusammen: „Wir wollen Spuren hinterlassen in Gebieten, die der Menschheit nutzen". Der Direktor der Abteilung Maschinelles Lernen von Amazon, Ralf Herbrich, konnte im Schwäbischen Tagblatt den Einzelhandel mit der nicht weiter begründeten Versicherung beruhigen: „Läden werden wichtig bleiben" (so der Titel des Beitrags im Zitat). Amazon wolle „die Zukunft transparenter" machen, heißt es weiter. Auf die Kritik an den schlechten Arbeitsbedingungen bei Amazon angesprochen, behauptete Herbrich: „von den Mitarbeitern dort [im Logistikzentrum] wirkt keiner gehetzt". Sofern es um die tatsächlichen Inhalte der Forschung geht, bleibt die Berichterstattung oberflächlich, unkritisch. So heißt es zur Tätigkeit der von Bosch mit 5,5 Mio. Euro finanzierten Stiftungsprofessur, es gehe um „automatische Entscheidungssysteme, bei denen durch maschinelle Lernverfahren sichergestellt ist, dass sie keine diskriminierenden Entscheidungen treffen können". Wird im Cyber Valley etwa der Würfel neu erfunden?

Nach der Kundgebung ging die Berichterstattung ebenso weiter. Es kursierten viele „Gerüchte" um das Cyber Valley, so Redaktionsleiter Stegner einleitend, bevor er zwei SprecherInnen des Cyber Valley viel Raum gab, die Kritik in beeindruckender Pauschalität zurückzuweisen: Trotz der Finanzierung durch die Industrie gehe es „um freie Grundlagenforschung, nicht um Produkt- oder Auftragsforschung … Wir sind nicht die verlängerte Entwicklungsabteilung." Das „Cyber Valley sei nicht das Technologiezentrum Tübingen-Reutlingen (TTR) oder einzelne Firmen" wird festgestellt und zur Differenzierung aufgerufen. Auf die Frage, ob sich „die KI-Forschung in Tübingen für militärische Zwecke missbrauchen" ließe, wird wenig differenzierend geantwortet: „Wir haben keinerlei Projekte, die in diese Richtung gehen … Wir machen keine militärische Forschung." Während offen bleibt, wer dabei mit „wir" gemeint ist – vermutlich sprechen die VertreterInnen des Cyber Valleys hier nur für ihr jeweils eigenes Institut – wird etwas weiter oben festgestellt, dass die Unternehmen ihre Entscheidungen selbstständig treffen. Eine „Zivilklausel" sei zwar „gut gemeint", berge aber „praktische und rechtliche Probleme bei der Auslegung".[21]

Wenig später veröffentlichte die Universität Tübingen ein Video zum Maschinellen Lernen, das „diesen wichtigen Teilbereich der Künstlichen Intelligenz für Laien verständlich" machen soll.[22] Im Video macht sich ein gezeichneter Charakter namens *Ben* Gedanken über Maschinelles Lernen, das er gar nicht richtig begreift: „Übernehmen nun die Computerhirne die Kontrolle?", fragt er sich. Seine Freundin Tea erklärt ihm darauf, dass maschinelles Lernen u. a. in „modernen medizinischen Verfahren" und bei der „Instandhaltung von Produktionsmaschinen" zur Anwendung käme. Maschnielles Lernen nutze die exponentiell anwachsenden Datenmengen, „um Vorhersagen zu machen" und so „langfristig für den Menschen neues Wissen" zu erschließen. In diesem Moment erscheinen im Video über einer gezeichneten Menschenmenge Glühbirnen als Symbole der Erleuchtung. Dann wird wieder Ben gezeigt, mit einem deutlich glücklicheren Gesichtsausdruck. „Das leuchtet Ben ein" erfahren wir. Es wird allerdings eingeräumt: „Wie das Feuer, kann dieses Instrument sowohl sehr nützlich als auch gefährlich sein". Untermalt wird dies mit einem Kochtopf auf einer Feuerstelle und einer brennenden Fackel vor einer Blockhütte. Deshalb sei es wichtig, „das Feld der Forschung nicht alleine den Großkonzernen zu überlassen", erfahren wir weiter: „Die akademische Forschung stellt sicher, dass die neuen Erkenntnisse allen Menschen zur Verfügung stehen". Im Video erscheint ein Globus, um den herum symbolisierte Menschen stehen und sich bei den Händen halten. „Das überzeugt Ben … und wegen feindseliger Computerhirne macht er sich auch keine Sorgen mehr". Das Video stammt von einer Agentur namens *Simpleshow*, die ihrem Namen hier alle Ehre macht. Ob es die Öffentlichkeit, die es als dumm darstellt und für dumm verkauft, so einfach überzeugen kann, wie *Ben*, ist fraglich. Die Bevölkerung Tübingens als Teil des Ökosystems „Cyber Valley" wird sich auch weiter dafür interessieren und einmischen wollen, wer hier mit welchen Zielen woran forscht und was das nicht nur an Kosten, sondern auch an möglichen Folgen für sie haben wird.

## Anmerkungen

1 *Roland Berger GmbH/Asgard Capital Verwaltung GmbH: Artificial Intelligence – A strategy for European startups.*

2 *„Start-ups sind die wichtigsten Innovatoren für Künstliche Intelligenz", www.rolandberger.com.*

3 *z. B. Jay Tuck: „Künstliche Intelligenz: Wird sie uns eines Tages töten?", www.pcwelt.de*

4 *Gernot Stegert: „Cyber-Valley-Initiative in Tübingen weist Vorwürfe der Militarisierung und des Ausverkaufs zurück", www.tagblatt.de.*

5 *„Glaubwürdigkeitskrise der gesellschaftlichen Eliten", Martin Stratmann im Gespräch mit Ralf Krauter, deutschlandfunk.de.*

6 *Internationale Politik Ausgabe Juli/August 2018, online unter: zeitschrift-ip.dgap.org.*

7 *Koalitionsvertrag zwischen CDU, CSU und SPD für die 19. Legislaturperiode, bundesregierung.de.*

8 *Ebd.*

9 *www.cyber-valley.de (17.8.2018).*

10 *„Startschuss für das Cyber Valley", www.mpg.de.*

11 *Ebd.*

12 *Universitätsstadt Tübingen, Fachabteilung Projektentwicklung: Vorlage 107/2018 vom 1.3.2018.*

13 *Universitätsstadt Tübingen, Fachabteilung Liegenschaften: Vorlage 9/2018 vom 1.3.2018.*

14 *„Neuer Raumfahrt-Hotspot für Hessen und Baden-Württemberg", www.esa.int.*

15 *„Cyber Innovation Hub", bmvg.de.*

16 *„Eyevis", www.tueinfo.org/cms.*

17 *Vgl. u.a. „VIGIA border monitoring" und „CENTINELA Checkpoint" unter www.atos.net.*

18 *Universitätsstadt Tübingen, Oberbürgermeister: Vorlage 432/2016 vom 1.12.2016.*

19 *Christoph Marischka: „Fraunhofer IOSB – Dual Use als Strategie", IMI-Studie 2017/02.*

20 *„Cyber Valley: Gegen den Ausverkauf der Stadt, der Universität und des Wissens", www.tueinfo.org/cms.*

21 *„Auf dem Weg in die Weltspitze der Künstlichen Intelligenz", „Max-Planck-Forscher und Firmen wollen Innovations-Ökosystem für künstliche Intelligenz schaffen", „Läden werden wichtig bleiben", „5,5 Millionen Euro für Stiftungsprofessur" und „Cyber-Valley-Initiative in Tübingen weist Vorwürfe der Militarisierung und des Ausverkaufs zurück", Schwäbisches Tagblatt vom (in der Reihenfolge ihrer Erwähung) 26.5.2018, 2.5.2018, 23.5.2018, 7.6.2018 und 18.7.2018.*

22 *„Universität Tübingen erklärt Maschinelles Lernen", uni-tuebingen.de.*

**Anja Heinrich, Stefan Hügel**

# Staatstrojaner – Förderung oder Gefährdung der inneren Sicherheit?

*Aktuell werden die Polizeiaufgabengesetze mehrerer Bundesländer novelliert – zuletzt unter anderem in Bayern, Nordrhein-Westfalen und Hessen. Gleichzeitig hat die* Große *Koalition in ihrem Koalitionsvertrag angekündigt, ein* Musterpolizeigesetz *vorzulegen, an dem sich die Polizeigesetzgebung in den Ländern orientieren soll.*

*Niedersachsen gehört zu den Ländern, die darauf nicht warten wollen. Die Fraktionen der Regierungskoalition in Hannover brachten einen Gesetzentwurf in den Landtag ein. Dieser Beitrag befasst sich mit der im Gesetzentwurf vorgesehenen Einführung von Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) und Online-Durchsuchung. Er basiert in großen Teilen auf der schriftlichen Stellungnahme der Humanistischen Union[1] für die im August 2018 stattgefundene öffentliche Sachverständigenanhörung und verortet den niedersächsischen Gesetzentwurf in der gesamtdeutschen Entwicklung.*



## Entwicklung der Quellen-TKÜ und Online-Durchsuchung in Deutschland

Durch den zunehmenden Einfluss informationstechnischer Systeme auf den Alltag der Menschen bestehen auch Begehrlichkeiten der Sicherheitsbehörden, auf diese Systeme zuzugreifen, entweder um an die darauf gespeicherten Daten zu gelangen (Online-Durchsuchung) oder die darüber laufende verschlüsselte Kommunikation (z.B. Skype oder Messenger-Dienste) zu überwachen (Quellen-TKÜ). Lange war jedoch umstritten, ob die neu entwickelten Instrumente der Quellen-TKÜ und der Online-Durchsuchung auf bereits bestehende Ermächtigungsgrundlagen gestützt werden können, insbesondere auf die Standardbefugnisnormen zur Telekommuniktionsüberwachung. Ungeachtet dessen wendeten Polizei- und Verfassungsschutzbehörden die grundrechtsintensiven Maßnahmen sowohl zwecks Strafverfolgung als auch zur Gefahrenabwehr ohne spezielle Gesetzesgrundlage an. Im Januar 2007 entschied der 3. Strafsenat des Bundesgerichtshofs (BGH), dass die repressive Online-Durchsuchung weder auf die strafprozessuale Regelung zur Wohnraumdurchsuchung (§ 102 StGB) noch auf diejenige zur Telekommunikationsüberwachung (§ 100a StPO) gestützt werden kann, sondern eine spezielle Ermächtigungsgrundlage erforderlich ist. Zu diesem Zeitpunkt hatte der Gesetzgeber in Nordrhein-Westfalen für den Landesverfassungsschutz bereits eine Befugnisnorm für die Anwendung der Online-Durchsuchung geschaffen. Im Februar 2008 wurde diese seit 2006 bestehende Regelung vom Bundesverfassungsgericht in seinem berühmten, das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme begründenden Urteil, für nichtig erklärt.[2]

Die Entwicklung, die Geheimdienste und Polizeibehörden zu diesen Maßnahmen zu ermächtigen, setzte sich jedoch fort. Noch im selben Jahr der Entscheidung traten in Bayern Regelungen in Kraft, die der Landespolizei und dem Landesamt für Verfassungsschutz die Online-Durchsuchung erlauben. Seit Januar 2009 war das Bundeskriminalamt zwecks Terrorismusbekämpfung in der Lage, Online-Durchsuchung und Quellen-TKÜ durchzuführen. Es folgte Rheinland-Pfalz, das seine Polizei seit Februar 2011 zur Anwendung beider Instrumente ermächtigt und Sachsen-Anhalt, welches 2013 eine Regelung zur Online-Durchsuchung in sein Polizeigesetz einfügte. Letztere wurde ein Jahr später vom Landesverfassungsgericht für nichtig erklärt.[3] Die erfolgte Novellierung des BKA-Gesetzes führte im April 2016 zu einem zweiten wegweisenden Urteil des Bundesverfassungsgerichts (sog. BKAG-Urteil), in dem das Gericht wesentliche Grundsätze für heimliche Überwachungsmaßnahmen aufstellte, darüber hinaus auch die im damaligen BKA-Gesetz enthaltenen Regelungen zur Quellen-TKÜ und Online-Durchsuchung für unvereinbar mit der Verfassung erklärte und bestimmte, dass die beiden Befugnisnormen nur mit Einschränkungen bis zum 30.6.2018 fortgelten.[4] Der Bundesgesetzgeber kam seinem Auftrag zur Neuregelung mit dem im Mai 2018 in Kraft getretenen Gesetz zur Umstrukturierung des Bundeskriminalamtes nach. Das Gesetz folgte den bereits im August 2017 in Kraft getretenen, strafprozessualen Ermächtigungsgrundlagen, die zum Zwecke der Strafverfolgung nun auch die Ermittlungsbehörden zur Quellen-TKÜ und Online-Durchsuchung ermächtigen. Gegen die Regelungen wurden bereits mehrere Verfassungsbeschwerden eingelegt.[5]

Derzeit geht der Trend dahin, insbesondere den Werkzeugkasten der Polizeibehörden der Bundesländer mit den Instrumenten der Quellen-TKÜ und der Online-Durchsuchung auszustatten. Das Bundesinnenministerium hat einen Mustergesetzentwurf angekündigt, der das Vorbild für runderneuerte Landespolizeigesetze liefern und auch Standardbefugnisnormen für die Quellen-TKÜ und Online-Durchsuchung enthalten soll. In vielen Bundesländern hat jedoch der Gesetzgebungsprozess bereits eingesetzt. Baden-Württemberg hat die Quellen-TKÜ schon im Jahr 2017 eingeführt und Bayern und Hessen haben ihre Polizeigesetze in diesem Jahr gründlich überarbeitet. In beiden Bundesländern sind nun Quellen-TKÜ und Online-Durchsuchung möglich; zumindest gegen das bayerische Gesetz wurden ebenfalls bereits mehrere Verfassungsbeschwerden eingelegt. Auch in Bremen wollte die rot-grüne Koalition das Polizeigesetz noch in diesem Jahr überarbeiten, inklusive der Einführung der Quellen-TKÜ. Massiver Protest in der Bevölkerung hat jedoch dazu geführt, dass der grüne Koalitionspartner den bereits vorgelegten Gesetzentwurf nicht mittragen will und das Gesetzesvorhaben vorerst auf Eis gelegt wurde. Neben dem niedersächsischen Landtag befasst sich derzeit auch der Landtag in Nordrhein-Westfalen mit der Novellierung des Polizeigesetzes, inklusive der Einführung von Quellen-TKÜ und Online-Durchsuchung. Der derzeit im Sächsischen Landtag befindliche Gesetzentwurf zur Novellierung des Polizeigesetzes sieht zwar in vielen Teilen erhebliche Erweiterungen der polizeilichen Befugnisse vor, wie die Vorverlagerung der Standardbefugnisse ins Gefahrenvorfeld und die Einführung neuer Befugnisse wie sog. elektronische Fußfessel, auf die Quellen-TKÜ und Online-Durchsuchung soll jedoch auf Grund des Widerstands der SPD vorerst verzichtet werden.

schwerpunkt

## Online-Durchsuchung und Quellen-TKÜ gefährden die Grundrechte

Vor dem Hintergrund, dass der Bundesgesetzgeber die Quellen-TKÜ als Instrument zur Abwehr terroristischer Gefahren gerade erst in das BKA-Gesetz eingefügt hat, stellt sich die Frage der tatsächlichen Notwendigkeit zusätzlicher Regelungen für die Landespolizeibehörden. In vielen Bundesländern hat nicht nur die Skepsis gegen die Einführung neuer grundrechtsintensiver Maßnahmen, sondern gerade auch die in Frage stehende tatsächliche Notwendigkeit solcher Regelungen zu erheblichem Widerstand und massiver Kritik geführt. Die Niedersächsische Landesdatenschutzbeauftragte, Barbara Thiel, hat zu dem niedersächsischen Gesetzentwurf in der öffentlichen Anhörung ebenfalls sehr kritisch Stellung bezogen. Ein Statement auf ihrer Homepage fasst ihre Kritik zusammen:

> *„Unter dem Deckmantel, den internationalen Terrorismus zu bekämpfen, beschneiden die vorgeschlagenen Regelungen die Freiheitsrechte der Bürgerinnen und Bürger bis zur Unkenntlichkeit. Aus dem Gesetzentwurf wird nicht ansatzweise erkennbar, warum derartige Verschärfungen erforderlich sind. Keine der einzelnen neuen Überwachungsmaßnahmen wird ausführlich begründet. Das betrifft insbesondere die Maßnahmen der elektronischen Fußfessel, Quellen-Telekommunikationsüberwachung (TKÜ) und Online-Durchsuchung. Ich habe vielmehr den Eindruck, dass alle verfassungsrechtlichen Möglichkeiten zur Stärkung der inneren Sicherheit auf Biegen und Brechen ausgeschöpft werden sollen, ohne dabei die Freiheitsrechte angemessen zu berücksichtigen."*[6]

Zu der berechtigten Kritik an der äußerst fraglichen Notwendigkeit stetiger grundrechtsintensiver Befugniserweiterungen kommt hinzu, dass es gegen die Einführung der Quellen-TKÜ und der Online-Durchsuchung aufgrund vieler technischer und rechtlicher Unwägsamkeiten insgesamt erhebliche Bedenken gibt.

## Grenzen rechtlicher Regelbarkeit

### Fehlende Eingrenzbarkeit der Quellen-TKÜ

Bedenken begründet besondere die Tatsache, dass die Regelungen zur Quellen-TKÜ formal zwar lediglich zur Überwachung der laufenden Kommunikation ermächtigen, jedoch erhebliche Zweifel an der Eingrenzbarkeit der Maßnahme bestehen.

Die technischen Schritte zur Aufbringung von Software für die Quellen-TKÜ sind mit denjenigen für die Online-Durchsuchung weitgehend identisch.[7] Für die für derartige Eingriffe verwendete *Remote Forensic Software*[8] hat sich in der politischen Debatte mittlerweile die Bezeichnung *Staatstrojaner*[9] eingebürgert. Inwieweit die Staatstrojaner derart programmiert werden können und in der Praxis dann auch derart programmiert werden, dass sie bei einer Maßnahme zur Telekommunikationsüberwachung keine weiteren Daten aus dem informationstechnischen System erfassen, ist zweifelhaft. Am 8. Oktober 2011 veröffentlichte der Chaos Computer Club (CCC) eine Analyse[10] eines Programms zur Quellen-TKÜ und deckte dabei auf, dass das untersuchte Programm über weit mehr Fähigkeiten verfügt als die Überwachung der Telekommunikation. Dazu gehörte das Erstellen von Bildschirmfotos, das Nachladen von beliebigen Programmen aus dem Internet sowie der Mitschnitt von Tastaturanschlägen. Zudem konnten auch einfache Daten wie Bilder auf den Computer aufgespielt werden.

Eingrenzbarkeitsprobleme entstehen zudem dadurch, dass technisch nicht zuverlässig zwischen Kommunikations- und anderen Prozessen auf dem Rechnersystem unterschieden werden kann. Denn bei der Quellen-TKÜ werden zur Überwachung der verschlüsselten Kommunikation die Daten (z.B. eine E-Mail) vor der Verschlüsselung und damit in einem Zeitpunkt abgefangen, zu dem weder der Trojaner erkennen kann noch der Verfasser vielleicht selbst weiß, ob die Daten später tatsächlich versendet werden. So werden bei der Überwachung des E-Mail-Verkehrs insbesondere auch alle Entwürfe unabhängig von ihrer späteren Versendung erfasst.[11]

### Erfassung kernbereichsrelevanter Daten bei der Online-Durchsuchung unvermeidbar

Das Bundesverfassungsgericht hat festgestellt, dass die Online-Durchsuchung anders als andere Überwachungsmaßnahmen keine Überwachung eines zeitlich gegliederten Geschehens an verschiedenen Orten darstellt, sondern dass der Zugriff stets auf ein gesamtes System erfolgt und dass damit in Bezug auf den Zugriff weitgehend nur die Alternativen von ganz oder gar nicht bestehen. Damit existiert faktisch keine Möglichkeit, Betroffene vor dem Zugriff auf kernbereichsrelevante – also höchstpersönliche, der Menschenwürde zuzuordnende – Informationen zu schützen. Als Konsequenz ist das Bundesverfassungsgericht in Bezug auf die Online-Durchsuchung von seinem vormals entwickelten 2-stufigen Schutzkonzept[12] abgewichen. Nach dem 2-stufigen Schutzkonzept hat der Schutz des Kernbereichs privater Lebensgestaltung bei heimlichen Überwachungsmaßnahmen sowohl bei der Datenerhebung (1. Stufe) als auch bei der Datenverarbeitung (2. Stufe) zu erfolgen. So ist der Gesetzgeber auf der 1. Stufe der Datenerhebung gehalten, Schutzmaß-


*Nein zum Polizeigesetz: 7. Juli 2018 Großdemo Düsseldorf Landesverband NRW von Bündnis 90/Die Grünen, CC BY-SA 2.0* nahmen vorzusehen, die verhindern, dass kernbereichsrelevante Daten überhaupt erst erhoben werden. Auf der 2. Stufe hat er zu regeln, dass höchstpersönliche Daten, die trotz dieser Schutzvorkehrung gleichwohl versehentlich erhoben worden sind, unverzüglich zu löschen sind. In Bezug auf die Online-Durchsuchung hat das Bundesverfassungsgericht jedoch zuletzt festgestellt, dass Schutzmaßnahmen vor Kernbereichsverletzungen nicht primär auf die Verhinderung der Erfassung und des Festhaltens höchstpersönlicher Daten zielen, sondern auf die Verhinderung des Auslesens dieser Informationen und hat damit den notwendigen Kernbereichsschutz auf der Erhebungsebene weitgehend zurückgefahren.[13] Die Anpassung der bundesverfassungsgerichtlichen Rechtsprechung an die Besonderheiten der Online-Durchsuchung hat die mit ihr verbundenen Zugriffe auf höchstpersönliche Informationen zwar rechtlich legitimiert, hat jedoch gleichzeitig die massiven Bedenken ihrer Kritiker bestätigt. Denn Fakt bleibt: Ein Zugriff auf höchst persönliche Informationen, wie Tagebuchaufzeichnungen, ist bei der Online-Durchsuchung kaum verhinderbar und Schutzmaßnahmen, die erst auf der Stufe der Datenverarbeitung und -verwendung greifen, können die bei der Datenerhebung eingetretenen Kernbereichsverletzungen lediglich noch kompensieren. Ein effektiver Schutz der Intimsphäre von Betroffenen muss daher nun zwar nicht mehr rechtlich, aber faktisch weiterhin bei der Datenerhebung ansetzen. D. h. bereits die Erhebung höchstpersönlicher Informationen ist zu unterlassen.[14]

### Rechtliche Grauzonen des Staatstrojaners

Es stellt sich zudem die Frage des Einsatzes – wie kann die Überwachungssoftware in rechtmäßiger Art und Weise auf die entsprechenden Rechnersysteme aufgespielt und aktiviert werden? Offensichtlich ist die Maßnahme nur sinnvoll, wenn der Zielperson die Tatsache ihrer Überwachung nicht bekannt ist, da sie sonst ihr Verhalten anpassen würde. Grundsätzlich sind drei Wege der Infiltration denkbar:

- Installieren der Software im Rahmen kurzzeitiger Verfügung über den zu überwachenden Rechner, in einem unbeobachteten Moment während einer Sicherheitskontrolle am Flughafen,
- Eindringen in die Wohnung der Zielperson, um an den Rechner zu gelangen – dies ist aber rechtlich kaum möglich, ohne dass die Zielperson Kenntnis davon erlangt,
- Nutzen von Trojanersoftware – dies ist in der Praxis unserer Einschätzung nach der häufigste Weg und wird im Folgenden schwerpunktmäßig behandelt.

### Keine Rechtsgrundlagen für den physischen Zugriff auf das informationstechnische System

Die *Remote Forensic Software* kann durch unmittelbaren physischen Zugriff auf dem informationstechnischen System installiert werden. „Nur auf diese Weise kann – was gelegentlich übersehen wird – ausgeschlossen werden, dass beispielsweise Rechner von unbeteiligten Dritten ebenfalls in den Fokus der Ermittler geraten".[15] Häufig wird ein solcher Zugriff am Aufbewahrungsort des informationstechnischen Systems erfolgen müssen. Bei Rechnern ist dies i. d. R. die Wohnung. Der damit unmittelbar verbundene Eingriff in die Unverletzlichkeit der Wohnung, Art. 13 Abs. 1 GG, kann jedoch schon deshalb nicht rechtmäßig erfolgen, weil es hierfür schlicht an entsprechenden Gesetzesgrundlagen fehlt. Entsprechendes gilt für die Mitnahme des informationstechnischen Systems unter einem Vorwand und das dabei erfolgende Aufspielen der Software.

*Nein zum Polizeigesetz: 7. Juli 2018 Großdemo Düsseldorf Landesverband NRW von Bündnis 90/Die Grünen, CC BY-SA 2.0*

Erfolgt der Zugriff und das Aufspielen der Software auf das System dagegen extern über eine Online-Verbindung, setzt dies voraus, dass es im Zielsystem eine Schwachstelle gibt, die für die Maßnahme genutzt werden kann. Solche Schwachstellen werden durch *Exploits*[16] ausgenutzt. Damit sind Strafverfolgungsbehörden nicht anders als das kriminelle Millieu darauf angewiesen, Schwachstellen bzw. die auf ihnen fußenden Exploits für die Quellen-TKÜ bzw. Online-Durchsuchung zu nutzen. In diesem Sinn sind Staatstrojaner nichts anderes als ein Schadcode, der auf dem zu infiltrierenden System installiert wird. Um die Wahrscheinlichkeit für den Erfolg der Maßnahme zu erhöhen, werden insbesondere Zero-Day-Exploits benötigt. Die Schwachstellen können durch entsprechende Analysen selbst *entdeckt* oder auf dem Schwarzmarkt *erworben* werden. Aufgrund des Aufwands für die Entdeckung von Schwachstellen und Entwicklung von Exploits wird es in der Praxis häufig zum Kauf kommen. Eine weitere Möglichkeit ist das bewusste Schaffen von Schwachstellen durch staatliche Stellen, beispielsweise durch die Standardisierung schwacher Sicherheitsstandards.

Alle Methoden führen dazu, dass bewusst und vorsätzlich Schwachstellen geschaffen oder aufrecht erhalten werden, die auch durch Dritte – beispielsweise in krimineller oder terroristischer Absicht – ausgenutzt werden können. Neben dem unmittelbaren Risiko der Nutzung untergräbt dies langfristig die Vertrauenswürdigkeit und damit die Funktionsfähigkeit der technischen Infrastruktur. Eine sichere Infrastruktur ist nicht zuletzt für Wirtschaftsunternehmen von hoher Bedeutung, um ihre geschäftlichen Transaktionen sicher abzuwickeln und Akzeptanz für die Digitalisierung der Wirtschaft zu schaffen. Das damit verbundene Ziel, keine Angriffsflächen für die Verursachung von Datenpannen oder Wirtschaftsspionage zu bieten, wird durch Staatstrojaner konterkariert.

Die Folge ist, dass durch das Offenhalten von Schwachstellen potenziell Terroristen ein Werkzeug in die Hand gegeben wird, durch das sie weiteren, erheblichen Schaden verursachen können, der möglicherweise den durch einen Ermittlungserfolg verhinderten Schaden bei Weitem übersteigt.[17] Ein Beispiel für eine Schadsoftware, die solchen Schaden verursachen kann, ist der *Ransomware-Trojaner WannaCry*[18], der 2017 unter anderem Systeme des britischen National Health Service und der Deutschen Bahn befallen und für erhebliche Beeinträchtigungen gesorgt hat. Der zugrundeliegende Exploit stammte aus dem Fundus der US-amerikanischen National Security Agency. Das Beispiel zeigt, dass die Kompromittierung von IT-Systemen nicht auf bestimmte Nutzungsweisen eingeschränkt werden kann.[19] Durch den Ankauf von Schwachstellen und Exploits sorgen staatliche Stellen zudem dafür, dass ein lukrativer Schwarzmarkt etabliert und gefördert wird, da sie für die notwendige Nachfrage sorgen bzw. sie fördern. Dies trägt zusätzlich dazu bei, die öffentliche Infrastruktur nachhaltig zu gefährden.[20] Der Staat begibt sich damit insgesamt in einen erheblichen Zielkonflikt: Durch die Nutzung von Software zum Eingriff in informationstechnische Systeme zur Verhinderung von Straftaten fördert er die Möglichkeit von Straftaten gleichzeitig in erheblichem Maß.[21]

Zu den technischen Rahmenbedingungen nimmt eine aktuelle Studie der *Stiftung Neue Verantwortung* Stellung.[22] Der Autor der Studie entwirft einen Prozess für das Schwachstellen-Management, nach dem beim Umgang mit Schwachstellen vorgegangen und entschieden werden soll. Der Vorschlag enthält vier Elemente:

- Institutioneller Aufbau und Workflow,
- Beurteilung der Schwachstellen,
- Management der Schwachstellen,
- Schutz- und Kontrollmaßnahmen.

Der Prozess soll durch ein Sekretariat gesteuert werden, das auch die Entscheidung zwischen Zurückhalten oder Offenlegung einer Schwachstelle koordiniert. Der Vorschlag sieht auch mehr Transparenz, unter anderem durch parlamentarische Kontrolle, vor.

Ob dies tatsächlich die Sicherheitsprobleme zu lösen imstande ist, erscheint zweifelhaft. Probleme wie die Schaffung eines Schwarzmarkts für Schwachstellen und Exploits werden durch den Vorschlag nicht adressiert. Die Prämisse, dass in einem rechtlichen Graubereich wie dem Handel mit Schwachstellen nach festgelegten Prozeduren und vertraglichen Vereinbarungen vorgegangen wird, wirkt naiv. Es ist wohl auch kaum vorstellbar, dass eine nachrichtendienstliche Behörde Schwachstellen – wie in der Studie unterstellt – auf dem Schwarzmarkt ankauft, nur um sie danach auf Empfehlung eines unabhängigen Gremiums sogleich offenzulegen. Zurückgehaltene Schwachstellen stellen stets eine Gefahr für die öffentliche Sicherheit dar – neben dem Risiko, dass die Information darüber durch die nutzende Behörde selbst an die Öffentlichkeit gerät, kann sie auch durch andere Akteure gefunden und anschließend genutzt werden. Eine parlamentarische Kontrolle ist zwar wünschenswert aber nicht besonders erfolgversprechend, nachdem die Kontrolle der Nachrichtendienste in der heutigen Form wohl als gescheitert zu betrachten ist[23].

## Manipulation, Dokumentation, Missbrauch

### Die Rechtmäßigkeit der verwendeten Software lässt sich nicht sicherstellen

Der Gesetzentwurf fordert für eine Maßnahme der Online-Durchsuchung sowie der Quellen-TKÜ eine richterliche Anordnung bzw. bei Gefahr im Verzug die Anordnung eines dazu befugten Polizeibeamten. Dafür ist es u. a. erforderlich, dass die Rechtmäßigkeit der für die Maßnahme verwendeten Software geprüft wird.

Diese Prüfung der Rechtmäßigkeit kann nur in Kenntnis der Funktionsweise der Software und damit des Quelltexts durch sachkundige Experten erfolgen. Um die Rechtmäßigkeit sicherzustellen, ist beispielsweise eine Zertifizierung durch eine unabhängige Zertifizierungsstelle erforderlich. Diese müsste für jedes Release erneuert werden, da jede Änderung prinzipiell der Software neue rechtswidrige Funktionalität hinzufügen kann.

### Durchsuchungsergebnisse können manipuliert werden

Die Kompromittierung eines IT-Systems ermöglicht weitergehende Manipulation bis hin zur Ablage kompromittierender Dateien auf dem System der Zielperson. Ebenso wie die Ermittlungspersonen sind die zu überwachenden Zielpersonen technisch prinzipiell in der Lage, die Ermittlungsergebnisse in ihrem Sinne zu manipulieren.[24] Damit haben die erhobenen Daten keine forensische Beweiskraft.

### Die Eingriffe in die informationstechnischen Systeme müssten rechtssicher dokumentiert werden

Wegen der mit dem Einsatz von Staatstrojanern verbundenen, äußerst weitgehenden Eingriffsmöglichkeiten müssten zur Gewährleistung von Transparenz und Kontrolle Eingriffe in informationstechnische Systeme stets dokumentiert werden. Die Möglichkeit zur rechtssicheren Dokumentation auf einem fremden System ist jedoch in der Regel sehr eingeschränkt, denn dieses System kann manipuliert werden, weil es in den meisten Fällen nicht vollständig durch die Ermittlungsbeamten kontrolliert wird.

Auch die kryptographische Absicherung solcher Protokolle kann die Authentizität nicht gewährleisten. Auf die dafür benötigten Schlüssel kann auch das infiltrierte System zugreifen.

## Regelungen zur Quellen-TKÜ und Online-Durchsuchung in Niedersachsen und Kritikpunkte an der dortigen Ausgestaltung der Maßnahmen

Niedersachsen ist auf dem Weg, die Quellen-TKÜ und die Online-Durchsuchung als Standardbefugnis für die Polizei zur Gefahrenabwehr einzuführen. Die allgemeinen Kritikpunkte, die es an der Einführung solcher Instrumente gibt, muss daher auch Niedersachsen gegen sich gelten lassen. Außerdem ist die spezielle gesetzliche Ausgestaltung der Regelungen mangelhaft, die die niedersächsische Polizei zur Quellen-TKÜ und Online-

Durchsuchung ermächtigen sollen. Das erhöht die Eingriffsintensität der Maßnahmen zusätzlich und wirft Bedenken bezüglich ihrer Verfassungsmäßigkeit auf.

Sowohl die Quellen-TKÜ als auch die Online-Durchsuchung reichen tief in das Privatleben der betroffenen Personen hinein und stellen einen schwerwiegenden Eingriff in das verfassungsrechtlich geschützte Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) dar. Die Anforderungen an die gesetzliche Ausgestaltung sind entsprechend hoch. Welche konkreten verfassungsrechtlichen Anforderungen an heimliche Überwachungsmaßnahmen wie die Quellen-TKÜ und die Onlinedurchsuchung zu stellen sind, hat das Bundesverfassungsgericht in seinem BKAG-Urteil aufgezeigt. Danach müssen die Maßnahmen auf den Schutz oder die Bewehrung hinreichend gewichtiger Rechtsgüter begrenzt sein, eine Gefährdung dieser Rechtsgüter muss hinreichend konkret absehbar sein, und sie dürfen sich nur unter eingeschränkten Bedingungen auf nichtverantwortliche Dritte aus dem Umfeld der Zielperson erstrecken. Erforderlich sind zudem besondere Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung sowie der Schutz von Berufsgeheimnisträgern. Solche Regelungen unterliegen Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle und müssen mit Löschpflichten bezüglich der erhobenen Daten flankiert sein.

## Eingriffsschwellen und Eingriffsbefugnisse

### Eingriffsschwelle zu weit und zu unbestimmt

Für heimliche Überwachungsmaßnahmen hat das Bundesverfassungsgericht in seinem BKA-Urteil Minimalanforderungen an die Eingriffsschwelle festgelegt. Für solche Maßnahmen, wie die Quellen-TKÜ und die Online-Durchsuchung, muss zwar keine konkrete Gefahr i. S. d. Polizeirechts vorliegen, wenn sie dem Schutz überragend wichtiger Rechtsgüter dienen. Es sind aber mindestens „tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr" nötig. Damit verzichtet das Bundesverfassungsgericht für den Schutz überragend wichtiger Rechtsgüter auf das Vorliegen einer hinreichenden Wahrscheinlichkeit des Schadenseintritts, fordert aber gleichwohl eine gewisse Konkretisierung ein. Zwei Konkretisierungen sind möglich: Entweder (1) muss es die geforderten tatsächlichen Anhaltspunkte geben, die auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen schließen lassen, sowie darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest soviel bekannt ist, dass die Überwachungsmaßnahmen gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden können. Oder (2) das individuelle Verhalten einer Person begründet die konkrete Wahrscheinlichkeit, dass sie in überschaubarer Zukunft terroristische Straftaten begehen wird.

Die im niedersächsischen Gesetzentwurf geregelten Voraussetzungen für die Quellen-TKÜ und die Online-Durchsuchung entsprechen in ihrem Wortlaut zwar in weiten Teilen den Ausführungen des Bundesverfassungsgerichts, in Bezug auf die Online-Durchsuchung gab es jedoch eine wesentliche Änderung. Sie steht im neuen § 33d im Niedersächsischen Gesetz über die öffentliche Sicherheit und Ordnung. Online-Durchsuchungen sollen u. a. dann zulässig sein, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums Leib, Leben oder Freiheit einer Person schädigen wird. Außerdem sollen Online-Durchsuchungen dann zulässig sein, wenn das so beschriebene Verhalten Rechtsgüter schädigen wird, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschheit berührt. Damit weicht der Gesetzentwurf vom Erfordernis der terroristischen Straftat ab. Denn die mögliche Gefährdung der im Gesetzentwurf aufgezählten gewichtigen Rechtsgüter stellt nicht automatisch auch eine mögliche Gefahr einer terroristischen Straftat dar. Für eine terroristische Straftat wird man zusätzlich zumindest auch immer eine politische, staatsfeindliche und umstürzlerische Absicht des Täters verlangen müssen. Die bloße Verletzung der im Gesetzentwurf genannten Rechtsgüter erfüllt diese Voraussetzung nicht.

Darüber hinaus stellt sich die Frage, ob die im Gesetzentwurf für die Quellen-TKÜ und Online-Durchsuchung definierten Eingriffsvoraussetzungen dem Bestimmtheitsgebot genügen. Fraglich ist insbesondere, ob BürgerInnen vorhersehen und Rechtsanwender und Gerichte feststellen können, wann die (Geschehens-)Weise einer Straftat zumindest „ihrer Art nach konkretisiert" ist. Indem der niedersächsische Gesetzentwurf in weiten Teilen Begrifflichkeiten aus dem BKA-Urteil des Bundesverfassungsgerichts quasi im Wege des Copy-and-Paste wiederverwendet, genügt er nicht automatisch dem verfassungsrechtlichen Bestimmtheitsgebot. Denn während es lediglich Aufgabe des Bundesverfassungsgerichts ist, dem Gesetzgeber allgemeingültige Grenzen der Einschränkbarkeit eines Grundrechts aufzuzeigen, ist es Aufgabe des Gesetzgebers, die Eingriffsvoraussetzungen für die Anwendung im Einzelfalls hinreichend bestimmt auszugestalten. Der Gesetzgeber muss die Eingriffsvoraussetzungen so klar definieren, dass die Bürger Eingriffe in ihre Grundrechte vorhersehen können, die Rechtsanwender (Polizis-



**Anja Heinrich und Stefan Hügel**

**Anja Heinrich** ist Rechtsanwältin in Berlin und Mitglied im Bundesvorstand der *Humanistischen Union*. Seit einigen Jahren befasst sie sich insbesondere auch mit präventiv-polizeilichen Befugnissen und deren Rechtmäßigkeit.

**Stefan Hügel,** Diplom-Informatiker, ist Vorsitzender des FIfF und Mitglied des Bundesvorstands der Humanistischen Union. Beruflich arbeitet er als Berater für IT-Prozesse. Er lebt in Frankfurt am Main.

ten und andere) die Maßnahmen anwenden und die Gerichte diese Maßnahmen überprüfen können. In Bezug auf den Gesetzentwurf stellt sich daher die Frage, ob der Gesetzgeber, der den Begriff der terroristischen Straftat in § 2 seines Gesetzentwurfs definiert hat, vor dem Hintergrund des Bestimmtheitsgebotes nicht auch definieren muss, wann die (Geschehens-) Weise eine derartigen terroristischen Straftat im Einzelfall „ihrer Art nach konkretisiert ist".



**Fehlender Richtervorbehalt bei der Quellen-TKÜ**

Bei der Quellen-TKÜ hat es die Regierungsfraktion zudem versäumt, die Maßnahme unter den Vorbehalt einer richterlichen Anordnung zu stellen. Das Urteil des Bundesverfassungsgerichts zum BKA-Gesetz verlangt eine richterliche Anordnung oder eine anderweitige unabhängige vorherige Kontrolle für eingriffsintensive heimliche Überwachungsmaßnahmen, bei denen damit zu rechnen ist, dass auch höchst private Informationen erfasst werden. Der Gesetzgeber hat hierbei zu normieren, dass es vor der Datenerhebung einer gerichtlichen Anordnung mit strengen Anforderungen an Inhalt und Begründung sowie eines hinreichend substantiierten sowie hinreichend begründeten Antrags auf eine solche Anordnung bedarf. Der Gesetzentwurf regelt den Richtervorbehalt für die TKÜ in § 32 Abs. 6 und 7 NPOG-E. Kein Richtervorbehalt ist für die Quellen-TKÜ vorgesehen. Ein Verweis in § 32 Abs. 6 auf § 33a Abs. 2 NPOG-E fehlt.

**Fehlende Eingrenzung der zulässigen Maßnahmen**

Wer die Rechtsfolgen betrachtet, wünscht sich bei so schwerwiegenden Eingriffen mindestens, dass die neuen Befugnisse die Polizei nicht nur pauschal ermächtigen. Sie darf in „von der betroffenen Person genutzte informationstechnische Systeme"[25] zwecks Überwachung der Telekommunikation (Quellen-TKÜ) oder der Erhebung von Daten (Online-Durchsuchung) eingreifen. Der Gesetzgeber hätte die informationstechnischen Systeme, bei denen ein Eingriff zulässig sein soll, benennen oder zumindest in anderen näheren Bestimmungen eingrenzen müssen. Denn in seiner jetzigen Form erfassen die Befugnisnormen Eingriffe in alle denkbaren informationstechnischen Systeme, d. h. vom PC übers Handy bis hin zum IT-gesteuerten Herzschrittmacher. Durch aktuelle informationstechnische Konzepte wie *Cloud Computing*, *Internet of Things*, *Smart City* oder *Industrie 4.0* ist der Kreis informationstechnischer Systeme, auf die durch die neuen Befugnisnormen zugegriffen werden kann, enorm weit.

Bedauernswert ist zudem, dass der Gesetzentwurf weder für die TKÜ noch für die Quellen-TKÜ eine zeitliche Höchstgrenze vorsieht. Die Maßnahme kann immer wieder um jeweils drei Monate verlängert werden. Damit wird dem Grunde nach eine unbegrenzte, also jahre- oder gar jahrzehntelange Überwachung von Telefonaten, E-Mails, SMS, Messengerdienstnachrichten und allen anderen informationstechnischen Systemen ermöglicht.

## Schutz des Kernbereichs privater Lebensgestaltung

Überwachungsmaßnahmen sind stets verfassungswidrig, wenn sie den Kernbereich privater Lebensgestaltung nicht hinreichend beachten und damit in die Menschenwürde der Betroffenen eingreifen. Können Überwachungsmaßnahmen typischerweise zur Erhebung kernbereichsrelevanter Daten führen, ist der Gesetzgeber verpflichtet, die Befugnisnormen mit Regelungen zu flankieren, die einen wirksamen Schutz gewährleisten.[26] Zu den kernbereichsnahen Überwachungsmaßnahmen gehören auch die Quellen-TKÜ und die Online-Durchsuchung.

Kernbereichsschützende Regelungen finden sich für alle kernbereichsnahen Überwachungsnormen zentral in § 31b des Gesetzentwurfs. In Bezug auf die Quellen-TKÜ und die Online-Durchsuchung weist § 31b jedoch erhebliche Defizite auf und wird den Anforderungen, die an einen verfassungsmäßig ausgestalteten Kernbereichsschutz zu stellen sind, nicht vollends gerecht.

**Keine technischen Sicherungen für die Online-Durchsuchung vorgesehen**

Nach dem Bundesverfassungsgericht hat der Gesetzgeber auf der Ebene der Datenerhebung Vorkehrungen zu treffen, die eine unbeabsichtigte Miterfassung von zum Kernbereich gehörenden Informationen nach Möglichkeit ausschließen.[27] Insbesondere muss der Gesetzgeber durch eine vorgelagerte Prüfung sicherstellen, dass die Erfassung von kernbereichsrelevanten Situationen und Gesprächen jedenfalls insoweit ausgeschlossen ist, als sich diese mit praktisch zu bewältigendem Aufwand im Vorfeld vermeiden lässt.[28] Bei der Online-Durchsuchung, bei der eine Nichterhebung von kernbereichsrelevanten Daten praktisch nicht ausschließbar ist, ist gesetzlich zu regeln, dass die Erhebung höchstpersönlicher Daten jedenfalls dann zu unterbleiben hat, wenn dies durch informationstechnische und ermittlungstechnische Mittel verhindert werden kann. Verfügbare informationstechnische Sicherungen, mit deren Hilfe höchstvertrauliche Informationen aufgespürt und isoliert werden können, sind dabei zu verwenden.[29] Ein solcher Einsatz von technischen Sicherungen zur Vermeidung der Erhebung kernbereichsrelevanter Daten ist in § 31b Abs. 1, der den Kernbereichsschutz für die Ebene der Datenerhebung im Wesentlichen regelt, nicht vorgesehen.

**Mangelhafte Regelung zum Abbruch der Datenerhebung und zur Protokollierung bei Datenlöschung**

Ein verfassungsmäßiger Kernbereichsschutz auf der Ebene der Datenerhebung setzt zusätzlich für alle Arten von Maßnahmen voraus, dass das Gesetz den Abbruch der Datenerhebung vorsieht, wenn erkennbar ist, dass die Überwachung den Kernbereich berührt.[30] Im niedersächsischen Gesetzentwurf ist mit § 31b Abs. 2 zwar eine solche Unterbrechung der Datenerhebung vorgesehen, die Regelung verengt die Pflicht zum Abbruch jedoch in nicht verfassungskonformer Weise, weil sie Ausnahmen vorsieht. Die Ausnahmen von der Pflicht zur Unterbrechung der Datenerhebung sollen gelten, wenn diese informationstechnisch nicht möglich ist oder durch die Unterbrechung dem/der Betroffenen die Datenerhebung bekannt wird. Diese Ausnahmen genügen nicht den Vorgaben des Bundesverfassungsgerichts, das beim erkennbaren Eindringen in den Kernbereich „in jedem Fall"[31] den Abbruch der Maßnahme vorsieht.

Für die Fälle, dass kernbereichsrelevante Daten trotz aller Vorkehrungen erhoben worden sind, hat das ermächtigende Gesetz sofortige Löschung der Daten vorzusehen. Zudem hat das Gesetz zu regeln, dass die Löschung in einer Art und Weise protokolliert wird, die eine spätere Kontrolle ermöglicht.[32] Der niedersächsische Gesetzentwurf sieht in § 32 b Abs. 2 S. 3 NPOG-E für solche Fälle vor, dass „die Tatsache, dass Daten aus dem Kernbereich privater Lebensgestaltung erhoben wurden, und die Löschung dieser Daten […] zu dokumentieren" sind. Diese Regelung dürfte jedoch unzureichend sein, denn allein die Dokumentation der Tatsache der Datenerhebung und der Löschung ermöglichen im Nachhinein keine Kontrolle. Für eine spätere Kontrolle dürfte vielmehr erforderlich sein, dass zumindest auch der Zeitpunkt der Löschung und die Person, die die Löschung vorgenommen hat, protokolliert werden.

**Unzureichende Sichtung**

Auf der Ebene der Auswertung und Verwertung der erhobenen Daten fordert das Bundesverfassungsgericht für den Fall, dass die Erfassung von kernbereichsrelevanten Daten nicht vermieden werden konnte, in der Regel die Sichtung der erfassten Daten durch eine unabhängige Stelle im Gesetz vorzusehen.[33] Da bei der Online-Durchsuchung immer auch kernbereichsrelevante Daten miterfasst werden, sieht es eine solche Sichtung hier als zwingend an.[34] Das Ziel dieser vorgeschalteten Sichtung ist sowohl das Herausfiltern von Daten als auch die Gewährleistung einer unabhängigen Kontrolle der dem Kernbereichsschutz dienenden Anforderungen insgesamt (Rechtmäßigkeitskontrolle).[35] Diesem Maßstab wird der Gesetzentwurf nicht in vollem Umfang gerecht, weil er in § 32b Abs. 4 lediglich regelt, dass eine gerichtliche Entscheidung darüber zu ergehen hat, „ob Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erhoben wurden". Zum einen lässt diese Regelung vermissen, dass das Gericht auch eine Gesamtschau bezüglich der Rechtmäßigkeit vorzunehmen hat. Zum anderen sollte die Regelung zwecks Normenklarheit ausdrücklich anordnen, dass gegebenenfalls gefundene höchstpersönliche Daten herauszufiltern sind, bevor die Aufzeichnungen an die Polizeibehörden übermittelt werden. Eine verfassungsrechtliche Ausgestaltung der Datenerhebung erfordert, dass die Sicherheitsbehörden zeitweise von einem Zugriff auf die Daten abgeschnitten werden. In dieser Zeit erfolgt eine externe Prüfung der Rechtmäßigkeit der Datenerhebung, und sofern diese bejaht wird, folgt eine Entscheidung darüber, welche Daten die Sicherheitsbehörden auswerten dürfen.[36]

## Ausblick

In den Bundesländern, welche die Maßnahmen bereits eingeführt haben, wurden zum Teil Verfassungsbeschwerden eingelegt oder angekündigt.

Die durch die Bevölkerung derzeit geäußerte und auf zahlreichen Demonstrationen zur Schau gestellte massive Kritik an der Einführung neuer grundrechtsintensiver Polizeibefugnisse wie Quellen-TKÜ und Online-Durchsuchung hat bisher dazu geführt, dass vorerst zumindest in Bremen und Sachsen auf diese Befugnisse verzichtet wird. Andere Bundesländer wie Niedersachsen halten weiterhin auch trotz Kritik von Fachleuten und aus der Bevölkerung an ihren Vorhaben fest. So hat der niedersächsische Ministerpräsident Weil noch vor Beendigung der Sachverständigenanhörung im Landtag erklärt, dass er eine Nachbesserung nicht für notwendig erachtet.[37] Welche Bundesländer dem Trend zur Einführung der neuen Befugnisse folgen


*Ned schee, Protest in München gegen das PAG*
*Foto: Günther Gerstenberg, CC BY*

und welche die Kritik daran berücksichtigen werden, bleibt abzuwarten. Es kann jedenfalls erwartet werden, dass auch allen künftigen Gesetzesvorhaben mit massiver Kritik und zahlreichen Protesten begegnet werden wird. Im Übrigen bleiben die Entscheidungen des Bundesverfassungsgerichts zu den Regelungen in der Strafprozessordnung und dem bayerischen Polizeiaufgabengesetz abzuwarten. Diese Gerichtsentscheidungen werden die Einführung von Quellen-TKÜ und Online-Durchsuchung zwar nicht verhindern können, jedoch dem Gesetzgeber zumindest erneut die rechtlichen Grenzen aufzeigen.

## Anmerkungen

1 *Heinrich A, Hügel S, Wiese K (2018) Stellungnahme zum Entwurf eines Reformgesetzes zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung und anderer Gesetze – Gesetzentwurf der Fraktionen der SPD und der CDU (LT-Drs. 18/850). Humanistische Union, http://www.humanistische-union.de/nc/aktuelles/aktuelles_detail/back/aktuelles/article/niedersachsen-erweiterung-polizeilicher-befugnisse/*

2 *BVerfG, U. v. 07.02.2008, BVerfGE 120, 274.*

3 *LVerfG Sachsen-Anhalt, U. v. 11.11.2014, LVG 9/13.*

4 *BVerfG, U. v. 20.04.2016, BVerfGE 141, 220 (sog. BKAG-Urteil).*

5 *Verfassungsbeschwerden wurden eingelegt von Tele Trust, von Digitalcourage und gemeinsam von der Gesellschaft für Freiheitsrechte, dem Deutschen Anwaltsverein und der Humanistischen Union. https://freiheitsrechte.org/home/wp-content/uploads/2018/08/GFF_Verfassungsbeschwerde_Staatstrojaner_anonym.pdf*

6 *https://www.lfd.niedersachsen.de/startseite/allgemein/presseinformationen/stellungnahme_polizeigesetz/entwurf-zum-neuen-polizeigesetz-2018-167435.html*

7 *Auf die Ununterscheidbarkeit zwischen Quellen-TKÜ und Online-Durchsuchung hinsichtlich des Ausnutzens von Sicherheitslücken weist Fredrik Roggan hin: Roggan F (2017) Die strafprozessuale Quellen-TKÜ und Online- Durchsuchung: Elektronische Überwachungsmaßnahmen mit Risiken für Beschuldigte und die Allgemeinheit. StV – Strafverteidiger, 12/2017, S. 821-829*

8 *Der Begriff „Remote Forensic Software" (RFS) ist aber irreführend. Er suggeriert, dass die damit gewonnenen Erkenntnisse den Beweiswert einer forensischen Analyse besitzen, was nicht der Fall ist. Dazu Fox D (2007) Stellungnahme zur „Online-Durchsuchung". Verfassungsbeschwerden 1 BvR 370/07 und 1 BvR 595/07, Karlsruhe: Secorvo Security Consulting GmbH, https://secorvo.de/publikationen/*

stellungnahme-secorvo-bverfg-online-durchsuchung.pdf. Man könnte von „Durchsuchungssoftware" sprechen; bei Software für die Quellen-TKÜ von „Remote Communication Interception Software" (RCIS). De Facto ist es aber nichts anderes als Schadsoftware, die das Rechnersystem infiltriert und seine Funktion manipuliert.

9 Der Begriff „Trojaner" entspricht dem „Trojanischen Pferd" aus der griechischen Mythologie. Die Schad- bzw. Überwachungssoftware ist technisch „eingepackt", um sie auf den Zielrechner zu bringen.

10 https://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf

11 Dazu Roggan F (2017), a. a. O., S. 824

12 BVerfG, U. v. 27. Februar 2008 – 1 BvR 370/07, 1 BvR 595/07 – Rn. (280-283).

13 BKAG-Urteil, a.a.O Rn. 218 f.

14 So auch Maximilian Warntjen (2008): Der Kernbereichsschutz nach dem Online-Durchsuchungsurteil. in: Fredrik Roggan (Hg.) (2008): Online-Durchsuchung. Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008. Berlin: Berliner Wissenschafts-Verlag.

15 Roggan F (2008) Präventive Online-Durchsuchungen. Überlegungen zu den Möglichkeiten einer Legalisierung im Polizei- und Geheimdienstrecht, in: Roggan F (Hg.) (2008) Online-Durchsuchungen. Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008. Berlin: Beliner Wissenschafts-Verlag, S. 100

16 Ein Exploit ist ein Stück Software, das eine Sicherheitslücke für einen Angriff ausnutzt. Von besonderem Interesse für Angreifer sind die sog. Zero-Day-Exploits, für die zum Zeitpunkt des Einsatzes noch keine Gegenmaßnahme entwickelt wurde.

17 Frank Kuhn kommt in einer Untersuchung zu diesem Ergebnis: Kuhn F (2018) Gefährdet der staatliche Einsatz von Spionagesoftware die Innere Sicherheit? Bachelor-Arbeit, Goethe-Universität Frankfurt am Main, https://cdn.netzpolitik.org/wp-upload/2018/09/2018-07-02_Frank-Kuhn_Bachelor_Gefaehrdet-Spionagesoftware-die-Innere-Sicherheit.pdf

18 Brieglebb V, heise.de (2017) WannaCry: Was wir bisher über die Ransomware-Attacke wissen. https://www.heise.de/newsticker/meldung/WannaCry-Was-wir-bisher-ueber-die-Ransomware-Attacke-wissen-3713502.html, 13. Mai 2017 und Stefan Hügel (2018): Öffentliche Sicherheit durch unsichere IT? Bundeswehr und Bundesnachrichtendienst gefährden die Sicherheit der öffentlichen Infrastruktur, in: Till Müller-Heidelberg, Marei Pelzer, Martin Heimig, Cara Röhner, Rolf Gössner, Matthias Fahrner, Helmut Pollähne, Maria Seitz: Grundrechte-Report 2018. Zur Lage der Bürger- und Menschenrechte in Deutschland. Frankfurt am Main: Fischer-Taschenbuchverlag

19 Das Beispiel zeigt auch, dass die Wirkung der Schadsoftware nicht an Landesgrenzen Halt macht. Damit stellt sich die Frage nach Cyberangriffen auf souveräne Staaten. Wird dadurch physischer Schaden verursacht, verletzten solche Angriffe nach Ansicht internationaler Experten die Souveränität. Vgl. dazu Schmitt MN (Hg.) (2013) Tallinn Manual on the International Law applicable to Cyber Warfare, Cambridge, UK u. a.: Cambridge University Press, Section 1, A 6.

20 Rehak R (2018) Stellungnahme des FIfF zur Anhörung des Hessischen Landtags am 8. Februar 2018 zum Gesetzentwurf für die Neuausrichtung des Verfassungsschutzes in Hessen: Hessischer Landtag, Ausschussvorlagen – Teil 3, S. 389-409, https://hessischer-landtag.de/sites/default/files/scald/files/INA-AV-19-63-T3-NEU.pdf

21 Fredrik Roggan weist darauf hin, dass der Staat „ein Interesse an der Lückenhaftigkeit des Schutzes von potentiell zu infiltrierenden Kommunikationsgeräten haben" muss, und: „Deutsche Strafverfolgungsbehörden müssen … ein Interesse an unsicherer IT-Infrastruktur haben. … Das freilich kollidiert – andererseits – mit dem staatlichen Auftrag das Schutzes derselben: Namentlich das Bundesamt für die Sicherheit in der Informationstechnologie hat die Sicherheit in der Informationstechnik zu fördern (§ 3 Abs. 1 S. 1 BSIG)". Roggan F (2017), a. a. O., S. 828-829

22 Herpig S (2018) Schwachstellenmanagement für mehr Sicherheit. Wie der Staat den Umgang mit Zero-Day-Schwachstellen regeln sollte. Berlin: Stiftung Neue Verantwortung, https://www.stiftung-nv.de/sites/default/files/vorschlag.schwachstellenmanagement.pdf

23 Zu einer ernüchternden Einschätzung der parlamentarischen Kontrolle der Geheimdienste kommt Daniel Leisegang: Er stellt fest, „… dass die politische und juristische Aufarbeitung des [NSA-] Abhörskandals hierzulande keine nennenswerten Konsequenzen zeitigte. Im Gegenteil hat die Macht des BND in den vergangenen Jahren erheblich zugenommen. […] Dafür verantwortlich ist vor allem das dramatische Versagen der parlamentarischen Kontrolle." Leisegang D (2018) Fünf Jahre NSA-Affäre: Die neue Macht des BND. Blätter für deutsche und internationale Politik 6'18, S. 21–24

24 Fox D (2007), a. a. O.

25 § 33a Abs. 2 und § 33d Abs. 1 S. 1 des niedersächsischen Gesetzentwurfs.

26 BVerfG, U. v. 20. April 2016 – 1 BvR 966/09 – Rn. (124).

27 BVerfG, U. v. 20. April 2016, a. a. O. – Rn. (126).

28 BVerfG, U. v. 20. April 2016, a. a. O. – Rn. (128).

29 BVerfG, U. v. 20. April 2016, a. a. O. – Rn. (219).

30 BVerfG, U. v. 20. April 2016, a. a. O. – Rn. (128).

31 BVerfG, U. v. 20. April 2016, a. a. O. – Rn. (128).

32 BVerfG, U. v. 20. April 2016, a. a. O. – Rn. (129).

33 BVerfG, U. v. 20. April 2016, a. a. O. – Rn. (129).

34 BVerfG, U. v. 20. April 2016, a. a. O. – Rn. (200 und 218).

35 BVerfG, U. v. 20. April 2016, a. a. O. – Rn. (200 und 204).

36 Entsprechend zum BKA: Roggan F (2016) Enzyklopädie des Polizeirechts. Das Urteil des Verfassungsgerichts zum BKA-Gesetz. Bürgerrechte & Polizei / CILIP 111 (Dezember 2016).

37 https://www.ndr.de/nachrichten/niedersachsen/Ministerpraesident-Niedersachsens-im-Sommerinterview,sommerinterview266.html


Freiheit ist den Aufstand wert, #NOPAG München
Foto: Günther Gerstenberg, CC BY

**Constanze Kurz**

# Seehofer soll die Ergebnisse des Tests am Südkreuz transparent machen

## – Ein Interview mit RA Ulrich Schellenberg zu biometrischer Überwachung –

*Automatisierte Gesichtserkennung ist ein massiver Eingriff in das Grundrecht auf informationelle Selbstbestimmung, sagt Ulrich Schellenberg, Präsident des Deutschen Anwaltvereins. Jetzt nach Ende des Biometrietests am Berliner Südkreuz sieht er Innenminister Horst Seehofer in der Pflicht, die konkreten Ergebnisse zu veröffentlichen.*

Das Pilotprojekt zur biometrischen Gesichtserkennung mit hochauflösenden Kameras am Berliner Bahnhof Südkreuz ist beendet. Der damalige Bundesinnenminister Thomas de Maizière hatte die Testphase des „Sicherheitsbahnhofs"[1] Ende 2017 um sechs Monate bis Ende Juli 2018 verlängert und angekündigt, dass er eine flächendeckende Einführung der biometrischen Videoüberwachung plane. Sein Nachfolger Horst Seehofer schweigt bisher zum Vorzeigeprojekt am Südkreuz, die genauen Ergebnisse des Tests stehen noch aus.

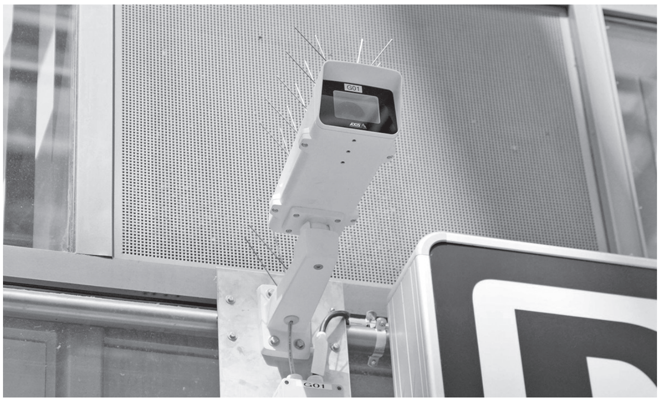
Bereits seit Beginn des Projektes, das vom Bundesinnenministerium, der Deutschen Bahn, der Bundespolizei und dem Bundeskriminalamt durchgeführt wurde, gab es harsche Kritik an dem biometrischen Pilotvorhaben. Der Deutsche Anwaltverein (DAV) kritisierte mehrfach die Missachtung verfassungsrechtlicher Grundsätze und machte auf weitere rechtliche und praktische Probleme bei der „intelligenten" Videoüberwachung aufmerksam[2]. Längst nicht alle technisch möglichen Anwendungsszenarien der biometrischen Videobeobachtung seien auch verfassungskonform. Die Hamburger Polizei[3] plant allerdings aktuell dennoch, Software zur Gesichtserkennung[4] für Bild- und Videomaterialien dauerhaft einzusetzen.

*Wir sprechen mit dem Rechtsanwalt und Notar Ulrich Schellenberg, Präsident des Deutschen Anwaltvereins (DAV[5]). Der DAV vertritt mit derzeit rund 65.000 Mitgliedern die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.*

### Wie steht es um die Rechtsgrundlage?

**Constanze Kurz**: *Der DAV hatte bereits zu Beginn des Testprojektes am Südkreuz im Jahr 2017 darauf hingewiesen, dass eine Rechtsgrundlage für das „massenhafte Scannen von Gesichtern" fehle. Wie bewerten Sie, dass das Innenministerium mit Verweis auf die Tatsache, dass man doch Freiwillige für den Test angeworben hätte, die Schaffung einer Rechtsgrundlage nicht für notwendig hielt?*

**Ulrich Schellenberg**: Der DAV kritisiert in erster Linie nicht die Testphase, sondern den zu erwartenden Echtbetrieb. Da kann dann von Freiwilligkeit nicht mehr gesprochen werden. Der Echtbetrieb einer automatisierten Gesichtserkennung ist ein massiver Eingriff in das Grundrecht auf informationelle Selbstbestimmung. Und bislang gibt es für diese Form des massenhaften Datenabgleichs keine Rechtsgrundlage.



*Kamera des Pilotprojekts vor der Rolltreppe am Bahnhof Südkreuz – Foto: Benjamin Kees*

**Constanze Kurz**: *Sind aus Ihrer Sicht Videokameras mit eingebauter Gesichtserkennungssoftware für den angestrebten Zweck der Terrorfahndung oder bei der Suche nach „Gefährdern" überhaupt sinnvoll?*

**Ulrich Schellenberg**: Auch Gefährder dürfen sich frei an öffentlichen Plätzen bewegen. Der Fall Anis Amri zeigt ja auch, dass Videotechnik Anschläge nicht verhindern kann. Amri hatte sich bewusst von einer Kamera an einem Berliner Bahnhof filmen lassen und einen IS-Gruß gezeigt. Selbst wenn die Gesichtserkennung also anschlägt, könnte ein terroristischer Angriff nicht verhindert werden.

**Constanze Kurz**: *Der DAV hatte bereits zu Beginn des Tests die Frage aufgeworfen, wann die biometrischen Systeme eigentlich anschlagen sollten. Ist diese Frage nach dem langen Testzeitraum nun beantwortet worden? Sind Sie einverstanden mit der Informationspolitik[6] des Innenministeriums zum Südkreuz-Test?*

**Ulrich Schellenberg**: Die Transparenz dieses Projekts lässt sehr zu wünschen übrig. Etliche Fragen bleiben seit über einem Jahr unbeantwortet: Wie fehleranfällig ist das System? Können Missbrauch und Manipulation der Technik verhindert werden? Welche Daten werden genau gesammelt? Und für wie lange, durch wen und wo werden diese Daten gespeichert?

Gerade, wenn Löschfristen nicht ausreichend geregelt sind, liefe ein flächendeckender Einsatz intelligenter Videoüberwachung auf eine „optische Vorratsdatenspeicherung" hinaus. Die Vorratsdatenspeicherung[7] hat der Europäische Gerichtshof jedoch abgelehnt. Die einseitige Wissenshortung seitens der Initiatoren stärkt jedenfalls nicht gerade das Vertrauen in die Rechtsstaatlichkeit dieses Vorhabens.

### „Technische und prozessuale Details bleiben im Dunkeln“

**Constanze Kurz**: *War der Test aus Ihrer Sicht als ein „ergebnisoffenes“ Experiment angelegt? Wie bewerten Sie die bisher veröffentlichten Ergebnisse des Tests?*

**Ulrich Schellenberg**: Das Südkreuzprojekt ist von Anfang an von nur sehr vagen Theorien und Erwartungen in Sachen Effizienz begleitet worden. Zwischenberichte werden nicht veröffentlicht, technische und prozessuale Details bleiben im Dunkeln.

Ganz zu schweigen davon, dass es bislang keinen wissenschaftlichen Beweis dafür gibt, dass Gesichtserkennungssysteme tatsächlich in der Lage sind, Verbrechensraten zu senken und die objektive Sicherheit zu erhöhen. Es liegt daher nahe, dass das Projekt unabhängig von konkreten Zahlen als erfolgreich verkauft werden soll.

**Constanze Kurz**: *Die Bundesregierung hatte im Sommer 2017 auf eine parlamentarische Anfrage[8] zur Erfolgsbewertung des Südkreuz-Tests folgende Antwort gegeben: „Ein erfolgreiches Erprobungsergebnis ist nicht abhängig von konkreten Erkenntnisraten. Aus Sicht des Bundesministeriums des Innern liegt ein erfolgreiches Erprobungsergebnis vor, wenn ein signifikanter Mehrwert für die polizeilichen Aufgaben der Bundespolizei festgestellt werden kann.“*

*Teilen Sie diese Einschätzung zu einem Testerfolg? Sollten aus Sicht des DAV die konkreten statistischen Testergebnisse und Erkenntnisraten mit den Ausschlag geben, ob biometrische Personenüberwachung künftig eingesetzt werden soll?*

**Ulrich Schellenberg**: Unklar ist bei dieser Aussage bereits, wann genau ein „signifikanter Mehrwert“ vorliegt. Testergebnisse und Erkenntnisraten sind als Teil der Gesamtauswertung selbstverständlich mit einzubeziehen. Momentan bestehen ja noch gravierende Zweifel, ob es „gute“ Ergebnisse unter Alltagsbedingungen überhaupt gibt.

Und auch die besten Ergebnisse müssen im Lichte der massiven Grundrechtseingriffe betrachtet werden. Im Übrigen ist es nicht die Aufgabe unbescholtener Bürger, auf ihre Freiheitsrechte zu verzichten, um der Polizei ihre Arbeit zu erleichtern.

### Flächendeckende Gesichtserkennung?

**Constanze Kurz**: *Wie bewertet der DAV die noch von Minister Thomas de Maizière geäußerte Forderung nach flächendeckender Gesichtserkennung? Was ist nach Abschluss der ersten Südkreuz-Testphase vom neuen Innenminister Horst Seehofer zu fordern?*

**Ulrich Schellenberg**: Bevor überhaupt Testergebnisse dieses Pilotprojektes vorliegen, erscheint die Forderung von de Maizière voreilig. Davon abgesehen, halte ich dieses Szenario weder für praktisch umsetzbar noch für objektiv erforderlich – und im Hinblick auf die Grundrechte erst recht nicht für gewollt.

Was die aktuelle Testphase angeht, bleibt zu hoffen, dass Seehofer den tatsächlichen Mehrwert darstellt, die konkreten Ergebnisse transparent macht und diese nicht vorschnell für gut befindet.

**Constanze Kurz**: *Vielen Dank für das Interview!*

---

*Quelle: https://netzpolitik.org/2018/interview-zu-biometrischer-ueberwachung-seehofer-soll-die-ergebnisse-des-tests-am-suedkreuz-transparent-machen/*

## Anmerkungen

1 *https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2017/12/sicherheitsbahnhof-verlaengerung.html*
2 *https://anwaltverein.de/de/newsroom/pm-9-17-deutscher-anwaltverein-gesichtserkennung-in-bahnhoefen-greift-massiv-in-grundrechte-ein*
3 *https://netzpolitik.org/2018/hamburg-polizei-will-software-zur-gesichtserkennung-dauerhaft-einsetzen/*
4 *https://de.wikipedia.org/wiki/Gesichtserkennung*
5 *https://anwaltverein.de/de/*
6 *https://twitter.com/BMI_Bund/status/943837416904908800*
7 *http://www.vg-koeln.nrw.de/behoerde/presse/Pressemitteilungen/01_180420/index.php*
8 *http://dipbt.bundestag.de/dip21/btd/18/133/1813350.pdf*
9 *http://gewissensbits.gi.de/constanze-kurz/*
10 *http://www.faz.net/aktuell/feuilleton/aus-dem-maschinenraum/*
11 *https://www.privacynotprism.org.uk/*
12 *https://www.youtube.com/watch?v=hj3gAsqrB18*
13 *https://de.wikipedia.org/wiki/Werner_Holtfort#Holtfort-Stiftung*
14 *https://media.ccc.de/search?q=Constanze+Kurz*
15 *http://www.ev-akademie-tutzing.de/toleranz-preis-fuer-christian-wulff-und-constanze-kurz/*



**Constanze Kurz**

**Constanze Kurz** ist promovierte Informatikerin, Autorin und Herausgeberin mehrerer Bücher[9], ihre Kolumne „Aus dem Maschinenraum“[10] erscheint im Feuilleton der FAZ. Seit Februar 2015 verstärkt sie das *netzpolitik.org*-Team. Sie ist Aktivistin[11] und ehrenamtlich Sprecherin[12] des Chaos Computer Clubs. Sie forschte an der Humboldt-Universität zu Berlin am Lehrstuhl *Informatik in Bildung und Gesellschaft* und war Sachverständige der Enquête-Kommission *Internet und digitale Gesellschaft* des Bundestags. Sie erhielt den Werner-Holtfort-Preis[13] für bürger- und menschenrechtliches Engagement[14], den Toleranz-Preis[15] für Zivilcourage und die Theodor-Heuss-Medaille für vorbildliches demokratisches Verhalten.

Wiebke Denkena

# Wischen, Tippen, Zoomen: Forscher tracken anhand von Touch-Gesten

*Unsere Bewegungen auf dem Touchscreen sind so individuell, dass sie uns trackbar machen, zeigt ein kürzlich veröffentlichter Forschungsartikel. Obwohl gerade diese Art des Trackings große Risiken birgt, wird bisher wenig darüber gesprochen.*

So unverwechselbar und einzigartig wie unsere Handschrift sind auch die Bewegungen, die wir auf unseren Touchscreens machen – das behauptet zumindest ein Forschungsteam der australischen Commonwealth Scientific and Industrial Research Organisation (CSIRO)[1]. Ein im April veröffentlichter Artikel[2] zeigt auf, dass diese Bewegungsdaten so individuell sind, dass sie eine genaue Wiedererkennung von Usern und damit eine Form des Trackings ermöglichen: „[M]it unserer Methodologie können wir User mit einer Erfolgsrate von über 90 % re-identifizieren".

Um herauszufinden, wie hoch der Informationsgehalt der individuellen Touch-Daten wirklich ist, wurde die Anwendung TouchTrack entwickelt, die jetzt auch in Googles PlayStore verfügbar[3] ist. In die App wurden mehrere kleine Open-Source-Spiele eingebunden, die über typische Touchbewegungen funktionieren. Die so abgegriffenen Daten von insgesamt 89 Versuchspersonen wurden dann mathematisch auf ihre Eindeutigkeit (Uniqueness) hin untersucht.

Das Ergebnis: Schon wenige Samples einer einzelnen Bewegung (zum Beispiel das Wischen nach links über den Bildschirm) enthalten signifikante Informationen über den User. Je mehr Daten verschiedener Bewegungen vorliegen, desto besser können User wiedererkannt werden. Wischbewegungen und die Handschrift auf dem Bildschirm sind besonders eindeutig. Tippbewegungen oder das Schreiben auf einer Touch-Tastatur eher weniger.

## Sind unsere Touch-Daten schutzbedürftig?

Daten über unsere sogenannten Touch-Events – also unsere individuelle Bedienung von Touchscreens über Bewegungen wie Wischen, Tippen, Zoomen oder die „Handschrift" auf dem Display – sind über Programmierschnittstellen (APIs) einfach zugänglich. Diese Programmierschnittstellen sind vorprogrammierte Funktionen, die eine Verständigung zwischen Hard- und Software ermöglichen, also beispielsweise zwischen Anwendung und Touchscreen.

Dass die Informationen darüber, wo und wie wir unseren Touchscreen berühren, so einfach zugänglich sind, ist nicht verwunderlich. Ansonsten könnten wir nicht mit unseren Apps auf Smartphones oder Tablets interagieren. Jedoch erlauben einige APIs auch das Abgreifen sehr spezifischer Details, bei denen es fragwürdig ist, ob eine App nicht auch ohne diese Informationen gut funktionieren könnte.

Die Forschungsergebnisse sind gerade deshalb so interessant, weil Touch-Daten so einfach abgreifbar sind und im öffentlichen Diskurs um Tracking und Privacy bisher wenig beachtet werden. Die Forscher weisen in ihrem Artikel auf eine Reihe von Besonderheiten und Risiken dieser Daten und des auf ihnen basierenden Trackings hin (eigene Übersetzung):

> *Im Vergleich zu „üblichen" Tracking-Mechanismen, z. B. basierend auf Cookies, Browser-Fingerprints, Browser-User-Agents, Log-Ins und IP-Adressen, gibt es mehrere Faktoren, die das Tracking basierend auf Touch-Informationen potenziell riskanter machen. Während die anderen Mechanismen virtuelle Identitäten wie Online-Profile tracken, birgt „touch-based tracking" das Potenzial, die eigentliche (physische) Person am Gerät zu tracken und zu identifizieren. Es kann mehrere User, die das gleiche Gerät verwenden, tracken und unterscheiden. Weiterhin erlaubt es das kontinuierliche Tracking von Usern und führt zum „cross-device tracking", durch das ein User potenziell über mehrere mobile Geräte verfolgt werden kann.*

Hassan Jameel Asghar stellte die Arbeit kürzlich im Rahmen eines Vortrags auf dem diesjährigen Privacy Enhancing Technologies Symposium[4] vor.

---

*Quelle: https://netzpolitik.org/2018/wischen-tippen-zoomen-forscher-tracken-anhand-von-touch-gesten/*

## Anmerkungen

1 https://www.csiro.au/
2 https://petsymposium.org/2018/files/papers/issue2/popets-2018-0016.pdf
3 https://play.google.com/store/apps/details?id=com.csiro.data61.touchtrack&hl=de
4 https://petsymposium.org/ (ab 2:45:00)
5 https://netzpolitik.org/author/wiebke-denkena/



**Wiebke Denkena**

**Wiebke Denkena**[5] studiert Liberal Arts and Sciences und beschäftigt sich mit Themen wie Online-Überwachung, Künstlicher Intelligenz oder Online-Dating – gerne aus kulturwissenschaftlicher Perspektive. Davor hat sie einen Bachelor in Geomatik gemacht. Sie unterstützt das Team von *netzpolitik.org* von August bis Oktober 2018 als Praktikantin.

**Alexander Fanta, Constanze Kurz**

# Eckpunkte für neue KI-Strategie: Bundesregierung will „Sprunginnovation“

*Ein heute vorgestelltes Eckpunktepapier der Bundesregierung beschwört die Segnungen der Künstlichen Intelligenz, vor allem für die deutsche Wirtschaft. Deswegen soll die Förderung der KI Deutschland an eine internationale Spitzenposition katapultieren. Öffentliche Daten will die Regierung dafür der wirtschaftlichen Nutzung zuführen.*

Deutschland möchte die Nummer eins werden. Das liest sich als Schlagzeile gut, zumal wenn es um das Hype-Thema Künstliche Intelligenz geht. Bedrohlich nahe am Rande des klaffenden Sommerlochs veröffentlichte die Bundesregierung am 18. Juli 2018 ein zwölfseitiges Papier mit Eckpunkten für eine nationale KI-Strategie[1]. Eine solche gibt es bereits in einigen führenden Industriestaaten[2]. Ähnlich wie in diesen deutet die Bundesregierung in ihren Eckpunkten einen Mix aus staatlichen Förderungen für die Wirtschaft und Lockerung des Rechtsrahmens an, um der Industrie bei der Entwicklung datenintensiver Technologien auf die Sprünge zu helfen. Dafür möchte die Regierung auch verstärkt öffentliche Daten für Firmen verfügbar machen.

Wie viel Geld die Bundesregierung für KI-Förderung konkret lockermachen will, ist vorerst nicht klar. Noch ist der Haushalt für 2019 nicht gemacht und auch mögliche Fördergelder aus dem Budget der Ministerien sind bisher ein Luftschloss. Im Papier ist die Rede davon, stärker sogenannte „Sprunginnovation“ zu fördern. Die Wortneuschöpfung soll den Begriff „disruptive Innovation“ ersetzen, der nach Geschmack der Bundesregierung zu negativ besetzt ist. Für innovative Projekte soll es etwa Wettbewerbe mit Millionenpreisen nach Vorbild des amerikanischen X-Prize[3] geben.

Dem Eckpunktepapier fehlt peinlicherweise eine Definition, die umreißen würde, was die Bundesregierung unter „Künstlicher Intelligenz“ versteht – und was nicht. Entsprechend sollten wir uns in Zukunft nicht wundern, wenn noch mehr Forschungsfelder mit dem Begriff KI geschmückt werden, um an einem möglichen Geldregen der Bundesregierung zu partizipieren. Denn das verspricht die Bundesregierung in erster Linie: Förderung von Projekten, Kompetenzzentren, Anwendungsforschung.

## Wissenschaft als Zulieferer der Wirtschaft

Generell wird die KI von der Bundesregierung als ein Bereich gesehen, in dem die Wissenschaft der Wirtschaft zuarbeiten müsse. Das entspricht dem von der Bundesbildungsministerin Anja Karliczek (CDU)[4] jüngst nochmal betonten Wissenschaftsverständnis: Karliczek verwechselt Bildung mit Ausbildung und hält Universitäten und Hochschulen für bloße Zulieferer der Wirtschaft, aus denen vor allem Innovationen generiert werden müssten.

Nachdem diese Strategie mit zunehmender Wucht den Wissenschaftsstandort Deutschland in eine Drittmittel-Mühle verwandelt und dabei insbesondere hochqualifizierte Wissenschaftler entnervt außer Landes getrieben hat, schreibt die Bundesregierung nun, dass sie eine Priorität in der „Gewinnung und Haltung von KI-Expertinnen und Experten [sic!] in Deutschland“ sieht. Wie sie das anstellen will, lässt sie allerdings nur schemenhaft durchblicken. Denn wer anderswo hochbezahlt an seinen Forschungsfragen arbeiten kann, während er hierzulande blumige Antragsprosa im Zwei-Jahrestakt zu produzieren hat, der wird sich gut überlegen, nach Deutschland zu kommen.

*Im KI-Labyrinth gefangen: Die Bundesregierung laboriert an einer Strategie*

## Fromme Wünsche

Auch andere Vorschläge postulieren Wünsche für den künftigen KI-Einsatz, ohne klarzumachen oder auch nur anzudeuten, auf welchem Wege sie erreicht werden könnten. Dazu gehört beispielsweise die Schaffung von „begründetem Vertrauen [in KI-Technologien] auf der Basis transparenter Verfahren und einer Nachvollziehbarkeit für die Bürgerinnen und Bürger“. Ein frommer Wunsch, der jedoch schon heute nichts weiter als genau das ist. Bei den KI-Anwendungen, mit denen Millionen Menschen bereits täglich konfrontiert sind, kann selten von Nachvollziehbarkeit der Entscheidungen die Rede sein. Bei kommerziellem Einsatz stellt sich zudem die Frage, warum bei den Unternehmen, die mit KI angereicherte Geschäftsmodelle haben, ein Interesse an „Transparenz“, Nachvollziehbarkeit oder auch nur partiellen Einblicken der Nutzer bestehen sollte.

Im Eckepunktepapier ist häufig die Rede von der Veränderung der Arbeitswelt, die durch den Einsatz der KI beschleunigt würde. Das ist weithin unumstritten, jedoch verliert das gesamte Papier kein Wort dazu, wie die Gewinne aus dieser Transformation in unserer Gesellschaft verteilt werden könnten und ob und wie die Bundesregierung steuernd einzugreifen plant.

## Offene-Daten-Hoffnungen

Die stärkere Nutzung öffentlicher Daten nimmt in den Eckpunkten eine gewichtige Rolle ein. Das ist richtig so, denn beim Thema Open Data[5] hinkt Deutschland schon länger hinterher[6]. Im Papier der Bundesregierung heißt es nun: „Daten der öffentlichen Hand und der Wissenschaft werden verstärkt für die KI-Forschung geöffnet und deren wirtschaftliche und gemeinwohldienliche Nutzung im Sinne einer Open Data Strategie [sic!] ermöglicht." Wie das bewerkstelligt werden soll, wird aber nicht näher ausgeführt.

Die Umsetzung von Open-Data-Gelöbnissen scheiterte bisher an fehlenden Mitteln für die Standardisierung auf allen Ebenen der öffentlichen Verwaltung. Auch zeigt die Bundesregierung mit ihrem Vorstoß zur Nutzung persönlicher Daten etwa im Gesundheitswesen wenig Sensibilität für die Gefahren: Denn selbst angeblich anonymisierte Daten lassen sich nur allzu leicht de-anonymisieren, wie zahlreiche Beispiele der letzten Jahre[7] zeigen.

Der Open-Data-Ansatz wirft eine weitere Frage auf. Zwar klingt die Forderung nach dem „Heben der Datenschätze der Forschungseinrichtungen" durchaus sinnvoll. Doch die von deutschen EU-Politikern vorangetriebene[8] geplante EU-Urheberrechtsreform[9] behindert das mit einem Artikel, der sogenanntes Data Mining stark einschränkt[10] und damit die Nutzung von offenen Daten erschweren könnte. Wo ist die Open-Data-Strategie der Bundesregierung, die diesen Namen auch verdient?

## Ungeklärte Fragen der IT-Sicherheit

Die Bundesregierung betont mehrfach, dass bei KI-Anwendungen auch Fragen der IT-Sicherheit betroffen wären, ohne die Zusammenhänge jedoch näher zu erklären. Hier bleibt wohl abzuwarten, welche Schwerpunkte künftig gesetzt werden können. Eines scheint aber bereits klar: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist aus dem Rennen, da lediglich eine „Abstimmung der Maßnahmen" mit der neugegründeten, aber bisher noch nicht voll arbeitsfähigen Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) geplant ist. Wir dürfen also gespannt sein, was die Möchtegern-Hackertruppe mit ihrem Ex-BND-Agent an der Spitze für Dienstleistungen bei KI-Technologien anzubieten hat.

Wie es sich für ein standesgemäßes Eckpunktepapier gehört, versichert die Bundesregierung, mit so gut wie allen gesellschaftlichen Gruppen „unter Beteiligung der Zivilgesellschaft" in den Dialog treten zu wollen. Dabei möchte sie auch ethische Fragen der KI[11] ansprechen. Welche Form dieser Dialog haben soll, ist in dem Papier allerdings noch nicht ausgewiesen. Es bleibt also nur Hoffnung, dass der „Dialog" nicht so ausfällt wie unter Verteidigungsministerin Ursula von der Leyen, die vollmundig eine Drohnendebatte in Deutschland ankündigte, dann aber ohne viel Gerede bewaffnete Drohnen für die Bundeswehr forderte.

Wer sich fragt, ob in dem Eckpunktepapier der ausgesprochen wichtige Bereich der militärischen[12] KI-Forschung auch nur angesprochen wird, der wird enttäuscht: Mit keinem Wort widmet sich das Papier der Problematik. Die noch immer breit diskutierte Frage der Kooperation ziviler Forschung in KI-Fragen mit den Militärs, die vor allem durch protestierende Google-Mitarbeiter jüngst entstanden ist, ignoriert die Bundesregierung komplett.

## Die dicken Walzen der Gremienmühle

Nach Jahren der Trägheit bearbeiten die Bundesregierung und der Bundestag das Thema Digitalisierung seit kurzem an mehreren Fronten gleichzeitig. Die Regierung Merkel traf sich zuletzt erstmals im Digitalkabinett[13] und erklärte, einen noch nicht näher bestimmten Digitalrat[14] gründen zu wollen. Zudem tagt wohl noch im August erstmals die neue Datenethik-Kommission der Bundesregierung. Deren sechzehn Mitglieder sollen bis Sommer 2019 Vorschläge für den Umgang mit KI, algorithmischen Prozessen und Datenpolitik liefern. Der Bundestag setzt inzwischen auch noch eine Enquête-Kommission[15] ein, die bis Sommer 2020 ebenfalls Anregungen zum Umgang mit KI und Algorithmen liefern soll.

Dem Digitalgedöns ist damit nicht genug. Ohne die Ergebnisse der eigenen Ethik-Kommission oder der Enquête-Kommission im Bundestag abzuwarten, plant die Bundesregierung die Präsentation einer Digitalstrategie bis Jahresende 2018[16]. Dass die Datenethik-Kommission bis dahin zu substantiellen Ergebnissen kommen könnte, kann wohl ausgeschlossen werden. Dennoch schreibt die Bundesregierung in ihrem Eckpunktepapier mehrfach davon, die Ergebnisse der Kommission einfließen lassen zu wollen.

Das Thema Künstliche Intelligenz spielt für die Digitalstrategie eine Schlüsselrolle. Die geplante KI-Strategie, deren Eckpunkte nun vorliegen, soll noch vor der Digitalstrategie präsentiert werden. Dafür müssen die federführenden Ministerien (BMWi[17], BMWF[18], BMAS[19]) einiges an Wegstrecke zurückzulegen. Die nun präsentierten Eckpunkte werden an alle möglichen Verbände und Stakeholder zur Konsultation verschickt, bis Ende September sollen diese konkrete Vorschläge einreichen. Zugleich halten verschiedene Bundesministerien Workshops zu für die KI-Strategie relevanten Themen ab, etwa Mobilität, Industrie 4.0 oder Gesundheit. Das Bundeswirtschaftsministerium strickt daraus einen Entwurf, den die Bundesregierung im November beschließen soll.

**Alexander Fanta und Constanze Kurz**

**Alexander Fanta** ist seit Januar 2018 Journalist bei *Netzpolitik.org* und schreibt dort über die digitale Gesellschaft und ihre Feinde. 2017 beschäftigte er sich als Stipendiat am *Reuters-Institut* für Journalismusforschung in Oxford und bei der *NZZ* in Zürich mit Projekten zum Roboterjournalismus. Davor arbeitete Alexander für die österreichische Nachrichtenagentur APA.
Er ist unter *alexander.fanta ett Netzpolitik.org* und unter *@FantaAlexx* erreichbar.

**Constanze Kurz** siehe Seite 44

Im neuen Jahr kann es dann mal langsam mit der deutschen KI-Förderung losgehen. Die amerikanischen und asiatischen Digitalgiganten bauen derweil ihre Dominanz aus und schaffen schon heute Fakten.

---

*Quelle: https://netzpolitik.org/2018/eckpunkte-fuer-neue-ki-strategie-bundesregierung-will-sprunginnovation/*

## Anmerkungen

1 *https://www.bmbf.de/files/180718%20Eckpunkte_KI-Strategie%20final%20Layout.pdf*
2 *https://netzpolitik.org/2018/nichts-als-wirtschaftsfoerderung-nationale-ki-strategien-in-ueberblick/*
3 *https://de.wikipedia.org/wiki/X-Prize_Foundation*
4 *https://www.tagesspiegel.de/wissen/zukunft-der-wissenschaft-bundesbildungsministerin-anja-karliczek-irritiert-die-universitaeten/22806872.html*
5 *http://www.bpb.de/gesellschaft/digitales/opendata/64055/was-sind-offene-daten?p=all*
6 *https://netzpolitik.org/2017/open-data-und-antikorruption-deutschland-hinkt-hinterher/*
7 *https://privacyinternational.org/types-abuse/claims-anonymised-data*
8 *https://netzpolitik.org/2018/eu-leistungsschutzrecht-axel-voss-geht-der-kommissionsvorschlag-nicht-weit-genug/*
9 *https://netzpolitik.org/2018/chance-fuer-aenderung-eu-parlament-verhindert-durchwinken-von-uploadfiltern-und-leistungsschutzrecht/*
10 *https://juliareda.eu/eu-copyright-reform/text-and-data-mining/*
11 *https://netzpolitik.org/2018/ethische-fragen-bei-kuenstlicher-intelligenz-mit-welchen-herausforderungen-muessen-wir-umgehen/*
12 *https://netzpolitik.org/2018/diskussion-ueber-killer-roboter-optimum-waere-ein-verbot-das-ist-aber-nicht-erreichbar/*
13 *https://netzpolitik.org/2018/zwischen-digitalrat-und-digitalkabinett-das-ringen-um-die-richtige-netzpolitik/*
14 *Dies ist inzwischen erfolgt: https://www.bundesregierung.de/Content/DE/Artikel/2018/08/2018-08-21-digitalrat.html (d. Red.)*
15 *https://netzpolitik.org/2018/bundestag-enquete-kommission-untersucht-kuenstliche-intelligenz/*
16 *https://www.bundesregierung.de/Content/DE/Artikel/2018/06/2018-06-28-merkel-morals-machines.html*
17 *https://www.bmwi.de/Navigation/DE/Home/home.html*
18 *https://www.bmbf.de/*
19 *http://www.bmas.de/DE/Startseite/start.html*

**Julia Krüger**

# Algorithmen und Künstliche Intelligenz: Wir reden an unserer Zukunft vorbei

*Maschinen treffen zunehmend selbstständig und intransparent Entscheidungen, die tief in unser Leben eingreifen. Aber statt längst überfällige Weichenstellungen demokratisch vorzunehmen, führen wir lieber irreführende Debatten über die EU-Datenschutzreform, Seehofers Asylpolemik und das vermeintliche Wundermittel Uploadfilter. Ein Aufruf zur Korrektur.*

Die vergangenen Wochen brannten vor Beschwerden über das angebliche „europäische Bürokratiemonster" EU-Datenschutz-Grundverordnung (DSGVO)[1], Seehofers Machtspiele um die Asylpolitik sowie die EU-Urheberrechtsreform, die Online-Plattformen zum Einsatz so genannter Upload-Filter verpflichten[2] könnte. Das alles sind natürlich wichtige Themen. Und sie hängen enger zusammen, als der erste Blick vermuten lässt. Dennoch gingen – und gehen – in den Debatten wesentliche Aspekte verloren, vernachlässigt man bei der Betrachtung die Entwicklung von „Algorithmen" und „Künstlicher Intelligenz"[3].

Längst haben diese „KI-Technologien" praktische Relevanz erlangt – unabhängig davon, ob man maschinelle Lernverfahren, Big Data und Quantencomputer als Lösung aller großen Probleme der Menschheit[4] betrachtet oder eine sich verselbständigende Intelligenz und das Ende der Menschheit fürchtet[5]. Es kommt bereits auf die richtige Gestaltung[6] an und die wartet leider nicht auf das Ende der geplanten Enquête-Kommission des deutschen Bundestages[7], sondern steht bereits jetzt zur Debatte.

*When I Grow Up (Symbolbild) Foto: Hldrmn, CC-BY-SA 2.0*

## Algorithmen und Künstliche Intelligenz: Wo stehen wir?

Durchbrüche in einer Reihe an Analysesystemen haben im Zusammenhang mit weltweiter Vernetzung, der massiven Verfügbarkeit von Daten und der exponentiell gewachsenen Rechnerleistung dazu geführt, dass langsam möglich wird, wovon Menschen seit Jahrzehnten träumen: Lernfähige Maschinen. Also smarte Software, die in Verbindung mit steuerungsfähiger Hardware immer mehr Arbeit (Entscheidungen) übernehmen[8] kann, die bislang Menschen vorbehalten war, etwa bei der Analyse komplexer Sachverhalte wie der Identitätsfeststellung eines Menschen[9], der Bewertung von nationalen Sicherheitsniveaus[10] oder der Steuerung autonomer Waffensysteme[11]. Hoffnungsvoll stimmt natürlich das Versprechen, dass Künstliche Intelligenz dazu beitragen kann, Krankheiten frühzeitig zu identifizieren und zu therapieren[12]. Einen Schreck bekommen die meisten beim Thema „Todesalgorithmus"[13] – wenn algorithmische Entscheidungssysteme darüber bestimmen sollen, welcher krebskranke Patient welche Therapie erhalten soll. All diese Themen werden an anderer Stelle gerade ausführlich debattiert[14], aber was hat das Ganze mit der DSGVO, Seehofer und Upload-Filtern zu tun?

## Warum die EU-Datenschutz-Grundverordnung von äußerster Bedeutung ist

Bekanntermaßen stellen diese Technologien gesellschaftliche Transparenz und Kontrolle vor große Herausforderungen, in Abhängigkeit von ihrer Komplexität und Dynamik[15]. Experten debattierten die Möglichkeiten der so genannten sich-selbst-erklärenden Algorithmen etwa jüngst auf der Cebit[16]. Bei diesen technischen Debatten geht jedoch regelmäßig der Blick für den politisch-ökonomischen Gesamtzusammenhang verloren. Denn es sind eben nicht die Algorithmen, die in neuronalen Netzen ganz unbestimmt nach Zusammenhängen suchen. Sondern Menschen beziehungsweise Unternehmen, die über die Daten verfügen, in denen Suchalgorithmen nach Zusammenhängen suchen – und die vorgeben, welche Daten für welchen Zweck in welcher Breite oder Tiefe durch welche Algorithmen durchforstet werden sollen[17]. Und die natürlich auch über die Daten verfügen, mithilfe derer algorithmische Systeme geprüft und erklärt werden können. Politisch betrachtet führt das Ganze zu zwei wesentlichen Fragen:

1. Wer soll mit welchen Daten KI-Technologien entwickeln, anwenden und überprüfen dürfen?

2. Wie lässt sich gewährleisten, dass KI-Technologien auf den „richtigen" Daten lernen – beispielsweise korrekten, aktuellen, repräsentativen und dem jeweiligen Zweck entsprechende Daten? (Um im Bild von Angela Merkel zu bleiben: Welches Futter braucht die KI-Entwicklung, damit aus den erwünschten Rindern keine Frösche erwachsen?[18])

Bei beiden Fragen bietet die DSGVO zwar keine erschöpfende Antwort, aber erste Ansätze: Denn einerseits verpflichtet sie Betreiber algorithmischer Entscheidungssysteme in Art. 22[19] dazu, den so genannten Datensubjekten im Falle einer automatisierten Entscheidungsfindung (inklusive Profiling) Information bezüglich der involvierten Logik eines Entscheidungssystemen, seiner Tragweite und angestrebter Auswirkungen zu geben. Dazu zählt auch das Recht auf menschliche Intervention. Ohne die Kenntnis der Betroffenheit von algorithmischer Entscheidungsfindung und ihrer Logik kann keiner überlegen, ob die Entscheidung korrekt ist oder überprüft oder in Frage gestellt werden muss. Andererseits beinhaltet sie in Art. 13-16[20] die Rechte, personenbezogene Daten einzusehen, sie zu korrigieren und der Nutzung zu widersprechen – und bietet so eine erste Form der Qualitätssicherung: dass Künstliche Intelligenz auf den „richtigen Daten" lernt. Darüber hinaus verpflichtet sie in Art. 35[21] die Betreiber algorithmischer Entscheidungssysteme dazu, in Abhängigkeit von den Risiken der Datenverarbeitung eine Datenschutz-Folgeabschätzung zu erstellen – und ein Sicherheitskonzept zu entwickeln, insbesondere für Worst-Cases. Auch das ist sinnvoll, denn jedes algorithmische System kann manipuliert oder gehackt werden.

Nun haben diese positiven Verpflichtungen aber einige Haken: Art. 22 und 35 erstrecken sich beispielsweise nur auf voll-automatisierte Entscheidungen, die meisten Systeme sind jedoch semi-autonom konzipiert. Zudem nutzen neuere Formen des Profiling eher die Daten, die sich aus der Kommunikation und Interaktion von Menschen mit Geräten ergeben als personenbezogene Daten. Dazu gehören etwa Suchanfragen oder Gesprächsinhalte von Messengern – Daten, die nicht von der DSGVO gedeckt sind. Allein deshalb brauchen wir ergänzend die E-Privacy-Verordnung[22] und eine kluge Regulierung von Datenzugangsrechten. Dennoch beinhaltet die DSGVO wesentliche Grundlagen, um die Gestaltung künstlich intelligenter Systeme anzugehen. Sie ist wegweisend.

## Warum Seehofer die falsche Sicherheitsdebatte vom Zaun bricht

Während unser Minister für Inneres und Heimat die x-te Asyldebatte vom Zaun bricht und die gesamte Regierung riskiert, scheinen die Risiken von Künstlicher Intelligenz völlig unbeachtet. Dabei berühren sie zentral die nationale Souveränität und Sicherheit der Bevölkerung: Wie etwa eine Schriftliche Anfrage zu Algorithmen in der Bundesverwaltung[23] durch die SPD-Politikerin Saskia Esken im Januar 2018 ans Licht brachte, gibt es laut Bundesregierung keine Kenntnisse darüber, auf Basis welcher Daten die Gesichtserkennungssoftware trainiert wurde, die am Berliner Südkreuz als Gemeinschaftsprojekt[24] des BMI, der Bundespolizei, des Bundeskriminalamts und der Deutschen Bahn AG erprobt wird. Mit dem Verweis auf „Mustererkennung" scheint alles gesagt – wobei es viele Verfahren gibt, Muster zu erkennen und gravierende Identifikationsfehler[25].

Leider betrifft die mangelnde Übersicht über eingesetzte Technologien nicht nur den Einzelfall. Sie betrifft auch die Frage, wie weit die gesellschaftliche Steuerung durch Algorithmen bereits entwickelt und in Anwendung ist: Sie ziele auf eine Kontextsteuerung, so der Verwaltungswissenschaftler Klaus Lenk[26]. Statt Zwang und Anreizen soll der Kontext von Menschen technologisch so gestaltet sein, dass sie möglichst automatisch das Richtige tun. Hier wirkten prospektiv verschiedene Technologien zusammen:

1. Personalisierung der informationellen Umgebung von Menschen und Organisationen

2. Profilbildung für die Zuweisung von Positionen und Lebenschancen

3. Verhaltenssteuerung durch technische Architekturen („Nudging"[27])

Im Endeffekt bekäme man nur das angeboten und zu sehen, was der individuellen Position und ihrer vermeintlichen Bedürfnisse entspricht. Die Beschreibung klingt zwar sehr einleuchtend. Allerdings ist unklar, wo wir stehen: Welche Systeme funktionieren und interagieren wie miteinander? Welche Rolle nehmen hier die Plattformen ein? Wo haben wir es mit Steuerung und wo mit Selbst-Steuerung zu tun? Welche Risiken ergeben sich daraus? Und letztlich: Funktioniert's überhaupt?

schwerpunkt

Hintergrund für dieses undurchsichtige Dickicht ist die Tatsache, so der KI-Forscher Matthew Scherer[28], dass ein Großteil der Entwicklung von Einzelkomponenten (Datensets, Algorithmen, algorithmischen Entscheidungssystemen, Schnittstellen, etc.) in einem bislang unregulierten, internationalen Setting stattfindet, das von einer unüberschaubaren Anzahl von Akteuren bestimmt wird. Da das Potenzial algorithmischer Entscheidungssysteme oft erst im Zusammenwirken dynamischer Technologien zutage tritt, sind Risiken hinsichtlich der Funktionalität und Kontrolle gegeben, die durch mangelnde Verantwortlichkeiten infolge unterschiedlicher territorialer Rechtsbereiche befördert wird. Hier Übersicht herzustellen über sich in der Entwicklung und Anwendung befindliche Technologien, inklusive involvierter Akteure und angemeldeter Patente, scheint wesentliche Voraussetzung für eine adäquate Risikoanalyse – und darauf aufbauend – Strategien der Risiko-Bewältigung.

Vermutlich sollte eine solche Übersicht zu Künstlicher Intelligenz Maßnahmen wie dem staatlichen „Hackback"[29] oder der Förderung der Interoperabilität von EU-Informationssystemen[30] voraus gehen, zumindest solange EU-Identifikationssysteme 33 % Sicherheitsrisiken[31] aufweisen. Sie könnte moderne Formen des E-Government[32] vielleicht sogar unterstützen.

Aber man kann stattdessen auch mit Asylpolitik Stimmung machen.

## Warum Upload-Filter eine schlechte Idee sind

Die Debatte um Upload-Filter – um Softwaresysteme, die auf großen Plattformen eingesetzt werden sollen, um die Veröffentlichung von strafbaren Materialien zu verhindern – ist aktuell Gegenstand der EU-Urheberrechtsreform[33]. Auch für die Bekämpfung von terroristischen oder extremistischen Inhalten[34] werden Upload-Filter als scheinbar passables Werkzeug regelmäßig ins Spiel gebracht. Für so manchen Politiker scheint es attraktiv zu sein, unliebsame Inhalte oder Hate Speech schon vor ihrer Veröffentlichung herauszufiltern. Technik wirkt natürlich immer viel neutraler und sauberer als lange Debatten in der Öffentlichkeit.

Aber das Ganze ist nicht unproblematisch: Einerseits können vielfältige Fehler[35] auftauchen, die beispielsweise von Julia Reda im Bereich vermeintlicher Urheberrechtsverletzungen gesammelt und veröffentlicht werden (ganz zu schweigen von den Problemen mit Memes und Satire). Andererseits scheint es gerade im Angesicht dieser Fehler bedenklich, die Meinungs- und Informationsfreiheit schon vor Veröffentlichung und möglicher Beschwerde zu beschränken[36]. Zudem würden durch eine Verpflichtung der Online-Plattformen auf den Einsatz von Upload-Filtern kleinere benachteiligt, welche die hohen Entwicklungskosten entsprechender Software nicht tragen können – und alternativ höchstens durch den Kauf von Software-Lizenzen rechtskonform arbeiten könnten. Das käme einer weiteren Monopolisierung der Plattformindustrie gleich.

Unterbeleuchtet bleibt auch hier die Rolle Künstlicher Intelligenz: Sie soll mit selbst-lernenden Algorithmen durch die Analyse großer Mengen an Daten dazu beitragen, neue Erkenntnisse zu generieren. Neue Erkenntnisse erlauben neue Strategien und tragen damit zu einem Wandel von Normen und Werten bei. Man muss nicht einmal den Sieg von Alpha Go![37] über den Menschen berücksichtigen, um die Bedeutung „maschineller Kreativität" zu entdecken. Eigentlich reicht das logische Durchdenken aktueller Probleme: Wenn 10.000 Kommentare als Hate Speech gelabelt werden oder 10.000 Kommentare wie bei Jigsaw (Alphabet Inc.) in einer Toxizitätsskala[38] danach verortet werden, wie hoch das Risiko ist, dass ein Teilnehmer die Debatte verlässt: Welche Zusammenhänge lernt eine Maschine, wonach entscheidet sie? Wahrscheinlich verschiebt sich der Fokus von der Idee hin zur Sprache, zum Ausdruck an sich. Möglicherweise kommen aber ganz andere Variablen ins Spiel – Variablen, über deren Angemessenheit Techniker und Geschäftsleute entscheiden anstelle von Richtern, Politikern oder Soziologen. Kann eine derart erwachsene maschinelle Entscheidung über Grundrechte legitim sein?

## Die Gesellschaft als lebendiges Experimentierfeld

Alle großen Plattformen experimentieren derzeit mit Formen automatisierter Inhalte-Regulierung[39] in verschiedenen thematischen und medialen Bereichen, die mitunter ganz neue Erkenntnisse über menschliche Debatten und Interventionsmöglichkeiten generieren dürfte. Aber wie gesagt: Zum gegenwärtigen Zeitpunkt ist all dies noch (hoch-)experimentell. So schätzte Facebook-Chef Mark Zuckerberg bei seinen Anhörungen zum

**Julia Krüger**

**Julia Krüger**[45] (Diplom-Politikwissenschaft) arbeitet an der Schnittstelle von Politik, Recht und Technik. Ihr Schwerpunkt liegt bei den Themen Algorithmen, Künstliche Intelligenz und Content-Regulierung. Als wissenschaftliche Mitarbeiterin von Saskia Esken (MdB SPD, seit Juni 2018) laufen zudem verschiedene Themen der deutschen Innen- und Digitalpolitik über ihren Schreibtisch. Zuvor arbeitete sie unabhängig für verschiedene Stakeholder (2015-18), darunter die *Bertelsmann Stiftung* und *netzpolitik.org*. Bei allen Fragen kommt ihr die frühere Forschung zum Politikfeld Internet (WZB, 2013-2015) ebenso zu Gute wie die Erfahrungen mit wirtschaftlicher Selbst- und Ko-Regulierung (SRIW, 2013) oder die Kenntnis der Datenkommunikation und Netzinfrastrukturen (Diplomarbeit: Netzsperren, Universität Potsdam 2012). Sie ist Fellow am *Center for Internet & Human Rights* (Viadrina, Frankfurt/ Oder).
Mehr Info findet sich unter *https://juliakrueger.org/* und auf Twitter unter *@phaenomen*. Man kann sie auch anschreiben unter *juliak@netzpolitik.org* (vorzugsweise verschlüsselt).

Cambridge-Analytica-Skandal im US-Kongress gleichermaßen optimistisch wie unscharf, es dauere noch rund 5-10 Jahre, bis Facebook „Hassrede“ zuverlässig erkennen könne[40]. Wie kann es dann sinnvoll oder gerechtfertigt sein, Online-Plattformen zum jetzigen Zeitpunkt auf Upload-Filter samt KI zu verpflichten – wo doch noch gar nicht klar ist, was deren Ergebnis ist? Wäre es nicht sinnvoll, die Plattformen zunächst zu Transparenz hinsichtlich ihrer Funktionsweise, Sicherheitsrisiken und Bewältigungsmaßnahmen zu verpflichten[41] und in einen Dialog zu treten mit Legislative und Judikative, um die Chancen und Risiken automatisierter Inhalte-Regulierung zu eruieren? Und so lange beim altbewährten (und mittlerweile technisch gut unterstützen) Notice-and-Take-Down-Verfahren zu bleiben? Immerhin: Wir leben in einem Informationskrieg[42], der gerade durch fehlende Verantwortlichkeiten[43] übelste Blüten trägt und durch falsche Reaktionen[44] noch viel schlimmer werden kann. Ist die Urheberrechtsindustrie tatsächlich willens, die Zerstörung demokratischer Debatten und Nationalstaaten auf ihre Kappe zu nehmen? I wouldn't.

Es ist längst überfällig, dass die drängenden Themen eine adäquate demokratische Bearbeitung finden durch die Bundesregierung, EU-Kommission, Bundestag und EU-Parlament. Dass überholte Machtkonflikte und kurzsichtige Wahlkampfmanöver mal beiseite gelegt werden könnten, damit die Themen Platz finden, die jetzt schon über das Schicksal zukünftiger Generationen bestimmen. Sicher gibt es mehr als Algorithmen und Künstliche Intelligenz. Aber sie wirken schon seit geraumer Zeit überall hinein und sollten entsprechende Berücksichtigung finden. Stellen wir die Weichen nicht rasch und gemeinsam, wird's allein der Markt richten. Zu seinen Gunsten, nicht zu unseren.

---

*Quelle: https://netzpolitik.org/2018/algorithmen-und-kuenstliche-intelligenz-wir-reden-an-unserer-zukunft-vorbei/*

## Anmerkungen


1 *https://netzpolitik.org/2018/datenschutzgrundverunsicherung-danke-merkel/*

2 *https://netzpolitik.org/2018/jetzt-uploadfilter-in-der-eu-urheberrechtsreform-verhindern-sag-dem-eu-parlament-deine-meinung/*

3 *https://www.bertelsmann-stiftung.de/de/publikationen/publikation/did/damit-maschinen-den-menschen-dienen/*

4 *https://www.heise.de/newsticker/meldung/EU-Plan-20-Milliarden-Euro-fuer-Kuenstliche-Intelligenz-bis-2020-4034360.html*

5 *https://www.heise.de/newsticker/meldung/Viel-gefaehrlicher-als-Atomwaffen-Elon-Musk-erneuert-seine-Warnung-vor-KI-3990782.html*

6 *https://www.youtube.com/watch?v=TuF5VLVMYso*

7 *https://www.heise.de/newsticker/meldung/Grosse-Koalition-Masterplan-fuer-KI-und-Aus-fuer-UKW-3959875.html*

8 *https://www.reclam.de/data/media/978-3-15-019499-7.pdf*

9 *https://www.fastcodesign.com/90174587/if-you-walk-breathe-or-talk-this-ai-probably-knows-who-you-are*

10 *https://www.theverge.com/2018/6/6/17433482/ai-automated-surveillance-drones-spot-violent-behavior-crowds*

11 *https://www.theverge.com/2018/4/24/17274372/ai-warfare-autonomous-weapons-paul-scharre-interview-army-of-none*

12 *https://www.amazon.de/App-vom-Arzt-Gesundheit-digitale/dp/3451375087*

13 *https://www.swr.de/swraktuell/standpunkt-wenn-software-einen-todesalgorithmus-liefert-der-algorithmus-ist-nur-ein-werkzeug/-/id=396/did=20819188/nid=396/18y6cm5/*

14 *https://www.oeffentliche-it.de/unberechenbar*

15 *https://www.bertelsmann-stiftung.de/de/publikationen/publikation/did/damit-maschinen-den-menschen-dienen/*

16 *http://www.spiegel.de/netzwelt/web/explainable-ai-auf-der-cebit-2018-wie-tickt-eine-kuenstliche-intelligenz-a-1213016.html*

17 *https://www.buecher.de/shop/robotik/kuenstliche-intelligenz/russell-stuart-j--norvig-peter/products_products/detail/prod_id/35926238/*

18 *https://twitter.com/phaenomen/status/996677469506867200*

19 *https://dsgvo-gesetz.de/art-22-dsgvo/*

20 *https://dsgvo-gesetz.de/kapitel-3/*

21 *https://dsgvo-gesetz.de/art-35-dsgvo/*

22 *https://netzpolitik.org/2018/algorithmen-regulierung-im-kontext-aktueller-gesetzgebung/*

23 *http://dipbt.bundestag.de/doc/btd/19/006/1900605.pdf*

24 *https://netzpolitik.org/2017/de-maiziere-plant-flaechendeckende-gesichtserkennung-trotz-hoher-fehlerquoten-am-suedkreuz/*

25 *https://www.youtube.com/watch?v=GTyNGhWv3wI*

26 *https://www.nomos-elibrary.de/10.5771/0947-9856-2016-5-227/die-neuen-instrumente-der-weltweiten-digitalen-governance-jahrgang-22-2016-heft-5*

27 *https://de.wikipedia.org/wiki/Nudge*

28 *https://poseidon01.ssrn.com/delivery.php?ID=197095009065071120001071069105117028041051023052059052078009120071071126074102066069035037056044123004055022012025000012095000103027053013003028103009024015124086095070092084088007066114026077094069110083087092030002105122105069121079123119003119004093&EXT=pdf oder kurz: http://t1p.de/svfn*

29 *https://www.tagesschau.de/inland/cyberangriffe-hacking-101.html*

30 *https://www.bundestag.de/blob/559014/9c09f7406023ff11891b2662147220b0/19wp-13-data.pdf*

31 *https://www.heise.de/newsticker/meldung/Identifikationsdienst-eIDAS-macht-Fortschritte-4001541.html*

32 *https://www.oeffentliche-it.de/oefit2017#session1*

33 *https://netzpolitik.org/2018/upload-filter-eine-gefahr-fuer-die-netzkultur/*

34 *https://netzpolitik.org/2018/eu-kommission-will-von-plattformen-freiwillige-und-weitreichende-internetzensur/*

35 *https://juliareda.eu/2017/09/when-filters-fail/*

36 *https://netzpolitik.org/2018/upload-filter-eine-gefahr-fuer-die-netzkultur/#*

37 *https://www.netflix.com/de-en/title/80190844*

38 *https://www.wired.com/2017/02/googles-troll-fighting-ai-now-belongs-world/*

39 *https://netzpolitik.org/2017/wie-man-den-hass-schuert-risiken-privatisierter-rechtsdurchsetzung/*

40 *https://twitter.com/tictoc/status/983786153974300673*

41 *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1686043*

42 *https://www.cbinsights.com/research/future-of-information-warfare/*

43 *https://www.cbinsights.com/research/future-of-information-warfare/*

44 *https://netzpolitik.org/2018/kommentar-die-oeffentliche-meinungsbildung-wird-fuer-facebook-zum-experimentierfeld/*

45 *https://netzpolitik.org/author/juliak/*

**Felix Sühlmann-Faul**

# Geliebtes Smartphone – bist Du böse?

*Wir alle lieben unsere Smartphones. Sie enthalten unsere Fotos, unsere Musik, Nachrichten unserer Freunde – sie sind quasi ein kleines, elektronisches „Ich". Unsere Liebe zu den Geräten erzeugt jedoch Nachhaltigkeitsdesaster in anderen Teilen der Erde.*

*Smartphone-Nutzer in der japanischen Stadt Shibuya*

Aktuell gibt es in Deutschland 57 Millionen Nutzerinnen und Nutzer[1] eines Smartphones. Das entspricht ungefähr 69 Prozent der gesamten Bevölkerung. 2009 waren es lediglich 6,3 Millionen Nutzende. 432 Millionen Smartphones[2] wurden weltweit allein im vierten Quartal 2016 im Einzelhandel verkauft. Diese enorme Verbreitung hängt mit einem ebenfalls großen Schwund zusammen: Smartphones werden im weltweiten Durchschnitt bereits nach rund 20 Monaten[3] gegen ein neues Gerät getauscht. Ein solch schneller Wechsel sollte aber dringend überdacht werden. Wie im Folgenden beschrieben wird, sind die Geräte von der Wiege bis zur Bahre eine Katastrophe für die ökologische und soziale Nachhaltigkeit[4].

Die Bauteile eines Smartphones bestehen aus 50[5] bis 75[6] verschiedenen chemischen Elementen. Und wie bei anderen elektronischen Geräten werden dafür Rohstoffe benötigt, die in Schwellen- und Entwicklungsländern abgebaut werden. Weil der Bedarf so hoch ist und die Nutzungsphase der Geräte so kurz, entsteht hier ein starkes Spannungsverhältnis. Denn in den Ländern, die die Rohstoffe für die Smartphones liefern, erzeugt die Gewinnung erhebliche soziale und ökologische Probleme. Etwa benötigen die Telefone die vier sogenannten „Konfliktmineralien"[7] Tantal, Zinn, Wolfram und Gold. Die Demokratische Republik Kongo (DRK) exportiert alle vier dieser Stoffe.

Konfliktbehaftet sind diese Mineralien, weil der Abbau vor Ort Rebellentruppen finanziert[8]. Die Rebellen sind im Besitz des Bergbaus und/oder Teilen des Handels mit den Mineralien. Sie finanzieren mit dem Gewinn die Waffen zur Sicherung ihrer Macht und destabilisieren so die Region, was noch viele weitere Probleme mit sich bringt. Im Umfeld der Bergbauanlagen wurde Zwangs- und Kinderprostitution beobachtet, HIV und Aids breiten sich aus. Laut der Weltflüchtlingsorganisation UNHCR liegt die Zahl der registrierten Geflüchteten aus der DRK bis dato bei einer dreiviertelmillion Menschen[9].

## Giftschlamm

Die ökologischen Probleme zeigen sich am deutlichsten beim Abbau seltener Erden, die für unsere smarten Geräte ebenfalls benötigt werden. Diese Metalle wie Neodym oder Lanthan werden aus Mineralgestein gewonnen, das mit Säuren ausgewaschen wird. Aufgrund der geringen Konzentration (daher „selten") der Stoffe müssen viele Tonnen Gestein ausgewaschen werden, um wenige Gramm der Metalle zu erhalten. Durch den Abbau entsteht giftiger Schlamm[10]. Der weltgrößte Tümpel dieses Schlamms befindet sich in der Mongolei mit 10 km² Fläche[11]. Er besteht aus 160 Millionen Tonnen Abfall, 17,5 Millionen Kubikmeter hochradioaktivem Abwasser, Schwefelsäure und Fluorwasserstoffsäure[12].

## Energieverbrauch der Produktion

Sind die Rohstoffe gewonnen, bringen die Einzelteile des Smartphones lange Wege hinter sich. Schon der Transport der einzelnen Bauteile erzeugt ein hohes $CO_2$-Aufkommen. Hinzu kommt die fossile Energieerzeugung in den Regionen, in denen die meisten Teile hergestellt werden. 85 Prozent der Anteile eines iPhones werden bspw. in China gefertigt. In den Ländern des südostasiatischen Raums ist Kohle als Grundlastversorgung[13] bislang unersetzbar. Durch die allgegenwärtige Digitalisierung ist Informations- und Kommunikationstechnologie (IKT) der Sektor, der den höchsten Anstieg von Emissionen erzeugt[14].

Am Beispiel des Samsung Galaxy S6 zeigt sich nach Angaben aus dem Nachhaltigkeitsbericht des Herstellers[15], dass Herstellung und Transport über 80 Prozent des Energieverbrauchs und damit der Emissionslast des Geräts ausmachen.

### Reparatur? Fehlanzeige!

Der Trend zu dünneren Geräten mit möglichst großem Display[16] und die Verwendung von Glas auf der Rückseite laufen der Option zuwider, etwa den Akku einfach wechseln zu können. Eine weitere Hürde stellt die Verwendung von Schrauben mit Sonderformat[17] dar. Damit ist eine Reparatur für einen Laien quasi unmöglich und für Fachleute zunehmend aufwendig. Ist ein Bauteil des Telefons defekt, ist es häufig ein „wirtschaftlicher Totalschaden", weil es so kompliziert ist, an das betroffene Bauteil überhaupt erst heranzukommen.

### Ätzender Müll

Am Ende des Smartphonelebens steht dann die Müllkippe. Der Fachbegriff für Technikschrott lautet „waste electrical and electronic equipment (WEEE)" bzw. „E-Waste"[18]. Die weltweite Menge an anfallendem E-Waste betrug im Jahr 2017 über 60 Millionen Tonnen[19]. Das entspricht dem Gewicht des Empire State Buildings multipliziert mit 200. Aufgrund des kurzen Lebenszyklus von Mobiltelefonen stellen diese das größte Problem dar[20]. Sie machen bei weitem den größten Anteil des anfallenden Schrotts aus.

Technik ist an sich keine ökologische Bedrohung während der Nutzungsphase. Als E-Waste ist sie jedoch eine besonders aggressive und schädliche Art Müll. Die Platinen und Akkus von Computern, Mobiltelefonen und anderen Geräten enthalten zumindest ein giftiges Metall, meist handelt es sich um Blei, Cadmium oder Beryllium.

Alle diese Stoffe können bei Kontakt schwere organische Erkrankungen erzeugen. Von den Müllkippen aus geraten giftige Chemikalien in Boden und Luft[21] und schädigen Umwelt und Menschen in den umliegenden Kommunen. Die Menschen vor Ort, darunter viele Kinder, zertrümmern ohne Schutzbekleidung die kaputten Geräte oder stecken deren Plastikgehäuse in Brand, um an verwertbare Rohstoffe zu kommen. Diese werden auf Schrottmärkten zu Geld gemacht.

### Verantwortung wird exportiert

Aber auch Recycling ist bei Tablets, Smartphones oder Computern nicht das, wofür man es halten könnte. Besonders für Elektronik existiert kein Stoffkreislauf, der eine Wiederverwertung verbauter Materialien ermöglicht. Auch können einmal verbaute seltene Erden nicht wiedergewonnen werden und gehen unwiederbringlich bei der Herstellung eines Geräts verloren[22].

In den USA werden 50 bis 80 Prozent der zu recycelnden Elektrogeräte in die Länder des Fernen Ostens, Indien, Afrika und China exportiert[23]. Dort angekommen, werden die Altgeräte von Hand, meist ohne geeignetes Werkzeug oder Schutzbekleidung, zerlegt.

### Konflikthafte Liebe

Fassen wir zusammen: Die Nachhaltigkeitsdefizite der Smartphones sind vielfältig. Hohe Absatzzahlen und kurze Lebenszyklen bedeuten mehr Bedarf an Rohstoffen und auch mehr Elektroschrott, was problematische Folgen für viele bedeutet: vergiftete Böden und Luft, Umweltzerstörung, Krankheit und Gewalt.

Was können wir tun? Das Smartphone ist aus unserem Alltag nicht wegzudenken, es enthält unsere Bilder, unsere Musik, stellt Kontakt zu unseren Freunden her, ist Arbeits- und Spaßmaschine, unser persönlichster Besitz – es ist ein erweitertes Selbst[24]!

### Lebensverlängernde Maßnahmen

Da die Herstellung des Telefons selbst schon so enorm viel Energie braucht, verbessern sämtliche lebensverlängernde Maßnahmen die Ökobilanz des Smartphones. Das eigene Telefon möglichst lange zu nutzen, ist das Beste, was man tun kann. Schutzhüllen, Displayfolien und akkuschonendes Laden[25] halten das Telefon lange schön und lebendig. Und Nutzerinnen und Nutzer von Android können stets neue Versionen des Betriebssystems über sogenannte Customs Roms[26] nach Ablauf der Garantie aufspielen.

Wenn man zwar ein altes funktionierendes Smartphone hat und ein neues Gerät haben möchte, ist das Recycling des alten Geräts – wie beschrieben – die am wenigsten nachhaltige Option. Das Smartphone kann aber ein zweites Leben führen: z. B. als interaktiver Tischkalender, als Babymonitor, Küchenradio oder digitaler Bilderrahmen[27]. Auch eine Spende für gute Zwecke[28] ist nachhaltig. Und das neue Gerät kann dann am besten ebenfalls ein Gebrauchtes[29] sein. Denn der wichtigste Nachhaltigkeitsfaktor ist Suffizienz[30] – die Begrenzung des eigenen Lebensstils und Konsums. Und wenn es einem in den Fingern juckt, weil etwa die Veröffentlichung des neuen iPhones vor der Tür steht, sollte man an einen gewissen Schlammsee in der Mongolei oder die Gewalt in der Republik Kongo denken.

---

*Quelle: https://netzpolitik.org/2018/geliebtes-smartphone-bist-du-boese/*

## Referenzen


Belk R 1988: Possessions as the Extended Self, in: Journal of Consumer Research 15(2):139-68, February 1988

Cornot-Gandolphe, Sylvie 2016: The Role of Coal in Southeast Asia's Power Sector and Implications for Global and Regional Coal Trade, Oxford Institute for Energy Studies

de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/

data2.unhcr.org/en/situations/drc

gartner.com/newsroom/id/3609817

greenpeace.org/international/en/campaigns/detox/electronics/the-e-waste-problem/

Hilty LM, Coroama VC, Ossés De Eicker M et al. 2009: The Role of ICT in


schwerpunkt

Energy Consumption and Energy Efficiency; researchgate.net/publication/267411194_The_Role_of_ICT_in_Energy_Consumption_and_Energy_Efficiency
Koebler J 2015: How to fix everything; motherboard.vice.com/en_us/article/how-to-fix-everything
Koebler J 2016: Instead of a Recycling Robot, Apple Should Sell Screwdrivers That Open iPhones; motherboard.vice.com/en_us/article/instead-of-a-recycling-robot-apple-should-sell-screwdrivers-that-open-iphones
Koebler J 2017: Apple Forces Recyclers to Shred All iPhones and MacBooks; motherboard.vice.com/en_us/article/apple-recycling-iphones-macbooks
Kuper J, Hojsik, M 2008: Poisoning the Poor, Greenpeace.org; greenpeace.org/denmark/Global/denmark/p2/other/report/2008/poisoning-the-poor-electroni.pdf
Margolin M 2016: The Periodic Table of iPhone Elements; motherboard.vice.com/en_us/article/the-periodic-table-of-iphone-elements
Martin-Jung H 2015: Müllkippe statt Mine; sueddeutsche.de/digital/alte-handys-muellkippe-statt-mine-1.2553381
Peterman A, Palermo T, Bredenkamp C 2001: Estimates and Determinants of Sexual Violence Against Women in the Democratic Republic of Congo, American Public Health Association
Samsung Sustainability Report 2016; https://images.samsung.com/is/content/samsung/p5/global/ir/docs/2016-samsung-sustainability-report.pdf
Sepulveda, A, Schluep M, Hagelüken C et al. 2010: A Review of the Environmental Fate and Effects of Hazardous Substances Released from Electrical and Electronic Equipments during Recycling: Examples from China and India, in: Environmental Impact Assessment Review, Januar 2010
Sutherland E 2001: Coltan, the Congo and your cell phone, University of the Witwatersrand; web.mit.edu/12.000/www/m2016/pdf/coltan.pdf
United Nations Conference in Trade and Development. 2014. Commodities At A Glance. 5. New York und Genf: UNCTAD
unu.edu/media-relations/releases/step-launches-interactive-world-e-waste-map.html#info
Woyke E 2014: The Smartphone. Anatomy of an Industry, New York
Wübbeke J 2012. „Bergbau in der Inneren Mongolei: Umweltverschmutzung und Konflikte“. Philippinenbüro e. V. im Asienhaus und der Südostasien Informationsstelle 8

## Anmerkungen

1 *https://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/*
2 *https://www.gartner.com/newsroom/id/3609817*
3 *https://www.businessinsider.de/how-long-people-wait-to-upgrade-phones-chart-2017-3?r=US&IR=T*
4 *https://www.nachhaltigkeit.info/artikel/nachhaltigkeit_1398.htm*
5 *https://motherboard.vice.com/en_us/article/4xaxem/instead-of-a-recycling-robot-apple-should-sell-screwdrivers-that-open-iphones*
6 *https://motherboard.vice.com/en_us/article/nz7kwm/the-periodic-table-of-iphone-elements*
7 *https://enoughproject.org/special-topics/progress-and-challenges-conflict-minerals-facts-dodd-frank-1502*
8 *http://web.mit.edu/12.000/www/m2016/pdf/coltan.pdf*
9 *http://data2.unhcr.org/en/situations/drc*
10 *http://www.sueddeutsche.de/digital/alte-handys-muellkippe-statt-mine-1.2553381*
11 *http://unctad.org/en/PublicationsLibrary/suc2014d1_en.pdf*
12 *https://www.asienhaus.de/public/archiv/bergbau-nr2_china.pdf*
13 *https://www.oxfordenergy.org/wpcms/wp-content/uploads/2016/12/The-role-of-coal-in-Southeast-Asias-power-sector-CL-4.pdf*
14 *https://www.researchgate.net/publication/267411194_The_Role_of_ICT_in_Energy_Consumption_and_Energy_Efficiency*
15 *https://images.samsung.com/is/content/samsung/p5/global/ir/docs/2016-samsung-sustainability-report.pdf*
16 *https://motherboard.vice.com/en_us/article/mbjwwq/heres-why-smartphones-are-getting-taller-and-slimmer*
17 *https://motherboard.vice.com/en_us/article/4xaxem/instead-of-a-recycling-robot-apple-should-sell-screwdrivers-that-open-iphones*
18 *https://www.theguardian.com/environment/gallery/2014/feb/27/agbogbloshie-worlds-largest-e-waste-dump-in-pictures*
19 *https://netzpolitik.org/2018/geliebtes-smartphone-bist-du-boese/#info*
20 *https://www.greenpeace.org/archive-international/en/campaigns/detox/electronics/the-e-waste-problem/*
21 *https://www.greenpeace.org/archive-international/en/news/features/poisoning-the-poor-electroni/*
22 *https://motherboard.vice.com/en_us/article/yp73jw/apple-recycling-iphones-macbooks*
23 *http://www.greenpeace.org/denmark/Global/denmark/p2/other/report/2008/poisoning-the-poor-electroni.pdf*
24 *https://www.thinkwithgoogle.com/intl/de-de/insights/kundeneinblicke/the-extended-self-die-bedeutung-von-smartphones-fur-nutzer-und-konsumenten/*
25 *https://www.sciencealert.com/how-to-charge-phone-battery-to-last-longer-advice-science*
26 *https://www.xda-developers.com/how-to-install-custom-rom-android/*
27 *https://www.howtogeek.com/335161/how-to-turn-an-old-android-tablet-into-an-auto-updating-digital-photo-frame/*
28 *https://www.handyverkauf.net/knowledgebase/handy-spenden*
29 *http://www.ebay.de/*
30 *https://www.nachhaltigkeit.info/artikel/suffizienz_2034.htm*
31 *http://www.suehlmann-faul.com/*
32 *http://www.bit.ly/digi-teaser*
33 *http://www.bit.ly/digi-summary*
34 *http://bit.ly/Digi_Nachhalt_RG*

**Felix Sühlmann-Faul**

Der Techniksoziologe **Felix Sühlmann-Faul**[31] forscht seit ca. drei Jahren im Bereich Digitalisierung und Nachhaltigkeit. Zuletzt verfasste er eine Studie zu den Nachhaltigkeitsdefiziten der Digitalisierung und möglichen Handlungsempfehlungen im Auftrag des *WWF Deutschland* und der *Robert-Bosch-Stiftung*. Hier finden sie eine kurze Zusammenfassung[32], eine ausführliche Zusammenfassung[33] und die komplette Studie[34].
Aktuelle Publikation, erschienen am 6. September 2018: Felix Sühlmann-Faul, Stephan Remmler: Der blinde Fleck der Digitalisierung, oekom-Verlag. Webseite: *www.suehlmann-faul.com*.

**Tomas Rudl**

# Unregulierte soziale Netzwerke zerstören Demokratie

*Ein Ausschuss des britischen Parlaments geht mit Facebook, Google & Co. hart ins Gericht. In einem umfangreichen Bericht fordern die Abgeordneten konkrete Maßnahmen, um das giftige Ökosystem aus Online-Werbung, Wahlbeeinflussung und Datenmissbrauch in den Griff zu bekommen.*



IT-Konzerne wie Facebook, Twitter oder Google und ihr giftiges Ökosystem haben mitgeholfen, die Volksabstimmung zum EU-Austritt des Vereinigten Königreichs zu beeinflussen, den Völkermord an der Rohingya-Minderheit in Myanmar umzusetzen und hätten zudem die Grundrechte von Millionen von britischen Bürgern mit Füßen getreten. Es sind gewichtige Anschuldigungen, die im Zwischenbericht des Ausschusses[1] für Digitales, Kultur, Medien und Sport des britischen Parlaments stecken, der am Sonntag veröffentlicht wurde.

*Facebook, Google, Twitter & Co. sind wie Giftmüll für unsere Gesellschaften, solange sie weitgehend unreguliert bleiben*

Über ein Jahr lang befragten die Abgeordneten Dutzende Zeugen, holten über 150 schriftliche Stellungnahmen ein und reisten sogar bis nach Washington, um dem Phänomen der Ausbreitung von Falschnachrichten und gezielt gestreuten irreführenden Informationen auf den Grund zu gehen. Im Zentrum standen soziale Netzwerke, deren Geschäftsmodelle und wie sich diese auf Wahlentscheidungen auswirken, etwa auf das Brexit-Referendum. Neue Fahrt nahm die Untersuchung nach dem Bekanntwerden des Datenskandals um Facebook und Cambridge Analytica[2] auf. Am Ende wurde daraus ein Verfahren, schreibt die von Beginn an berichtende Guardian-Journalistin Carole Cadwalladr[3], das die „gesamte Struktur, Maschinerie und Zukunft unserer Demokratie“ unter die Lupe nahm.

Der 89 Seite starke und weitreichende Zwischenbericht nimmt kein Blatt vor den Mund. Insbesondere Facebook kommt darin schlecht weg. Das soziale Netzwerk habe sich bei den Untersuchungen unkooperativ gezeigt, ganz abgesehen von den fragwürdigen Methoden, die zum Alltagsgeschäft des Konzerns gehören. „Facebook hat alle Informationen“, schreiben die Abgeordneten. „Außenstehende haben sie nicht, außer Facebook entscheidet sich, sie zu veröffentlichen. Facebook war unwillig, Informationen mit dem Ausschuss zu teilen, was nichts Gutes verheißt für künftige Transparenz.“

## IT-Konzerne sind nicht „neutral“

Das will das britische Parlament nun ändern und fordert konkrete Maßnahmen. Bislang hätten sich diese wenigen, monopolistisch agierenden Anbieter etwa hinter der fadenscheinigen Ausrede versteckt, „neutrale“ Plattformen zu sein, um sich der Regulierung zu entziehen. Aber sie seien keineswegs neutral, so wie auch der Begriff „Plattform“ irreführend sei: „Das Wort ‚Plattform‘ suggeriert, dass diese Unternehmen passiv handeln und einfach nur Informationen veröffentlichen, die ihre Nutzer hochladen – ohne selbst zu beeinflussen, was wir sehen oder nicht“, heißt es im Bericht. Aber das würde nicht stimmen, schließlich sei genau das ihr Geschäftsmodell: „Sie wollen uns einnehmen („engage“), von dem Moment an, zu dem wir uns einloggen, um Umsätze zu erwirtschaften mit den Werbeeinblendungen, die wir sehen.“

Aber statt sie in veraltete Schubladen wie „Plattform“ oder „Verleger“ zu stecken, brauche es ein gänzlich neues Konzept für die Regulierung sozialer Netzwerke. Dieses soll bis Ende des Jahres entstehen und von der Regierung in einen Gesetzentwurf gegossen werden. Letztlich sollen die Konzerne unter anderem haftbar gemacht werden können für „schädigende und illegale“ Inhalte, die sie verbreiten. Im Blick haben die Abgeordneten dabei sowohl Inhalte, die Nutzer den Betreibern melden, als auch Inhalte, bei denen es den Konzernen „leicht fallen sollte, sie selbst zu erkennen“.

In der Praxis dürfte dies wohl auf den Einsatz Künstlicher Intelligenz hinauslaufen, anders lässt sich die täglich auflaufende

**Tomas Rudl**

**Tomas Rudl**[13] ist in Wien aufgewachsen, hat dort für diverse Provider gearbeitet und daneben Politikwissenschaft studiert. Seine journalistische Ausbildung erhielt er im *Heise-Verlag*, wo er für die *Mac & i*, *c't* und *Heise Online* schrieb.
Er ist unter +49-30-92105-9861 oder *tomas@netzpolitik.org* erreichbar und twittert mal mehr, mal weniger unter *@tomas_np*.

Datenmenge sonst kaum bewältigen. Allerdings ist diese Technologie aus vielen Gründen noch lange nicht so weit[4], um zuverlässig Inhalte zu erkennen und richtig einzustufen. „Die Heilung könnte schlimmer sein als die Krankheit", warnen die Fakten-Checker von „Full Fact"[5], die als Sachverständige vom Ausschuss befragt wurden. „Wir müssen so handeln, dass sowohl die Meinungsfreiheit gewahrt bleibt als auch der Schaden, der von Desinformation ausgeht, limitiert wird."

### Neue Transparenzregeln

Weniger kontrovers, leichter umsetzbar und vermutlich effektiv dürften die anderen Vorschläge sein, die der Ausschuss unterbreitet. So wie die Firmen etwa dem Finanzamt Rechenschaft schuldig sind, sollen sie künftig ihre Sicherheitsmechanismen und Algorithmen gegenüber Regulierern offenlegen. Für mehr Transparenz sollen neue Regeln für politische Kampagnen sorgen. Alle digitalen Anzeigen sollten ein einfach zugängliches Impressum aufweisen und offenlegen, wer die Anzeige veröffentlicht und wer sie bezahlt hat. Briefkastenfirmen, hinter denen sich anonyme Geldgeber verstecken können, um nicht nachvollziehbar politische Anzeigen zu schalten, sollen der Vergangenheit angehören. Ein öffentliches Register mit allen digitalen Anzeigen steht ebenfalls im Pflichtenheft. Und Nutzer sollten in der Lage sein, bestimmten Formen von Microtargeting zu widersprechen.

Diese hoch umstrittene manipulative Form[6] der auf einzelne Nutzer zugeschnittenen Wahlwerbung[7], verknüpft mit irreführenden Informationen[8], hatte für Großbritannien schwerwiegende Folgen. Wie der Bericht offenlegt, gab es zahlreiche zwielichtige Verbindungen zwischen Facebook, Cambridge Analytica sowie anderen Datenfirmen und der auf den EU-Austritt drängenden Leave-Kampagne. Diese hatte teils illegal und mit Hilfe von Psychogrammen gezielt „Dark Ads" auf sozialen Netzwerken ausgespielt und soll damit entscheidend das Ergebnis der Brexit-Abstimmung beeinflusst haben.

### Russland steckt tief drin

Dabei erhielt die Brexit-Austrittskampagne tatkräftige Unterstützung aus Russland, das an einer Destabilisierung des Westens interessiert ist. Den Verflechtungen widmet der Bericht ein eigenes Kapitel. Erst im Laufe der Untersuchung hätten sich auf jedem Schritt des Weges die vielen Verbindungen zu Russland offenbart, sagte der konservative Ausschussvorsitzende Damian Collins dem Guardian[9]. „Es gab keinen Punkt, an dem wir dachten ‚Oh, es ist nicht so schlimm wie befürchtet'", sagte er. „Die Verbindungen scheinen nur tiefer und signifikanter geworden zu sein."

Bislang fielen solche Formen der unlauteren Beeinflussung leicht, da praktisch unreguliert teils legal, teils illegal beschaffte Nutzerdaten nach Gutdünken ge- und missbraucht werden können. Der Bericht samt seinen Empfehlungen wird sicherlich noch für heiße Diskussionen sorgen, stellt aber in seiner Gesamtheit den ersten nennenswerten Schritt dar, um die stetig und ungehindert wachsende Macht der großen Plattformen einzuhegen. Ein noch weitergehender Bericht soll im Herbst folgen, der tiefer die Rolle und Mechanismen von Online-Werbung beleuchten wird.

Ob jedoch die britische Regierung, die ausgerechnet von den EU-Austrittsverhandlungen überfordert ist, tatsächlich ein stimmiges Gesetz entwickeln kann, steht auf einem anderen Blatt. Alleine auf das Vereinigte Königreich ist das Problem freilich nicht beschränkt. So warnt die EU-Kommission gebetsmühlenartig vor möglicher Meinungsmanipulation im Internet[10]. Die Botschaft scheint aber bei den meisten EU-Mitgliedstaaten noch nicht so richtig angekommen zu sein. Ergebnislos blieb bisher ein von der EU-Kommission angestoßener Verhaltenskodex für Online-Plattformen[11], der Desinformation in ihren Netzen eindämmen soll. Ursprünglich für Juli geplant, wurde die Veröffentlichung jedoch auf September verschoben[12].

*Quelle: https://netzpolitik.org/2018/unregulierte-soziale-netzwerke-zerstoeren-demokratie/*

## Anmerkungen

1 *https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf*
2 *https://netzpolitik.org/2018/cambridge-analytica-was-wir-ueber-das-groesste-datenleck-in-der-geschichte-von-facebook-wissen/*
3 *https://www.theguardian.com/politics/2018/jul/28/dcms-committee-report-finds-truth-fake-news-facebook-brexit*
4 *https://netzpolitik.org/2017/wie-man-den-hass-schuert-risiken-privatisierter-rechtsdurchsetzung/*
5 *https://twitter.com/FullFact/status/1023248165665943552*
6 *https://netzpolitik.org/2017/wahlkampf-in-der-grauzone-die-parteien-das-microtargeting-und-die-transparenz/*
7 *https://netzpolitik.org/2018/wie-die-britische-labour-partei-ihren-eigenen-parteichef-mit-microtargeting-linkte/*
8 *https://www.bbc.com/news/uk-politics-44966969*
9 *https://www.theguardian.com/politics/2018/jul/28/dcms-committee-report-finds-truth-fake-news-facebook-brexit*
10 *https://netzpolitik.org/2018/eu-kommissarin-warnt-vor-manipulation-in-sozialen-medien-bei-europawahl/*
11 *https://netzpolitik.org/2018/eu-experten-erklaeren-den-begriff-fake-news-fuer-tot/*
12 *https://ec.europa.eu/digital-single-market/en/news/draft-code-practice-online-disinformation*
13 *https://netzpolitik.org/author/tomas/*


**Stefan Hügel**

# BigBrotherAwards 2018

*Mit bemerkenswerter Chuzpe wurde auch im vergangenen Jahr die Überwachung vorangetrieben. Beispiele gibt es viele – Polizei- und Verfassungsschutzgesetze, die die Nutzung eines Staatstrojaners oder eine Vorratsdatenspeicherung etablieren, unter konsequenter Missachtung höchstrichterlicher Rechtsprechung, sind nur zwei davon.*

Wir fassen in diesem einleitenden Beitrag des Schwerpunkts zum BigBrotherAward 2018[1] zunächst die Laudationes für die PreisträgerInnen kurz zusammen. Die Verleihung fand am 20. April 2018 in Bielefeld statt; dieses Mal im Stadttheater, was der Veranstaltung einen besonderen, zusätzlichen Reiz verlieh. Danach drucken wir drei Laudationes im Wortlaut ab.

## Kategorie *Arbeitswelt*

Der BigBrotherAward in der Kategorie *Arbeitswelt* ging an die **Soma Analytics**, die mit ihrer Gesundheits-App *Kelaa* Gesundheitsdaten ihrer Nutzerinnen und Nutzer sammelt und an Arbeitgeber weiterleitet. Allein dies ist bereits ein Tabubruch. Laudator Peter Wedde erläuterte die Preisvergabe im weiteren:

> *„Vor Gesundheitsapps warnen wir seit Jahren. Soma Analytics führt unsere Kritik aber in eine neue Dimension. Die von dieser Firma entwickelte Kelaa-App kann zwar jeder auf sein Mobiltelefon laden. Sie funktioniert aber nur, wenn der Arbeitgeber über die Software ‚Kelaa Dashboard' verfügt. Mit dieser Software können sich die Arbeitgeber die aktuellen Stress- und Vitalwerte ihrer Beschäftigten in (Zitat) ‚aggregierter und anonymisierter Form' anzeigen lassen. Die entsprechenden Auswertungen stellt Soma Analytics bereit."*

Die App wertet die Daten über das Smartphone umfassend aus: Gesundheitsdaten, Stressinformationen. Man soll das Smartphone mit ins Bett nehmen, um auch das Schlafverhalten erfassen zu können. Gefühlsregungen der Stimme, das Schreib- bzw. Tippverhalten und ganz allgemein die Nutzung des Smartphones werden ausgewertet. Dazu sollen die Beschäftigten einen Self-Assessment-Fragebogen ausfüllen. Die ArbeitgeberIn soll mit dem Kelaa-Dashboard Bereiche identifizieren können, in denen Verbesserungsbedarf für die Gesundheit und Produktivität der MitarbeiterInnen besteht. Aus Sicht des Laudators:

> *„Soma Analytics versucht, Arbeitgebern die Rundumkontrolle des physischen und psychischen Befindens ihrer Beschäftigten zu ermöglichen. Dass dieses Angebot Arbeitgeber begeistert und auf neue Ideen bringt, zeigen erste Erfahrungen aus Großbritannien, wo Kelaa in einer großen Anwaltskanzlei mit über tausend Mitarbeitern eingesetzt wird. Dort hat der für die Nutzung der Kelaa-App zuständige Mitarbeiter festgestellt: ‚Die App zeigt uns die Potentiale auf, die wir realisieren können, wenn wir mit unseren Mitarbeitern zusammen an ihrem Schlaf arbeiten'."*

Letztlich entscheidet jeder selbst, ob er Apps zur Stresserkennung und Stressreduzierung nutzt. Doch, so Laudator Peter Wedde:

> *„Wenn Sie als Beschäftigte meinen, dass es Ihrer Gesundheit förderlich ist, auf Ihrem Smartphone eine App zur Stresserkennung und Stressreduzierung zu installieren, dann steht es Ihnen natürlich frei, dies zu tun. Aber achten Sie darauf, dass es keine Software ist, die ihrem Arbeitgeber gehört. Wer diese simple Grundregel beachtet, der muss auch keinen Ausschlag des ‚Stress-O-Meters' in seiner App befürchten, wenn der Arbeitgeber wieder einmal davon redet, dass er olympiareife Mannschaften braucht und dass deshalb die nicht so leistungsfähigen Beschäftigten das Boot verlassen müssen."*

## Kategorie *PR & Marketing*

Der BigBrotherAward in der Kategorie *PR & Marketing* ging in diesem Jahr nicht an einen einzelnen Preisträger sondern an ein Gesamtkonzept: das **Konzept der „Smart Cities"**, der mit Sensoren bestückten, ferngesteuerten und kommerzialisierten Stadt, so erläuterte Laudatorin Rena Tangens:

> *„Das Smart City-Konzept propagiert die „Safe City": die mit Sensoren gepflasterte, total überwachte, ferngesteuerte und kommerzialisierte Stadt. Smart Cities reduzieren Bürger auf ihre Eigenschaft als Konsumenten, machen Konsumenten zu datenliefernden Objekten und unsere Demokratie zu einer privatisierten Dienstleistung."*

Und weiter:

*„Der Begriff Smart City ist eine schillernd-bunte Wundertüte – er verspricht allen das, was sie hören wollen: Innovation und modernes Stadtmarketing, effiziente Verwaltung und Bürgerbeteiligung, Nachhaltigkeit und Klimaschutz, Sicherheit und Bequemlichkeit, für Autos grüne Welle und immer einen freien Parkplatz.“*

Was ist eine *Smart City*? Beispielsweise Straßenlaternen, die nicht nur leuchten, sondern auch Videoüberwachung enthalten, Fußgänger erkennen, Kfz-Kennzeichen lesen, durch Sensoren die Umwelt überwachen, mit Mikrophonen die Umgebung abhören – einschließlich der Erkennung von Schüssen – und ihre Position kennen. Mit der Erkennung von Smartphones über WLAN, Gesichtserkennung und Bewegungsanalyse ergibt sich daraus die Möglichkeit einer umfassenden Überwachung.

Wohin das führt, ist an anderer Stelle bereits zu erkennen:

*„Während in Deutschland noch mit Begriffen wie Nachhaltigkeit, Umweltschutz, Effizienz und Bequemlichkeit für die Smart City geworben wird, sprechen die Technologiefirmen in China, Dubai und der Türkei offen aus, um was es geht: Lückenlose Überwachung und Kontrolle der Bevölkerung.“*

Besonders weit bei der Überwachung ist China:

*„In Shenzhen, der südchinesischen Sonderwirtschaftszone in unmittelbarer Nachbarschaft zu Hongkong, werden Menschen, die bei Rot über die Straße gehen, identifiziert und sogleich auf großen Monitoren mit Angabe ihrer Personalien an den Pranger gestellt, es wird ein Bußgeld berechnet und der Arbeitgeber benachrichtigt. Außerdem gibt es Punktabzug bei ihrem „Social Score“, der darüber entscheidet, ob sie eine Wohnung, einen Job, einen Studienplatz bekommen.“*

Doch auch in Deutschland hat der Ausbau der Überwachung schon begonnen: Am Bahnhof Berlin-Südkreuz wird intelligente Videoüberwachung durch die Bundespolizei getestet. Im Koalitionsvertrag der „großen“ Koalition wird die Weiterentwicklung zu „intelligenter“ Überwachungstechnik vereinbart.

*„Wir haben die Wahl: Wollen wir in einer post-demokratischen Konsumwelt leben, in der andere für uns entscheiden und die einzig mögliche Antwort „ok“ ist? Oder wählen wir die Freiheit?“,*

so die Laudatorin abschließend.

Die vollständige Laudatio von Rena Tangens ist ab Seite 61 nachzulesen.

## Kategorie *Technik*

Der BigBrotherAward in der Kategorie *Technik* ging in diesem Jahr an **Microsoft Deutschland für die kaum deaktivierbare Telemetrie in ihrem Betriebssystem *Windows 10*, die selbst für versierte Nutzerinnen und Nutzer fast nicht zu verhindern ist**. Die Laudatio hielt Frank Rosengart.

*„Mit der Einführung von Office 365 und Windows 10 ist Microsoft einem allgemeinen Trend gefolgt: Viele Daten werden jetzt in der Cloud gespeichert, die Software wird abonniert, anstatt einmalig gekauft und Microsoft als Konzern ist sehr neugierig, was die Nutzerinnen und Nutzer so treiben. Allein schon für die Lizenzaktivierung ist eine Online-Verbindung erforderlich. Möchte ich aus gutem Grund auf eine Internet-Verbindung verzichten, ist das mit Windows 10 praktisch nicht mehr möglich.“*


*Laudatio von Frank Rosengart – Foto: Fabian Kurz, CC BY-SA 4.0*

Es sei heutzutage normal, dass Geräte oder Programme „nach Hause telefonieren“, um beispielweise statistische Daten an den Hersteller zu übermitteln. Bei Microsoft geht das mittlerweile sehr weit: Es werden Informationen übermittelt, welche Programme auf dem System installiert sind, aber auch beispielweise, wie häufig mit *Alt+Tab* zwischen Programmen hin- und hergeschaltet wird. Offen bleibt, was der Hersteller Microsoft mit diesen Informationen macht, wie und wofür er sie nutzt.

Nach einiger Suche findet man ein Menge an Schaltern, mit denen man die Übermittlung ausschalten kann. Der Datenschutz by Default and by Design, den die europäische Datenschutz-Grundverordnung vorgibt, müsste verlangen, dass alle diese Schalter zu Beginn auf *keine Übermittlung* gestellt sind – Laudator Rosengart empfiehlt, darauf ein Auge zu haben. Es gebe aber Informationen anderer Anwendungen unter Windows 10, die sich nicht abschalten ließen. Auch bei „abschaltbaren“ Datenübermittlungen hat man nur die Wahl zwischen einfacher und vollständiger Übermittlung – die Option keine Übermittlung fehlt.

Der Bayerische Beauftragte für den Datenschutz stellt in einer Studie fest, dass

*„Selbst wenn sämtliche Telemetrie-Einstellungen über knapp 50 Änderungen in der sogenannten Registry verändert werden (die ausdrücklich nur für ExpertInnen gedacht ist und die das Potential hat, den Rechner durch einen unbedachten Eingriff unbrauchbar zu machen), senden Windows 10-Rechner immer noch jede Menge Anfragen an Internet-Dienste für Kacheln, Updates oder Empfehlungsdienste. Dort wird mindestens die IP-Adresse des Nutzers registriert, bereits ohne dass man bewusst*

*eine Webseite aufgerufen hätte. Möglich ist eine Änderung der Registry überhaupt nur in der „Enterprise"-Variante von Microsoft, also für Geschäftskunden."*

Nicht zuletzt hatte auch Caspar Bowden als Datenschutzberater von Microsoft bereits 2011 auf die Zugriffsmöglichkeiten von Geheimdiensten auf die Daten in der Cloud hingewiesen. Er wurde dafür gefeuert. „Dadurch, dass Windows 10 nun auch noch ständig ‚nach Hause telefoniert'", so schließt die Laudatio, „werden Microsoft-Produkte zu einem nicht mehr tragbaren Problem!"

## Kategorie *Verwaltung*

Den BigBrotherAward in der Kategorie *Verwaltung* erhielt die **Cevisio Software und Systeme GmbH für die Software QMM (Quartiermanagement), die das Management von Flüchtlingsunterkünften ermöglicht und dabei die Bewohner dieser Unterkünfte umfassend überwacht.** Die Laudatio hielt Thilo Weichert:

> *„Mit dieser Software werden Bewegungen zum und auf dem Gelände, Essenausgaben, medizinische Checks wie durchgeführte Röntgen-, Blut- und Stuhluntersuchungen, Verwandtschaftsverhältnisse, Religions- und Volkszugehörigkeiten und vieles mehr erfasst und gespeichert. Die Daten ermöglichen eine Totalkontrolle der Flüchtlinge und zeigen anschaulich, auf wie vielen Ebenen Privatsphäre verletzt werden kann."*

Doch nicht nur die damit verbundenen Datenschutzverstöße machen die Preiswürdigkeit dieser Software aus. Auch das dahinter stehende Menschenbild spielt eine Rolle:

> *„Flüchtlinge sind Menschen, keine Sachen. [...] Sie suchen Schutz bei uns und haben Rechte – Menschenrechte und Grundrechte, die für Cevisio keine Rede wert sind."*

Die Software wurde von der Cevisio GmbH gemeinsam mit dem Deutschen Roten Kreuz Landesverband Sachsen entwickelt. Laut Eigendarstellung wird sie in 280 Aufnahmeeinrichtungen eingesetzt und die Daten von mehr als 380.000 Flüchtlingen damit verwaltet. Die Daten werden mit denen des Bundesamts für Migration und Flüchtlinge (BAMF) und den Ausländerbehörden zusammengeführt. Erfasst werden die wesentlichen Angaben zur Person einschließlich medizinischer Daten, Verwandte und „sämtliche Dokumente". Auch die Abrechnung der Kosten wird über die Software abgewickelt. Über einen RFID-Chip melden sie die Personen an Lesegeräten an; so kann jederzeit ihr Aufenthaltsort in der Aufnahmeeinrichtung nachvollzogen werden. Das gleiche gilt für den Empfang von Mahlzeiten einschließlich eines Hinweises auf die „Mehrfachausgabe" an eine Person.

Im Fazit weist Weichert abschließend auch auf die Verantwortung der HerstellerInnen einer solchen Überwachungssoftware hin:

> *„Beim Umgang mit den Daten von Flüchtlingen müssen wir besonders umsichtig sein. […] Die Regierungen der Länder, aus denen Menschen zu uns flüchten, quälen ihre Bevölkerung nicht selten durch Kontrolle, Willkür und Verwendung von dem, was sie über diese Menschen wissen. Die Gefahr, dass wir bei der Datenverwaltung à la Cevisio bestehende Traumata vertiefen, und auch die Gefahr, dass unsere Datensammlungen in falsche Hände geraten, etwa von Geheimdiensten des Heimatlandes, ist groß. Auch Software-Unternehmen haben eine Verantwortung dafür, dass solche Gefahren gebannt werden. Wir sollten uns bewusst machen: Was heute an Flüchtlingen praktiziert wird, wird morgen vielleicht schon auf uns angewendet."*

Die vollständige Laudatio von Thilo Weichert ist ab Seite 63 nachzulesen.

## Kategorie *Verbraucherschutz*

Selbst durfte sich der Preisträger in der Kategorie Verbraucherschutz ansagen: „Der BigBrotherAward 2018 in der Kategorie *Verbraucherschutz* geht an die Firma **Amazon, für ihren Sprachassistenten Alexa**", antwortete dieser auf die von Laudator padeluun gestellte Frage.

Alexa erhält den Preis stellvertretend für eine Reihe ähnlicher Assistenten wie Apple Siri, Google Assistant, Microsoft Cortana, Samsung Bixby und Nuance; der Sprachassistent von Amazon sei aber der preiswürdigste.

> *„Das Gerät lauscht 24 Stunden am Tag in meiner Wohnung, weil es darauf lauert, dass ich das Wort „Alexa" sage. Sobald es dieses Wort ‚hört', zeichnet es die nachfolgenden Sätze auf und sendet diese zur Analyse zu den Rechnern in der Amazon-Cloud. Dort wird mein Text übersetzt, analysiert und dann werden Aktionen fernausgelöst. Zum Beispiel wird ein Timer oder Wecker gestellt, Musik, meiner Stimmung entsprechend – oder was das Gerät dafür hält – abgespielt, ein Trommelwirbel gestartet oder auf Amazon ein neuer Goldhamster bestellt",*

so padeluun weiter.

Eigentlich könnte damit alles gesagt sein – doch Laudator padeluun schlägt noch einen Bogen zu der Laudatio von Rena Tangens und der *Smart City* mit der „perfekten Verbindung des totalitären Überwachungsstaates aus George Orwells ‚1984' und den normierten, nur scheinbar freien Konsumenten in Aldous Huxleys ‚Schöne Neue Welt'". Zu Hause Alexa, im öffentlichen Raum die „smarten" Straßenlaternen, die uns in allen Situationen überwachen. „Skylla und Charybdis in einem", so padeluun. Er habe sich angewöhnt, beim Betreten eines fremden Haushalts zunächst „Alexa, bestelle 100 große Dosen Ravioli" zu rufen und die Reaktion der Inhaber zu beobachten, ob er sich in einem verwanzten Haus befinde.

Zweifellos sei der Komfort, den die Sprachschnittstelle biete, angenehm. Doch alle Informationen, die Alexa aufnimmt, werden bei Amazon gespeichert – der Konzern „weiß" dadurch sehr viel. Ob der Sprachassistent auch aufzeichnet, wenn man gerade nicht „Alexa" gerufen hat, ist nicht ohne weiteres festzustellen – die an Amazon übermittelten Daten werden verschlüsselt und sind damit nicht direkt verfolgbar.

Will man in die Zukunft der Sprachassistenten schauen, lohnt sich ein Blick auf die bereits angemeldeten Patente:

> *„Die Konzerne halten nicht nur Patente dafür, zu erkennen, WER spricht, sondern auch, aus der Stimme zu erkennen, in welcher Stimmung man gerade gerade ist. […] Wenn Mama vormittags verzweifelt weint, wird gleich Klosterfrau Melissengeist geliefert. Der Ruf ‚Alexa, Musik' spielt dann entsprechend des Psychogramms, das dem Konzern geläufig ist, Punkrock oder Gregorianische Choräle ein. Oder Amazon ruft präventiv die Polizei, die die Wohnung ‚swattet', wenn die Algorithmen aus der Stimme den Eindruck gewinnen, dass jemand vielleicht gleich ein Attentat verüben will."*

Außerdem ist Alexa ein lernendes System: Es versucht, anhand von Parametern wie Stimme, Intonation oder bestimmten Wörtern immer besser unsere Wünsche zu erkennen – und mit entsprechender Werbung gleich zu befriedigen. Das „Ausforschen von Menschen und ihren Angewohnheiten, ihren geheimsten Wünschen, ihren Freundschaften, ihren politischen Überzeugungen bis hin zu ihren Gesundheitsproblemen das Geschäftsmodell dieser Konzerne" ist das Geschäftsmodell von Konzernen wie Google, Facebook – und Amazon.

Doch auch die NutzerInnen sind in die Verantwortung zu nehmen. Deswegen schloss die Laudatio mit einem Appell: „Liefert Euch nicht aus, behaltet Eure Widerstrebsamkeit, ohne die Zivilisation und Demokratie nicht lebendig existieren können."

## Kategorie Politik

Das kam vielleicht für einige unerwartet: Der BigBrotherAward in der Kategorie *Politik* ging in diesem Jahr an die **Fraktionen von CDU und Bündnis 90/Die Grünen im Hessischen Landtag für ihr geplantes neues Verfassungsschutzgesetz und die Novellierung des Hessischen Polizeigesetzes**. Die Laudatio hielt Rolf Gössner.

Einleitend zählte Rolf Gössner die wichtigsten Regelungen des geplanten Gesetzes auf:

1. *Der Inlandsgeheimdienst „Verfassungsschutz" soll auch vorbestrafte V-Leute rekrutieren und kriminell gewordene Verfassungsschutz-MitarbeiterInnen weiter einsetzen und abschöpfen können. [...]*

2. *Erlaubt werden soll auch, Berufsgeheimnisträger wie Ärzte, Anwälte oder Journalisten als V-Leute anzuheuern oder V-Leute in deren beruflichem Umfeld zu platzieren. [...]*

3. *Selbst Daten über Minderjährige unter 14 Jahren, also von Kindern, sollen in Dateien und Akten des Verfassungsschutzes erfasst und gespeichert werden dürfen. [...]*

4. *Der Verfassungsschutz soll ermächtigt werden, personenbezogene Überwachungsdaten an öffentliche Stellen zu übermitteln – und zwar zur „Überprüfung der Verfassungstreue von Personen, die sich um Einstellung in den öffentlichen Dienst bewerben". [...]*

5. *Spionage-Programme, also sogenannte Staatstrojaner, sollen künftig über gefundene oder aufgekaufte Sicherheitslücken in Computern oder Smartphones Verdächtigter eingeschleust werden, um sie präventiv per Onlinedurchsuchung oder Quellen-Telekommunikationsüberwachung (TKÜ) umfassend ausforschen zu können. [...]*

> *Und die Polizei soll künftig u. a. ermächtigt werden, sogenannte „Gefährder" vorsorglich in elektronische Fußfesseln zu legen, um ihren Aufenthalt, ihre Bewegungen und Kontakte über Wochen und Monate lückenlos kontrollieren zu können. [...]*

„Mit dieser Gesetzesinitiative geht die schwarz-grüne Regierungskoalition in Hessen einen großen Schritt in Richtung präventiv-autoritärer Sicherheitsstaat", so Gössner weiter. Während man von der CDU mittlerweile nichts anderes mehr erwartet, ist die Beteiligung von Bündnis 90/Die Grünen verstörend. Offenbar haben sie derzeit ein ungeklärtes Verhältnis zu den Bürgerrechten. Gössner weiter: „Interessanterweise klagt die grüne Oppositionsfraktion im bayerischen Landtag gegen das dortige Verfassungsschutzgesetz[2] – ausgerechnet gegen ein Gesetz, das sich das hessische Regierungsbündnis unter Mitwirkung der Grünen zum Vorbild genommen hat." Es wäre noch hinzuzufügen, dass sich die Landtagsfraktion mit ihrer Entscheidung gegen das Votum ihrer eigenen Basis auf dem Landesparteitag gewendet hat.

Anhand zweier Beispiele illustrierte der Laudator anschließend die Auswirkungen eines solchen Gesetzes: Der heimliche Angriff auf Computer und Smartphones mit Staatstrojanern und elektronische Fußfesseln zur Aufenthaltskontrolle von Gefährdern. Zusammengefasst:

1. *Die künftig gesetzlich abgesicherte Zusammenarbeit mit vorbestraften und kriminell gewordenen V-Leuten widerspricht rechtsstaatlichen Grundsätzen.*

2. *Die geplante geheimdienstliche Regelüberprüfung künftiger Mitarbeiter.innen von Demokratieprojekten bedeutet Gesinnungsschnüffelei und erinnert an unselige Zeiten grundrechtswidriger Berufsverbote.*

3. *Verhaltenssteuernde und freiheitsberaubende elektronische Fußfesseln verletzen Privatsphäre und Persönlichkeitsrechte – und letztlich auch die Menschenwürde.*

4. *Und Staatstrojaner bedrohen den Kernbereich privater Lebensführung und gefährden Sicherheit und Vertraulichkeit des IT-Systems.*

Gössners Fazit: „Mit solchen Geheimdienst- und Polizeigesetzen, wie im schwarz-grün regierten Hessen geplant oder im grün-schwarz regierten Baden-Württemberg teilweise schon umgesetzt, können die Grünen ihr Selbstverständnis als Bürgerrechtspartei allmählich begraben." Er wies abschließend auf Initiativen für Verfassungsbeschwerden gegen das Gesetz hin und rief dazu auf, solche Verfassungsbeschwerden als Akt bürgerrechtlicher Notwehr zu unterstützen.

Die vollständige Laudatio von Rolf Gössner ist ab Seite 65 nachzulesen.

### Publikumspreis

Der Preis aus der *Publikumswahl* ging mit großer Mehrheit an den Gewinner des BigBrotherAwards in der Kategorie *Politik*, die **Fraktionen von CDU und Bündnis 90/Die Grünen im Hessischen Landtag**. Einige Kommentare dazu auf den Abstimmungszetteln:

- *Die Grundrechte, die der Staat besonders zu schützen hat, sind die Basis für alles andere!*
- *Ich finde es schlimm, dass die Politik die Bürger nicht schützt, sondern kriminalisiert!*
- *Die Unwissenheit, mit der die Politik an dieses Gesetz herangeht, ist absolut niederschmetternd. Entgegen jeglicher Empfehlungen von ExpertInnen versuchen die Fraktionen CDU und Grüne, wieder einmal ein Überwachungsgesetz durchzupeitschen.*
- *Schade, dass es den Grünen so leicht fällt, die Ideale der Freiheits- und Bürgerrechtsbewegung für etwas politische Macht zu opfern.*

### Anmerkungen

1 Weitere Informationen und Nachweise finden sich auf der Webseite der BigBrotherAwards, http://www.bigbrotherawards.de. Von dort stammen auch alle Zitate aus den Laudationes.

2 Vgl. Süddeutsche Zeitung vom 4. August 2017, http://www.sueddeutsche.de/bayern/innere-sicherheit-landtags-gruene-klagen-gegen-verfassungsschutzgesetz-1.3614760.

**Rena Tangens**

## Kategorie PR & Marketing – Laudatio

### Der BigBrotherAward in der Kategorie „PR & Marketing“ geht an das Konzept der „Smart City“!

Das *Smart City*-Konzept propagiert die „Safe City“: die mit Sensoren gepflasterte, total überwachte, ferngesteuerte und kommerzialisierte Stadt. *Smart Cities* reduzieren Bürger auf ihre Eigenschaft als Konsumenten, machen Konsumenten zu datenliefernden Objekten und unsere Demokratie zu einer privatisierten Dienstleistung.

Eine *Smart City* ist die perfekte Verbindung des totalitären Überwachungsstaates aus George Orwells *1984* und den normierten, nur scheinbar freien Konsumenten in Aldous Huxleys *Schöne Neue Welt*.

Der Begriff *Smart City* ist eine schillernd-bunte Wundertüte – er verspricht allen das, was sie hören wollen: Innovation und modernes Stadtmarketing, effiziente Verwaltung und Bürgerbeteiligung, Nachhaltigkeit und Klimaschutz, Sicherheit und Bequemlichkeit, für Autos grüne Welle und immer einen freien Parkplatz. Angefangen hat das 2008 mit IBM und ihrem Werbeslogan vom *Smarter Planet*, mit dem sie sagen wollten, dass sie unseren Planeten „schlauer“ machen können. Im Business tummeln sich inzwischen eine Menge weiterer Firmen, die ihre Dienstleistungen an Städte verkaufen wollen, zum Beispiel Siemens, Microsoft, Cisco, Huawei, Hitachi und Osram.

Doch wie sieht so eine *Smart City* konkret aus?

Als große Errungenschaft für eine *Smart City* wird zum Beispiel ein neuer Typ Straßenlaterne angepriesen. Die leuchtet nicht nur, sondern enthält auch gleich Videoüberwachung, Fußgänger-Erkennung, Kfz-Kennzeichenleser, Umweltsensoren, ein Mikrophon mit Schuss-Detektor und einen Location-Beacon zum Erfassen der Position. Stellen wir uns dies noch kombiniert mit WLAN vor, mit dem die Position von Smartphones ermittelt werden kann, Gesichtserkennung und Bewegungsanalyse, dann ist klar: Wenn diese Technik in unsere Stadt kommt, werden wir keinen Schritt mehr unbeobachtet tun.

> *„Mit der heutigen Technologie (…) können vollkommen sichere Städte gestaltet werden. Die neue Gesichtserkennungstechnologie ermöglicht es Regierungen und privaten Unternehmen, alle Gesichter zu erkennen und zu archivieren, während dies zuvor auf eingetragene Straftäter beschränkt war,“*

schwärmt der türkische Überwachungstechnik-Anbieter Ekin in einer Pressemeldung über die *Safe City*. Das Gesichtserkennungssystem ordnet den Merkmalen jedes Gesichts eine ID zu, mit der eine Person später wiedererkannt werden kann, auch wenn ihr Name nicht bekannt ist, und analysiert außerdem Alter, Geschlecht und Ethnie.

Während in Deutschland noch mit Begriffen wie Nachhaltigkeit, Umweltschutz, Effizienz und Bequemlichkeit für die *Smart City* geworben wird, sprechen die Technologiefirmen in China, Dubai und der Türkei offen aus, um was es geht: Lückenlose Überwachung und Kontrolle der Bevölkerung.

In China boomt die Kombination von Videoüberwachung und Künstlicher Intelligenz. Der chinesische Marktführer für Gesichtserkennungssoftware, SenseTime, freut sich über „die hohe Nachfrage, die von Smart Cities und Überwachung angetrieben wird“[1].

In Shenzhen, der südchinesischen Sonderwirtschaftszone in unmittelbarer Nachbarschaft zu Hongkong, werden Menschen, die bei Rot über die Straße gehen, identifiziert und sogleich auf großen Monitoren mit Angabe ihrer Personalien an den Pranger gestellt, es wird ein Bußgeld berechnet und der Arbeitgeber benachrichtigt. Außerdem gibt es Punktabzug bei ihrem *Social Score*, der darüber entscheidet, ob sie eine Wohnung, einen Job, einen Studienplatz bekommen.

Die ganze Provinz Xinjiang im Nordwesten Chinas ist inzwischen ein Echtzeit-Labor für Massenüberwachung. Dort werden von der gesamten Bevölkerung zwischen 12 und 65 Jahren DNS und Blutgruppe getestet, Iris-Scans, Fingerabdrücke und 3D-Bilder erstellt – im Rahmen einer sogenannten „kostenlosen Gesundheitsuntersuchung“[2]. Dazu hat die chinesische Regierung 2017 in Xinjiang ein Überwachungssystem installiert, das die Polizei automatisch informiert, wenn ein Verdächtiger sich mehr als 300 Meter von seiner Wohnung oder seinem Arbeitsplatz entfernt[3]. Verdächtig sind nicht nur Kriminelle, sondern auch Angehörige der muslimischen Minderheit oder Personen, die sich für Menschenrechte einsetzen.

Sie meinen, China ist weit weg?

Nun, am Bahnhof Südkreuz in Berlin testet die Bundespolizei seit August 2017 intelligente Videoüberwachung mit Gesichtserkennung. Das ist der Anfang. Denn völlig egal, wie der „Test“ ausgeht – Ex-Innenminister Thomas de Mazière hat schon zu Beginn dieses Freilandversuchs betont, dass Gesichtserkennung bundesweit an möglichst vielen öffentlichen Orten eingeführt werden soll. Und der neue Innenminister Horst Seehofer hat längst bestätigt, dass er das auch so sieht. Mehr noch: Die neue Bundesregierung hat in ihrem Koalitionsvertrag bereits eine Weiterentwicklung zu einer „intelligenten“ Videoüberwachung vorgemerkt. Geschmackvolle Straßenlaternen mit Überwachungskameras und Sensoren können Sie übrigens auch bereits in *Arcadia*, einer Gated Community in Potsdam, besichtigen.

Oder schauen wir mal in unser direktes Nachbarland, nach Holland, wo die *Smart Cities* wie Tulpen aus dem Boden sprießen: Die Stadt Enschede will wissen, wer sich wie oft wo lang bewegt und trackt dafür alle Menschen, die ein Smartphone mit aktiviertem WLAN bei sich tragen, mit Hilfe der eindeutigen MAC-Adresse. Die Traffic-App von Enschede belohnt Menschen für gutes Verhalten – zu Fuß gehen, Fahrrad fahren, öffentliche Verkehrsmittel nutzen – ironischerweise mit einem Tag freiem Parken in der Stadt. Was man erst im Kleingedruckten der App findet: Die gesammelten persönlichen Bewegungsprofile gehen an eine Firma namens Mobidot.

In Eindhoven ist die Partymeile Stratumseind zu einem Überwachungslabor geworden: Dort gibt es Straßenlaternen mit WLAN-Tracking, Kameras und Mikrophonen, mit denen aggressives Verhalten erkannt werden soll. Ab Frühjahr 2018 soll bei Bedarf Orangenduft versprüht werden, um die Menschen zu beruhigen.

Utrecht schließlich überwacht die Jugendlichen der Stadt, wenn sie sich in den Straßen bewegen: Wie viele sind es? Welche Altersgruppe? Kennen sie sich? Wie gehen sie miteinander um? Und machen sie Ärger oder nicht? Seit 2014 hat Utrecht 80 „smarte“ Projekte in der Stadt und den Überblick verloren, was wo läuft, denn das meiste davon liegt in den Händen von Firmen.[4]

*Smart City*-Firmen sammeln Daten und weigern sich, darüber Auskunft zu geben. Sie geben oft auch den Städten selbst keinen Zugriff auf die Daten – denn die sind Firmengeheimnis! Der Eindruck drängt sich auf, dass sich die Städte von den Firmen über den Tisch ziehen lassen. Doch das können weder Bürgerinnen und Bürger noch Presse überprüfen, denn die Verträge, die die Städte mit den *Smart City*-Dienstleistern abschließen, dürfen zumeist nicht eingesehen werden – aus Wettbewerbsgründen.

Ja, „smarte“ Technik ist teuer. Wo soll das Geld herkommen? Städte lassen sich von günstigen Einstiegsangeboten locken und von den Landes- und EU-Fördermitteln.

Städte werden wieder einmal verlockt, ihre Infrastruktur in kommerzielle Hände abzugeben – wie in den 90er-Jahren beim Cross-Border-Leasing[5]. Das ist weder clever noch smart, sondern kurzsichtig und gefährlich.

Und es droht mehr als das billige Verscherbeln städtischer Infrastruktur: Städte verkaufen hier leichtfertig etwas, was ihnen gar nicht gehört, nämlich die Daten der Bürgerinnen und Bürger – und damit deren Privatsphäre, deren Autonomie und deren Freiheit.

Die Bürger werden nicht gefragt. Denn die Tech-Firmen wollen doch nur spielen – das kann man denen doch nicht übel nehmen! Bei innovativen Tech-Projekten müssen alle anderen Interessen schweigen: „Digital first, Bedenken second“. Das amerikanische Original heißt *Permissionless Innovation*[6], also „Innovation ohne Erlaubnis“. Das bedeutet: Das Vorsorgeprinzip wird außer Kraft gesetzt – wer behauptet, innovativ zu sein, muss sich nicht an lästige Regeln halten.

Den Firmen ist klar: Nicht der Service, sondern die Daten der Bürgerinnen und Bürger sind die eigentliche Cash Cow. Wer wüsste das besser als Alphabet, Googles Mutterfirma. Die hat sich gerade im kanadischen Toronto eingekauft, um das dortige Waterfront Viertel als *Smart City* zu entwickeln. Name des Projektes: *Sidewalk Labs*, also „Bürgersteig-Labor“. Google hat sich wohl nicht träumen lassen, wie viel Kritik und konkrete Nachfragen zu Datenschutz aus der kanadischen Bevölkerung kommen würden.[7] Sidewalk Labs hat mittlerweile die ehemalige Datenschutzbeauftragte von Kanada, Ann Cavoukian, eingestellt. Smart Move. Ann Cavoukian hat 2009 das Konzept der *Privacy by Design* entwickelt (also so etwas wie „eingebaute Privatsphäre“). *Smart Cities* aber sind eher *Surveillance by Design* (eingebaute Überwachung). Wir sind ehrlich gespannt, wie sie das Eine in das Andere bringen will, ohne das Geschäftsmodell von Google komplett umzukrempeln.

Doch wir wollen ja gar nicht so negativ sein. Denn eigentlich mögen wir Technik. Wir nehmen jetzt einfach mal an, dass die Hack-Sicherheit der vernetzten Systeme kein Problem wäre. Dass der Staat mit der Komplett-Überwachung ausschließlich unser Wohl im Auge hätte. Und dass die Tech-Firmen nur Gutes mit unseren Daten tun würden. Und jetzt stellen wir uns diese freundliche *Smart City* vor, deren Sensoren uns ständig begleiten, die uns sagen, was wir als Nächstes tun sollen und deren Algorithmen aus unserem Profil in Echtzeit unsere Wünsche errechnen, bevor wir sie selber kennen. Immer grüne Welle, immer sofort einen Parkplatz finden und stets die aktuellen Stickoxid-Werte der Umgebung auf meinem Handy – klingt das nicht verlockend?

Im Märchen vom Schlaraffenland fliegen den Menschen die gebratenen Gänse essfertig in den Mund. Aber: Das Schlaraffenland ist nicht das Paradies. Es macht satt, aber nicht glücklich. Bequemlichkeit macht träge und dumm. Wir brauchen das Beinahe-Stolpern, um unseren Gleichgewichtssinn zu trainieren. Wir brauchen die Anstrengung, um uns über das aus eigener Kraft Erreichte zu freuen. Wir brauchen den Zufall, das Andere, das Unbekannte, die Überraschung, die Herausforderung, um zu lernen und uns weiterzuentwickeln. Wir müssen uns als Menschen frei entscheiden können und es muss uns möglich sein, Fehler zu machen. Wie anders sollten wir unseren „Moral-Muskel" trainieren?

Auch deshalb müssen wir uns wehren gegen die Bevormundung durch Technik und Technik-Paternalismus.

Eine Stadt ist nicht „smart" – klug sind die Menschen, die darin leben.

Wir haben die Wahl: Wollen wir in einer post-demokratischen Konsumwelt leben, in der andere für uns entscheiden und die einzig mögliche Antwort „ok" ist?[8] Oder wählen wir die Freiheit?

Albus Dumbledore sagt in Harry Potter Band 4:

> *„Es wird die Zeit kommen, da ihr euch entscheiden müsst zwischen dem, was richtig ist und dem, was bequem ist."*

Die Zeit ist jetzt.

Herzlichen Glückwunsch zum BigBrotherAward, „Smart City"!

## Anmerkungen

1. *Quelle: https://www.forbes.com/sites/shuchingjeanchen/2018/03/07/the-faces-behind-chinas-omniscient-video-surveillance-technology/#36d3d504afc1*
2. *Quelle: Human Rights Watch, China: Minority Region Collects DNA from Millions – Private Information Gathered by Police, Under Guise of Public Health Program https://www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions*
3. *Quelle: The Guardian: China testing facial-recognition surveillance system in Xinjiang – report https://www.theguardian.com/world/2018/jan/18/china-testing-facial-recognition-surveillance-system-in-xinjiang-report*
4. *The Guardian: 'Living laboratories': the Dutch cities amassing data on oblivious residents https://www.theguardian.com/cities/2018/mar/01/smart-cities-data-privacy-eindhoven-utrecht*
5. *zeit.de, 12.3.2009 : Cross-Border-Leasing: Für dumm verkauft: http://www.zeit.de/2009/12/DOS-Cross-Border-Leasing/komplettansicht*
6. *Adam Thierer: Permissionless Innovation – The Continuing Case for Comprehensive Technological Freedom. Mercatus Center at George Mason University 2016.*
7. *Torontoist, October 30, 2017: Civic Tech: A list of questions we'd like Sidewalk Labs to answer https://torontoist.com/2017/10/civic-tech-list-questions-wed-like-sidewalk-labs-answer/*
8. *Siehe Buch von Marc-Uwe Kling: „Qualityland", ullstein, Berlin 2017*

**Thilo Weichert**

# Kategorie Verwaltung – Laudatio

## Der BigBrotherAward 2018 in der Kategorie Verwaltung geht an die Cevisio Software und Systeme GmbH aus Torgau

für ihre Software *Cevisio QMM* (Quartiermanagement), die in Zusammenarbeit mit dem Deutschen Roten Kreuz speziell für Flüchtlingsunterkünfte entwickelt wurde. Mit dieser Software werden Bewegungen zum und auf dem Gelände, Essenausgaben, medizinische Checks wie durchgeführte Röntgen-, Blut- und Stuhluntersuchungen, Verwandtschaftsverhältnisse, Religions- und Volkszugehörigkeiten und vieles mehr erfasst und gespeichert. Die Daten ermöglichen eine Totalkontrolle der Flüchtlinge und zeigen anschaulich, auf wie vielen Ebenen Privatsphäre verletzt werden kann.

Die Software ist nicht nur preiswürdig wegen der mit ihr möglichen Datenschutzverstöße, sondern vor allem wegen des Menschenbildes, das dahinter steht. Flüchtlinge sind Menschen, keine Sachen. Sie liegen nicht in einem Regal zur späteren Abholung und Verwendung, sie sind keine Gefangenen und bedürfen keiner verschärften Beobachtung. Sie suchen Schutz bei uns und haben Rechte – Menschenrechte und Grundrechte, die für Cevisio keine Rede wert sind.

Als 2015 viele Flüchtlinge nach Deutschland kamen, war das Chaos bei Behörden groß. Die Erhebung von Daten sowie die Organisation von Unterbringung und Versorgung stellten die Beteiligten vor große Herausforderungen. Der Mittelständler Cevisio erarbeitete mit dem Deutschen Roten Kreuz Landesverband Sachsen e. V. die Lösung. Das Unternehmen wirbt für seine Software auf seiner Homepage damit, dass sie in über 280 Aufnahmeeinrichtungen eingesetzt wird. Insgesamt würden „bereits mehr als 380.000 Flüchtlinge verwaltet."


*Dr. Thilo Weichert verleiht den BigBrotherAward – Foto M. Hornung CC BY-SA 4.0*

Über all diese Menschen liegen demnach in der Cevisio Quartiersmanagement-Software erfasste Daten vor. Basis für die Erfassung ist eine Ausweiskarte mit RFID-Chip oder Barcode. Mit dieser Karte bewegen sich die BewohnerInnen in ihrer Unterkunft und – so der Plan der Software-Macher – halten sie an verschiedenen Stellen vor ein Lesegerät: Am Ein- und Ausgang, bei der Essensausgabe, bei der Wäschestelle, wenn sie Taschengeld

bekommen, beim Ausleihen von Büchern oder Videofilmen, bei medizinischen Untersuchungen oder bei ehrenamtlicher Arbeit.

Diese in den Unterkünften erfassten sogenannten „Aktionen" führt die Software über Schnittstellen zusammen mit den Daten des Bundesamtes für Migration und Flüchtlinge – dem BAMF – und mit den Dateien der Ausländerbehörden. Erfasst werden u. a. Angaben zu bestehender Schwangerschaft, zu den verwandten Personen, medizinische Daten mit „Erst- und Folgeuntersuchungen inkl. Befund". Gewährleistet wird auch die Erfassung „sämtlicher Dokumente". Die Software ermöglicht damit nicht nur die „Verwaltung", sondern auch die (Zitat) „Abrechnung der Flüchtlinge". Sie erlaubt die „Erfassung sämtlicher Daten zum Asylverfahren, wie EASY-Optimierung und BAMF-Daten".

Das ist Totalkontrolle. Tagesabläufe, Gewohnheiten, Kontakte, Verwandtschaft, Gesundheitszustand, Asylstatus – alles an einem Ort. Verknüpft und auswertbar.

Manches ist sicher sinnvoll, z. B. Hinweise auf Allergien, oder ob spezielle Ramadan-Verpflegung gewünscht wird. Die Cevisio-Software geht aber deutlich weiter: In der Broschüre zum Funktionsumfang ist z. B. die Rede von der „Erfassung aller an eine Person ausgegebenen Mahlzeiten" sowie „Hinweis bei Mehrfachausgabe einer Mahlzeit an eine Person". Wofür braucht man das?

Ist es nötig, jede Bewegung ins Haus oder aus dem Haus heraus minutiös zu erfassen und zu speichern? Ja, sagt die besagte Broschüre (Zitat): „Über die integrierte Anwesenheitsübersicht ist immer sekundenaktuell erkennbar, welche Flüchtlinge und Helfer/Mitarbeiter sich aktuell in einer Unterkunft befinden. Neben einer reinen Kontrollfunktion ist diese Übersicht insbesondere im Katastrophenfall (Brand etc.) unverzichtbar."

„Unverzichtbar!" Es kommt einem fast seltsam vor, dass hunderttausende von Schulen, Kaufhäusern oder Jugendherbergen noch ohne eine solche sekundenaktuelle Übersicht auskommen. Sind die alle verantwortungslos?

Nein, das ist Leben. Inklusive einem gewissen Lebensrisiko. Die Datensammlung von Cevisio hingegen ist ein feuchter Traum für Überwachungs-Fanatiker. Wir sehen hier keinerlei Empathie mit Menschen, die auch wegen eines Lebens in Freiheit nach Deutschland geflüchtet sind.

Vielleicht ist es also Pragmatismus nach dem Motto „interessiert doch keinen", wenn das Wort „Datenschutz" in der 15-seitigen Systemdarstellung nicht ein einziges Mal vorkommt. Technische Datensicherheitsvorkehrungen verbergen sich hinter dem Begriff „Administration". Funktionalitäten zu den Betroffenenrechten, z. B. für eine Auskunftserteilung oder Transparenz für die Flüchtlinge, konnte ich nicht finden.

Auch in der Praxis gibt es Mängel: Die Datenschutzbeauftragte in Bremen äußert in ihrem aktuellen Jahresbericht[1] „erhebliche datenschutzrechtliche Bedenken". Speicherfristen waren viel zu lang. Weshalb jede Essensausgabe kontrolliert werden muss, erschloss sich ihr nicht. Die Speicherung der Gesundheitsdaten musste auf ihre Veranlassung massiv zurückgefahren werden. Bei Verwandtschaftsangaben wurde den Betroffenen keine Optionen eröffnet. Viele Fragen sind bis heute offen.

Die bremische Datenschutzkontrolle bezog sich nur auf wenige der Einrichtungen. Es besteht keine Gewähr und Kontrollmöglichkeit, dass in den anderen über 270 Einrichtungen rechtswidrige Überwachungsmöglichkeiten abgestellt werden. Die Rechtslage ist überall gleich und könnte, z. B. mit automatischen Löschfristen, in der Software voreingestellt sein. Cevisio könnte den Betreibern Hilfen und Hinweise zur Wahrung des Datenschutzes geben.

Wir fragen: Hat diese Softwaregestaltung damit zu tun, dass hier Flüchtlinge die Betroffenen sind? Sicher – Flüchtlingsunterkünfte sind logistisch komplexe Systeme und die Betreiber wie das DRK und andere können digitale Unterstützung gut gebrauchen. Doch wie sollen Flüchtlinge sich bei uns integrieren, wenn ihnen dabei die Werte unserer gern beschworenen Leitkultur vorenthalten werden, also die Werte unseres Grundgesetzes? Zu diesen Werten gehört Selbstbestimmung, das Recht auf informationelle Selbstbestimmung.

Die Cevisio Software *Quartiersmanagement* steht nur exemplarisch für einen bevormundenden, intransparenten und überwachungsgierigen Umgang mit Flüchtlingen generell. Da gibt es Schweigepflichtentbindungen der Bundesagentur für Arbeit, die alle und jeden von der Vertraulichkeit entbinden, einschließlich Sozialämter und Migrationsberatungsstellen. In einem sogenannten Datenaustauschverbesserungsgesetz wurde 2016 festgelegt, dass praktisch jede Stelle jede andere über Flüchtlinge unterrichten darf, wenn es erforderlich erscheint. Um die Herkunft von Flüchtlingen bestimmen zu können, ließ sich das BAMF den Zugriff auf die Smartphones der Flüchtlinge genehmigen, auf denen sämtliche Kommunikationen und viel Privates gespeichert sind.

Gleichzeitig berichten unabhängige Flüchtlingsberatungen, dass ihnen manche Behörden mit dem Verweis auf den Datenschutz Informationen verweigern, die für Beratung und Hilfestellung wichtig wären. Hier wird der Datenschutz als falscher Vorwand missbraucht, um soziale Arbeit zu behindern.

Beim Umgang mit den Daten von Flüchtlingen müssen wir besonders umsichtig sein. Sowohl die Nationalsozialisten als auch das DDR-Regime haben mit Informationen und Datenerfassung ihre Bevölkerung kontrolliert und malträtiert. Die Regierungen der Länder, aus denen Menschen zu uns flüchten, quälen ihre Bevölkerung nicht selten durch Kontrolle, Willkür und Verwendung von dem, was sie über diese Menschen wissen. Die Gefahr, dass wir bei der Datenverwaltung à la Cevisio bestehende Traumata vertiefen, und auch die Gefahr, dass unsere Datensammlungen in falsche Hände geraten, etwa von Geheimdiensten des Heimatlandes, ist groß. Auch Software-Unternehmen haben eine Verantwortung dafür, dass solche Gefahren gebannt werden. Wir sollten uns bewusst machen: Was heute an Flüchtlingen praktiziert wird, wird morgen vielleicht schon auf uns angewendet.

Herzlichen Glückwunsch zum BigBrotherAward 2018 in der Kategorie Verwaltung, Cevisio.

## Anmerkung

1 *https://www.datenschutz.bremen.de/sixcms/media.php/13/40.%20JB%20Datenschutz.pdf*

Rolf Gössner

# Kategorie Politik – Laudatio

## Der BigBrotherAward 2018 in der Kategorie Politik geht an die Fraktionen von CDU und Bündnis90/Die Grünen im hessischen Landtag.



Die beiden Regierungsfraktionen erhalten den Negativpreis für ihr geplantes neues Verfassungsschutzgesetz und für die geplante Novellierung des hessischen Polizeigesetzes. Ihre Gesetzesinitiative enthält eine gefährliche Ansammlung gravierender Überwachungsermächtigungen, die tief in Grundrechte eingreifen und den demokratischen Rechtsstaat bedrohen. Die schlimmsten Regelungen im Überblick:

1. Der Inlandsgeheimdienst „Verfassungsschutz" soll auch vorbestrafte V-Leute rekrutieren und kriminell gewordene Verfassungsschutz-MitarbeiterInnen weiter einsetzen und abschöpfen können. Das tut er zwar schon heute, wie die Praxis zeigt; neu aber ist, dass dies erstmals gesetzlich abgesichert werden soll und kriminelle V-Leute ganz legal der strafrechtlichen Verfolgung entzogen werden können – anstatt solche V-Leute unverzüglich abzuschalten. Ein rechtsstaatswidriger Freibrief für kriminelles Handeln in staatlicher Mission. Diese Regelung legalisiert praktisch die bisherigen Skandale und mit ihnen die obszönen Verflechtungen des Verfassungsschutzes in rassistische, kriminelle und gewalttätige Neonaziszenen.

2. Erlaubt werden soll auch, Berufsgeheimnisträger wie Ärzte, Anwälte oder Journalisten als V-Leute anzuheuern oder V-Leute in deren beruflichem Umfeld zu platzieren. Damit werden die Verschwiegenheitspflichten und zu schützenden Vertrauensverhältnisse zu ihren Mandanten, Patienten oder Informanten verletzt. Nur Abgeordnete und ihre MitarbeiterInnen sollen vor dieser geheimdienstlichen Instrumentalisierung und Ausforschung ausdrücklich geschützt werden.

3. Selbst Daten über Minderjährige unter 14 Jahren, also von Kindern, sollen in Dateien und Akten des Verfassungsschutzes erfasst und gespeichert werden dürfen. Diese frühzeitige geheimdienstliche Stigmatisierung kann fatale Folgen für die weitere Entwicklung der Betroffenen haben – etwa bei der späteren Berufswahl, Lehrstellen- oder Jobsuche.

4. Der Verfassungsschutz soll ermächtigt werden, personenbezogene Überwachungsdaten an öffentliche Stellen zu übermitteln – und zwar zur „Überprüfung der Verfassungstreue von Personen, die sich um Einstellung in den öffentlichen Dienst bewerben". Das erinnert fatal an die menschenrechtswidrige Berufsverbotspraxis früherer Zeiten. Auch Organisationen und künftigen MitarbeiterInnen staatlich geförderter Demokratie- und Präventionsprojekte, etwa gegen Rechtsextremismus oder Salafismus, drohen anlasslose geheimdienstliche Überprüfungen – womit sie pauschal zu Sicherheitsrisiken erklärt und unter Generalverdacht gestellt werden. Dieses gesetzliche Misstrauensvotum untergräbt Akzeptanz und Vertrauen, die für eine erfolgreiche Arbeit solcher zivilgesellschaftlichen Projekte unerlässlich sind.

5. Spionage-Programme, also sogenannte Staatstrojaner, sollen künftig über gefundene oder aufgekaufte Sicherheitslücken in Computern oder Smartphones Verdächtigter eingeschleust werden, um sie präventiv per Onlinedurchsuchung oder Quellen-Telekommunikationsüberwachung (TKÜ) umfassend ausforschen zu können.

6. Und die Polizei soll künftig u. a. ermächtigt werden, sogenannte „Gefährder" vorsorglich in elektronische Fußfesseln zu legen, um ihren Aufenthalt, ihre Bewegungen und Kontakte über Wochen und Monate lückenlos kontrollieren zu können. Das sind Menschen, die keine Straftaten begangen haben, sondern denen die Polizei aufgrund bestimmter Anhaltspunkte künftige Straftaten zutraut.


*Dr. Rolf Gössner bei seiner Laudatio – Foto: F. Kurz, CC BY-SA 4.0*

### Auf dem Weg in den präventiv-autoritären Sicherheitsstaat

Mit dieser Gesetzesinitiative geht die schwarz-grüne Regierungskoalition in Hessen einen großen Schritt in Richtung präventiv-autoritärer Sicherheitsstaat. Mit besonders prekären Regelungen reiht sie sich damit in die bundesweiten Reformen ein, mit denen u. a. der Staatstrojaner zur Quellen-TKÜ und Online-Durchsuchung sowie die elektronische Fußfessel für „Gefährder" legalisiert werden. So etwa im BKA-Gesetz (2017), in der Strafprozessordnung (2017), in den Geheimdienstgesetzen Baden-Württembergs (2017) und Bayerns (2016). Interessanterweise klagt die grüne Oppositionsfraktion im bayerischen Landtag gegen das dortige Verfassungsschutzgesetz[1] – ausgerechnet gegen ein Gesetz, das sich das hessische Regierungsbündnis unter Mitwirkung der Grünen zum Vorbild genommen hat.

Ursprünglich sollten die Verfassungsschutzgesetze in Bund und Ländern novelliert werden, um überfällige Konsequenzen zu ziehen aus den zahlreichen Missständen, Pannen und Skandalen im Zusammenhang mit der NSU-Mordserie und NSA-Massenüberwachung. Primäre Ziele müssten demnach sein, den Verfassungsschutz und seine Befugnisse wirksam rechtsstaatlich zu zähmen und die Kontrolle über ihn erheblich zu stärken. Doch stattdessen erhalten ausgerechnet diese demokratisch kaum kontrollierbaren Geheimbehörden des Bundes und der Länder – geschichtsvergessen muss man sagen – wieder unverdienten Auftrieb, werden abermals aufgerüstet und massenüberwachungstauglicher gemacht, anstatt die Bevölkerung endlich vor ihren klandestinen Machenschaften und Skandalen wirksam zu schützen. Das heißt: Der Verfassungsschutz geht gestärkt aus dem Desaster und seiner Skandalgeschichte hervor. Und auch die Polizei wird weiter hochgerüstet.

Was bedeutet das für unmittelbar Betroffene und für uns alle? Zwei Beispiele:

### 1. Heimlicher Angriff auf Computer und Smartphones mit Staatstrojanern

Der hessische Verfassungsschutz soll unter bestimmten Bedingungen erstmals mit technischen Mitteln heimlich „informationstechnische Systeme" angreifen dürfen – bei „Gefahr im Verzug" zunächst sogar ohne richterliche Anordnung. Das heißt im Klartext: Dieser Inlandsgeheimdienst darf zur verdeckten Informationsgewinnung Computersysteme mit Hilfe von Spionage-Programmen hacken – und zwar mit Hilfe der berüchtigten „Staatstrojaner", die im Land der Hessen auch „Hessentrojaner" heißen.[2] Diese Überwachungssoftware wird heimlich in Computer, Tablets oder Smartphones von Verdächtigten eingeschleust, um diese unter Ausnutzung von Sicherheitslücken zu infiltrieren. So können dann Quellen-Telekommunikationsüberwachungen oder Online-Durchsuchungen durchgeführt werden.

Mit diesen Methoden, die der Abwehr einer „dringenden Gefahr" dienen sollen, bricht der Staat massiv in Privatsphäre und Persönlichkeitsrechte, in Informationelle Selbstbestimmung und Meinungsfreiheit der Betroffenen ein: Denn damit können PC-Mikrofone und Webcams eingeschaltet sowie sämtliche laufenden Kommunikationsinhalte vor ihrer Verschlüsselung überwacht werden – inklusive SMS, Mails, Chats und Messenger-Dienste. Mit Hilfe der Trojaner kann der Geheimdienst auf sämtliche Datenbewegungen, auf alle gespeicherten Festplatten-Inhalte, auf Textdokumente, Gesundheits- und Finanzdaten, auf intimste Informationen, Fotos und Filme zugreifen – letztlich auf das gesamte digitale und vernetzte Leben der Betroffenen. Angesichts der hieraus entstehenden Persönlichkeits-, Kontakt- und Bewegungsprofile ist an den verfassungsrechtlich gebotenen Schutz des Kernbereichs persönlicher Lebensgestaltung praktisch nicht mehr zu denken – ganz abgesehen davon, dass solche Geheimmethoden weder gerichtlich noch parlamentarisch wirksam kontrollierbar sind. Es handelt sich um einen der schwersten staatlichen Grundrechtseingriffe mit totalitärem Potential – um einen Einbruch in alle Lebensbereiche bis hinein in die Gedanken- und Gefühlswelt der Betroffenen.

Diese digitale Waffe unterminiert darüber hinaus das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[3]: Denn der Verfassungsschutz muss Software-Sicherheitslücken ausfindig machen, um einen Staatstrojaner auf dem Gerät installieren und aktivieren zu können. Er wird versuchen, solche Schwachstellen für eigene Zwecke künftig weiter offenzuhalten – anstatt sie sofort schließen zu lassen, um Attacken Dritter abzuwehren, das IT-System insgesamt zu schützen und damit die Allgemeinheit. Stattdessen werden also mutwillig Sicherheitslecks als Einfallstore aufrechterhalten, über die auch andere Geheimdienste, Cyber-Kriminelle, Betrüger, Erpresser und Terroristen gefährliche Angriffe auf private, betriebliche oder staatliche Computersysteme ausführen können oder auf die kritische Infrastruktur insgesamt (etwa von Strom- und Wasserversorgern, des Krankenhaus-, Gesundheits- oder Verkehrswesens).

Dieses unverantwortliche Staatsverhalten öffnet Missbrauch und gefährlichen Cyberattacken Tür und Tor. Abschreckendes Beispiel: der Erpressungs-Trojaner *Wannacry*, der im Mai 2017 neben Privat-PCs auch Automobilkonzerne, Bahnunternehmen und Krankenhäuser lahmlegte und Schäden in Milliardenhöhe verursachte. Die dabei genutzte Sicherheitslücke war dem US-Auslandsgeheimdienst NSA bereits seit Jahren bekannt. Verantwortungsvolle Sicherheitspolitik, die diese Bezeichnung verdient, sieht anders aus. Denn es gehört zum Auftrag des Staates, seine Bürger zu schützen und Sicherheitslücken zu schließen, und nicht, sie mutwillig für eigene Trojaner sperrangelweit offenzuhalten – und damit auch für andere Cyberangreifer.

### 2. Beispiel: Elektronische Fußfesseln zur Aufenthaltskontrolle von Gefährdern

Die hessische Polizei soll künftig – wie seit 2017 das BKA auf Bundesebene – so genannte „terroristische Gefährder" präventiv in elektronische Fußfesseln legen sowie Meldepflichten, Aufenthaltsbeschränkungen, Hausarrest und Kontaktverbote verhängen können. Nach einer gerichtlichen Anordnung sollen diese Freiheitsbeschränkungen mit einer elektronischen Fußfessel über GPS lückenlos überwacht werden, selbst innerhalb von Wohnungen. Zulässig soll dies dann sein, so heißt es im schwarz-grünen Gesetzentwurf wörtlich, „wenn bestimmte Tatsachen die Annahme rechtfertigen", dass die betreffende Person „innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise" eine Straftat begehen wird, „oder deren individuelles Verhalten eine konkrete Wahrscheinlichkeit dafür begründet, dass sie innerhalb eines übersehbaren Zeitraums" eine Straftat begehen wird.

Die elektronische Überwachungsmaßnahme, mit der u. a. terroristische Straftaten verhütet werden sollen, ist auf höchstens drei Monate zu befristen, kann aber um jeweils drei Monate verlängert werden – das heißt im Zweifel: unbeschränkt. Weigern sich Betroffene gegen die Maßnahme, können sie mit richterlicher Entscheidung bis zu zehn Tage lang in Polizeigewahrsam gesteckt werden.

Solche eingriffsintensiven Polizeimaßnahmen, die lückenlose Bewegungsprofile liefern und Rückschlüsse auf die persönliche Lebensführung zulassen, sollen gegen sogenannte Gefährder verhängt werden – also gegen Menschen, die bislang nicht straffällig geworden sind, denen dies aber in Zukunft aufgrund bloßer Indizien und Annahmen oder unterstellter Absichten und Gesinnung polizeilicherseits zugetraut wird. Solche Prognosen für künftiges Verhalten können entweder aus polizeilichen oder geheimdienstlichen Persönlichkeits- und Kontaktprofilen oder auch aus Risikobewertungen per Computeranalyse (z. B. Precrime-Programm „Radar-iTE") resultieren. Doch wie lässt sich dabei verhindern, dass institutioneller Rassismus und Islamophobie zu folgenschweren Einschätzungen führen?

Derart gravierende Grundrechtseingriffe auf mehr oder weniger vage Mutmaßungen zu stützen, dürfte den Verfassungsgrundsatz der Verhältnismäßigkeit verletzen. Denn rund um die Uhr und in Echtzeit überwachte Aufenthalts- und Kontaktverbote schränken die Betroffenen, die ja als unschuldig zu gelten haben, unmittelbar in ihrer Handlungs- und Bewegungsfreiheit ein und verletzen ihre Privatsphäre und Persönlichkeitsrechte – und letztlich auch ihre Menschenwürde. Solche verhaltenssteuernden und freiheitsberaubenden Präventionsmaßnahmen gleichen letztlich einer vorweggenommenen Verdachtsstrafe – also einer rechtsstaatswidrigen Strafe ohne Tat.

Im Übrigen dürfte die elektronische Fußfessel, die ohnehin relativ leicht manipulierbar und entfernbar ist, im Ernstfall auch ungeeignet zur Verhinderung terroristischer Straftaten sein – besonders wenn es sich um potentielle Täter handelt, die zu allem entschlossen sind: So trug etwa einer der beiden Täter, die 2016 einem katholischen Pfarrer in der Normandie die Kehle durchtrennten, eine elektronische Fußfessel; und auch das Berliner Attentat auf dem Weihnachtsmarkt im Dezember 2016 hätte damit wohl kaum verhindert werden können – wohl aber mit anderen, längst gesetzlich erlaubten Polizeibefugnissen, die aber, wie sich herausgestellt hat, nicht genutzt worden sind.

### Zivilgesellschaftliche Proteste und innergrüner Streit um „Hessentrojaner"

Gegen die hessische Gesetzesinitiative regt sich heftiger Protest und Widerstand: Ein breites Bündnis von Demokratieprojekten sowie Bürgerrechts- und Datenschutz-Organisationen unterstützen eine gemeinsame Erklärung, in der sie die geplanten Verschärfungen ablehnen, weil sie Demokratie und Grundrechte schädigen.[4] Während einer Anhörung im Hessischen Landtag hat die überwiegende Mehrzahl der Sachverständigen die Gesetzespläne heftig kritisiert und erhebliche Änderungen angemahnt.[5]

Auch die grüne Basis in Hessen votierte schon Ende 2017 gegen die schwarz-grünen Pläne, speziell gegen die Legalisierung des „Hessentrojaners". Damit verweigerte sie der grünen Landtagsfraktion ihre Unterstützung.[6] Vollkommen zu Recht, lehnen doch die Grünen die Staatstrojaner generell ab und hatten doch die hessischen Grünen im letzten Wahlkampf versprochen, keine Online-Durchsuchung zur Gefahrenabwehr zuzulassen.[7] Doch die Landtagsfraktion bleibt stur und begründet ihr gebrochenes Versprechen mit „terroristischen Bedrohungen", die es nötig machten, die digitale Kommunikation weitgehender als bisher zu überwachen. Das miese Spiel mit der Angst vor Terror zur Beschränkung der Freiheitsrechte, um angeblich mehr Sicherheit zu erlangen, das haben die Grünen bislang eher gemieden und anderen überlassen, wie etwa der CDU/CSU oder auch der Großen Koalition. Die grüne Fraktion in Hessen aber spielt nun selbst beim Überwachungspoker mit, beteiligt sich am sicherheitspolitischen Überbietungswettbewerb und behauptet noch dreist, ihr Gesetzentwurf trage eine „grüne Handschrift".

Mit solchen Geheimdienst- und Polizeigesetzen, wie im schwarz-grün regierten Hessen geplant oder im grün-schwarz regierten Baden-Württemberg teilweise schon umgesetzt, können die Grünen ihr Selbstverständnis als Bürgerrechtspartei allmählich begraben.

Ich bringe die Kritik an der hessischen Gesetzesinitiative noch einmal auf den Punkt:

1. Die künftig gesetzlich abgesicherte Zusammenarbeit mit vorbestraften und kriminell gewordenen V-Leuten widerspricht rechtsstaatlichen Grundsätzen.

2. Die geplante geheimdienstliche Regelüberprüfung künftiger MitarbeiterInnen von Demokratieprojekten bedeutet Gesinnungsschnüffelei und erinnert an unselige Zeiten grundrechtswidriger Berufsverbote.

3. Verhaltenssteuernde und freiheitsberaubende elektronische Fußfesseln verletzen Privatsphäre und Persönlichkeitsrechte – und letztlich auch die Menschenwürde.

4. Und Staatstrojaner bedrohen den Kernbereich privater Lebensführung und gefährden Sicherheit und Vertraulichkeit des IT-Systems.

Das ist „digitale Inquisition", so Heribert Prantl von der Süddeutschen Zeitung. Und er fragt erstaunt, weshalb die allermeisten BürgerInnen sich das gefallen lassen.[8] Und liefert drei Antworten gleich mit: 1. wegen der Politik mit der Angst vor Terror, die die WählerInnen selbst maßlose Freiheitsbeschränkungen schlucken lässt, wenn sie angeblich mehr Sicherheit versprechen; 2. weil die meisten Freiheitsbeschränkungen nicht zu spüren sind, da sie heimlich stattfinden, und 3. weil die BürgerInnen letztlich darauf vertrauten, dass das Bundesverfassungsgericht es wieder richten möge.

Apropos Bundesverfassungsgericht: Es gibt bereits Initiativen für Verfassungsbeschwerden, so u. a. von Digitalcourage, um etwa Staatstrojaner stoppen zu lassen. Und so mündet diese Laudatio in einen öffentlichen Appell, solche Verfassungsbeschwerden kräftig und massenhaft zu unterstützen – als Akt bürgerrechtlicher Notwehr.

Herzlichen Glückwunsch, CDU- und grüne Fraktion im hessischen Landtag, zum BigBrotherAward 2018.

## Anmerkungen

1 *Vgl. Süddeutsche Zeitung vom 4.8.2017, http://www.sueddeutsche.de/bayern/innere-sicherheit-landtags-gruene-klagen-gegen-verfassungsschutzgesetz-1.3614760*

2 *Entwickelt werden die Staatstrojaner für die bundesdeutschen Sicherheitsbehörden u. a. von der 2017 in München eingerichteten „Zentralstelle für Informationstechnik im Sicherheitsbereich" (ZITiS).*

3 *BVerfE vom 27.02.2008; vgl. auch BVerf-Urteil 1 BvR 966/09.*

4 *Gemeinsame Erklärung: http://vs.hu-hessen.de*

5 *Gutachten zum hessischen Verfassungsschutz-Gesetzentwurf: https://hessischer-landtag.de/node/2490; Bericht: https://netzpolitik.org/2018/breitseite-gegen-staatstrojaner-in-hessen-verfassungswidrig-und-gefaehrlich/*

6 *https://netzpolitik.org/2017/streit-um-geplantes-hessentrojaner-gesetz-bei-den-gruenen/; https://www.gruene-hessen.de/partei/beschluss/digitale-gefahrenabwehr-statt-digitaler/*

7 *https://www.gruene-hessen.de/landtag/files/2013/01/KP24-NETZPOLITIK-web4.pdf*

8 *Süddeutsche Zeitung vom 27.01.2018*

Marie-Theres Tinnefeld

# Grundrechte-Report 2018

Der frühere Grünen Abgeordnete Volker Beck stellte im Mai 2018 den Grundrechte-Report, den alternativen Verfassungsschutzbericht mehrerer Bürgerorganisationen, in Karlsruhe vor. Dieser Bericht ist u.a. eine Plattform für die Forderungen zu Rechten von Flüchtlingen. Von den 45 Kurzbeiträgen widmen sich explizit zwei dem Grundrecht auf Asylrecht für politisch Verfolgte (Art. 16a Abs. 1GG). Bellinda Bartolucci betont in ihrem Beitrag „Vom Aufnahmeland zum Abschiebeland" (S. 143 ff.), dass Flüchtlinge nach einer Kaskade von nationalen Gesetzen zu ihrer „Entrechtung" und „Zerstörung ihrer Privatsphäre" (S. 145) auf den Schutz der Zivilgesellschaft angewiesen sind. Christian Jakob weist auf „Die verfolgten Retter" S. 142 ff. hin – gemeint sind Seerettungs-NGOs im Einsatz, häufig zivile Helfer aus Deutschland –, die versuchen Menschenleben im Mittelmeer zu retten. Sie stören vielfach Politiker, deren Sinnen auf alte oder/und neue Wähler ausgerichtet ist! Ist es Medusa, der Wähler und Wählerinnen ins Auge sehen und die den so Versteinerten sagt, welchen Wert eine Schiffslast von Flüchtlingen besitzt? Wie anders ist es möglich, dass die Frage nach dem Schutz von Asylbewerbern im Juni zu einer mit „maßloser Härte" (Frank-Walter Steinmeier, SZ v. 27. Juni 2018, 1) geführten Debatte auf nationaler deutscher Ebene geführt hat? Hat sie nicht bereits zu Rissen in den Fundamenten der EU geführt? So wie sich der Nationalismus nicht zuletzt in Fragen des Asylrechts in Europa und den USA entwickelt hat, versteht er „nationale Identität" als Gegensatz zur individuellen Identität und wendet sich damit auch gegen den elementaren Schutz von Privatheit und Datenschutz sowie der Meinungsfreiheit, dem *free speech* als Kennzeichen einer offenen Demokratie.

Einen weiteren Schwerpunkt des Reports bildet das Thema *Überwachung und Sicherheitsbehörden*. Katharina Mangold zeigt in ihrem Beitrag „Der verweigerte Grundrechtsschutz für sog. Gefährder" (S. 170 ff.), dass für polizeiliche Maßnahmen eine „drohende" statt einer „konkreten" Gefahr genügen soll. Der Soziologe Ulrich Beck hat in seinem Buch „Risikogesellschaft" (1986) die Begriffe Risiko und Gefahr näher definiert. Wie aber soll der von dem Wissenschaftler definierte Begriff „Gefahr", der eine hinreichende Wahrscheinlichkeit eines bevorstehenden Schadenseintritts bedeute, auf einen Gefährder übertragen werden? Handelt es sich im Sinne der BT-Drs. 16/3750 S. 6) um „eine Person, bei der bestimmte Tatsachen, die motivierte Annahme rechtfertigen, dass sie politisch motivierte Straftaten von erheblicher Bedeutung … begehen wird"? Läuft auf diese Weise der Begriff „Gefährder" nicht auf die unbestimmte Prognose einer Prognose hinaus (S.172)?

Ein übermächtiges Sicherheitsbedürfnis in Deutschland dokumentieren auch weitere Beiträge. Dazu gehören die lesenswerten Ausführungen von Katharina Ruhwedel über das Pilotprojekt zur Gesichtserkennung am Bahnhof Südkreuz in Berlin (S. 26 ff.) sowie der Beitrag von Fredrik Roggan über Quellen-Telekommunikationsüberwachung und Online-Durchsuchung zur Strafverfolgung und der Beitrag von Dorothee Wildt „Vorratsdatenspeicherung 2017 – kein Ende in Sicht" (S. 179 ff.). Peter Schaar weist darauf hin, dass der „Weg zu einer biometrischen Verbunddatei der Sicherheitsbehörden" (S. 34 ff.) bzw. die unbestimmte Ermächtigung von Polizei, Nachrichtendiensten und anderen Behörden zum digitalen Abruf von Pass- und Ausweisbildern den Grundprinzipien des Datenschutzes widerspricht und ein „Türöffner zur virtuellen Zusammenschaltung der verteilten biometrischen Datenbestände für alle erdenklichen Zwecke" und somit zur „Vollüberwachung" werden könne (S. 37).


Grundrechte-Report 2018 – Zur Lage der Bürger- und Menschenrechte in Deutschland.
Herausgeber: Till Müller-Heidelberg, Marei Pelzer, Martin Heiming, Cara Röhner, Rolf Gössner, Matthias Fahrner, Helmut Pollähne und Maria Seitz.
Fischer Taschenbuch Verlag, Frankfurt/M., Juni 2018,
ISBN 978-3-596-70189-6
240 Seiten, 10,99 Euro.

Die neuen „intelligenten" Überwachungstechniken nagen an digitalen Freiheiten der Bürger und Bürgerinnen. Darauf verweist auch Stefan Hügel in seinem Beitrag „Öffentliche Sicherheit durch unsichere IT?" (S. 42 ff.). Das gemeinsame Terrorübungen von Polizei und und Bundeswehr grundrechtswidrig (Art. 87a Abs. 2 GG) sein können, mahnt Rolf Gössner (S. 201 ff.) als „Geschichtsvergessene Grenzüberschreitung" an (S. 210 f.).

Die Freiheit von Bürgerinnen und Bürgern basiert in einer offenen Demokratie nicht zuletzt auf der Meinungs- und Informationsfreiheit, die Till Müller-Heidelberg (S. 97 ff.) gerade in Zeiten eingeschränkter Freiheitswahrnehmung von Bürgerinnen und Bürgern betont. Denn Zensurmaßnahmen können über die bloße Verbotswirkung hinaus zur Selbstzensur führen und Menschen nachhaltig davon abhalten, ihre kommunikativen Grundrechte wahrzunehmen. Der facettenreiche Report ist bürgernah und dient der Aufklärung Betroffener nach der Maxime „Wissen ist ein Pfeiler demokratischer Macht".

# Wissenschaft & Frieden 3/2018
# „Gender im Visier“

*Gender* bezeichnet die soziale Kategorie Geschlecht ebenso wie Fragen der sexuellen Orientierung und Selbstbestimmung. Beide Aspekte wurzeln tief in unseren gesellschaftlichen Konfliktlinien und wirken in die Wahrnehmung von Konflikten und ihrer Lösung hinein. Wo aber liegt konkret der Zusammenhang von Gender und Konflikt bzw. Krieg? Dieser Frage gehen in vielfältiger Weise die Artikel im Schwerpunktthema *Gender im Visier* von W&F 3/2018 nach.

Es schreiben:

- *María Cárdenas*: Gender im Visier
- *Ralf Buchterkirchen*: Männlichkeit im Militär. Historische Zugänge und Ansatzpunkte für die Friedensarbeit
- *Sarah Steube*: Militär und Männlichkeit. Die Funktion militärischer Männlichkeitsmythen
- *Ray Acheson*: Gender und Drohnen. Folgen des bewaffneten Drohneneinsatzes
- *Claudia Brunner*: Zwei Paar Schuhe? Friedens- und Konfliktforschung braucht Gender Studies
- *Alejandra Londoño*: „Gender-Ideologie“ in Kolumbien. Oder: Wie man Ängste schürt, um den Frieden zu behindern
- *Heidi Meinzolt*: UN-Resolution 1325 in Deutschland
- *Ruth Seifert*: Sexualisierte Gewalt als „Kriegsstrategie“?
- *Monika Hauser*: Verantwortung für gewaltfreie Zukunft. Politik gegen sexualisierte Kriegsgewalt muss feministisch sein
- *Anne Menzel*: Geld ist unser Hauptproblem! Kann Aufklärung gewalthaltige Geschlechterverhältnisse verändern?
- *Tim Bausch* und *Carolina Rehrmann*: Gewalt, Geschlecht und Militär. Die Bundeswehr auf feministischen Terrain?
- *Anne Bieschke*: Historisches Vorbild. Bertha von Suttner und die Frauen für Frieden
- *Jana Hornberger*: Dieser Körper gehört mir! Der Kampf gegen Feminizid in Guatemala

Außerhalb des Schwerpunktes befassen sich AutorInnen mit der Aktualität des Dreißigjährigen Krieges und des Westfälischen Friedens – markiert durch die Jahreszahlen 1618 und 1648 – für uns heute, im Jahr 2018, sowie mit Themen der Jungen Friedensforschung und dem Treffen von Donald Trump und Kim Jong-Un. Die Presseschau wirft einen Blick zurück auf den „Abschiebe-Poker“ innerhalb der Bundesregierung.

**Wissenschaft & Frieden, 3/2018**: „Gender im Visier“, 9,00 € Innland, EU plus 3,00 € Porto (Bitte um Vorkasse: Sparkasse KölnBonn, DE86 3705 0198 0048 0007 72, SWIFT-BIC COLSDE33XXX)

W&F erscheint vierteljährlich. Jahresabo 35 €, ermäßigt 25 €, Ausland 45 €, ermäßigt 35 €, Förderabo 60 €. W&F erscheint auch in digitaler Form – als PDF und ePub. Das Abo kostet für Bezieher der Printausgabe zusätzlich 5 € jährlich – als elektronisches Abo ohne Printausgabe 20 € jährlich.

Bezug: W&F c/o BdWi-Service, Gisselberger Str. 7, 35037 Marburg, E-Mail: service@wissenschaft-und-frieden.de, *www.wissenschaft-und-frieden.de*

**Wissenschaft und Frieden ist Trägerin des Göttinger Friedenspreises 2018**

# FIfF e.V.

Im FIfF haben sich rund 700 engagierte Frauen und Männer aus Lehre, Forschung, Entwicklung und Anwendung der Informatik und Informationstechnik zusammengeschlossen, die sich nicht nur für die technischen Aspekte, sondern auch für die gesellschaftlichen Auswirkungen und Bezüge des Fachgebietes verantwortlich fühlen. Wir wollen, dass Informationstechnik im Dienst einer lebenswerten Welt steht. Das FIfF bietet ein Forum für eine kritische und lebendige Auseinandersetzung – offen für alle, die daran mitarbeiten wollen oder auch einfach nur informiert bleiben wollen.

Vierteljährlich erhalten Mitglieder die Fachzeitschrift FIfF-Kommunikation mit Artikeln zu aktuellen Themen, problematischen Entwicklungen und innovativen Konzepten für eine verträgliche Informationstechnik. In vielen Städten gibt es regionale AnsprechpartnerInnen oder Regionalgruppen, die dezentral Themen bearbeiten und Veranstaltungen durchführen. Jährlich findet an wechselndem Ort eine Fachtagung statt, zu der TeilnehmerInnen und ReferentInnen aus dem ganzen Bundesgebiet und darüber hinaus anreisen. Darüber hinaus beteiligt sich das FIfF regelmäßig an weiteren Veranstaltungen, Publikationen, vermittelt bei Presse- oder Vortragsanfragen ExpertInnen, führt Studien durch und gibt Stellungnahmen ab etc. Das FIfF kooperiert mit zahlreichen Initiativen und Organisationen im In- und Ausland.

## FIfF-Mailinglisten

**FIfF-Mailingliste**
An- und Abmeldungen an:
*http://lists.fiff.de/mailman/listinfo/fiff-L*
Beiträge an: *fiff-L@lists.fiff.de*

**FIfF-Mitgliederliste**
An- und Abmeldungen an:
*http://lists.fiff.de/mailman/listinfo/mitglieder*

**Mailingliste Videoüberwachung:**
An- und Abmeldungen an:
*http://lists.fiff.de/mailman/listinfo/cctv-L*
Beiträge an: *cctv-L@lists.fiff.de*

## FIfF online

**Das ganze FIfF**
*www.fiff.de*
Twitter FIfF e.V. – *@FIfF_de*

**Cyberpeace**
*cyberpeace.fiff.de*
Twitter Cyberpeace – *@FIfF_AK_RUIN*

**Faire Computer**
*blog.faire-computer.de*
Twitter Faire Computer – *@FaireComputer*

**Mitglieder-Wiki**
*https://wiki.fiff.de*

## FIfF-Beirat

**Ute Bernhardt** (Berlin); **Peter Bittner** (Kaiserslautern); **Dagmar Boedicker** (München); Dr. **Phillip W. Brunst** (Köln); Prof. Dr. **Wolfgang Coy** (Berlin); Prof. Dr. **Wolfgang Däubler** (Bremen); Prof. Dr. **Leonie Dreschler-Fischer** (Hamburg); Prof. Dr. **Christiane Floyd** (Hamburg); Prof. Dr. **Klaus Fuchs-Kittowski** (Berlin); Prof. Dr. **Michael Grütz** (Konstanz); Prof. Dr. **Thomas Herrmann** (Bochum); Prof. Dr. **Wolfgang Hesse** (Marburg); Prof. Dr. **Wolfgang Hofkirchner** (Wien); Prof. Dr. **Eva Hornecker** (Weimar); **Werner Hülsmann** (Konstanz); **Ulrich Klotz** (Frankfurt); Prof. Dr. **Klaus Köhler** (Mannheim); Prof. Dr. **Jochen Koubek** (Bayreuth); Prof. Dr. **Herbert Kubicek** (Bremen); Dr. **Constanze Kurz** (Berlin); Prof. Dr**. Klaus-Peter Löhr** (Berlin); **Werner Mühlmann** (Oppung); Prof. Dr. **Frieder Nake** (Bremen); Prof. Dr. **Rolf Oberliesen** (Bremen); Prof. Dr. **Arno Rolf** (Hamburg); Prof. Dr. **Alexander Rossnagel** (Kassel); **Ingo Ruhmann** (Berlin); Prof. Dr. **Gerhard Sagerer** (Bielefeld); Prof. Dr. **Gabriele Schade** (Erfurt); **Ralf E. Streibl** (Bremen); Prof. Dr. **Marie-Theres Tinnefeld** (München); Dr. **Gerhard Wohland** (Waldorfhäslach)

## FIfF-Vorstand

**Stefan Hügel** (Vorsitzender) – Frankfurt am Main
**Rainer Rehak** (stellv. Vorsitzender) – Berlin
**Michael Ahlmann** – Kiel / Blumenthal
**Sylvia Johnigk** – München
**Benjamin Kees** – Berlin
Prof. Dr. **Hans-Jörg Kreowski** – Bremen
Prof. Dr. **Dietrich Meyer-Ebrecht** – Aachen
**Kai Nothdurft** – München
**Jens Rinne** – Mannheim
Prof. Dr. **Britta Schinzel** – Freiburg im Breisgau
**Ingrid Schlagheck** – Bremen
**Anne Schnerrer** – Berlin
Prof. Dr. **Werner Winzerling** – Fulda
Prof. Dr. **Eberhard Zehendner** – Jena

## FIfF-Geschäftsstelle

**Ingrid Schlagheck** (Geschäftsführung) – Bremen
**Michael Jacobsen** – Bremen

# Impressum


| | |
|---|---|
| **Herausgeber** | Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF) |
| **Verlagsadresse** | FIfF-Geschäftsstelle<br>Goetheplatz 4<br>D-28203 Bremen<br>Tel. (0421) 33 65 92 55<br>*fiff@fiff.de* |
| **Erscheinungsweise** | vierteljährlich |
| **Erscheinungsort** | Bremen |
| **ISSN** | 0938-3476 |
| **Auflage** | 1 200 Stück |
| **Heftpreis** | 7 Euro. Der Bezugspreis für die FIfF-Kommunikation ist für FIfF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIfF-Kommunikation für 28 Euro pro Jahr (inkl. Versand) abonnieren. |
| **Hauptredaktion** | Dagmar Boedicker, Stefan Hügel (Koordination), Sylvia Johnigk, Hans-Jörg Kreowski, Dietrich Meyer-Ebrecht, Ingrid Schlagheck, Eberhard Zehendner |
| **Schwerpunktredaktion** | Stefan Hügel, Hans-Jörg Kreowski |
| **V.i.S.d.P.** | Stefan Hügel |
| **FIfF-Überall** | Beiträge aus den Regionalgruppen und den überregionalen AKs. Aktuelle Informationen bitte per E-Mail an *hubert.biskup@gmx.de*. Ansprechpartner für die jeweiligen Regionalgruppen finden Sie im Internet auf unserer Webseite *https://www.fiff.de/regionalgruppen* |
| **Retrospektive** | Beiträge für diese Rubrik bitte per E-Mail an *redaktion@fiff.de* |
| **Lesen, SchlussFIfF** | Beiträge für diese Rubriken bitte per E-Mail an *redaktion@fiff.de* |
| **Layout** | Berthold Schroeder, München |
| **Cover** | https://de.wikipedia.org/wiki/Danaergeschenk#/media/File:The_Procession_of_the_Trojan_Horse_in_Troy_by_Giovanni_Domenico_Tiepolo.jpg |
| **Druck** | Meiners Druck, Bremen |

Die FIfF-Kommunikation ist die Zeitschrift des „Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V." (FIfF). Die Beiträge sollen die Diskussionen unter Fachleuten anregen und die interessierte Öffentlichkeit informieren. Namentlich gekennzeichnete Artikel geben die jeweilige Autor.innen-Meinung wieder.

Die FIfF-Kommunikation ist das Organ des FIfF und den politischen Zielen und Werten des FIfF verpflichtet. Die Redaktion behält sich vor, in Ausnahmefällen Beiträge abzulehnen.




**Wichtiger Hinweis:** Wir bitten alle Mitglieder und Abonnenten, Adressänderungen dem FIfF-Büro möglichst umgehend mitzuteilen.

# Aktuelle Ankündigungen

(mehr Termine unter *www.fiff.de*)

**~ Bits & Bäume ~**
Die Konferenz für Digitalisierung und Nachhaltigkeit
17. bis 18. November 2018, Berlin

**FIfF-Kommunikation**

**4/2018** „Alter(n)sgerechte Informatik"
Eberhard Zehendner, Stefanie Jäckel, Henning Lübbecke
Redaktionsschluss: 2. November 2018

**1/2019** „Brave New World"
Rainer Rehak, Benjamin Kees, Anne Schnerrer u. a.
Redaktionsschluss: 1. Februar 2019

**W&F – Wissenschaft & Frieden**

4/17 Eingefrorene Konflikte
(mit Dossier 85: Transhumanismus und Militär)
1/18 USA – eine Inventur
2/18 Wissenschaft im Dienste des Militärs?
(mit Dossier 86: Cyberrüstung und zivile IT-Sicherheit)
3/18 Gender im Visier

**vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik**

#219 Soziale Menschenrechte
#220 Europa in der Krise
#221/222 Datenschutz nach der DSGVO
#223 Bürgerrechte im Sport
#224 Wandel der Kommunikationsfreiheit durch Digitalisierung und Internet
#225 Polizei und Technikeinsatz

**DANA – Datenschutz-Nachrichten**

1/17 Verbraucherschutz
2/17 BDSG-Nachfolgegesetz
3/17 40 Jahre DVD
4/17 Gesundheitsdatenschutz
1/18 Polizeigesetze
2/18 25.05.2018 – und jetzt?

## Das FIfF-Büro


**Geschäftsstelle FIfF e. V.**
Ingrid Schlagheck (Geschäftsführung), Michael Jacobsen
Goetheplatz 4, D-28203 Bremen
Tel.: (0421) 33 65 92 55, Fax: (0421) 33 65 92 56
*E-Mail: fiff@fiff.de*
Die Bürozeiten finden Sie unter *www.fiff.de*

**Bankverbindung**
Bank für Sozialwirtschaft (BFS) Köln
Spendenkonto:
IBAN: DE79 3702 0500 0001 3828 03
BIC: BFSWDE33XXX

**Kontakt zur Redaktion der FIfF-Kommunikation:**
*redaktion@fiff.de*

**Vergil**

## Die Zerstörung von Troja,

### im zweyten Buch der Aeneide

[...]

(1) Der ganze Saal war Ohr, jedweder Mund verschlossen,
und Fürst Aeneas, hingegossen
auf hohen Polstersitz, begann:
Dein Wille, Königinn, macht Wunden wieder bluten,
die keine Sprache schildern kann;
wie Trojas Stadt vergieng in Feuerfluten,
den Jammer willst du wissen, die Gefahr,
wovon ich Zeuge, ach und meistens Opfer war.

(2) Wer, selbst aus der Dolopen rauhem Schwarme,
gibt thränenlos den traurigen Bericht?
Und uns umschattet schon die Nacht mit feuchtem Arme,
zum Schlummer winkt der Sterne sinkend Licht.
Doch du hast Lust, mein Schicksal zu betrauern,
der Teukrer Noth und Trojas letzten Tag.
Sey's denn! Wie sehr mir auch vor der Erinnrung schauern,
der Geist davor zurücke fliehen mag.

(3) Der Griechen Fürsten, aufgerieben
vom langen Krieg, vom Glück zurückgetrieben,
erbauen endlich durch Minervens Kunst
ein Roß aus Fichtenholz, zum Berge aufgerichtet,
beglückte Wiederkehr, wie ihre List erdichtet,
dadurch zu flehen von der Götter Gunst.
Der Kern der tapfersten birgt sich in dem Gebäude,
und eisern ist sein Eingeweide.

[...]

(6) Mit Staunen weilt der überraschte Blick
beym wunderbaren Bau des ungeheuren Rosses,
Thimät, seys böser Wille, seys Geschick,
wünscht es im innern Raum des Schlosses.
Doch bang vor dem versteckten Feind
räth Capys an, und wer es redlich meynt,
den schlimmen Fund dem Meer, dem Feuer zu vertrauen,
wo nicht, doch erst sein innres zu beschauen.

[...]

(8) Wenn in dem Rosse nicht versteckte Feinde lauren,
so droht es sonst Verderben unsern Mauren,
so ist es aufgethürmt, die Stadt zu überblicken
so sollen sich die Mauren bücken
vor seinem stürzenden Gewicht,
so ists ein anderer von ihren tausend Ränken,
der hier sich birgt. Trojaner trauet nicht,
Die Griechen fürchte ich, und doppelt, wenn sie schenken.

[...]

(31) Jetzt zwar sind sie nach Argos heimgefahren,
doch führt sie Kalchas bald mit neuen Kriegerschaaren
und Göttern furchtbarer zurück. Dieß Roß
ward aufgethürmt, den Zorn der Pallas zu versöhnen,
und nicht umsonst seht ihrs so riesengroß.
Es sollte seine Last das schmahle Thor verhöhnen,
nie sollt euch der Besitz des Wunderbilds erfreun,
nie sollt es eurer Stadt den alten Schutz erneun.

[...]

(41) Und hoch beglückt, den Strang berührt zu haben
der es bewegt, begleiten Jungfrauen und Knaben
mit heilgen Liedern die verehrte Last.
O meine Vaterstadt! So reich an Siegeskronen,
o heilges Land, wo so viel Götter thronen!
in deiner Mitte steht der fürchterliche Gast.
Viermal hat es am Eingang still gehalten,
und viermal klang das Erz in seines Bauches Falten.

(42) Uns warnt es nicht! Von wüthender Begierde
verblendet setzen wir die unglückschwangre Bürde
beym Tempel ab. Apolls Orakel spricht
weißagend aus Kaßandrens Munde,
es spricht von Trojas letzter Stunde,
wir glauben selbst der Gottheit nicht.
Von festlich grünem Laub muß jeder Tempel wehen
und – morgen ists um uns geschehen!

[…]

(44) Geleitet von dem Feuerbrande
der aus dem königlichen Schiffe blitzt,
dringt sie hinan zum wohlbekannten Strande,
und, von der Götter Grimm beschützt,
eröfnet Sinon still den Bauch der Fichte.
Gehorsam gibt das aufgethane Roß
die Krieger von sich, die sein Leib verschloß,
und hoch erfreut entspringen sie zum Lichte.

[...]

(55) Jetzt lag es kund und aufgethan,
wie Danaer auf Treu und Glauben halten,
das Bubenstück sieht man jetzt schrecklich sich entfalten!
Schon liegt, besiegt vom prasselnden Vulkan,
Deiphobus majestätsche Burg im Staube,
schon wird Ukalegon's, ihr Nachbar, ihm zum Raube,
vom flammenrothen Wiederscheine brennt
des Meeres Spiegel und das Firmament.

[…]

*Quelle: Wikisource (https://de.wikisource.org/wiki/Die_Zerstörung_von_Troja): Vergil, Die Zerstörung von Troja, Im zweyten Buch der Aeneide, aus: Neue Thalia 1792, Erster Band, S. 3-78, Hrsg. Friedrich Schiller*

Geeignete Texte für den SchlussFIfF bitte mit Quellenangabe an *redaktion@fiff.de* senden.