H 7625

FIfF Kommunikation

Zeitschrift für Informatik und Gesellschaft

34. Jahrgang 2017 Einzelpreis: 7 EUR

3/2017 – September 2017

FREIHEIT 2.0

ISSN 0938-3476

• BigBrotherAwards 2017 • Cyberpeace • Hackerangriff auf die Wahlfreiheit •

FIfF Kommunikation

Zeitschrift für Informatik und Gesellschaft

Titelbild: Teil des Leitsystems des Kunstprojekts FREIHEIT 2.0 von Florian Mehnert

Inhalt

Ausgabe 3/2017

inhalt

Editorial

Im September und Oktober 2016 realisierte der Künstler Florian Mehnert in Weil am Rhein, Basel und Huningue sein Kunstprojekt FREIHEIT 2.0 *(freiheit.florianmehnert.de)*, das sich mit den Wechselwirkungen zwischen digitaler und analoger Welt auseinandersetzte und Selbstreflexion über den Wert der Privatheit bewirken wollte. Geschäfte wurden in „Freiheit" umfirmiert und ein Leitsystem installiert, das zum Büro der FREIHEIT 2.0 führte (siehe Titelbild). Begleitet wurde die Kunstinstallation durch die BIG DATA KOLLOQUIEN mit Referent.innen aus Medientheorie, Informatik, Datenschutz, Wirtschaft und Philosophie – Schwerpunkt in dieser Ausgabe der FIfF-Kommunikation. Britta Schinzel leitet ihn in ihrem Editorial ab Seite 12 ein.

Im zweiten Schwerpunkt berichten wir von den BigBrotherAwards, die auch in diesem Jahr in Bielefeld verliehen wurden. Auch im Jahr 4 nach Snowden ist es erschreckend, in welchem Umfang die Privatsphäre – durch Ausforschung von Kund.innen und Bürger.innen – und die Sicherheit unserer Kommunikationsinfrastrukturen angegriffen werden. Die Themen der diesjährigen Veranstaltung gingen dabei über den Bruch des Datenschutzes in der IT hinaus – auch in der „analogen" Religionsausübung ist man nicht vor Bespitzelung sicher, wie der Award für die Türkisch-Islamische DİTİB zeigt, und die massive Gefährdung der IT-Sicherheit durch digitale Aufrüstung der Bundeswehr wurde ebenfalls mit einem BigBrotherAward „honoriert".

In seinem Beitrag *Hackerangriff auf die Wahlfreiheit* außerhalb der Schwerpunkte begrüßt Rainer W. Gerling, dass es in Deutschland auch auf absehbare Zeit keine politischen Wahlen im Internet geben wird. Er will sich „*… einen Wahlvorgang komplett im Internet für politische Wahlen lieber nicht vorstellen. Ein Angriff auf die Computer der Wähler könnte von jedem Ort der Welt vorgenommen werden, Manipulationen von den verschiedensten Seiten wären Tür und Tor geöffnet.*" Doch auch durch Desinfomation, Propaganda, *Fake News* werde der demokratische Diskurs beeinflusst und gefährdet. „*Nichts Neues*", so Gerling, aber der Anstieg der Zahl der Informationsanbieter erlegt den Bürger.innen eine größere Verantwortung auf. Letztendlich wirkt auch hier, wie so oft, das Internet als Verstärker. „*Da hilft nur eines: Bildung*", so das Fazit.

Nach Redaktionsschluss wurde durch eine Untersuchung des *Chaos Computer Clubs* bekannt, dass auch in Deutschland Software, die bei der Bundestagswahl eingesetzt wird, nicht sicher ist. Zwar ist die eigentliche Wahl hier nicht automatisiert, die Software, die die Ergebnisse übermittelt und zusammenführt, enthält aber offenbar Sicherheitslücken in erschreckendem Ausmaß.

Lähmenden Pessimismus stellt Dagmar Boedicker in ihrem Essay fest und fragt nach den Gründen für den Zerfall der Europäischen Union als Zukunftsprojekt. „*Eine Generation neoliberaler Ellbogengesellschaft hat dazu geführt, dass soziale Verantwortung, Anstand und rücksichtsvoller Umgang miteinander als altmodisch betrachtet oder als Gutmenschentum verspottet werden.*" Großbritannien wird die EU wohl verlassen, mehrere osteuropäische Länder fallen in einen vordemokratischen Nationalismus zurück. „*Jeder Mitgliedstaat versucht, den eigenen Nutzen auf Kosten der anderen zu maximieren*", so Dagmar Boedicker, und: „*Ziel der EU muss es sein, ihre Grundwerte zu verwirklichen, sie lebbar zu machen! Das kann kein Land allein erreichen.*"

Unter dem Label *Betrifft: Cyberpeace* steht ein Nachtrag zu einer Veranstaltung des FIfF in Bremen, von der wir bereits in der letzten Ausgabe berichteten: Der Protest gegen die Messe und Konferenz *Undersea Defence Technology* und ein Resümee des Cyberpeace-Forums von Ekkehard Lentz vom Bremer Friedensforum.

Zu aktuellen Themen ist das FIfF mit Erklärungen in die Öffentlichkeit gegangen: Der Erpressungstrojaner *WannaCry* ist fast schon wieder vergessen – ein besonders eindringliches Beispiel, wie das Treiben von Geheimdiensten und sogenannten Sicherheitsbehörden unsere Infrastruktur gefährdet. Zum Beispiel durch den *Staatstrojaner*, der mit parlamentarischen Winkelzügen im Schatten öffentlicher Berichterstattung durch den Bundestag geschleust wurde, und der das staatliche Hacking zum Alltagsinstrument der Behörden erhebt. In die Acht-Uhr-Nachrichten der Tagesschau schaffte es unsere Stellungnahme zum Berliner Bahnhof *Südkreuz* (Seite 10), an dem seit 1. August 2017 großflächige Videoüberwachung mit biometrischer Gesichtserkennung und später auch Verhaltenserkennung erprobt werden sollen – unter grundrechtlich und methodisch zweifelhaften Rahmenbedingungen.

Unsere diesjährige FIfF-Konferenz wird vom 20. bis 22. Oktober 2017 in Jena stattfinden. *TRUST – Wem kann ich trauen im Netz und warum?*, so das Motto der Tagung, die Eberhard Zehendner und Stefanie Jäckel vorbereiten und organisieren. Einen Überblick über das Programm gibt es ab Seite 63. Es lohnt sich sicher, nach Jena zu kommen – wir freuen uns auf eine spannende Tagung und auf viele Besucher.innen.

Sorge bereiten verstärkte Versuche, kritische Politik zu diskreditieren und in die Nähe des Rechtsextremismus zu rücken. Der G20-Gipfel war offenbar ein willkommener Anlass, vor allem für (rechts-) konservative Politiker.innen. Waren in Hamburg die Verstöße Einzelner gegen das (ohnehin fragwürdige) Vermummungsverbot der Anlass für massive Polizeieinsätze, war man offenbar beim wenige Tage später stattfindenden Rechtsrock-Konzert im thüringischen Themar wesentlich zurückhaltender, obwohl u. a. mit dem Zeigen des Hitlergrußes schwerwiegendere Straftaten begangen wurden. Als US-Präsident Trump nach den Ereignissen von Charlottesville ebenfalls rechte und linke Aktivisten über einen Kamm scheren wollte, war dann die Empörung groß – muss es immer erst Tote geben, bevor die Menschen zur Besinnung kommen?

Auch der Abschluss des NSA-Untersuchungsausschusses des Deutschen Bundestages hätte eine ausführlichere Stellungnahme verdient. Nachdem zuvor bereits das BND-Gesetz verabschiedet worden war, das das Handeln des BND legalisiert, wo es bisher rechtswidrig war, versuchte der Vorsitzende, der zuvor bereits ein Buch über die Ergebnisse herausgegeben hatte, das Sondervotum der Opposition unter Hinweis auf Geheimhaltung zu verhindern. Offensichtlich geht es schon lange nicht mehr um Aufklärung, sondern um die Deutungshoheit. Wovor haben die Verantwortlichen Angst?

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

Stefan Hügel
für die Redaktion

Der Brief

Unsere Träume sind nie gefeit / gegen eine Überdosis Wirklichkeit
(Wolf Maahn)

Grundrechte in der Praxis – von Hamburg bis Berlin

Liebe Leserinnen und Leser, liebe Mitglieder des FIfF,

es ist überhaupt keine Frage: Die Ausschreitungen, die sich – den Medienberichten zufolge – während des G20-Gipfels im Hamburger Schanzenviertel ereigneten, sind nicht hinnehmbar. Das gilt unabhängig von ihrem tatsächlichen Umfang. Auch wenn in der Berichterstattung in endloser Folge immer wieder dieselben brennenden Autos gezeigt werden, so oft, bis der Eindruck entsteht, ganz Hamburg habe lichterloh in Flammen gestanden, und es dadurch schwer ist, das wirkliche Ausmaß zu beurteilen. Auch über die letztendlichen Verursacher.innen der Krawalle sollten wir nicht vorschnell urteilen. Aber unabhängig davon ist klar: Gewalt ist kein Mittel der Politik und darf es auch nicht sein.

Doch auch das Verhalten der Polizei in Hamburg lässt Fragen offen. Zu einer Art Ikone wurde inzwischen das Bild einer jungen Frau, die, auf einem gepanzerten Fahrzeug stehend, von mehreren Polizisten mit „Pfefferspray" angesprüht wird, einem Kampfstoff, der nach Genfer Konvention für den Einsatz in militärischen Konflikten verboten ist. Welche konkrete Gefahr war der Anlass für so einen massiven Angriff?

Leider wehrt sich der rot-grüne (!) Senat der Stadt Hamburg dagegen, die Ereignisse während des Gipfels in einem Untersuchungsausschuss angemessen aufzuarbeiten. Ein „Sonderausschuss", mit weit weniger Rechten ausgestattet, soll nun gebildet werden. Man kann auf die Ergebnisse gespannt sein. Die Humanistische Union hat in einem offenen Brief erneut einen Untersuchungsausschuss gefordert und einen Fragenkatalog dazu formuliert.[1]

Nachdem der Erste Bürgermeister der Stadt Hamburg kurzerhand bestritten hat, dass es überhaupt irgendeine Form von Gewalt von Polizeibeamten gegeben habe – angesichts von rund 100 Ermittlungsverfahren gegen Polizeibeamte, häufig wegen Körperverletzung im Amt, eine zumindest überraschende Aussage – konzentrierten sich Berichte außerhalb der Filterbubble bürgerrechtlicher Vereinigungen zunächst auf die Ausschreitungen im Schanzenviertel. Kritische Stimmen hatten es schwer – wir erinnern uns an Wolfgang Bosbach, der die Talkshow *Menschen bei Maischberger* nach Kritik von Jutta Ditfurth theatralisch verließ – was ihm das Hashtag *#BosbachLeavingThings* und ein paar witzige Tweets eintrug.

Weniger lustig ist der erneute Versuch, kritische Politik zu diskreditieren und die Aktivisten in die Nähe von rechten Mördern zu rücken. Das passiert in einer Zeit, in der ein Gerichtsverfahren in München auf die Zielgerade einbiegt, in dem über zehn Morde der sich selbst *nationalsozialistisch* nennenden Organisation NSU verhandelt wird, die offensichtlich über Jahre durch die Behörden nicht verhindert werden konnten. Solche Versuche erinnern wirklich an die Weimarer Republik, in der rechte Gewalt verharmlost wurde, mit den bekannten Folgen. Wer einmal auch nur das Vorwort eines Geschichtsbuchs gelesen hat, sollte sich dessen bewusst sein.

Später waren aber auch in konservativen Blättern nachdenkliche Berichte zu lesen. Ein unerwartet unvergessliches Wochenende erlebten wohl einige Aktivisten von der SPD und den Grünen *nahestehenden* Jugendorganisationen, die unmittelbar mit den Folgen der von diesen beiden Parteien verantworteten Innenpolitik in Hamburg konfrontiert waren, als sie bereits bei der Anreise ohne ersichtlichen Grund in Gewahrsam genommen wurden. Die teilweise unappetitlichen Details, über die die *Frankfurter Allgemeine Zeitung* berichtete[2], spare ich mir hier. In der *Welt*[3] – auch nicht gerade ein Kampfblatt der *Antifa* – ist die Geschichte eines 18-jährigen Italieners zu lesen, der zum Zeitpunkt der Abfassung dieses Kommentars immer noch in Untersuchungshaft sitzt und dem bereits eine „empfindliche Freiheitsstrafe" avisiert wurde – nach dem Bericht der *Welt,* ohne dass er bis dahin angehört wurde, die Hauptverhandlung gegen ihn eröffnet oder wenigstens ein konkreter Tatvorwurf erhoben wurde. Stattdessen werde über „schädliche Neigungen" und „erhebliche Anlage- und Erziehungsmängel ..., die ohne längere Gesamterziehung des Täters die Gefahr weiterer Straftaten begründen", spekuliert.

Zuletzt ein Wort zur Einsatzleitung: Damit beauftragt wurde ein Mann, für dessen von ihm verantworteten Einsätze offenbar bereits mehrfach von Gerichten die Rechtswidrigkeit festgestellt wurde[4]. Ein Rechtsstaat, der solche wiederholte Rechtswidrigkeit nicht verhindern kann, ist bei der Verteidigung der Bürgerrechte zahnlos.

Ergebnisse hatte der Gipfel übrigens auch. Aus einem Pressestatement der Bundeskanzlerin[5]: „Hier werden die Mitgliedstaaten der G20 mit den Anbietern der Plattformen sehr intensiv sprechen und deutlich machen, dass wir das schnelle Löschen von terroristischen Informationen erwarten." Bei G20-Mitgliedern wie Brasilien (Rang 103 auf der Rangliste der Pressefreiheit), Indonesien (124), Indien (136), Mexiko (147), Russland (148), Türkei (155), Saudi-Arabien (168) und China (176)[6] darf man auf die Ergebnisse dieser „Gespräche" wohl besonders gespannt sein.

Am Berliner Bahnhof Südkreuz begann in diesen Tagen ein Versuch zur Videoüberwachung mit automatisierter Gesichtserkennung. Was davon zu halten ist, kann in unserer Pressemitteilung ab Seite 10 nachgelesen werden; unser Vorstandsmitglied Benjamin Kees hatte in den vergangenen Tagen bereits mehrfach die Gelegenheit, seine Kompetenz und die des FIfF in den Medien unter Beweis zu stellen und unsere Position deutlich zu machen. Schon an der Validität des Versuchs bestehen erhebliche Zweifel, von dem weiteren Ausbau der Überwachung überhaupt nicht zu reden.

Wir beobachten regelmäßig, dass bürgerrechtliche Forderungen – sei es in der Online- oder in der Offline-Welt – in der institu-

tionalisierten Politik nicht die Berücksichtigung finden, die ihrer Bedeutung entspricht. Ein Grund dafür mag sein, dass solche Themen in der Regel keinen nennenswerten Einfluss auf die Ergebnisse von Wahlen haben. Doch auf eine Idee ist nicht einmal der in dem Zusammenhang bereits arg strapazierte George Orwell gekommen: Dass Menschen für ein Butterbrot bereit sind, an ihrer eigenen Überwachung mitzuwirken. 300 Personen fanden sich offenbar, die gegen einen Amazon-Gutschein im Wert von 25 € den Versuch am Bahnhof Südkreuz tatkräftig unterstützen wollten – ist das der Wert, den wir unseren Grundrechten heute beimessen?[7]

Das fragt mit Besorgnis und FIfFigen Grüßen

Stefan Hügel

Anmerkungen

1 *http://www.humanistische-union.de/nc/aktuelles/aktuelles_detail/back/aktuelles/article/g20-aufklaeren-statt-aussitzen/*
2 *http://www.faz.net/aktuell/politik/g-20-demonstranten-erheben-vorwuerfe-gegen-polizei-15127924.html*
3 *https://www.welt.de/regionales/hamburg/article167543211/Muss-Fabio-V-wegen-Erziehungsmaengeln-ins-Gefaengnis.html*
4 *http://www.tagesspiegel.de/themen/reportage/g20-einsatzleiter-hartmut-dudde-der-mann-fuers-grobe/20035074.html*
5 *https://netzpolitik.org/2017/die-inhalte-des-g20-gipfels-handel-und-wettbewerb-ueberwachung-und-zensur/*
6 *ebd.*
7 *Freilich können die Testpersonen diesen „Wert" noch erhöhen, wenn sie sich kooperativ zeigen und möglichst häufig erkannt werden. Was das wiederum für die Validität der Testergebnisse bedeutet, mag sich jede.r selbst überlegen.*

Betrifft: Cyberpeace

Protest gegen *Undersea Defence Technology*

Wie in den vergangenen Jahren regelmäßig, soll auch in dieser Ausgabe der FIfF-Kommunikation auf Aktivitäten in der Cyberpeace-Kampagne eingegangen werden.

Der erste Beitrag von Birgit und Michael Ahlmann sowie von Hans-Jörg Kreowski berichtet kurz über eine Kundgebung am 30. Mai 2017 in Bremen, mit der gegen die Undersea-Defence-Technology*-Messe und -Konferenz protestiert und demonstriert wurde. Der zweite Beitrag von Ekkehard Lentz ist ein Nachtrag zum Schwerpunkt Cyberpeace-Forum aus der letzten FIfF-Kommunikation.*

Birgit Ahlmann, Michael Ahlmann, Hans-Jörg Kreowski

Undersea Defence Technology (UDT) – Waffen, die die Welt nicht braucht

Unter diesem Motto fand am 30. Mai 2017 zwischen Hauptbahnhof und den Bremer Messehallen eine Protestkundgebung gegen die Messe und Konferenz Undersea Defence Technology *statt – eine der großen Waffenmessen für den Unterwasserkrieg. Andere vergleichbare Messen sind in 2018 die Euronaval, die Navexpo und die Eurosatory sowie in 2019 die iMDEX Asia. Die dreitägige Veranstaltung fand zum 30. Mal statt – erstmals in Bremen. Mehr als 80 Unternehmen, darunter bekannte Rüstungsfirmen wie ATLAS ELEKTRONIK, Babcock, BAE Systems, DCNS, Gabler, Kongsberg, L3, Lockheed Martin, LÜRSSEN, QinetiQ, Rheinmetall Defence, SAAB, Siemens, Thales und thyssenkrupp Marine Systems boten in Bremen ihre todbringende Technik an. Eröffnet wurde die Messe vom Inspekteur der Deutschen Marine, Vizeadmiral Andreas Krause.*

Die UDT wird als Verteidigungs- und Sicherheitsmesse dargestellt. Doch der Begriff „Verteidigung" in diesem Zusammenhang ist höchst fragwürdig, zweischneidig und irreführend. „Unterwasserwaffen- und -kriegstechnologie" wäre allemal ehrlicher:

1. Ein gewichtiger Teil des Programms rankt sich um U-Boot-Technologie, also um Waffensysteme, die der Zerstörung von Handels- und Kriegsschiffen, der Aufklärung, der Verminung von Häfen und Seeschifffahrtsstraßen, der Abschreckung und der Erst- und Zweitschlagsfähigkeit dienen.

2. Viele Vorträge behandeln Seeminensuche und -beseitigung. Das klingt defensiv. Aber es handelt sich bei den *Suchern* und *Zerstörern* von Seeminen um die gleichen Industrien, die die Seeminen überhaupt erst entwickeln und herstellen. Das Auslegen ist dann Sache der Marinen. Sind das nicht auch die Waffenschmieden und Marineeinheiten, die die UDT bestreiten?

Banner zum Protest

3. Ein Schwerpunktthema der UDT ist die Autonomie aktueller und zukünftiger Unterwasseraufklärung und -bewaffnung. Die Waffensysteme sollen somit künftig selbständig, ohne menschliches Einwirken, entsprechend ihren Informationen „handeln", d. h. kriegerische Handlungen ausführen.

Allerdings werden ganz überwiegend technische Detailaspekte behandelt. Auf die rechtliche und ethische Problematik solcher „entmenschlichten" autonomen Kriegführung ohne menschliche Entscheidung wird nur am Rande eingegangen. Darf man kriegsrelevante Entscheidungen und letztlich Entscheidungen über Leben und Tod auf Waffensysteme verlagern? Kann denn ein Waffensystem selbstständig „denkend" entscheiden, Krieg zu führen? Ist Autonomie überhaupt technisch machbar? Wir sind überzeugt, dass autonome Waffen eine Fehlentwicklung mit unabsehbaren Folgen sind.

Deshalb wurden folgende Forderungen gestellt:

- Verbot von Seeminen analog zum Verbot von Landminen
- Bergen und Entsorgen von Seeminen und Altmunition weltweit, z. B. auch in Nord- und Ostsee
- Verbot von Unterwasserwaffen und -kriegführung analog zum Verbot biologischer und chemischer Waffen
- Stopp der Entwicklung von Unterwasser-Kriegstechnologie
- Einsatz der freiwerdenden Mittel und Expertise für zivile Unterwassertechnologie und zur Lösung ökologischer und sozialer Probleme

Der Protest gegen die UDT wurde organisiert vom Bremer Friedensforum, der Bremischen Stiftung für Rüstungskonversion und Friedensforschung, dem Cyberpeace-Team Bremen und der Regionalgruppe des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF).

Etwa 80 Bürgerinnen und Bürger aus den verschiedensten Stadtteilen hatten sich trotz der Gewitterschwüle eingefunden, um ihrem Unmut über diese Messe Ausdruck zu verleihen. Hans-Jörg Kreowski (FIfF), der die Kundgebung moderierte, stellte die Messe für *Undersea Defence Technology* und die Gefahren vor, die von dieser dort angebotenen Technik ausgehen. Außerdem sprachen die Bremer Rüstungsexpertin Andrea Kolling (Gemeinsame Konferenz Kirche und Entwicklung, GKKE) zur Werbung der Rüstungsexporte in Bremen, Michael Ahlmann (FIfF), ehemaliger Betriebsrat, von der Notwendigkeit der Rüstungskonversion, Norbert Schepers von der Rosa-Luxemburg-Stiftung über die Gefahren unbemannter Technologie im Krieg, Birgit Ahlmann (FIfF), ehemalige Betriebsrätin, über Arbeitsplätze, die von Rüstung und Militär abhängig sind, und Günter Matthiessen (Bremerhavener Initiative *Mut zum Frieden*) über autonome Unterwasserfahrzeuge, die sinnvoll für Umwelttechnologie und -forschung eingesetzt werden können. Zum Schluss sprach Eva Böller, Sprecherin des Bremer Friedensforums. Sie endete mit der Forderung nach Einhaltung der Zivilklausel an den Bremer Hochschulen und der Universität Bremen und der Feststellung: „Wir brauchen nicht mehr Geld für Rüstung und Militär, sondern für Arbeitsplätze im Bereich neue Energien, Klimaschutz, Umwelt, Soziales, Gesundheit, Bildung und gegen den Hunger von Millionen in der Welt." Das Ensemble *Rotes Krokodil* umrahmte die Protestveranstaltung musikalisch und stimmte auch zwischen den Wortbeiträgen Lieder an. Der Moderator schloss mit dem Laut- und Antikriegsgedicht *schtzngrmm* des österreichischen Lyrikers Ernst Jandl.

Birgit Ahlmann, Michael Ahlmann, Hans-Jörg Kreowski

Nach dem Studium des Informationsdesigns an der FH Kiel arbeitete **Birgit Ahlmann** zunächst als Grafikerin, studierte dann Soziologie und Anglistik/Amerikanistik an der CAU Kiel und arbeitete danach als PR-Managerin und Messespezialistin in der Maschinenbauindustrie. Anschließend war sie elf Jahre Betriebsratsvorsitzende und stellvertretende Gesamtbetriebsratsvorsitzende, leitete die IT-Ausschüsse in Betriebsrat, Gesamtbetriebsrat und Konzernbetriebsrat und war viele Jahre im Europäischen Betriebsrat des Konzernes aktiv. Sie ist seit einigen Jahren aktives Mitglied im FIfF. Weiterhin gilt ihr aktuelles Interesse der Gestaltung der Zukunft von Arbeit und Umwelt.

Michael Ahlmann studierte an der CAU in Kiel Mathematik und Physik. An der Universität Hannover erwarb er den Diplom-Ingenieur für Allgemeine Elektrotechnik. An der Universität Bremen nahm er an einem Kontaktstudium für Erwachsenenbildung und einem Studium der Politikwissenschaft teil. In einem Elektronikunternehmen in Bremen arbeitete er als Softwareentwickler und Betriebsrat. Elf Jahre lang war er Vorsitzender des Betriebsrates, des Gesamt- und Konzernbetriebsrates im Unternehmen und wirkte in zwei großen Konzernen in Deutschland im Konzernbetriebsrat und den entsprechenden IT-Ausschüssen sowie in einem Europäischen Betriebsrat mit. Seit 1981 ist er europaweit für die Rüstungskonversion im Rahmen der IG Metall aktiv, seit ca. 30 Jahren ist er Mitglied im FIfF und im AK RUIN. Er ist Mitglied im FIfF-Vorstand. Seine politischen Interessen liegen in den Themen Rüstungskonversion, Cyberpeace und einem nachhaltigen Leben.

Hans-Jörg Kreowski ist Professor (i. R.) für *Theoretische Informatik* an der Universität Bremen und Vorstandsmitglied des *Forums 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..

Impression von der Kundgebung (mit freundlicher Genehmigung von Hartmut Drewes)

Der Protest fand in den Medien ein beachtliches Echo. Da die Berichterstattung überwiegend positiv ausfiel, fühlte sich Joerg Helge Wagner, Ressortleiter Politik bei der *Bremer Tageszeitungen AG*, bemüßigt, eine harsche Kritik zu verfassen, die am nächsten Tag im Weserkurier als Kommentar auf Seite 2 erschien. Sein Tenor: „Für Bremen geht es aber auch darum, sich als bedeutender Industriestandort mit maritimer Kompetenz zu bekennen – und nicht als Wolkenkuckucksheim …" Es ist ein Erfolg, wenn Befürworterinnen und Befürworter von Rüstung und Krieg, von denen es in Politik, Wirtschaft, Wissenschaft und in den Medien viele gibt, aus ihrer Deckung gelockt werden. Wir sollten diesen Damen und Herren viel öfter und kräftiger auf die Füße treten.

Ekkehard Lentz

Cyberpeace-Forum in Bremen

Eine gelungene Zusammenarbeit

Bundes„verteidigungs"ministerin Ursula von der Leyen nutzt die öffentliche Debatte zu Cyberattacken *und* Cyberwar*, um das Thema an sich zu reißen. Bereits im Frühjahr 2016 kündigte sie an, in der Bundeswehr eine Organisationseinheit* Cyber- und Informationsraum *aufzubauen. Spätestens bei der Erstellung des neuen Weißbuchs hat das Bundesverteidigungsministerium die Entscheidung getroffen, dass die Bundeswehr auch Angriffe in fremde Netze verüben soll. Damit wurde ein Kurswechsel eingeleitet, der erhebliche Gefahren und ein großes Eskalationspotenzial birgt.*

Das Cyberpeace-Forum am 11./12. November 2016 im Haus der Wissenschaft in Bremen passte somit in die Zeit. In der Einladung zu der zweitägigen Veranstaltung hieß es:

> *„Neben Land, Luft, Wasser und Weltraum wird … ein fünftes Schlachtfeld offiziell eröffnet. Diese Maßnahme reiht sich ein in die weltweite Aufrüstung für den Cyberkrieg – und dabei geht es keineswegs nur um die Abwehr von Cyberattacken, sondern immer auch um die Fähigkeit zu eigenen Angriffen. Das bedroht nicht nur die militärischen Informations- und Kommunikationssysteme, sondern vor allem auch zivile Infrastrukturen wie Strom- und Wasserversorgung, Verkehr, Gesundheitswesen und die Netzwerke von Staat und Wirtschaft in den Industriestaaten, weil sie wegen ihrer immensen Abhängigkeit von Informations- und Kommunikationstechnik extrem angreifbar sind …"*

Die Zusammenarbeit des Veranstalterkreises habe ich in der Vorbereitung und Durchführung des Bremer Cyberpeace-Forums sehr positiv wahrgenommen: Cyberpeace-Team Bremen, Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) Regionalgruppe Bremen, Gewerkschaft Erziehung und Wissenschaft (GEW), Bremer Friedensforum und Bremische Stiftung für Rüstungskonversion und Friedensforschung.

Im Ansatz erinnerte die Anlage des Cyberpeace-Forums an erfolgreiche Zeiten in der deutschen Friedensbewegung. Von großer Bedeutung in der Auseinandersetzung um die Stationierung neuer atomarer Mittelstreckenraketen in der Bundesrepublik der 1980er-Jahre war das Auftreten führender Naturwissenschaftler, denen man zutraute, über die Wirkung moderner Massenvernichtungswaffen kompetent Auskunft geben zu können. In berufsbezogenen Friedensinitiativen bildeten sich vor 35 Jahren unterschiedliche Strukturen heraus, die sich teilweise bis heute stabil halten: Vereine mit einer festen Mitgliedschaft wie die Ärzte-Organisation IPPNW und die Naturwissenschaftler-Initiative gründeten sich, andere arbeiteten als lose Zusammenschlüsse. Neu war, dass sich hier Menschen zusammenfanden, die aus einer Berufsgruppe kamen und ihre Hauptaufgabe darin sahen, die Friedensthematik Kolleginnen und Kollegen nahe zu

Ekkehard Lentz

Ekkehard Lentz arbeitet als Erzieher und ist seit vielen Jahren in der Friedensbewegung aktiv. Momentan fungiert er ehrenamtlich als Sprecher des Bremer Friedensforums *(www.bremerfriedensforum.de, www.facebook.com/bremerfriedensforum, https://twitter.com/ekkehardlentz1).*

bringen und mit ihrer speziellen fachlichen Kompetenz Beiträge für die Friedensbewegung zu liefern.

Heute geht es darum, sich auf internationaler Ebene für konkrete Vereinbarungen zu einem friedlichen Miteinander im Cyberraum einzusetzen, statt die militärische Logik ins Netz zu tragen. Die Zusammenarbeit von Wissenschaftlern und Friedensgruppen sollte fortgesetzt und intensiviert werden. Die Cyberpeace-Kampagne des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. bietet eine gute Grundlage für weitere politische Aktivitäten.

Das Bremer Friedensforum hat die Kampagne auf seiner Website verlinkt: *http://www.bremerfriedensforum.de/743/aktuelles/Die-Cyberpeace-Kampagne-geht-weiter/*

FIfF e.V. – Pressemitteilung

WannaCry, ein Kollateralschaden des Cyberwar

18. Mai 2017 – Die Schadsoftware WannaCry wütet in der Welt. Vier Tage zuvor feierte der Kurzfilm „Cyberpeace statt Cyberwar" Premiere auf der re:publica 2017. Der Film erklärt, warum das Geheimhalten von Schwachstellen zum Zweck eines Cyberwars eine Gefahr für die Bevölkerung ist. Die WannaCry-Pandemie traf auch Betreiber kritischer Infrastrukturen wie die Deutsche Bahn und britische Krankenhäuser und zeigt, wie verwundbar diese für Malware-Angriffe sind. Dies ist ein weiterer Aspekt, auf den der Film eingeht.

WannaCry veranschaulicht, dass Betreiber von kritischen Infrastrukturen nicht in der Lage sind, sich selbst und uns vor Angriffen aus dem Internet zu schützen. Und WannaCry hat eine Geschichte. Die Schadsoftware nutzt eine Schwachstelle, die von der NSA seit fünf Jahren geheim gehalten wurde. Vor einigen Monaten ist dieses Wissen von der NSA zu nichtstaatlichen Kriminellen gelangt. Dies veranschaulicht exemplarisch, was passieren kann, wenn staatliche Stellen wie Geheimdienste, Strafverfolgung und Militär Schwachstellen geheim halten, um sie zur Spionage, für Überwachung oder in Cyberwaffen zu verwenden.

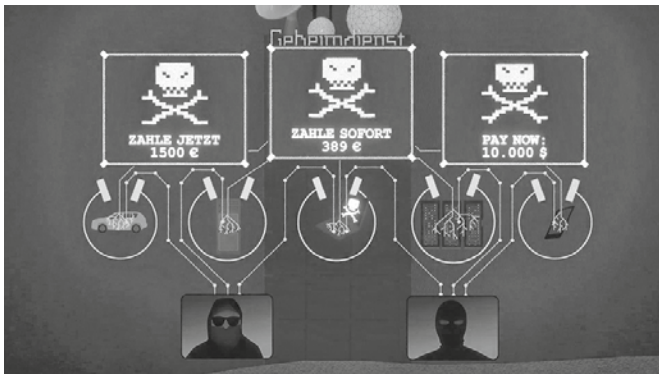
Ausschnitte aus dem Film: Cyberpeace statt Cyberwar

Sylvia Johnigk, Vorstandsmitglied des FIfF, stellt fest: „Durch die Geheimniskrämerei bei Schwachstellen werden auch eigene Infrastrukturen und die von Verbündeten gefährdet." Über kurz oder lang scheitert die Geheimhaltung ohnehin. Schwachstellen können auch von anderen entdeckt werden. Sie besitzen einen enormen Wert, der sich sowohl bei Behörden als auch im Darknet zu Geld machen lässt.

Kai Nothdurft, ebenfalls im Vorstand, ergänzt: „Mit der Geheimhaltung einer Schwachstelle ist es vorbei, wenn jemand durch Hacking an die Information gelangt."

Das FIfF fordert, dass gerade staatliche Stellen alle gefundenen Schwachstellen unverzüglich an die Hersteller melden und dann in einem verantwortlichen Zeitrahmen veröffentlichen. Insbesondere öffentliche Stellen müssen die Integrität und Sicherheit von Informationssystemen bewahren. Sie sind an die Wahrung der Verfassung gebunden, die das Grundrecht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme einschließt.

Der Film ist unter https://vimeo.com/216584485 abrufbar.



Schwachstellen werden auch von Kriminellen, wie Betrügern und Terroristen, gefunden und gegen uns eingesetzt.

cyberpeace.fiff.de, gefördert durch die Stiftung Bridge

Entfesselter Staatstrojaner: Große Koalition verhöhnt IT-Sicherheit und Demokratie

23. Juni 2017 – Gestern haben CDU/CSU und SPD im Bundestag das staatliche Hacking zum Alltagsinstrument für Behörden erklärt. Es geht dabei nicht einmal um die Verhinderung des sonst so gern herangezogenen internationalen Terrorismus, sondern um die Aufklärung bereits erfolgter Taten wie etwa Steuerhinterziehung, Betäubungsmitteldelikten oder missbräuchlicher Asylantragstellung.[1]

Unter den gleichen rechtlichen Voraussetzungen, mit denen zuvor Telefonleitungen abgehört werden konnten, können nun ganze Computersysteme jeglicher Art mit staatlicher Schadsoftware angegriffen, infiltriert, kontrolliert und ausgespäht werden. „*Einmal ins System gelangt, hat der Staatstrojaner dann technisch freie Hand, egal ob in Handys, Autos, Kühlschränken, Laptops oder Herzschrittmachern*“, erklärt Rainer Rehak aus dem Vorstand des FIfF. An der rechtlich fantasievollen, aber technisch nicht haltbaren Unterscheidung von „grundrechtsschonender“ Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) einerseits und vollaktivierter heimlicher Online-Durchsuchung andererseits wurde ebenfalls naiverweise festgehalten.

Der Einsatz von Quellen-TKÜ oder Online-Durchsuchung ist nur dann überhaupt ansatzweise nachvollziehbar, wenn Polizeien im absoluten Notfall auf die Nachrichten von Ende-zu-Ende-verschlüsselten Messengern wie WhatsApp (Facebook) oder Signal (Open Whisper Systems) zugreifen oder unbemerkt (verschlüsselte) Festplatten auslesen wollen, um etwa Leben zu retten. Doch in den vorliegenden Anlässen geht es gerade nicht um Notfälle, sondern schon verübte Straftaten. Es werden also Maßnahmen, die das Bundesverfassungsgericht im Jahre 2008 gerade noch bei tatsächlichen Anhaltspunkten einer konkreten Gefahr für Leib, Leben oder den Bestand des Staates[2] für verfassungsmäßig erachtet hat, nun für die Verfolgung gewöhnlicher Delikte vorgesehen.

Doch zu den direkten, hoch problematischen Komplikationen einer heimlichen Infiltration fremder Systeme, der prinzipiellen Undokumentierbarkeit und Unbelegbarkeit von Trojaneraktivitäten oder der technisch nach wie vor ungelösten Frage, wie laufende Kommunikation klar von anderen Datenverarbeitungsprozessen unterschieden werden kann, kommen noch unzählige weitere folgenschwere Eigenschaften hinzu. Einerseits sind die so erlangten Informationen technisch bedingt in der Regel nicht forensisch – also gerichtsfest – und damit für die Strafverfolgung größtenteils wertlos; und andererseits sind für die Infiltration von Systemen in der Regel unveröffentlichte, ausnutzbare IT-Sicherheitslücken vonnöten.

Diese benötigten IT-Sicherheitslücken sind auf internationalen Schwarzmärkten teuer zu erwerben und ein Ankauf solcher Lücken stützt, ja legitimiert derartige Märkte sogar noch. Je mehr finanziell potente, staatliche Akteure derartiges nachfragen, umso unsicherer wird die gesamte IT-Infrastruktur, weil Lücken nicht mehr an Hersteller gemeldet, sondern lieber an Behörden versteigert und von diesen gehortet werden. Das jüngste Beispiel war der Erpresserwurm *WannaCry*, der beispielsweise ganze Krankenhäuser lahmlegte und aus dem Sicherheitslückenfundus des US-Geheimdienstes NSA stammte. Anstatt also mit Softwarehaftung und allgemeinen Sicherheitslücken-Meldepflichten[3] unsere IT-abhängige Gesellschaft wirklich sicherer zu machen, wird hier ein kurzfristiges Sicherheitsversprechen mit langfristiger brandgefährlicher IT-Unsicherheit[4] erkauft.

Neben der inhaltlichen Kritik verurteilt das FIfF auch den Gesetzgebungsprozess aufs Schärfste. Erstens wurden diese bislang tiefgreifendsten Ermächtigungen für Polizeien in einer digitalen Gesellschaft im Eiltempo durch den Gesetzgebungsprozess gepeitscht, sodass geladene sachverständige Personen und Parlamentarier gleichermaßen nur wenige Tage für die Vorbereitung der mündlichen Anhörung hatten. Zweitens wurden diese Änderungen als „Formulierungshilfe“ in einem ganz anderen Gesetzgebungsprojekt untergebracht, was sich eigentlich mit Schwarzarbeit, Fahrverbot oder Wilderei beschäftigte.[5] Drittens „vergaß“ das Bundesjustizministerium, die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Andrea Voßhoff, von dieser auswirkungsreichen „Formulierungshilfe“ in Kenntnis zu setzen,[6] sodass sie „erst am 17. Mai 2017 durch Medienberichte“ davon erfuhr. Dieser herrschaftliche und ignorante Gesetzgebungsstil scheint insgesamt langsam politischer Usus zu werden.[7]

Um es ganz deutlich zu sagen: Das FIfF glaubt nicht mehr an eine Häufung von *Zufällen* oder *bedauerlichen Missverständnissen* und ist daher geschockt, mit welcher Dreistigkeit die große Koalition aus CDU/CSU und SPD uns allen ins Gesicht lügt, dass sie Partizipation und Demokratie als Grundwerte Deutschlands schätzt. Jede aufrechte Person in der Politik hätte sich – unabhängig vom Inhalt der „Formulierungshilfe“ – weigern müssen, solche undemokratischen Abläufe zu unterstützen, auch nicht „mit Bauchschmerzen“. Gerade in der aktuell so aufgeladenen politischen Situation fördert diese objektiv hintertückische Gesetzgebungsweise verständlicherweise die Politikverdrossenheit und extreme Positionen. Bei einem solchen Parlament brauchen wir nicht einmal *fake news* oder *social bots*, um unsere Gesellschaft weiter zu spalten. Wenn schon regelmäßig nach einer Leitkultur gesucht wird, warum nicht ernsthaft einmal eine gute Demokratie in Erwägung ziehen?

Abschließend möchten wir an die Überwachungsgesamtrechnung des Bundesverfassungsgerichtes erinnern. Grundrechtsrelevante Maßnahmen dürfen nicht allein, sondern immer im Kontext aller anderen Maßnahmen bewertet werden, um additive Folgen mitzudenken. Mit den ständigen Ausweitungen und Ausweitungsversuchen von Überwachungsgesetzen, namentlich der neuerlichen Nutzungsfreigabe biometrischer Datenbanken, der Vorratsdatenspeicherung, der Fluggastdatenweitergabe, der Videoüberwachung oder der Bestandsdatenauskunft kommt nun ein weiterer Puzzlestein hinzu, der die Bundesrepublik einen weiteren Schritt weg von der freiheitlichen Grundorientierung hin zu einem repressiven Gesellschaftsmodell führt.

Keines der oben genannten Gesetze bringt bislang einen messbaren Sicherheitsgewinn bei teilweise haarsträubenden Grundrechtsfolgen, während auf der anderen Seite die Polizeien kontinuierlich beklagen, dass überall massiv Personal und Ausrüstung fehlt, um vorliegende Daten auswerten, um vorhandene Ermittlungsansätze verfolgen oder um einfach genug Beamte auf den Straßen haben zu können. Auch für eine Sicherheitserhöhung durch Prävention sind vielfache Ansätze bekannt, vom Einbezug von Schulstrategien bis hin zu Sozialangeboten. Nichts davon würde Grundrechte einschränken und alles würde tatsächlich Sicherheit bringen. Es würde eben Geld kosten, aber das wäre gut investiert.

Weitere Stimmen

Peter Schaar: „Arroganter Umgang mit der Macht zulasten der Demokratie und des Rechtsstaats“,
http://www.berliner-zeitung.de/politik/interview-ehemaliger-datenschutzbeauftrager-schaar-sieht-staatstrojaner-kritisch-27843956

Heribert Prantl: „Man soll nicht bei jeder Gelegenheit von einem Skandal reden. Aber das, was heute am späten Nachmittag im Bundestag geschehen soll, ist eine derartige Dreistigkeit, dass einem die Spucke wegbleibt.“,
http://www.sueddeutsche.de/digital/ueberwachung-der-staatstrojaner-ist-ein-einbruch-ins-grundgesetz-1.3555917

Patrick Beuth, Kai Biermann: „Wir analysieren es Satz für Satz und erklären, warum es wohl verfassungswidrig ist.“,
http://www.zeit.de/digital/datenschutz/2017-06/staatstrojaner-gesetz-bundestag-beschluss

Markus Reuter: „Dauerfeuer gegen das Grundgesetz – so treibt die Große Koalition das Land in den Überwachungsstaat“,
https://netzpolitik.org/2017/dauerfeuer-gegen-das-grundgesetz-so-treibt-die-grosse-koalition-das-land-in-den-ueberwachungsstaat/

Anmerkungen

1 *https://www.gesetze-im-internet.de/stpo/__100a.html*
2 *https://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html*
3 *https://cyberpeace.fiff.de/Kampagne/Forderung10*
4 *https://vimeo.com/216584485*
5 *http://dip21.bundestag.de/dip21/btd/18/112/1811272.pdf*
6 *https://netzpolitik.org/2017/bundesdatenschutzbeauftragte-ruegt-vorhaben-den-staatstrojaner-einsatz-drastisch-zu-erweitern/*
7 *http://www.faz.net/aktuell/feuilleton/aus-dem-maschinenraum/netzwerkdurchsetzungsgesetz-nicht-einmal-mehr-die-simulation-von-partizipation-15015559.html*

FIfF e. V. – Pressemitteilung

Verfälschte Studie zur Tauglichkeit grundrechtswidriger Techniken

FIfF lehnt automatisierte Identifizierung und Verhaltenskontrolle am Berliner Bahnhof Südkreuz ab

1. August 2017 – Am Berliner Bahnhof Südkreuz testen die Deutsche Bahn, das Bundesministerium des Innern und die Bundespolizei in Kooperation mit dem Bundeskriminalamt ab heute, ob es möglich ist, mit biometrischer Gesichtserkennung im öffentlichen Raum nach Menschen zu fahnden. In einer späteren Phase des Projektes sollen zusätzlich Verhaltenserkennung und Verhaltensbewertung zum Einsatz kommen.

Beim aktuellen Test könne man die als beobachtet markierten Bereiche noch umgehen, kündigte die Bundespolizei an. Tatsächlich sind die Bereiche jedoch so gewählt, dass zum Beispiel diejenigen, die auf eine Rolltreppe angewiesen sind, dem Blick der Kameras nicht ausweichen können. Wenn es zu einem späteren Echt-Einsatz solcher Systeme kommt, wird es einen unüberwachten Ausweichbereich ohnehin nicht mehr geben. Alle, die am öffentlichen Leben teilnehmen, müssen dann damit umgehen, dass sie in ihrer täglichen Nutzung der öffentlichen Verkehrsmittel von Computern in Echtzeit vermessen, analysiert, bewertet und in allen möglichen privaten Momenten identifiziert werden können. Gleichzeitig können diejenigen, nach denen gefahndet wird, sich mit einfachsten Maßnahmen wie Sonnenbrillen, Mützen, Bärten, Make-up oder dem einfachen Blick nach unten aufs Smartphone der Identifizierung entziehen.

Aussagekraft des Versuchs

Die Tests am Südkreuz sind nicht die ersten. Schon vor zehn Jahren testete das Bundeskriminalamt mit dem Projekt „Foto-Fahndung“ biometrische Gesichtserkennung am Mainzer Hauptbahnhof.[1]

Einer der Hauptgründe, warum dieser und vergleichbare Tests scheiterten, war, dass die überwachten Menschen einfach nicht gehorsam in die Kamera schauten. Auch ohne tieferes technisches Verständnis ist offensichtlich, dass ein Mensch, der vom Computer per Gesichtserkennung erkannt werden soll, kooperieren muss, indem er zumindest grob in die Richtung der Kamera schaut. Nur so können individuelle Merkmale wie Augen, Wangenknochen und Nasenrücken vom Blick der Kamera und der Analysesoftware erfasst und zur Identifizierung herangezogen werden.

Ganz offensichtlich will die Bundespolizei dem Problem der mangelnden Kooperation aus dem Weg gehen, um den Test am Südkreuz möglichst erfolgreich dastehen zu lassen – den Testpersonen wurden nämlich ausgerechnet dann „Attraktive Preise“ in Aussicht gestellt,[2] wenn sie besonders häufig vom System erfasst werden. Bei solchen Anreizen ist von den Testpersonen, vielleicht sogar unbewusst und mit den besten Absichten den

Test zu unterstützen, mit einer überdurchschnittlichen Kooperation zu rechnen. Selbst im Falle, dass die Teilnehmer nicht durch das Versprechen von Preisen aktiv kooperieren, ist doch davon auszugehen, dass sich die Probanden der Erkennung nicht absichtlich dauerhaft entziehen, wie es von tatsächlich Gesuchten bei einem späteren Einsatz zu erwarten ist.

Der Versuchsaufbau am Südkreuz ist somit realitätsfern. Das gilt auch deshalb, weil die Testpopulation nicht die Bevölkerung repräsentiert. Das verzerrt die Ergebnisse zusätzlich.[3] Nach wissenschaftlichem Maßstab und nach gesundem Menschenverstand hat der Test daher kaum Aussagekraft: Vom Test abgeleitete Aussagen über die Tauglichkeit von Gesichtserkennung für einen späteren Einsatz sind stark anzuzweifeln.

Qualität und Fehler der Gesichtserkennung

Um die Qualität von Gesichtserkennung zu bewerten, misst man, wie häufig es bei der Identifikation zu Fehlern kommt – wie häufig ein gesuchter Mensch tatsächlich im Bild erkannt wird und wie häufig jemand fälschlicherweise erkannt wird, also mit einem gesuchten Menschen verwechselt wird.

Diese Rate bewegt sich bei Gesichtserkennung sogar unter Laborbedingungen, also mit hochaufgelösten Kameras und sehr guter Ausleuchtung, immer noch zwischen 1:1000 bis 1:10000. Das bedeutet, dass bei einem späteren Einsatz sogar unter Idealbedingungen pro Tausend beobachteter Menschen einer als gesucht erkannt wird, der nicht gesucht wird, und einer, der tatsächlich gesucht wird, nicht erkannt wird. Im öffentlichen Raum sind wir sehr weit weg von solchen technischen Idealbedingungen, daher liegen die Raten von falsch zugeordneten und nicht erkannten Menschen weitaus höher. Auf eine Stadt wie Berlin hochgerechnet, in der Millionen Menschen täglich die öffentlichen Verkehrsmittel nutzen, ist die Zahl der verpassten Gesuchten und der Fehlalarme immens hoch und wahrscheinlich nicht praktikabel.

Am Südkreuz werden alle Menschen, die dem markierten Bereich nicht ausweichen oder aufgrund von körperlichen Einschränkungen nicht ausweichen können oder die die werbeähnlichen Markierungen gar nicht wahrnehmen, nun für mindestens sechs Monate von mehreren Kameras erfasst, ihr Gesicht vermessen und mit den Gesichtern aus der Testdatenbank abgeglichen. Auch hier wird es über den langen Zeitraum statistisch gesehen zu einer beträchtlichen Anzahl von Fehlern kommen, so dass Unbeteiligte fälschlicherweise erkannt werden. Bilder von Erkannten werden für die spätere Auswertung aufgehoben, so der Pressesprecher der Bundespolizei heute bei der Einführung des Tests. So ist damit zu rechnen, dass auch biometrisch vermessene Gesichter von Unbeteiligten wesentlich länger als die bei Videoüberwachung üblichen 48 Stunden gespeichert werden.

Ausbau der Videoüberwachung

Aus wissenschaftlicher Sicht ist vor mehr als zehn Jahren deutlich geworden, dass Videoüberwachung in den meisten Anwendungsgebieten keinen signifikanten präventiven Nutzen hat. FIfF-Vorstandsmitglied und Experte für Videoüberwachung und ihre Automatisierung Benjamin Kees kommentierte: „Ich bin empört und besorgt, dass trotz ausbleibender Präventionswirkung die Videoüberwachung immer weiter ausgebaut wird, dabei völlig unverhältnismäßig Grundrechte abgebaut werden und dies der Bevölkerung als notwendiges Eingeständnis für einen vermeintlichen Sicherheitsgewinn verkauft wird. Automatisierte Bewertung von Verhalten und Identifikation verunsichert Menschen bei der Teilnahme am öffentlichen Leben und ist ein weiterer durch Technikgläubigkeit fehlgeleiteter Versuch, ein gesellschaftliches Problem mit Computern zu lösen, die das nicht leisten können."

Verhaltensbewertung und Identifizierungssysteme im öffentlichen Raum reihen sich als invasive Elemente ein in eine nicht enden wollende Reihe von fragwürdigen Maßnahmen, die längst viel zu viele Bereiche des privaten und öffentlichen Lebens beeinflussen.

Das FIfF lehnt die Anfänge automatisierter Videoüberwachung entschieden ab. Ein System zu testen, das im aktiven Einsatz massiv gegen die Grundrechte verstoßen würde, ist absurd und verschwendet Steuergelder, die anderswo für echte Prävention und Sicherheit verwendet werden könnten.

Anmerkungen

1 *https://www.bka.de/DE/UnsereAufgaben/Forschung/Foto-Fahndung/foto-fahndung_node.html*

2 *https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/Nohomepage/170619_gesichtserkennung.html*

3 *https://netzpolitik.org/2017/ortstermin-am-suedkreuz-die-automatische-gesichtserkennung-beginnt/*

Hier findet der Versuch statt: Bahnhof Berlin Südkreuz bei einem Rundflug über Berlin Foto: Denis Apel, CC-BY-SA 4.0

Britta Schinzel

FREIHEIT 2.0, ein Kunstprojekt von Florian Mehnert

Editorial zum Schwerpunkt

Florian Mehnert realisierte im September und Oktober 2016 mit FREIHEIT 2.0 ein partizipatives Kunstprojekt im öffentlichen Raum in drei Ländern und drei Städten, in Weil am Rhein (D), Basel (CH) und Huningue (F).

Zunächst beschreibt Florian Mehnert sein Projekt und die Gründe, die ihn dazu veranlasst haben, ein politisch wirksames Kunstwerk zu schaffen. Er möchte damit einen anderen Zugang und ein besseres Hintergrundverständnis über die Gefahren von Big Data erzeugen. Könnte eine Kunstinstallation so einen Bewusstseinsprozess in der Gesellschaft einleiten, der den Geschäftspraktiken von Big Data die kollektive Zustimmung entzieht, so seine Frage.

Die Installation FREIHEIT 2.0 bestand aus 4 Elementen: Der *Self-Tracking-App*, die mittels der GPS-Funktion von Smartphones die Bewegungsprofile der Nutzenden generiert, zweitens den *FREIHEIT*-Umfirmierungen von Geschäften, drittens einem Leitsystem durch die Straßen der Stadt Weil am Rhein und schließlich den Big-Data-Kolloquien. Die letzteren werden in diesem Schwerpunkt verschriftlicht. Am Ende können auch aus der *Self-Tracking-App* erzeugte Bilder als Kunstwerke verkauft werden.

Christa Karpenstein-Eßbach erklärt in ihrem Text *Auf der Spur von Daten* von mehreren Seiten her Sinn, Ergebnisse und Erfolg des IT-getriebenen Projekts FREIHEIT 2.0: Einmal, welche Freiheitsbegriffe in diesem Zusammenhang von Bedeutung sind; dann, wieso dieses und ähnliche Projekte Kunst sind, obgleich dabei nicht immer Kunstobjekte im klassischen Sinne produziert werden; und schließlich, auf welche Weise die künstlerische Einlassung die Folgen von IT-Überwachung durch Datenerhebungen, Datensammlung und Big Data für Freiheiten einem breiteren Publikum sinnfällig macht. Sie geht dabei Mehnerts vier Elementen des Projekts nach, die eine Inszenierung von Big Data zwischen dem öffentlichen Raum und dem Alltagsverhalten von IT-Nutzenden darstellen, und so Abstraktes in den Raum sinnlicher Erfahrung bringen. Karpenstein-Eßbach zeigt, was diese Elemente uns zu erfahren und zum Nachdenken geben.

Benjamin Kees' Text schließt direkt an Florian Mehnerts Absichten an, die letzterer mit künstlerischen Mitteln verfolgt. Kees will Nicht-IT-Spezialisten, die zum Absaugen ihrer Daten die Haltung einnehmen „ich habe nichts zu verbergen", näherbringen, was man zu verlieren hat, wenn man überwacht wird. In seinem Vortrag verwendete er eine drastische Erzählung für die Folgen, wenn man seine eigenen Daten hinter- oder überlässt, indem er einem Menschen bei jeder Datenerhebung einen seine Aktivitäten notierenden Studierenden folgen ließ, sodass ihm am Ende abertausende protokollierende Studierende folgten. Hier allerdings wendet er sich an die Informatik-Community, um Hilfestellung zu geben, wie man der Vorstellung, die eigenen Daten gäben nur Auskunft über Regelverstöße, entgegnen kann. So beschreibt er die Möglichkeiten der technischen Mittel, und die Ableitungsfähigkeiten aus deren Gebrauch, durch Profilbildung analog einer Landkarte der unterschiedlichen Interessen und Eigenschaften einer Person. Um sich zu fragen, wozu die Daten dienen können, muss man sich einfach nur die Ziele der Datensammelwut vor Augen führen, nämlich aus den Daten auswertbare Informationen zu ziehen und diese gewinnbringend zu nutzen oder weiter zu geben, genau auf Kosten der Menschen, von denen die Daten erhoben wurden. Diese Ziele sind nämlich in den Modellen der Datenverarbeitung verbacken, und sie dienen nicht dem Vorteil der Daten Gebenden, sondern denen der Datenabsauger.

Udo Kauß diskutiert aus rechtlicher Sicht die präventive Überwachung, etwa des öffentlichen Straßenverkehrs durch eine automatische Kennzeichenerfassung, durch den Einsatz von Gesichtserkennungssystemen bei der Video-Überwachung von öffentlichen Räumen, oder – bisher verboten – vermittels automatisierter PKW-Mautsysteme. Während das Bundesverfassungsgericht im Volkszählungsurteil von 1983 Überwachung und Kontrolle des Verhaltens von Individuen als rechtlich bedeutsamen Eingriff in das allgemeine Persönlichkeitsrecht erkannt hat, hat es diesen Grundsatz in seiner Entscheidung zum Kfz-Kennzeichenscanning vom 11. März 2008 – ziemlich versteckt – konterkariert. Denn es hat zwar in dieser Entscheidung vom 11. März 2008 die große Bedeutung der Freiheit von Überwachung nochmals bestätigt, aber es liege kein Eingriff in das Grundrecht auf informationelle Selbstbestimmung vor, wenn sofort nach dem ergebnislosen Abgleich der erfassten Kfz-Kennzeichen mit der Datenbasis diese „spurenlos" gelöscht würden. Damit ist den dabei millionenfach erfassten Bürger.innen nicht nur jede rechtliche Kontrolle verwehrt, sondern die Exekutive kann dieses Überwachungsinstrument auch ohne gerichtliche Kontrolle zum Einsatz bringen. Zu meinen, mit einer sofortigen spurenlosen, so es sie gäbe, Löschung der Daten unbescholtener Bürger.innen sei das Problem gelöst, ist zu kurz gegriffen: Denn schon vor der Löschung sind diese bereits millionenfacher Gegenstand des digitalen Zugriffs und damit der Überwachung geworden.

Da die Logik dieser Entscheidung sich in gleicher Weise auf die Videoerfassung, die automatisierte Gesichtserkennung und andere automatisierte Kontrollinstrumente und die beim autonomen Fahren entstehenden Datenströme anwenden bzw. erweitern lässt, wäre damit die rechtsfreie staatliche (und zivile) Kontrolle des öffentlichen Raumes konstituiert. Dies ist von allergrößter Relevanz und hier ist Gegenwehr geboten. Eine hoffentlich korrigierende Entscheidung des Bundesverfassungsgerichts wird für dieses Jahr erwartet.

Der Ausbeutung der Daten nicht nur aus den Kennzeichen, sondern aller verbundenen Geräte und Instrumente würde beim autonomen Fahren kaum mehr Grenzen gesetzt sein, ginge es nach den Vorstellungen der Autoindustrie. Der Text *Connected Cars* von Christoph Stürmer und Britta Schinzel betrachtet die prospektive Zukunft autonomen Fahrens und der damit verbundenen Datensammlung aus Sicht der Automobilindustrie bzw. einer von ihr beauftragten Unternehmensberatung. Das künftige Geschäftsmodell der Fahrzeugfirmen werden nicht die materiellen Autos selbst sein, sondern die mit ihrer Hilfe zu gewinnenden Daten und die folgend aus ihnen zu entwickelnden Dienstleistungen. Der Text behandelt die komplexen Entwicklungsschritte, die auf dem Wege hin zu autonomen Fahrzeugen und autonomem Fahren zu berücksichtigen sind, so etwa die Notwendigkeit des Einsatzes selbstlernender Systeme, da die Vielzahl der komplexen Umweltkonditionen nicht explizit kodierbar wäre. Im Text werden auch die dafür notwendigen politischen Änderungen, etwa des Datenschutzes, und die damit einhergehenden rechtlichen, sozialen und ethischen Probleme nicht ausgespart. Es gibt innerhalb des Europäischen Parlaments Bestrebungen, Robotern und KI einen eigenen Rechtsstatus als „elektronische Person" zuzubilligen. Aber KI und selbstlernende Systeme können zwar haftbar gemacht, aber nicht wirksam sanktioniert werden. Jedoch sind die ursprünglichen Designer der Softwaresysteme auch nicht mehr haftungspflichtig, denn sie sind nicht mehr die Autoren einer Software, die sich durch autonome stochastische Prozesse und Lernvorgänge in nicht nachvollziehbarer Weise verändert hat.

Mit *Everyware* betrachtet Britta Schinzel die Möglichkeiten, die das Internet der Dinge (IoT) für immer neue Geschäftsmodelle geschaffen hat. Während ein wichtiges Element für die Wertschöpfung im verdrahteten IT-Bereich, etwa bei Apple, Google und Facebook, die Kundenbindung ist, konnte die Monetarisierung der Nutzungsdaten so auf die bisherige Offline-Welt des IoT ausgeweitet werden. Diese Monetarisierung der Nutzungsdaten gereicht gerade den beiden kostenlosen Internetdiensten Google und Facebook zu enormen Gewinnen. In mehreren Stufen, beginnend mit Datennutzung für die Werbung, und später der verbesserten personalisierten Werbung mittels Profilbildung der Nutzenden aus ihren Daten wurden die Datenvolumina vermehrt und in immer größeren Serverfarmen ausgebeutet. Ihre Zentralisierung in Clouds, ihre Auswertung durch Data Mining, Lernverfahren und „Künstliche Intelligenz" in Big Data hat die sogenannten *Big Five* zu übermächtigen Firmen anwachsen lassen, die heute praktisch jedes Unternehmen auf der Welt kaufen können. Datenkapitalismus und Überwachungskapitalismus, und schließlich ihre Verwertung in immer neuen Dienstleistungen, das gelingt in einem neuen Entwicklungsschritt durch die Einschaltung in alle möglichen Beziehungen zwischen Personen und Institutionen. Die *Smartness* der Gadgets liegt dabei nicht in ihrer lokalen Intelligenz, sondern in ihrer Konnektivität. Sie sind Interfaces einer globalen „Intelligenz", automatisch gesteuert über die Clouds und ihre Dienste, die sich in unsere Relationen einschaltet. Doch es sollte dabei nicht vergessen werden, dass die Automatisierung absichtsvoll von einer kapitalistischen Logik instanziiert und – kontingent – demgemäß modelliert wurde.

Matthias Kampmanns Text *Die Einheit. Aufgehoben im Zustand des Aufgehobenen* stellt ein eigenes schriftstellerisches Kunstwerk dar.[1] Während er bei den Big-Data-Kolloquien einen Text in Gedichtform verlas, verwendet er hier die Fließtextform. Er behandelt in einer zynisch-ironischen Dystopie eine nicht allzu ferne Zukunft von einem von Technik getriebenen Paradies. Der Autor versucht, sich in radikal affirmativer Weise in die vorstellbaren Mutationen der Gesellschaft und des freiheitlichen Denkens unter der Ägide jener Techno-Vorstellungen einer hybriden Menschheit einzudenken. Eine scheinbar glückliche Ära ohne Kriege, Polizei und Verbrechen wird projiziert, ein neues *Goldendes Zeitalter*, in der jede Herrschaftsform außer der technischen Totalität ihr Ende gefunden hat.

Mögen wir beurteilen, was uns lieber ist, die Risiken einer Aufgehobenheit in einem solchen totalitären Paradies, oder vielleicht doch die in anderer Weise risikobehafteten Freiheiten in Abwesenheit von Überwachung.

Anmerkung

1 *Im Übrigen findet sich unter https://www.weisskunst.de/dr/node/56 ein aufschlussreiches Wechselgespräch zwischen Florian Mehnert und ihm.*

Florian Mehnert

Die soziale partizipative Kunstinstallation FREIHEIT 2.0

Google kennt unsere Sorgen, unsere Interessen und unser nächstes Urlaubsziel. WhatsApp weiß, mit wem wir kommunizieren. YouTube weiß, welche Videos wir betrachten und Instagram kennt unser gepostetes Leben. Amazon Echo und Google Home wissen, was zu Hause gesprochen wird, und der smarte Fernseher blickt in unser Schlafzimmer. Facebook kennt uns besser als unsere Freunde, und Amazon weiß schon heute, was wir morgen kaufen werden. Das System Big Data registriert unser Leben in allen seinen Verästelungen.

Erhoben werden persönliche und private Daten permanent, immer und überall.

Wir alle, die Nutzer des Internets, die Verbraucher und Konsumenten sind die Quelle des kostenlosen Daten-Rohstoffs für einen neuartigen Produktionsprozess: die Vorhersage unseres menschlichen Verhaltens. Die Big-Data-Industrie strebt deshalb nach einem Echtzeitmodell unseres täglichen Lebens. Die daraus resultierenden Geschäftsmodelle und Kommerzialisierungsprozesse sind risikoarm und schaffen Milliardengewinne. Big Data stellt die Prinzipien der Selbstbestimmung über psychisches und soziales Leben und ebenso unser Verständnis vom politischen System in Frage. Unsere Privatsphäre und unser Selbstverständnis von Freiheit stehen vor der völligen Auflösung, indem die Geschäftsmodelle der Big Data die Souveränität des Menschen angreifen.

Gibt es einen Ausweg?

Könnte man einen Bewusstseinsprozess in der Gesellschaft einleiten, der den Geschäftspraktiken der Big Data die kollektive Zustimmung entzieht?

Könnte eine Kunstinstallation einen anderen Zugang, ein besseres Hintergrundverständnis von Big Data erzeugen?

Im September und Oktober 2016 realisierte ich in Weil am Rhein (D), Basel (CH) und Huningue (F) die partizipative Kunstinstallation FREIHEIT 2.0.

FREIHEIT 2.0 wurde als trinationales Kunstprojekt im öffentlichen Raum in drei Ländern und drei Städten umgesetzt. Die Installation sollte eine differenzierte Sicht auf die Herausforderung durch den Umgang mit Big Data in unserer digitalen Parallelrealität ermöglichen und die Wechselwirkungen zwischen der digitalen und der analogen Welt sichtbar machen.

Ich wollte darauf hinweisen, dass demokratische Errungenschaften wie die persönliche Freiheit ein kostbares Gut sind, die es in einer zunehmend digitalen Welt zu verteidigen gilt. Ich wollte die vielschichtige Thematik der Big Data über eine Kunstinstallation in den öffentlichen Raum transportieren. Mir ist es wichtig, FREIHEIT 2.0 nicht mit einer politischen Aktion verwechselt zu sehen, oder einen Erfolg des Projekts an der erreichten oder nicht erreichten Tiefenwirkung seiner Aufklärung zu messen. Hinter FREIHEIT 2.0 stand für mich auch die Fragestellung, inwieweit eine groß angelegte partizipative Installation über Freiheit im öffentlichen Raum umsetzbar ist. Ob es eine Bereitschaft zur Partizipation gibt und inwieweit Menschen bereit sind, sich auf die abstrakte Form der Installation einzulassen.

Die Installation FREIHEIT 2.0 bestand aus 4 Elementen: Der *Self-Tracking-App*, den Umfirmierungen von Geschäften, einem Leitsystem durch die Straßen der Stadt und den Big-Data-Kolloquien.

Die *Self-Tracking-App*

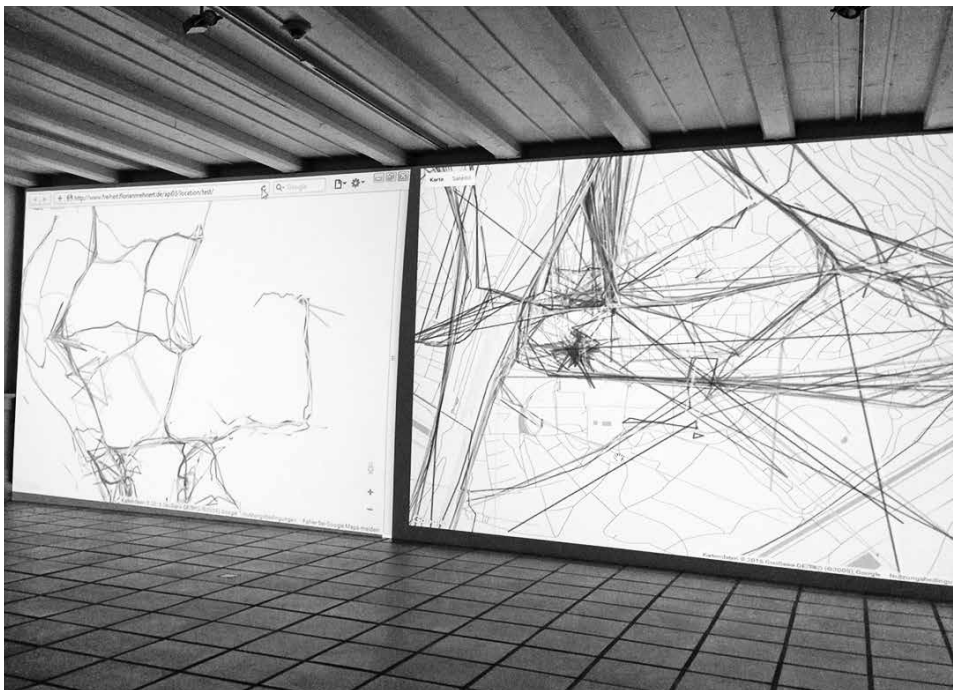
Für das Projekt FREIHEIT 2.0 wurde eine *Self-Tracking-App* programmiert. Die App war Teil des Kunstprojekts und nutzte die GPS-Funktion des Smartphones, um alle 30 Sekunden die geographische Position zu bestimmen. Dadurch entstanden Daten, die es ermöglichten, Bewegungsprofile der Nutzenden zu generieren. Die Daten wurden anonymisiert und verschlüsselt an den projekteigenen Server versendet. Die *Self-Tracking-App* veranschaulichte, wie aus individuellen Bewegungen in der analogen Welt Daten gewonnen werden.

Bewegungsprofile gelten in der Daten-Industrie als eine der wichtigsten Ressourcen, die gehandelt und ausgewertet werden. Die *Self-Tracking-App* diente als Schnittstelle zwischen der analogen und digitalen Welt. Sie wurde dazu eingesetzt, ein Bewusstsein für die Sensibilität der eigenen Daten zu schaffen.

Die Auswertung der *Self-Tracking-App* konnte während der Projektphase im Kunstverein der Stadt Weil am Rhein als Großprojektion betrachtet werden.

Florian Mehnert

Der Künstler **Florian Mehnert** erlangte mit mehreren Kunstprojekten und Ausstellungen über das Thema Überwachung international Aufmerksamkeit. In seinem Kunstprojekt *Waldprotokolle* verwanzte er Wälder mit Mikrofonen, die vorbeigehende Passanten abhörten. In seiner Videoinstallation *Menschentracks* zeigt er 42 Videosequenzen gehackter Smartphones, deren Kameras und Mikrofone ferngesteuert aktiviert wurden. *(www.florianmehnert.de)*



Großprojektion *im* Kunstverein der Stadt Weil am Rhein

Tracking App

Die App ist nach wie vor in drei Sprachen (Deutsch, Französisch, Englisch) verfügbar und kann von jedem Smartphone in Google Play und im AppStore gratis geladen und verwendet werden. Der Server nimmt nach wie vor verschlüsselte Daten entgegen. Viele Nutzer sind aktiv und haben inzwischen Spuren von Zagreb bis Stockholm und von Irland bis Budapest gelegt. Eine aktuelle Visualisierung ist unter *http://www.freiheit.florianmehnert.de/tracking.html* zu sehen.

Die Umfirmierungen

Im Vorfeld des Projekts überzeugte ich in Vorträgen und Einzelgesprächen über 20 Geschäftsleute in Weil am Rhein, Basel Riehen (Schweiz) und Huningue (Frankreich), sich an FREIHEIT 2.0 durch eine Umfirmierung an ihrem Geschäft zu beteiligen. Darunter befanden sich unter anderem Optikergeschäfte, eine Apotheke, ein Sportgeschäft, ein Weingeschäft, ein Spielwarenladen, eine Buchhandlung, ein Blumengeschäft und auch die Weiler Zeitung.

Ich plante und gestaltete alle Umfirmierungen im jeweiligen Design der Geschäfte und installierte diese für den Projektzeitraum von 5 Wochen an den Geschäften. Bestehende Schriftzüge wurden mit Folien überklebt oder teilweise auch mit Planen auf aufwendigen Unterkonstruktionen überhängt.

Aus der Apotheke am Rathaus wurde die „Apotheke der Freiheit". Aus Intersport wurde „FREIHEITSport", das Blumengeschäft wurde zu „Blumen der Freiheit", die Buchhandlung zur „Buchhandlung der Freiheit", die Weiler Zeitung zur „Zeitung der Freiheit". Die temporäre Umfirmierung der Geschäfte durch den Begriff der FREIHEIT stellte öffentlich die Frage nach dem Wert und der Bedeutung der Privatheit und individuellen Freiheit. Die Umfirmierungen dienten dazu, die Unsichtbarkeit des Freiheitsverlusts zu thematisieren und die Auseinandersetzung

Apotheke der Freiheit

Drogerie der Freiheit

darüber öffentlich anzustoßen. Es entstand für die Passanten eine Art Stolperstein, eine Plattform der Diskussion und Auseinandersetzung über die Bedeutung und notwendige Neudefinition der Privatheit in ihrem Bezug zur digitalen Welt.

Das Leitsystem

Das über Tage hinweg auf den Straßen der Stadt Weil aufgebrachte, über 20 Kilometer lange Leitsystem visualisierte den unsichtbaren Datenfluss der digitalen Welt. Gleichzeitig spiegelte das Leitsystem die Bewegungsprofile der Tracking-App FREIHEIT 2.0 wider.

Von jedem teilnehmenden umfirmierten Geschäft führte je eine Linie über die Straßen und Bürgersteige bis hin zum „Büro der Freiheit" (im umfirmierten Kunstverein), wo sich alle Linien bündelten. Um Publikumsverkehr zu vermeiden, arbeitete ich entweder nachts oder in den sehr frühen Morgenstunden an dem Leitsystem. Es kam meist zu positiven Reaktionen und Gesprächen. Nur in einer Nacht musste ich meine Arbeit aufgrund zu aggressiver Reaktionen von Nachtschwärmer.innen abbrechen. Das Leitsystem wurde von der Bevölkerung teilweise als unerhörter Eingriff in ihren öffentlichen Raum empfunden. Es gingen zahlreiche Beschwerden bei der Stadtverwaltung ein, die mich daraufhin dringend bat, im Vorfeld eine Pressemeldung über das Leitsystem zu veröffentlichen.

Ausschnitt aus dem 20 Kilometer langen Leitsystem

Die Big-Data-Kolloquien

Die Kolloquien fanden jedes Wochenende während des 5-wöchigen Projekts im Büro der Freiheit statt. Die Kolloquien waren ein wichtiges Element des Projekts, denn sie hinterfragten und diskutierten mit der Unterstützung von eingeladenen Referent.innen die Hintergründe und Vorgehensweisen der Big Data. Die Referent.innen kamen aus den Fachgebieten der Medientheorie, Informatik, Wirtschaft, Recht und Philosophie.

Die Kolloquien vertieften und intensivierten den partizipativen Ansatz des Projekts. Sie boten den Teilnehmer.innen nicht nur die Möglichkeit zur Bildung, sondern schufen einen Treffpunkt des Gedankenaustauschs und der Entwicklung neuer Denkmodelle.

Alle Vorträge der Kolloquien sind online unter *http://www.freiheit.florianmehnert.de/tv* abrufbar.

Die Paneldiskussion mit (von links) dem Programmierer Benjamin Kees, Professorin Christa Karpenstein-Eßbach, dem Medienwissenschaftler Andreas Leo Findeisen und dem Künstler Florian Mehnert – Foto: Adrian Steineck

Die Partizipation als künstlerisches Element

FREIHEIT 2.0 war eine soziale partizipative Installation, in der die Menschen ein wichtiges mitgestaltendes Element des Werks waren. FREIHEIT 2.0 integrierte den öffentlichen Raum, die Teilnehmenden und Passant.innen in die Kunstinstallation. Jede.r konnte das Projekt mitformen: Durch das Nutzen der *Self-Tracking-App*, durch Diskussionen auf dem Bürgersteig oder in den Geschäften, durch eigene Gedanken, die er/sie auch in den Big-Data-Kolloquien zum Ausdruck bringen konnte.

FREIHEIT 2.0 war in seinem Aufbau, durch die Umfirmierungen und das Leitsystem, auch eine künstlerische Form der initiierten sozialen Revolte.

FREIHEIT 2.0 arbeitete mit einem erweiterten Kunstbegriff, in dem jeder auf seine Weise Gestaltender und „Former" seiner Umwelt und Gesellschaft ist. Die teilnehmenden Geschäfte und ihre Mitarbeiter, die Stadt Weil am Rhein, die Passanten im öffentlichen Raum, die Besucher der Kolloquien, alle waren Teil und gestaltendes „nach- und mitdenkendes" Element von FREIHEIT 2.0. Zahlreiche hinterlassene und sich bis heute erweiternde Spuren von Nutzern der *Self-Tracking-App* zeugen von der Begeisterung zur Mitgestaltung. Die Mitarbeiter der umfirmierten Geschäfte waren täglich den Fragen ihrer Kunden ausgesetzt und es ergaben sich lebhafte Diskussionen.

Ich traf während der Projektzeit Schüler.innen, die eine Stadtrally entlang des Leitsystems machten. Ältere Menschen erbaten Hilfe bei der Installation der App. Ich führte unzählige Gespräche mit Menschen in und auch außerhalb der Kolloquien.

Der Oberbürgermeister der Stadt Weil ließ als Statement während der Projektzeit anstelle der Stadtfahne die FREIHEIT 2.0-Fahne hissen.

Oberbürgermeister Wolfgang Dietz vor der gehissten Fahne – Foto: Ulrich Senf

FREIHEIT 2.0 hat auch mein Verständnis über die Haltung der Gesellschaft zu den Entwicklungen der Big Data vertieft. Der Begriff der Freiheit, im Zusammenhang mit der digitalen Parallelwelt stehend, traf bei vielen Menschen auf Interesse. Das Projekt FREIHEIT 2.0 zeigte auf, dass vor allem jüngere Menschen (15 bis 18 Jahre) ein häufig ungetrübtes Verhältnis zur ihren Daten haben. Manche fragen sich gar, warum ein „öffentliches" Ich denn nicht in Ordnung ist. Ganz nach der Aussage von Zuckerberg, „Privacy is obsolete", halten viele junge *Digital Natives* die Diskussion um die Privatsphäre für wenig relevant. Dies liegt zum einen am natürlicherweise starken Bedürfnis nach Kommunikation mit Gleichaltrigen. Sie findet über Smartphones mit den bekannten Apps wie WhatsApp, SnapChat und auch Facebook statt. Es ist das Grundbedürfnis des Menschen, zu kommunizieren, sich mitzuteilen, Erlebnisse zu teilen. Das Internet und Smartphones sind wie geschaffen dafür. Dass wir alle die kostenlosen Kommunikations- und Expressions-Werkzeuge der Industrie begeistert annehmen, entspricht dem Naturell des Menschen.

Zudem arbeitet die Big-Data-Industrie mit einer operanten Konditionierung und positiven Verstärkung. Wer viel postet, macht sich interessant und wird durch viele Likes, Follower und Kommentare belohnt und vielleicht zum Instagram- oder YouTube-Star gekrönt. Wer nicht mitmacht, rutscht in die soziale Exklusion. Ein Aufruf zu mehr Vorsicht im Umgang mit den eigenen Daten oder Verschlüsselung lindert, aber löst die Grundproblematik nicht.

Versicherer experimentieren mit smarten Gesundheits- oder Telematiktarifen. Facebook und Google arbeiten mit Microtargeting, Amazon mit *Dynamic Pricing* oder *Anticipatory Shipping*. Wer keine Echtzeitdaten liefert, ist nicht einschätzbar und wird in Zukunft für das Recht auf seine Privatsphäre teuer bezahlen müssen. Die Möglichkeit der im Voraus berechenbaren Kund.in rückt in greifbare Nähe. Das systematische Auswerten und die Korrelation aller persönlichen Daten, das Anlegen von Persönlichkeitsprofilen, Psychogrammen und dem digitalen Profiling führen zur systematischen Vernichtung unserer Privatsphäre.

Jungen Menschen fehlt darüber teilweise der Einblick und die Weitsicht in Bezug auf ihre Daten und die dahinterstehende verwertende Industrie. Es fehlt Wissen darüber, welchen monetären Wert Daten haben. Welcher begeisterte jugendliche Pokémon-Go-Spieler durchschaut im Vorfeld, dass das Gratisspiel in Wahrheit mit jeder Menge persönlicher Daten bezahlt wird? Nicht das Spiel ist das Produkt, sondern der Mensch, der spielt.

Unterschiedlich ist es bei den *Digital Immigrants*. Hier herrscht eher ein wertkonservativeres Weltbild in Bezug auf ihre Privatsphäre, die als wichtiges und elementares Gut angesehen wird. Aber auch hier existiert sozialer Druck. Ein Teilnehmer der Kolloquien berichtete, wie er durch den Austritt aus einer WhatsApp-Gruppe in Konflikt mit seiner Partnerin geriet, die sich vor Freunden rechtfertigen musste, weil sein Austritt als Ablehnung und Desinteresse interpretiert wurde.

Vor allem die *Digital Natives* nehmen wenig wahr, dass die digitalen Persönlichkeitsprofile in vielfacher Weise in ihre reale Welt zurückwirken. Manchmal entstand für mich der Eindruck, dass das „gläserne Ich" bereits zur Selbstverständlichkeit geworden ist. Es schien manchmal, als ob das Verhältnis zur Privatsphäre im Begriff ist, sich in eine andere, weit weniger kritische Haltung zu wandeln. Die Gründe liegen womöglich in der Bequemlichkeit, dem Wunsch nach Sicherheit, in einem optimistischen Glauben an das Gute, an den Fortschritt und in der Begeisterung für die technischen Möglichkeiten.

Häufig steht die Begeisterung für die Möglichkeiten und Verheißungen der Big Data im Vordergrund: „Wenn man beständig alle verfügbaren Daten sammelt und korreliert, wird man der Wahrheit näherkommen. Man wird das menschliche Leben in all seinen komplexen Prozessen besser verstehen und für jeden Einzelnen ein besseres Leben erschaffen," so wirbt die Big-Data-Industrie.

Allerdings müssen dafür die Selbstbestimmung und die Privatsphäre im Gegenzug geopfert werden.

Bei dem Glauben an einen *Dataismus*, der den Konsumenten eine kontrollierte, berechenbare und sichere Welt verspricht, wird übersehen, dass es sich in erster Linie um neue kommerzielle Wertschöpfungsprozesse und um wirtschaftliche Interessen großer Datenindustriegiganten handelt. Diese Konzerne sammeln die Daten ihrer Milliarden Nutzer in ihren unerschöpflichen Datenspeichern. Deren hochqualifizierte Teams programmieren die intransparenten Algorithmen, die aus unseren Daten Informationen und Auswertungen berechnen. Es handelt sich um eine unidirektionale Vorgehensweise, in der wir Nutzer eine Industrie mit unseren Daten versorgen, oft ohne zu wissen, in welcher Form diese ausgewertet und kommerzialisiert werden.

Allen Gruppen gemeinsam war häufig das fehlende Hintergrundwissen und eine Vorstellung davon, wie tiefgreifend sich das tägliche und auch gesellschaftliche Leben durch Datenkorrelationen und deren Auswertungen verändert. Es fehlt eine Vorstellung davon, was es bedeutet, ein Leben als berechneter, berechenbarer Mensch zu führen, über den Konzerne mehr wissen als man über sich selbst weiß. Es fehlen Kenntnisse darüber, auf welche Art und Weise und wie tief die Big-Data-Industrie in viele Lebensbereiche schon vorgedrungen ist. Die Frage nach Lösungen im Umgang mit Big Data wurde am Ende der Diskussionen der Kolloquien oft thematisiert, es blieb die Erkenntnis, dass die Bewusstseinsprozesse in der Gesellschaft und Politik erst begonnen haben.

Eine Idee der Big Data ist es, Persönlichkeitsmuster zu extrahieren und Echtzeit-Ergebnisse über menschliches Verhalten vorauszusagen und dies dann kommerziell zu verwerten. Die Zerstörung der menschlichen Würde und der freiheitlichen demokratischen Grundordnung wird von der globalen Big-Data-Industrie, ihren Investoren und Aktionären in Kauf genommen.

FREIHEIT 2.0 hat einen ersten Schritt unternommen, die Vorgehensweisen der Big Data in Form einer sozialen partizipativen Kunstinstallation zu hinterfragen. Es gilt, sie als Plattform zu nutzen, um zu diskutieren, zu lernen und zu erkennen, dass wir in Bezug auf Big Data eine globale Wirtschaftsethik entwickeln müssen, die den Menschen auch in Zukunft in seiner Würde schützt.

Christa Karpenstein-Eßbach

Auf den Spuren von Daten

Künstlerische Sichtungen im Unsichtbaren digitalisierter Alltäglichkeit

Wie können Vorgänge wie das Sammeln, Speichern und Vernetzen von Daten, die sich unserer sinnlichen Erfahrung entziehen, künstlerisch ansichtig gemacht werden? Die Kunstinstallation FREIHEIT 2.0 *von Florian Mehnert komponiert vier Elemente, die die Datenfrage zwischen dem öffentlichen Raum und der Privatheit des Alltagsverhaltens von Datenjägern und -sammlern ansiedeln. In der inszenierten Verdopplung von BIG DATA liegt der ästhetische Widerstand von FREIHEIT 2.0.*

1. Freiheit im informationstechnischen Kontext von Big Data

FREIHEIT 2.0 lautet der Name der interaktiven Kunstinstallation von Florian Mehnert. Was ist das für eine Freiheit, mit der wir es hier zu tun haben? Der Frage nach *Freiheit* und *Big Data* gelten zunächst die Überlegungen, um dann die vier Elemente dieser Kunstinstallation und ihre Bedeutungen wie Erfahrungspotentiale für die *Nutzer* zu entschlüsseln; abschließend geht es um die Versprechungen und die Faszination von Verdatungen sowie um die Frage nach der spezifischen ästhetischen Leistungskraft dieser Kunstinstallation.

Lässt man beim programmatischen Namen FREIHEIT 2.0 die Zahlen Zwei und Null erst einmal fort, dann kann man einen kleinen Katalog von Freiheitsvorstellungen anlegen. Freiheit ist die Abwesenheit von Zwang, Gewalt und Unterdrückung; ist die Freiheit, Nein sagen zu können und sich dem Ansinnen eines anderen zu entziehen; ist, so die berühmte Formulierung Rosa Luxemburgs, die Freiheit des Andersdenkenden; sie besteht in der Freiheit, die eigene Lebensweise zu wählen und vielleicht anderem mehr. Es sind positive und negative Bestimmungen von Freiheit, die aber eines gemeinsam haben: mit ihnen verbinden sich ideelle Momente, die auf wesentliche Weise die Lebensführung orientieren. Solche Freiheitsvorstellungen materialisieren sich auf vielfältige Weise im individuellen Verhalten wie in sozialen Verhältnissen und finden dort einen bemerkbaren und sichtbaren Ausdruck. Freiheit ist nicht gleichbedeutend mit einem guten oder angenehmen Leben, denn bekanntlich kann man auch in Diktaturen ein solches Leben führen, weil es auch dort Sicherheit und Wohlstand geben kann. *Freiheit* und *Leben* sind Begriffe, die auseinanderzuhalten sind, weil sie in sehr verschiedene Werthorizonte eingelagert sind, einmal bezogen auf ideelle Regulative der Lebensführung und Gesellschaftlichkeit, zum anderen auf Steigerungsprozesse des bloßen Lebens selbst.

Wenn der Freiheit die beiden Ziffern Zwei und Null angehängt werden, könnte diese Differenz von Freiheit und Leben fraglich und problematisch werden. *2.0* verweist auf die virtuellen Welten digitaler Rechenoperationen im 0/1-Code, auf das Sammeln, Speichern, Verarbeiten und Vernetzen von Datenmengen. Im Unterschied zur jüngst ausgerufenen Welt der *Industrie 4.0*, in der Maschinen sich selbst und im Verbund untereinander ohne die Anwesenheit von Menschen nach Programmen selbst steuern, spielt die Körperlichkeit des Menschen auf einer 2.0-Stufe noch eine Rolle, denn die Prozessualisierung von Daten ist an die *Wetware* des Menschenkörpers noch angeschlossen. Genauer: ohne diese *Wetware* der Leute, die etwas machen, sich bewegen oder irgendwie verhalten, gäbe es keine Daten, mit denen zu rechnen wäre. In der Polarität von Sichtbarkeit und Unsichtbarkeit formuliert: das Verhalten von Menschen fällt in das Gebiet des Sichtbaren, die Datenmengen, die aus ihm gewonnen werden, sind in der Regel unsichtbar – mit Ausnahme für diejenigen, die die Daten auswerten.

Eine ziffernlose Freiheit zeigt sich und wird erfahrbar in individuellem Verhalten und gesellschaftlichen Beziehungen. Eine *Freiheit 2.0* hingegen etabliert ein Gebiet, das sich sinnlicher und sozialer Erfahrung entzieht. In der Welt des digitalen Sammelns und Prozessierens von Daten kann alles gerechnet und verschaltet werden, weil der basale Code von Null/Eins und alle Bits ge-

genüber dem, was gesammelt und gerechnet wird, völlig indifferent sind und sich unterschiedslos auf alles beziehen können. Mit den Worten des Medienphilosophen Jean Baudrillard gesagt: „Auf dem Höhepunkt einer immer weiter vorangetriebenen Vernichtung von Referenzen und Finalitäten, eines Verlustes von Ähnlichkeiten und Bezeichnungen entdeckt man das digitale und programmatische Zeichen, dessen ‚Wert' rein *taktisch* durch die Überschneidung mit anderen Signalen (Informationskorpuskel/Text) bestimmt wird, und dessen Struktur ein mikro-molekularer Code von Kommando und Kontrolle ist. (…) es bleibt nur die ‚black box' des Codes."[1]

2. Ästhetische Erfahrungselemente der Installation FREIHEIT 2.0

Freiheit unter den Bedingungen von 2.0 zum Gegenstand von Kunst zu machen, ist mit dem Problem konfrontiert, eine solche *black box* sichtbar zu machen. Nun haben es sich die Künste immer schon angelegen sein lassen, etwas sichtbar zu machen, was man zuvor so nicht gesehen hatte, wenn z. B. Adolph von Menzel im 19. Jahrhundert sein *Eisenwalzwerk* malt und die harten Arbeitsbedingungen von Industriearbeitern anschaulich macht. Hier ist es so, dass etwas, das man wirklich sehen kann, in einer neuen Sichtweise erscheint, die mit einem anderen Sehen und einer Verschiebung gewohnter Wahrnehmungen einhergeht. Das ist aber im Fall der digitalen Datenwelten nicht der Fall. Es hätte Florian Mehnert wohl nicht viel genutzt, den Maschinenraum eines Datensammelunternehmens aufzusuchen, um daraus Material für ein Kunstwerk zu gewinnen, denn hier muss man etwas anderes tun als ein Bild zu malen. Um die Datenfrage in den Raum sinnlicher Erfahrung und bemerkbaren Ausdrucks zurückzuholen, hat er die Kunstinstallation aus vier Elementen komponiert, die im Folgenden skizziert werden, indem ich mich auf die Frage einlasse, was diese Elemente uns zu erfahren geben und für unser Nachdenken erzeugen könnten.

2.1. Bewegung im Raum: Laufbahnen

Das sind zunächst die Markierungen auf der Straße. Wie bei einem Leitsystem handelt es sich um vorgebahnte Wege, denen ich folge. Anders als bei Schildern, die aufgestellt sind und die mit erhobenem Haupt gelesen werden, fällt der Blick hier von oben auf die Erde, ganz so, wie in der Perspektive von Google Earth auf die Erde geschaut wird. Die Laufbahnen geben mir Wege vor, scheinen aber mit einem Parcours, auf dem Hindernisse zu überwinden wären, so wenig zu tun zu haben wie mit einer Schatzsuche, an deren Ende eine Belohnung für die Mühen des Suchens steht. Ein Ziel wie bei Schildern – etwa „Rathaus 500 m" oder „Bielefeld 378 km" – ist nicht angegeben. Die Laufbahnen markieren eine vororganisierte Bewegung im öffentlichen Raum, einen Weg, der nicht *mein* Weg ist, sondern eine Bahnung für alle, deren Ziel nicht bekannt gemacht wird.

Nun gibt es zwar durchaus ziellose Bewegung in der Stadt in Gestalt des Flaneurs oder Streuners, aber von diesem Leitsystem, dessen Ziel erst einmal nicht ausgewiesen ist, geht vor allem der Imperativ aus, doch nicht vom Wege abzukommen. Dass das gefährlich sein kann, wissen wir schon von Rotkäppchen. Auf dem Weg zu bleiben: dies könnte auch für den Touristen gelten, der die Tour der Sehenswürdigkeiten absolviert. Aber die Laufbahnen der Kunstinstallation bieten nichts Spektakuläres an, im Gegenteil: wer ihnen folgt, kommt im Geschäft an. Eben dies ist eine wiederkehrende Erfahrung der Bewegung im öffentlichen Raum der Stadt. In gewohnten Bahnen zu laufen, zum Bäcker, Supermarkt oder Copy-Shop, gehört zur gewöhnlichen Alltäglichkeit. Wenn ich nun, statt meiner gewohnten Wege zu gehen, bei denen ich gemeinhin annehme, dass sie keine Spuren hinterlassen, den Laufbahnen der Installation folge, dann spure ich im doppelten Sinne: ich folge der Spur, die durch sie markiert ist, und ich spure in dem Sinne, wie es einer tut, der etwas befolgt und gehorcht. Ich bemerke einen Doppelsinn, vielleicht gar einen Widerspruch in meinem Tun, denn ich füge mich in etwas ein und ich spüre etwas auf, während ich auf den Boden gespurter Bahnen blicke.

Diese Straßenmarkierungen verweisen auf nichts, weil sie ja nicht wie Schilder funktionieren. Sie eröffnen eher einen Erfahrungsraum, der verschiedene Aspekte miteinander verknüpft: Bewegung im öffentlichen Raum, alltägliches Verhalten mit seinen Gewohnheiten, und am Ende: Geschäft. Gehend auf etwas, das sonst nicht da ist, merke ich, dass mein Weg durch eine Aufzeichnung, eine Markierung verdoppelt wird. Ich bin nicht allein, meine Wege werden begleitet und geleitet, nicht göttlich, sondern sehr irdisch, weil diese Verdopplung sich aus dem speist und dem korrespondiert, was ich tue. Die Straßenmarkierung der Installation wäre für sich genommen nichts, wenn niemand auf ihr laufen würde. Wirklichkeit gewinnt sie allererst dadurch, dass sie von ihren Nutzern als solche konstituiert wird – weshalb es sich ja auch um eine partizipative Installation handelt.

Man könnte versucht sein, das Installationselement der Straßenmarkierung als Metapher für Datenströme zu bezeichnen, und zweifellos gewinnen diese Ströme in ihnen auch eine gewisse Anschaulichkeit. Aber bei der Deutung mit Hilfe von Metaphern oder Symbolen Zuflucht zu suchen, ist gerade dann unzureichend und unpassend, wenn die Kunst sich einem Gebiet zuwendet, in dem Metaphern und Symbole längst schon zu Tode gekommen sind. Datenströme haben mit Metaphern und Symbolen nichts zu tun, und Datensammler interessieren sich nicht für sie, sondern dafür, wer wann wo was tut und wahrscheinlich wieder tun wird. Weder sind die Straßenmarkierungen für sich noch ist FREIHEIT 2.0 insgesamt in einer symbolischen Ordnung zu begreifen. Die Elemente der Installation zusammengenommen haben weitaus eher den Charakter von künstlerischen Daten, die für ihre Nutzer bzw. Partizipanten ganz unsymbolisch miteinander verschaltet werden.

2.2. Geschäft, Daten, Werte

Die gespurte Laufbahn der Straße führt zum nächsten Element: einem Geschäft. Geschäfte aufzusuchen, gehört ebenfalls – wie das Laufen in gewohnten Bahnen – in das Gebiet des Alltäglichen, und es handelt sich ebenfalls um ein Verhalten im öffentlichen Raum, genauer um Räume des Marktes zum Zwecke des Verkaufens und Kaufens. Vor dem Betreten bemerke ich die Umbenennung der mir wohlvertrauten Drogerie in „Drogerie Freiheit" – ein irritierender Bruch der Alltäglichkeit. Das Wort Freiheit ist mir vertraut, allein die Deutung ist hier schwierig. Ist die Freiheit der Produktwahl und des Konsums gemeint? Macht

der Laden Reklame für die Freiheit schlechthin? Für was will man mich mit der neuen parolenartigen Wortfolge gewinnen? Auf jeden Fall liegt hier eine Doppeldeutigkeit, vielleicht sogar ein Widerspruch vor. Im Geschäft und auf dem Markt der Produkte geht es um materielle Werte, so dass ich meinen Zehn-Euro-Schein gegen die Produkte tauschen kann, deren Wert im Preis angegeben ist. Das Wort *Freiheit* ernstgenommen hingegen verweist auf ideelle Werte, die sich nicht in Begriffen des Marktes ausdrücken lassen. Zwar weiß ich, dass ich auch solche ideellen Werte habe, aber diese eigentümliche Kontamination von materiellem Wert mit einem ideellen hier im Geschäft hat etwas Verwirrendes. Trage ich irgendwelche ideellen Werte mit in das Geschäft und den Warenverkehr hinein, sind sie vielleicht ein Mehrwert, der beim Warenkauf zu Buche schlägt? Und für wen? Sollten die Bonuspunkte, die mir beim letzten Einkauf gutgeschrieben wurden, etwas mit meiner Freiheit zu tun haben?

Der Gedanke, dass ich beim Bezahlen meiner frei gewählten Konsumgüter auch mit meiner Freiheit bezahlen könnte, ist bedrückend und abstrakt zugleich – es könnte angeraten sein, das Geschäft zu verlassen. Aber der Kauf einer neuen Tube Zahnpasta ist dringlich, außerdem sollte ich die Sorte wechseln. An der Kasse macht mich die freundliche Kassiererin darauf aufmerksam, dass ich mich wohl in der Sorte geirrt habe, gewöhnlich würde ich doch eine andere bevorzugen. Auf jeden Fall aber seien mir so viele Bonuspunkte gutgeschrieben, dass ich heute nichts zu bezahlen hätte – womit sie die materiellen Werte in meinem Portemonnaie meint. Jetzt weiß ich: ich habe Daten-Werte, ich bin ein Daten-Wert, mein Leben ist ein Daten-Wert, und ich werde zu einem Mehr-Wert, wenn sich meine Käufe in Datensammlungen abbilden.

Kurz vor dem Ausgang fällt mein Blick auf aufgestellte Informationstafeln, schöne Stelen, die meinen Blick nicht mehr auf den Boden zwingen, sondern die ich erhobenen Hauptes lesen kann. Beim Verlassen der *Drogerie Freiheit*, dem Ort, an dem meine Vorstellungen von Freiheit in die Welt des Marktes und Geschäfts hineingeraten sind, werde ich am Ausgang auf eine neue Spur gesetzt – ganz so, als ob es sich doch um einen Parcours handele, an dessen Ende ich auf etwas Wesentliches treffen könnte. Diese Spur wird zum „Büro der Freiheit 2.0" führen, dem vierten Element von Mehnerts Kunstinstallation. Zunächst jedoch zum dritten: der *Self-Tracking-App*.

2.3. Daten-Sendung: Smartphone und *Self-Tracking-App*

Die Beteiligung, die auch hier dazugehört, hat einen anderen Charakter als im Fall der beiden vorigen Elemente. Die Partizipanten konnten eine von Florian Mehnert entwickelte App auf ihren Smartphones installieren. Dieses Zusatzprogramm zeichnet die Bewegungen der Smartphoneträger auf und sendet alle dreißig Sekunden eine Standortmeldung an die zentrale Sammelstelle aller Bewegungsdaten. Mit der Smartphone-Applikation wird die Grenze zwischen Bewegungen im öffentlichen und solchen im privaten Bereich überschritten, genauer: sie ist gegenüber dem Unterschied zwischen beiden völlig indifferent. Ob ich mich in Küche und Schlafzimmer oder auf dem Sportplatz, in einer Bar oder im Finanzamt aufhalte, mag für mich ein Unterschied sein, ist aber vom Programm des technischen Gerätes her gesehen gleich wichtig oder unwichtig, d. h. im wahrsten Sinne des Wortes gleich gültig. Was aber nicht gleichbedeutend mit wertlos ist.

Es ist nötig, die Wertformen zu unterscheiden. Während ich den Besuch auf dem Sportplatz als Fußballfan außerordentlich wertschätzen, aber auch allein nur deshalb dort sein kann, weil ich jemanden zu seiner Freude begleite, kennt die Applikation kein solch spezifisches Quale des Wertes. Hier geht es um das bloße Registrieren, um das positivistische Sammeln von allen möglichen Daten, so dass mein Alltagsverhalten, wie es in Gestalt meiner Bewegungen erfasst wird, digital verdoppelt wird. Der Wert dieser Daten liegt nicht in einer je besonderen Qualität, sondern in ihrer Quantität, weil sich erst auf ihrer Basis eine Statistik von Vorlieben oder Gewohnheiten erstellen lässt. Warum aber benötige ich eine solche technische Datensammlung, wenn ich auch ohne sie weiß, was meine Vorlieben sind?

Nun ist diese Frage zu egozentrisch oder, wenn man den Ausdruck bevorzugt, zu individualistisch. Das Smartphone, auf dem ich die Applikation installiert habe, ist zwar mein überaus persönliches Gerät, mir an- und zugehörig und geradezu intim mit meinem Körper verbunden, aber die Installation weist mich darauf hin, dass es einen Ausgang hat, der von mir wegführt zur Zentrale. Vermittels meines Gerätes werde ich vom Datensammler zum Datensender. An dieser Stelle ist an eine alte Medientheorie mit revolutionärem Impuls zu erinnern, die anlässlich des Radios formuliert wurde. Bekanntlich sendet das Radio von einer Zentrale, die in alle Richtungen ausstrahlt und Kollektive zu Empfängern macht. Dagegen haben Bertolt Brecht und später Hans Magnus Enzensberger[2] eingefordert, dass die Empfänger auch senden können sollten, so dass das Radio demokratischen Absichten zur Verfügung gestellt und das Prinzip der Partizipation verwirklicht wird. Sollte sich mit dem Smartphone die alte Utopie einer anderen, freien medialen Technopolitik realisiert haben? Als Partizipant mit meiner *Self-Tracking-App* bin ich in der Tat ein Sender, aber das Material, das ich sende, wird in einer Zentrale zu einem Datenkonglomerat verrechnet, das als solches nicht gesendet wird und allein in der Verfügungsgewalt der Verrechner liegt, für die meine Stimme, anders als im Fall des projektierten Radios, nicht zählt; ich bin Sender ohne Mitsprache.

An eine zweite Medientheorie ist zu erinnern, um dem App-Element der Installation auf die Spur zu kommen. Der kanadische Medientheoretiker Marshall McLuhan hat Medien, technische Mittel überhaupt, als Verlängerungen und Ausweitungen unserer natürlichen Organe aufgefasst: das Rad verlängert den Fuß, das Telefon Ohr und Mund, das Fernsehen das Auge und, natürlich, der Computer das Hirn.[3] Man kann darüber streiten, ob es sich so verhält. Wichtig ist etwas anderes. Im Vergleich zu jenen Medien fehlt bei der Smartphone-App die spezifische Referenz auf ein Organ oder einen Einzelsinn, die mit ihr irgendwie transformiert werden könnten. Relevant sind der Körper überhaupt und die Bewegungen im Raum schlechthin als Informationsträger und -lieferanten, so dass wir von einer medialen Unsinnlichkeit auf App-Basis sprechen können, zumal mich dieses Gerät begleitet, ohne weitere sinnliche Aufmerksamkeit von mir zu fordern. Dieses Smartphone mit seiner App hat mit den alten technischen Medien wenig zu tun, und ob wir überhaupt den Terminus Medium dafür verwenden sollten, wäre der Diskussion wert. Hier fehlt noch ein angemessener Begriff.

Ein Blick auf den Bedeutungsgehalt des Wortes „Applikation" könnte weiterhelfen. Im Lexikon ist folgendes zu finden: „Applikation: 1) veraltet für Anwendung, Bewerbung, Fleiß, Hinwendung. 2) Verabreichung (von Heilmitteln), medizinisch. 3) Darbringung eines katholischen Messopfers für bestimmte Personen oder Anliegen. 4) Aufnäharbeit." Lässt man die Aufnäharbeit beiseite, dann geht es beim Applizieren weniger um einen besonderen, individualisierten Handlungsakt, sondern darum, von etwas, das zur Verfügung steht, nach bestimmten Regeln Gebrauch zu machen, also um Verfahrensweisen. Das trifft auch für ein Messopfer zu, bei dem um des hoffentlich eintretenden Erfolges willen Verfahrensweisen, Rituale einzuhalten sind – sonst funktioniert es nicht. Auf jeden Fall hat *Applikation* hier etwas mit einem Opfer zu tun. Schließlich: *Applikation* in der Bedeutung von Verabreichung verweist darauf, dass nicht ich etwas tue, sondern etwas mit mir gemacht wird, wobei ich davon ausgehen soll, dass dies in meinem Interesse geschieht. Medizinisch gesehen, sollen die Medikamente genau zu meinen Beschwerden passen. Datenmäßig gesehen, soll das, was mir verabreicht wird, genau zu den Daten passen, in denen sich meine Gewohnheiten und Vorlieben niedergeschlagen haben. Ich darf also hoffen, dass ich aufgrund meiner digitalen Werte auch auf der Basis dieser Daten bedient und behandelt werde. Die App sollte so funktionieren wie die Applikation eines Arztes und das Datensammeln so wie die Erhebung eines Befundes. Anstatt den Begriff des Mediums zu benutzen, wäre wohl besser davon zu sprechen, dass es sich hier um einen technisch-digital implementierten Kurator handelt und bei der zentralen Datensammelstelle um ein Kuratorium. Wozu das Daten-curare gut ist, darauf ist zurückzukommen.

2.4. Daten-Sammlung und Aufsicht im *Büro der Freiheit*

Man könnte deshalb das vierte Element dieser Kunstinstallation, das *Büro der Freiheit 2.0*, versuchsweise als Kuratorium bezeichnen. Ein Kuratorium ist eine Aufsichtsbehörde von öffentlichen Körperschaften oder privaten Institutionen. In dem Kuratorium dieser Kunstinstallation finden die einzelnen Elemente von *Freiheit 2.0* zusammen. Die Laufbahnen auf der Straße bzw. von den Geschäften führen hierher. Die Daten der App-Nutzer werden hier gebündelt und ausgewertet, vor allem aber auch sichtbar gemacht. Die Visualisierung in Computer-Diagrammen mit ihren seltsamen Mustern aus Linien verzeichnet kollektives Bewegungsverhalten, das sich an bestimmten Stellen überschneidet, bündelt oder deutliche Knoten wie bei einem Netz bildet, so dass sich die Orte markieren lassen, die von vielen Leuten aufgesucht werden. Zugleich kann jedes Verhalten auch individuell zugeordnet werden.

Während ich früher davon ausgehen konnte, mich in einer Masse verstecken zu können, sorgt hier die Kombination von Massenerfassung und Personalisierbarkeit dafür, dass ich ein Einzelner bleiben oder werden kann. Man kann dies auch Überwachung nennen. Der französische Philosoph Michel Foucault hat gezeigt, wie innig Praktiken der Überwachung und der Macht mit der Herstellung dessen, was wir Individuum nennen, verschränkt sind. Dabei ist ein wichtiger Unterschied zu machen. Die Praktiken der Macht, die Foucault in *Überwachen und Strafen* untersucht hat, zielen auf die Körper der Subjekte, um sie der Disziplinierung zu unterwerfen und ein bestimmtes Verhalten zu erzwingen. In den Studien zur *Geschichte der Gouvernementalität* hingegen geht es nicht um Disziplin, sondern darum, dass eine ganze Bevölkerung als Informationsquelle für Steuerungsprozesse zur Optimierung des Einzelnen und der Gesellschaft dient, um das *Leben* durch seine Erfassung zu steigern, so dass sich die politische und soziale Informationsgewalt der Marktwirtschaft möglichst unbegrenzt erstrecken kann.[4] Die Überwachung, um die es hier geht, hat sich weit entfernt von Praktiken der Unterdrückung, der Disziplin oder des gewaltförmigen Verhinderns von etwas, weil ihre ganze Sorge darauf gerichtet ist, die Gewohnheiten des alltäglichen Lebens in ihrer ganzen Positivität registrativ zu verdoppeln. Die grundlegende Orientierung von Big Data als einer Machttechnik der Gouvernementalität liegt nicht im Gebiet des Negativen, sondern ist durchweg positiv. Gemeinhin wird mit dem Wort *positiv* assoziiert, dass etwas gut ist, wie etwa bei dem geläufigen Rat, man solle positiv denken. Die andere, hier wichtige Bedeutung liegt darin, dass aus der Welt der Daten nichts ausgeschlossen, sondern alles in diese Welt eingeschlossen ist.

Dem Kuratorium im *Büro der Freiheit 2.0* liegt hier ein Problem vor, bei dem es letztlich um das Verständnis von Freiheit geht. Bei der grundsätzlichen Positivität des Datensammelns zählt nichts als Faktizität, das rohe Gegebensein von Tatsachen. Allein diese feststellbare Wirklichkeit hat hier einen Wert, alles andere fällt in das Nichts und zählt nicht. Alle Datenwerte sind Wirklichkeitswerte und haften am So-Sein. Aber bekanntlich gehen Menschen in der Orientierung am bloßen So-Sein nicht auf, sondern darüber hinaus, denn sie können eine Kluft zwischen sich und dem So-Sein eröffnen, sie kennen ein Wollen und ein Sollen.[5] In der Welt von Big Data gibt es einen solchen Abstand nicht, er kann nicht einmal gedacht werden, weil es hier nur den Ge-

Christa Karpenstein-Eßbach

Christa Karpenstein-Eßbach, geb. 1951, ist apl. Professorin für Neuere deutsche Literaturwissenschaft an der Universität Mannheim. Wichtigste Veröffentlichungen neben zahlreichen Aufsätzen: Einführung in die Kulturwissenschaft der Medien (2004); Orte der Grausamkeit. Die Neuen Kriege in der Literatur (2011); Deutsche Literaturgeschichte des 20. Jahrhunderts (2014).

gensatz zwischen einem Sein als Faktizität und dem Nichts gibt, so dass Faktizität und Wert zusammenfallen, identisch werden.

Zur Freiheit gehört es aber, nicht allein in der Welt der ganz und gar feststellbaren Tatsächlichkeiten angesiedelt zu sein. Freiheit ist nicht in Datenwirklichkeiten gegeben, die kein Geheimnis kennen. Freiheit ist das Recht, versteckt zu sein, sie existiert in der Verborgenheit, im Entzug der Sichtbarkeit. Dem Datensammeln, dessen digitale Unsichtbarkeit mit der Registratur des Faktischen verschwistert ist, steht mit der verborgenen Freiheit eine andere Unsichtbarkeit gegenüber.

Mit dem vierten Element dieser Installation befinden wir uns an einem unsicheren Ort, der dazu provoziert, nach den Beziehungen zwischen Freiheit 1.0 und Freiheit 2.0 und deren jeweiligem Wert zu fragen. Insofern hat dieses Kuratorium eine doppelte Funktion als Aufsichtsbehörde: es ist die Zentrale, in der die 2.0-Datenwelt technisch-materiell zusammenläuft und ansichtig gemacht wird, und zugleich derjenige Ort, an dem die ideelle Dimension in Gestalt der Frage nach Freiheitswerten ins Spiel gebracht wird: Welcher Freiheit gilt die Aufsicht?

3. Macht – Daten – Leben

Was ist die Logik, die das Datensammeln motiviert und die die massenhafte Bereitschaft erzeugen soll, hier mitzumachen? Die Verschaltung unserer analogen Lebenswelt mit der digitalen der Daten dient – ganz frei von Repression – dem guten Leben, dient der Lebenssteigerung und -optimierung, dem Konsum und Komfort. Ihr Prinzip ist die Durchsetzung des Lebens als Regulativ und oberstem Wert der Verwaltung der Körper und der rechnerischen Planung dieses Lebens. Hier verschränken sich Leben, Technologie und Macht. Foucault hat für diese Durchsetzung des Lebens als Prinzip der Regulation von Bevölkerungen den Begriff der Bio-Politik bzw. der Bio-Macht geprägt. Er schreibt: „Die Fortpflanzung, die Geburten- und die Sterblichkeitsrate, das Gesundheitsniveau, die Lebensdauer, die Langlebigkeit mit allen ihren Variationsbedingungen wurden zum Gegenstand eingreifender Maßnahmen und *regulierender Kontrollen: Bio-Politik der Bevölkerung*."[6] Dass das Leben zum umfassenden Gegenstand des Wissens und der Sorge gemacht wird, ist ein Prozess, der in der Mitte des 18. Jahrhunderts einsetzt. Die zitierten Sätze wurden vor vierzig Jahren geschrieben. Bio-Politik gibt es lange vor Big Data.

Mit der universellen Maschine des Computers und dem ebenso universellen 0/1-Code, der alles einlesen, auslesen und verrechnen kann, hat sich aber die materielle Basis der Bio-Macht verändert. Es ist nicht mehr nötig, dass Datenerheber wie im analogen Leben zu den Leuten kommen, um sie zu befragen. Wir sind selbst im Besitz der Geräte, die es, wenn wir sie benutzen, ermöglichen, alles zu erkunden, anzuzeigen und zu entschleiern. Bei Foucault heißt es weiter: „Der abendländische Mensch lernt allmählich, was es ist, eine lebende Spezies in einer lebenden Welt zu sein, einen Körper zu haben sowie Existenzbedingungen, Lebenserwartungen, eine individuelle und kollektive Gesundheit, die man modifizieren, und einen Raum, in dem man sie optimal verteilen kann"; einer solchen Politik geht es „um den Eintritt des Lebens und seiner Mechanismen in den Bereich der bewussten Kalküle und die Verwandlung des Macht-Wissens in einen Transformationsagenten des menschlichen Lebens", darum, „das Lebende in einem Bereich von Wert und Nutzen zu organisieren".[7] Mit unseren allseitig rechnenden Geräten sind wir zu Mitarbeitern dieser Bio-Politik geworden, und dass wir das bereitwillig in Kauf nehmen, hat eben damit zu tun, dass es um unser Leben geht. Wollte man die Frage nach einem möglichen Widerstand gegen eine solche Bio-Politik ins Spiel bringen, so dürfte die erste Erkenntnis darin bestehen, dass es schwierig ist, sich auf das Leben zu berufen, wenn eben dies zum regulativen Prinzip dessen geworden ist, wogegen man sich wendet.

Die Kunst ist von solchen aporetischen Lagen tangiert, aber sie geht darin nicht auf, weil sie Potenziale eines ästhetischen Widerstands entwickeln und mit ihren Mitteln die Erfahrung einer Reibung oder Dissonanz erzeugen kann. Mit der Installation FREIHEIT 2.0 wird uns eine inszenierte Verdopplung von Big Data dort vorgeführt, wo wir sie gemeinhin *nicht* finden: im öffentlichen Raum. Sie macht das, was wir alltäglich nicht sehen, aber tun, sichtbar, setzt uns auf Spuren des Erkundens und provoziert ein Bewusstsein davon, was unser analoges Leben – zum Datenträger gemacht – mit seiner digitalen Verdopplung zu tun hat. Diese inszenierte Verdopplung hat darüberhinaus ein ästhetisches Surplus, denn es handelt sich um eine entwendende Verwendung der Elemente, die zur Welt des digitalisierten Datensammelns gehören. Anders gesagt: es gibt hier eine Verfremdung, die genau mit dem arbeitet, was ihr problematischer Gegenstand ist. Wenn es hier einen ästhetischen Widerstand gibt, dann dürfte er darin liegen, dass wir als alltägliche Mitarbeiter der Bio-Politik durch die Beteiligung an dieser interaktiven Installation in dieser unserer Mitarbeiter-Position ein Stück weit verrückt oder deplatziert werden. Womit vielleicht jener Abstand von der Faktizität des So-Seins entsteht, der mit zur Freiheit gehört.

Anmerkungen

1 *Jean Baudrillard, Der symbolische Tausch und der Tod, München 1982, S. 90*

2 *Bertolt Brecht, Radiotheorie 1927-1932, in: Gesammelte Werke Bd. 18. Schriften zur Literatur und Kunst I, Frankfurt 1967; Hans Magnus Enzensberger, Baukasten zu einer Theorie der Medien, in: Kursbuch 20, Frankfurt 1970, S. 159–186*

3 *Marshall McLuhan, Die magischen Kanäle. Understanding Media, Frankfurt u. Hamburg 1970*

4 *Michel Foucault, Überwachen und Strafen. Die Geburt des Gefängnisses, Frankfurt 1977; ders., Geschichte der Gouvernementalität I. Sicherheit, Territorium, Bevölkerung; Geschichte der Gouvernementalität II. Die Geburt der Biopolitik, Frankfurt 2004*

5 *Helmuth Plessner, Die Stufen des Organischen und der Mensch. Einleitung in die philosophische Anthropologie, in: Gesammelte Schriften Bd. IV, hg. v. G. Dux u. a., Frankfurt 1981, S. 363*

6 *Michel Foucault, Sexualität und Wahrheit. Der Wille zum Wissen, Frankfurt 1977, S. 166*

7 *Ebd., S. 170 f.*

Benjamin Kees

Das Problem des Datensammelns – einfach erklärt

Bei den Big-Data-Kolloquien zur Veranstaltung Freiheit 2.0 in Weil am Rhein wurde versucht, einem fachfremden Publikum die Problematik des Datensammelns durch Firmen bei der Nutzung von Onlineangeboten aus Sicht einer kritischen Informatik nahezubringen. Es wurde versucht, ein Problembewusstsein zu schaffen, indem die zugrundeliegenden Mechanismen der Informatik an einem verständlichen Gleichnis veranschaulicht wurden. Und es wurde beschrieben, wie Firmen die gesammelten Informationen im eigenen Interesse nach einer kommerziellen Logik, mitunter gegen die Interessen der Datenpreisgebenden einsetzen. Der folgende Text ist der Erklärungsversuch des Vortrags in überarbeiteter Fassung und soll vor allem als Orientierung für Informatiker.innen dienen, die selbst in die Situation kommen, das Thema einfach erklären zu wollen.

„Ich habe doch nichts zu verbergen“

Sucht man mit einer Bildersuchmaschine wie *Startpage.de* nach „Überwachung“, findet man einige der Versuche, den Begriff der Überwachung symbolhaft darzustellen. Man findet Bilder von wachen Pupillen, Augen, die durch Schlüssellöcher gucken, starrende Kameras auf Pfählen und an Häuserwänden, Ferngläser mit anonymen Beobachtern und auf Menschenköpfe gerichtete rote Fadenkreuze.

All diese Symbole und Metaphern bleiben in ihrer Darstellung jedoch bei dem Akt des Beobachtens stehen: Etwas Anonymes starrt. Die benutzten Symbole selbst erzeugen auf die Betrachtenden den Effekt von Eingeschüchtertheit und Undurchschaubarkeit. Sie stellen also weder den Mechanismus der Einschüchterung, wie Jeremy Bentham ihn mit seinem Panopticon beschreibt, noch die hinter der Überwachung ablaufenden Prozesse der Informationsverarbeitung bildlich dar. In den Bildern wird man als Betrachter. in selbst der betroffene Mensch. Oft hört man als Reaktion auf die Konfrontation mit dem Thema Überwachung den Satz „Ich habe doch nichts zu verbergen.“ Dieser rührt genau aus dieser Perspektive her. Man nimmt sich zwar selbst als beobachtet wahr, doch antizipiert als den Zweck der Beobachtung, dass Fehlverhalten entdeckt und geahndet werden soll. Man nimmt an, die einzig negative Konsequenz aus der Überwachung für einen selbst sei die zu erwartende Reaktion auf eine unerwünschte Handlung, die beobachtet wird. Da man von sich selbst in diesem Zusammenhang annimmt, nicht gegen die antizipierten Regeln zu verstoßen und daher selbst nicht im Fokus der Überwachung zu stehen, erwartet man keine Ahndung und sieht kein Problem mit dem Beobachtetwerden. Grund zu dieser Annahme hat man jedoch nur, wenn man annimmt, dass Überwachungsmaßnahmen ausschließlich der Durchsetzung von Regeln oder einem Sicherheitsgewinn dienen sollen und gegen bestimmte Geschehnisse gerichtet sind.

Im Gegensatz zur Überwachung durch Kameras im öffentlichen Raum, wird bei der Sammlung von Daten durch Anbieter von Onlinediensten wie sozialen Netzwerken und Verkaufsplattformen selten der Begriff Überwachung benutzt.

Trotzdem scheinen deren User bei der Abwägung über die Preisgabe von Informationen einer ganz ähnlichen Logik zu folgen. Man nimmt an, aus dem, was man an Inhalten preisgibt, könne einem kein Strick gedreht werden, da man die Art der preisgegebenen Inhalte kontrollieren könne und nicht gegen Regeln verstoße. Diese Art der Reaktion auf Warnungen von Datenschützer.innen offenbart jedoch ein Missverständnis, das Edward Snowden in einem Satz auf den Punkt bringt: „Es geht nicht darum etwas zu verbergen, sondern etwas zu verlieren.“

Um zu verstehen, was es zu verlieren gibt, soll erklärt werden, nach welchen Prinzipien die gesammelten Daten ausgewertet und genutzt werden und welche Rolle die Informatik mit ihrer Herangehensweise dabei spielt.

Informatik sieht die Welt als Zahlen

Für Nichttechniker wird der Begriff Informatik zugänglicher, wenn man sie darauf aufmerksam macht, dass es im Kern nicht um Computer, diese unbegreifbaren Blechkisten mit dem Bildschirm geht, die andauernd nicht das tun, was die User wollen, sondern dass Informatik die Wissenschaft der automatisierten Verarbeitung von Informationen ist. Wichtig zu wissen ist allerdings, dass die Verarbeitung dabei aber sehr wohl den begrenzten Möglichkeiten einer solchen Blechkiste unterliegt. Dass die Hardware nämlich nichts anderes kann, als Zahlen zu speichern und nach formalen Regeln zu verarbeiten. Die Informationsverarbeitung unterliegt damit nicht nur den begrenzenden Regeln der Physik, sondern auch den Grenzen der Berechenbarkeit, an die man schneller stößt, als einem als Informatiker.in lieb ist.

Um also Informationen im Computer zu verarbeiten, müssen diese in abstrakter Form, d. h. als Zahlen darstellbar vorliegen. Um Informationen in diese Form zu bringen und dabei nicht am Speicherplatz oder der Langsamkeit der Berechnung zu scheitern, bedient sich die Informatik des Mittels der Abstraktion. Der Computer rechnet nicht mit den Sachverhalten selbst, um die es gehen soll, sondern mit einem mathematisch beschreibbaren Modell des Sachverhaltes. Ein solches Modell ist nicht nur eine einfachere Darstellung der Wirklichkeit. Die Einschränkungen, Weglassungen und Vereinfachungen, aus denen sich das

Geheimagent 2, Rudolf Schönwald, Kaltnadelradierung 1976, gemeinfrei

Modell dann ergibt, folgen bestimmten Annahmen, die sich aus dem Ziel ergeben, das mit der Informationsverarbeitung verfolgt wird.

Die Unterschiedlichkeit von Modellen ein und derselben Sache für verschiedene Zwecke wird gern anhand von Katzen erklärt: Denken unterschiedliche Menschen an eine Katze, haben sie unterschiedliche Modelle einer Katze im Kopf. Ein Katzenbesitzer, der seine Katze vor allem streichelt, hat ein Katzenmodell im Kopf, das eher einem weichen Fellball mit Augen, Schwanz und Beinen gleichkommt. Das Wesentliche eines Katzenmodells einer Tierchirurgin sind hingegen Skelett und Organe. Beide Modelle funktionieren für die jeweilige Aufgabe (Streicheln bzw. Operieren), sind dabei aber sehr unterschiedlich und nicht austauschbar.

Modelle sucht und benutzt die Informatik nicht nur für Informationen, die mathematisch leicht und nahezu abschließend beschrieben werden können, sondern auch für abstraktere und viel schwieriger und uneindeutiger mit mathematischen Mitteln beschreibbare Sachverhalte wie etwa die Interpretation eines Gesichtes in den Bildern eines Videos.

Ein anschauliches Beispiel für die Findung und Nutzung eines Modells ist der Wetterbericht: Jeden Tag aufs Neue sieht man in den Medien Landkarten, auf denen sich bunte Flächen bewegen, die für Temperatur, Wolken, Wind und Luftdruck stehen. Dies wird gezeigt, obwohl es keinen vollständigen aktuellen Datensatz über Luftdruck und Temperaturen für jeden Quadratkilometer des gezeigten Gebietes gibt. An vielen kilometerweit auseinanderliegenden Messstationen werden einzelne Aspekte des Wetters gemessen und ausgewertet. Aus jahrelangen Beobachtungen wurden mathematische Modelle des Wetters erstellt, mit denen man anhand der aktuellen Messungen Prognosen berechnet. Obwohl nur einige wenige Messpunkte bekannt sind, werden für jeden einzelnen Punkt auf der gezeigten Karte Informationen gegeben, um zu entscheiden ob ein Regenschirm oder eher Sonnencreme nötig ist. Allerdings wird die Vorhersage für einen Ort umso ungenauer, je weiter die Prognose in die Zukunft reicht und je ungenauer das Modell eine geografische Besonderheit einer bestimmten Region berücksichtigt.

Vermessung der User

Vergleichbar mit der Messung von Wetterdaten durch einzelne verteilte Messstationen, werden Informationen erhoben, die Menschen bei der Nutzung von Internetdiensten wie sozialen Netzwerken, Online-Marktplätzen und/oder während der Benutzung ihrer Smartphones erzeugen. Ganz im Gegensatz zur Annahme, dass es hier nur um die wissentlich erstellten und geteilten Inhalte wie geschriebene und gesprochene Worte oder Fotos geht, werden bei der Nutzung wesentlich mehr Informationen erhoben. Um im Bild des Wetterberichtes zu bleiben – es werden unzählige von Messpunkten auf der ganz persönlichen Landkarte des datengebenden Menschen gesammelt. Die einzelnen Gebiete dieser persönlichen Landkarte stehen für verschiedenste Aspekte eines einzelnen Menschen, seines Lebens, seiner Handlungen und seiner Psyche. Weitläufige Gebiete dieser Landkarte der Aspekte unserer selbst sind bereits von einigen wenigen Firmen abgedeckt:

Amazon hat Messpunkte darüber, welche Bücher wir in welcher Geschwindigkeit lesen und wie viel wir für Technik zu bezahlen bereit sind. *Spotify* sammelt Informationen, zu welchen Zeiten wir welche Musik hören und kann Schlussfolgerungen über unsere Stimmung ziehen. *YouTube* und *Netflix* führen Listen darüber, wofür wir uns interessieren und welche Szenen wir uns zweimal anschauen. Die Spieleplattform *Steam* kann unsere Reaktionszeiten bei Simulationsspielen messen und unsere Problemlösestrategien bei Rätselspielen aufzeichnen. *Facebook* speichert, wann wer was liest und teilt uns mit, mit wem wer über was wann in welchen Kreisen kommuniziert. Fitness Apps messen und übermitteln unsere physische Konstitution und *Payback* schreibt mit, was wir essen, trinken, wie viel Benzin wir verbrauchen und welche Kleidung wir tragen.

Mit Sensoren in Smartphones für Luftdruck, Lage, Beschleunigung, Temperatur und hochqualitativen Mikrofonen wird jetzt schon den Apps unserer Telefone die Möglichkeit gegeben, viele der blinden Flecken auf unserer Landkarte zu beleuchten, die man mit der Art der Sensoren gar nicht intuitiv in Zusammenhang bringen würde. Forscher fanden zum Beispiel heraus, dass Bewegungen eines Schlafenden, die mit den Beschleunigungssensoren eines Smartphones, das nachts auf dem Bett liegt, gemessen wurden, mit hoher Wahrscheinlichkeit auf eine Disposition des Schlafenden für Alkoholismus geschlossen werden kann. Auf dem *Chaos Communication Congress* 2016 schloss ein Datenforscher allein anhand der Veröffentlichungstermine

von Artikeln auf *Spiegel Online* auf die Urlaubszeiten der Autorinnen und Autoren und entdeckte, über einen längeren Zeitraum betrachtet, auch auffällig häufige Übereinstimmungen der Urlaubszeiten einzelner Autorinnen und Autoren. Beide Beispiele machen deutlich, was das Bundesverfassungsgericht schon beim Volkszählungsurteil 1983 feststellte: Es gibt keine mehr oder weniger schützenswerten Daten. Aus einzelnen, unbedeutend wirkenden Daten können Informationen privatester Natur gewonnen werden. Jede Vorstellung, man habe bei der Nutzung von Onlineangeboten und ans Internet angebundener Hardware unter Kontrolle, welche Informationen man über sich selbst preisgibt, ist eine Illusion.

Komodifikation von Daten und Beeinflussbarkeit

Das Ziel einer kommerziellen Organisation, diese Mengen von Daten zu sammeln, ist deren Komodifikation – das Herauslesen auswertbarer Informationen und deren gewinnbringende Nutzung oder Weitergabe an Dritte. Das gewählte Modell, nach dem die Daten analysiert werden, ist genau wie das Katzenmodell entsprechend genau auf dieses Ziel ausgelegt. Aus den vielen einzelnen Messpunkten der vielen Gebiete unserer Landkarten wird kein möglichst vollständiger Blick auf uns als Mensch erzeugt, in dem wir uns wiedererkennen würden und mit dem wir uns identifizieren würden, sondern ein verzerrtes Abbild von uns entworfen, dessen Gestalt dieser kommerziellen Logik folgt. Es ist zu erwarten, dass diese Abbilder hauptsächlich dann gewinnbringend eingesetzt werden können, wenn man sie nutzt, um genau mit den Menschen Gewinn zu erzielen, von denen die Daten ursprünglich erhoben wurden. Der bereits offenkundig betriebene und einleuchtendste Weg, dies zu tun, ist das Einblenden individueller Werbung während der Nutzung der Dienste. Auch wenn die Ergebnisse zu den eigenen Interessen zu passen scheinen, muss man doch davon ausgehen, dass einem hier nicht die Produkte angeboten werden, die am besten zu den eigenen Ansprüchen, z. B. Haltbarkeit, Qualität und Reparierbarkeit passen, sondern Produkte von denjenigen Anbietern angezeigt werden, die für die Werbung bezahlt haben. In diesem Fall ist man selbst der- oder diejenige, der oder die das Geld durch den möglichen Kauf des Produktes wieder einbringt.

Weniger offenkundig sind allerdings die Möglichkeiten der Beeinflussung der Entscheidungen und Handlungen der Nutzenden – dem sogenannten Nudging (englisch anstupsen). Je mehr Informationen, je mehr Messpunkte auf der eigenen Landkarte man preisgibt, desto größer wird die Angriffsfläche für Beeinflussung und desto präziser können diese Beeinflussungen auf den Einzelnen und die Einzelne abgestimmt werden. Durch gezieltes Setzen oder Weglassen von Informationen kann die Beschäftigung mit Themen und Inhalten beeinflusst werden. Studien konnten außerdem zeigen, dass allein die Reihenfolge der Inhalte einer Timeline eines sozialen Netzwerks bereits signifikant die Diskussionen und Beschäftigung beeinflussen konnte. In diesem Fall bringt die Organisation, die ein Interesse an dem Einfluss hat, das Geld ins Spiel.

Neben diesen Arten von Beeinflussung werden, basierend auf dem gesammelten Wissen, Optionen eingeschränkt. Eine dafür besonders gewinnbringend verwertbare Information ist die über die angenommene Zahlungsfähigkeit. So wurden Kunden in Abhängigkeit der genutzten Hardwaremarke oder der ermittelten Region, aus der jemand die Verkaufsplattform in Anspruch nahm, unterschiedliche Preise und eine unterschiedliche Produktauswahl angezeigt. Es ist damit zu rechnen, dass in Zukunft eine ganze Palette derartiger Mechanismen der kommerziellen Ausnutzung der preisgegebenen Informationen genutzt werden wird.

In beiden Fällen – ob einerseits durch die Akzeptanz der Preisgabe von Daten und das Inkaufnehmen der Beeinflussung, oder andererseits durch die vorsichtige, stets überlegte Preisgabe von Daten und der damit verbundenen Einschränkung der Nutzung der Vorteile der Digitalisierung bis hin zum Ausschluss vom sozialen Leben, das sich zunehmend unter Nutzung datensammelnder Dienste abspielt – hat die Datensammlung einen Einfluss auf das eigene Leben, der nicht im eigenen Interesse liegt. Und nicht nur auf das eigene Leben – denn mit vielen Akten der Preisgabe von Daten gibt man auch Daten von anderen preis und trifft damit Entscheidungen für andere gleich mit.

Es geht bei der Kritik an Überwachung und Datensammelei nicht darum, etwas zu verbergen, was gegen die Regeln verstößt, sondern darum, nicht seine Selbstbestimmtheit und Gleichberechtigung zu verlieren und die von den Mitmenschen aufs Spiel zu setzen.

Twitter: *@algoropticon*
Website: *www.algoropticon.de*

Benjamin Kees

Dipl.-Inf. **Benjamin Kees** studierte an der Humboldt-Universität zu Berlin Informatik und Psychologie. Schwerpunkte seines Studiums waren Überwachungstechnik am *Lehrstuhl für Informatik in Bildung und Gesellschaft* und Mensch-Technik-Interaktion am *Lehrstuhl für Ingenieurpsychologie*. Seit November 2015 ist Benjamin Vorstandsmitglied des FIfF und Mitglied der Fachgruppe *Informatik und Ethik* der Gesellschaft für Informatik. Seit 2012 ist er IT-Leiter bei der *Smart Energy for Europe Platform* und seit Sommersemester dieses Jahres Lehrbeauftragter an der Hochschule für Technik und Wirtschaft Berlin.

Christoph Stürmer (Transkription, Überarbeitung und Erweiterung: Britta Schinzel[1])

Connected Cars

Ich stelle die Situation der deutschen und europäischen Automobil-Industrie dar, und die Gründe, warum sie auf autonomes Fahren setzt. Die Automobil-Industrie ist dabei, ihre Geschäftsmodelle grundlegend umzugestalten, und dabei ihre Wertschöpfung weniger aus den materiellen Autos selbst, denn aus den von ihnen beim autonomen Fahren gewonnenen Daten zu holen, also aus immateriellen Gütern. Dabei liefert autonomes Fahren naturgemäß wesentlich mehr Daten als selbstgesteuertes Fahren. Ich beschreibe die Probleme, die bei der Entwicklung zu bewältigen sind, und die Planungen der deutschen und europäischen Fahrzeugfirmen. Schließlich wende ich mich Sicherheits- und rechtlichen Fragen zu.

1. Gründe für die Entwicklung von autonomen Fahrzeugen in Europa

Dass das Auto autonom werden soll, ist eine spezifisch männliche Idee.[2] Denn das Bedürfnis nach der Erschaffung von autonomen Maschinen, und solcher auch von Autos, scheint häufiger, wie auch immer entstandenen, männlichen Wünschen zu entspringen.[3] Doch genügt diese Motivlage natürlich nicht, um die anstehenden Transformationen eines riesigen Industriezweiges zu verstehen und zu erklären.

Die deutsche und europäische Automobil-Industrie befindet sich in einer prekären Situation. Sie muss den Schock des Verlustes ihrer Börsenwerte nicht nur gegenüber dem Elektroautobauer *Tesla*[4], sondern auch gegenüber den amerikanischen IT-Firmen bewältigen, die zunehmend auch auf dem Fahrzeugmarkt unterwegs sind. Die Gründe haben die deutschen Autobauer noch kaum verstanden, da diese Elektro- und IT-getriebenen Automobilbauer technisch viel weniger erfahren und vermeintlich nicht konkurrenzfähig sind. Und sie haben erhebliche finanzielle Herausforderungen, sowohl wegen der mit dem Verlust des Börsenwerts verbundenen großen Image-Krise, als auch, weil die Unternehmen seit Jahrzehnten sparen, um sich gegen immer neue Billig-Konkurrenz zu behaupten. Die Produktion der Autoindustrie besteht im Wesentlichen nur mehr aus dem Zusammenfügen von Teilen in der richtigen Reihenfolge, die von der Zulieferindustrie zeitgerecht zur Verfügung gestellt werden – ein logistisches Problem –, und dem anschließenden Vermarkten. *Sie können nur noch rennen,* und sie haben sich *dumm gehungert,* spitze ich zu, d. h., sie können eigenständig keine Strategien mehr entwickeln. Sie haben keine freien Kapazitäten für Planung und Entwurf, und lagern daher das „Nachdenken" an Unternehmensberater wie *PricewaterhouseCoopers (PwC)* aus.

Das autonome Fahren soll die Firmen aus der Sackgasse herausführen und zukunftsfähig machen. Doch von der Planung zur Realisierung vergehen bei der Fahrzeugentwicklung sieben Jahre, d. h., ein Auto, das heute in die Fehlertestphase und erst anschließend in die Massen-Produktion geht, wurde vor sieben Jahren geplant, ist demgemäß dann für den Stand des technischen Wissens schon veraltet. Bereits seit zwanzig Jahren sind unsere Autos voll mit Elektronik und sind vielfach digitalisiert, was also ist neu an autonomen Fahrzeugen? Der Name sagt es, *Connected Cars,* es ist die Verbundenheit, mit der Umwelt, miteinander, dass die Dinge in dem und um das Auto – und es sind viele Dinge im Spiel – miteinander kommunizieren.

Motivation für automatisiertes Fahren sind neue Möglichkeiten, in und mittels dieser Situation der Verbundenheit Geld zu verdienen. Denn derzeit gibt es nur zwei Situationen im Leben, wo der moderne Mensch nicht im Internet ist: erstens, wenn er schläft, und zweitens, während er Auto fährt. Da es 1,2 Milliarden Autos weltweit gibt, mit einem Nutzungsgrad von 5 % pro Tag, also im Durchschnitt 1,2 Stunden pro Auto und Tag genutzt werden, befinden sich Menschen pro Tag 1,44 Milliarden Stunden im Auto. Das Zeitpotential soll in Geld umgewandelt werden. Wenn die Bewertung von einer Stunde im Internet auch nur 1 $ betrüge – und es ist mehr – würde die Zeit, die wir im Auto verbringen, von der Internetindustrie mit 1,44 Milliarden $ pro Tag bewertet. Die Zeit, die im Auto verbracht wird, soll also umgewandelt werden in Internetzeit und somit in Daten.

Die Transformation von der Monetarisierung aus dem Materiellen zum Virtuellen wird überdies getrieben von der Angst der Autobauer vor Übernahmen durch Internet-Unternehmen wie *Google, Facebook, Apple* oder *Amazon.* Sie haben genug Geld, um jede Firma auf der Welt zu kaufen. Und sie wissen seit langem, wie sich Geld verdienen lässt, auch wenn die Kunden für die von ihnen angebotenen Services nichts zahlen wollen.

2. Digital Enterprise und Connected Services

Beim autonomen Fahren treffen sich Datenwelt und Automobilwelt in den Dienstleistungen, die im Auto erbracht werden. Die dazu zu beantwortenden Fragen werden nicht nur im Kontext des europäischen, sondern eines weltweiten Rechtsraums gestellt, mit je unterschiedlichen Rechtsanforderungen und -regelungen. Prognosen dazu müssen mindestens 5–7 Jahre haltbar sein und sie müssen um des weltweiten Marktes willen globalen Ansprüchen genügen.

Connected Cars sind anders als alles, was in der Automobil-Industrie in den letzten 100 Jahren gemacht wurde. Sie erfordern auch ein digitales Unternehmen, digitale Kundenbetreuung, digitale Protokolle, so dass die Prozesse reibungslos laufen, und die jeweils entsprechenden Kompetenzen. Dazu erweitert sich der Bereich digitaler Produkte und Dienstleistungen ständig, während sich gleichzeitig die Arbeitsteilung, die mit automatisiert werden muss, verstärkt. Das Planen, die Formulierung technischer Anforderungen an die Automobil-Hersteller und Zulieferer, ist keine Kernkompetenz der Automobil-Industrie mehr, noch ist es das Eruieren der Provenienz der Dienstleistungen, die nötig sind, um neue Autos zu entwickeln. Sie hat keine Kapazitäten dafür, forschend und planend auf Veränderungsanforderungen zu reagieren. Doch traditionelle Autos soll es in Zukunft kaum noch geben. Und, es wird sehr viel gleichzeitig anders.

Das erste große Problem sind die dabei auftretenden Ungleichzeitigkeiten. Wie schon erwähnt, wurden heute verkaufte Autos vor 7 Jahren erdacht, vor 5 Jahren die Technologien gesammelt und Lösungen entworfen und vor 3 Jahren fertig entwickelt. Sodann müssen sie noch 2 Jahre fehlerfrei im Probebetrieb laufen, ehe sie in die Massenproduktion und in den Verkauf gehen können. In diesem Zeitraum können sich die Regularien und Kundenansprüche je nach Rechtsraum mehrfach geändert haben.

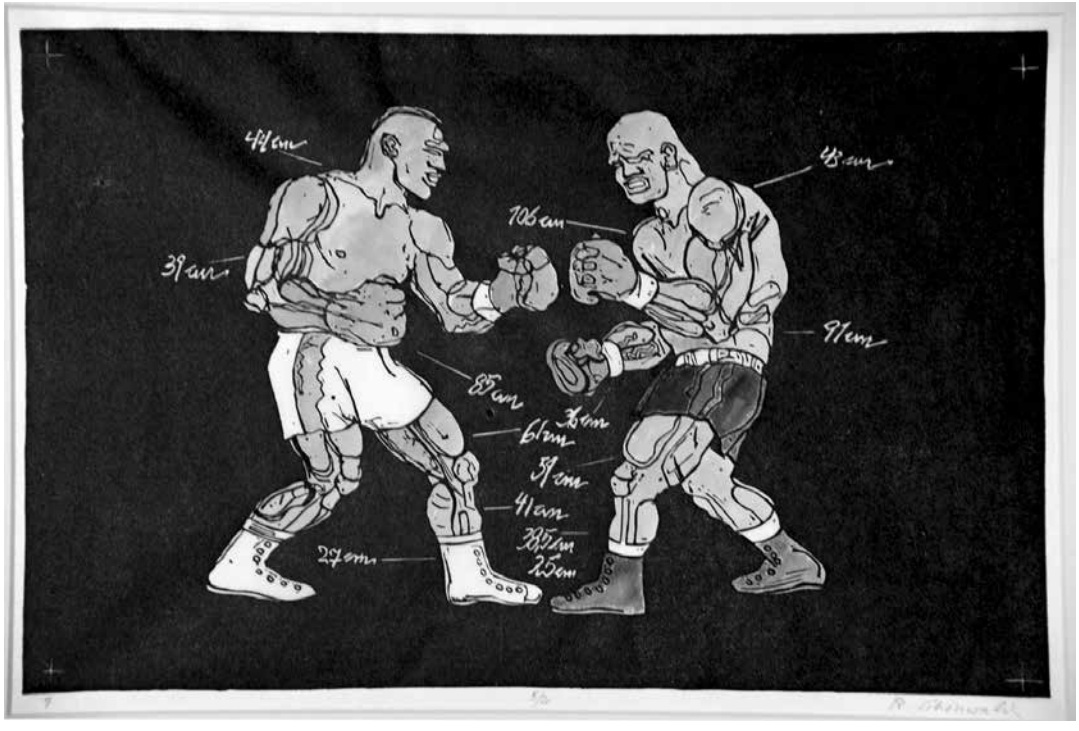
Die zweite Aufgabe ist die Transformation des *Business Model:* Die Art und Weise wie die Automobil-Industrie ihr Geld verdient, ändert sich gerade grundlegend. Die Firmen kombinieren bisher die Teile von den Zulieferern. Gerade auch die komplexen materiellen Systeme und IT-Komponenten kommen aus Zulieferbetrieben. Deutschland hat eine ausgezeichnete und hoch spezialisierte Zulieferindustrie, was die Planungen erschwert. Die Zulieferer müssen natürlich in die Überlegungen und Kompetenzfindung mit eingebunden werden, was Planung und Logistik erschwert. Vor allem fragt man sich, wo die neuen, mit IT-Kompetenz verbundenen Dienstleistungen herkommen sollen, denn in Deutschland ist eine entsprechende Kompetenzverknüpfung noch nicht gegeben. Da es sich nun um eine ganz andere, neue Art handelt, Geld zu verdienen, müssen für die zu treffenden Prognosen über die Marktbedingungen erst einmal Methoden entwickelt werden. Das betrifft auch Fragen, wie die Rechteherkunft bzw. notwendige Rechtsänderungen (Technologieneutralität, Lobbyismus). Ein weiteres – weitgehend ungelöstes – Problem ist die *Cybersecurity,* die Sicherheit im Daten- und Informationsraum. Auch hier ist das Problem die Veränderung, auch die der *Legacy.*

Neue Anforderungen stellen *Ride Sharing, Ride Hailing* und *Car Sharing* mit ihren *Connected Services,* aber auch Ansprüche an digitale Kundenerfassung. Dabei wird die Produktion immer arbeitsteiliger, es gibt immer mehr Schnittstellen, die mit durchgängigen Protokollen automatisiert werden müssen.

In der kommerziellen Fahrt gibt es bereits Lösungen, genannt *Connected Trucking.* Die Fahrer in diesen Fahrzeugen, wie LKWs, haben kaum einen eigenen Spielraum mehr, alles wird zentral verwaltet. Nun erwarten wir die Erweiterung der im kommerziellen Bereich teilweise bereits entwickelten Features und Systeme auf PKWs.

3. Was muss digitalisiert werden?

Wenn man ein Auto bewegt, werden nur sehr wenige Bewegungsmodalitäten benötigt: das Lenkrad für den Richtungsvektor, das Gaspedal als Akzelerator und die Bremse als Dezelerator. Doch warum bewegt eine Fahrer.in wie selbstverständlich all diese Steuerungsmittel? Die Schwierigkeit beim autonomen Fahren liegt nicht im Auto, sondern um es herum. Wie kann ein Auto sich in seiner Umgebung sicher bewegen? Dazu bedarf es einer Analyse von Fahrverhalten anderer Verkehrsteilnehmer.innen, und dann der Simulation der Bewegungskonsequenzen. Die erste Schwierigkeit liegt in der Wahrnehmung der Umgebung, für die Digitalisierung in der Sensorik um das Auto herum. Schon Plato hatte sich mit der Frage beschäftigt „Wie kommt der Baum in unseren Kopf?“ Das wissen wir bis heute auch nur sehr partiell. Aber für die Automatisierung muss diese Kompetenz bis in jedes Detail expliziert sein und in die „Intelligenz“ des Autos programmiert sein. Von den Kameras aus muss es seine Umgebung „verstehen“. Dazu gehört zunächst die Wahrnehmung, die über digitale Kameras Licht-Punkte abbildet. Die Sensorausstattung von Autos ist auch heute schon extrem aufwändig. Dazu muss der Erkennungsprozess stattfinden, relevante Muster müssen erkannt und mit gespeicherten Mustern abgeglichen werden. Für das autonome Fahren genügt es auch nicht, statische Bilder zu interpretieren, es werden immer bewegte Sequenzen benötigt – und die Bewegung des eigenen Autos muss unterscheidbar sein von Bewegungen aus der Umgebung. Dazu bedarf es der Verortung des Fahrzeugs in einem Absolutbild der Umgebung, sowie der Extrapolation in einem digitalen Modell der Umgebung, in dem das digitale Modell des eigenen Gefährts eingebettet wird.



Boxer, Rudolf Schönwald, Linolschnitt aus der Serie Mahagonny 1973

Das macht die Echtzeitüberwachung der statischen Umgebung und aller am Verkehr Beteiligten nötig, von jedem autonom fahrenden Fahrzeug aus gesehen, und dann die Berechnung je von deren Bewegungsfreiheiten, um nichts und niemand zu beschädigen. Zudem muss die Steuerung des Fahrzeugs unter diesen Bedingungen auf dem gewünschten Weg zum gewünschten Ziel berechnet werden. Seine Geschwindigkeit und Richtung muss erkannt und mit Bezug auf die Umgebung extrapoliert werden. Weiter muss die bewegte Umgebung mit all ihren Geschwindigkeits- und Richtungsvektoren in die virtuellen Fahrintentionen integriert werden. Beispielsweise muss ein Punktmuster, das als Fahrradfahrer.in erkannt wurde, in eine bewegte virtuelle Hülle eingebettet werden, die vom autonomen Auto aus gesehen genügend Abstand für ihre künftigen Bewegungen lässt.

Die Kamera erzeugt laufend ein virtuelles Modell des Straßenverlaufs und beobachtet permanent Straßenschilder, z. B. Geschwindigkeitsschilder. Diese müssen interpretiert werden, die Zeichen müssen in ihrer Bedeutung erkannt und die darin enthaltenen Schriftzeichen mittels OCR-Software aufbereitet werden. Ebenso werden auch die Kennzeichen der anderen stehenden und fahrenden Fahrzeuge der Umgebung aufgenommen, ja sie sollen irgendwann auch Menschen identifizieren. Die autonome Fahrzeug-Software muss dabei „sehr tief" interpretieren, d. h. in gewisser Weise die Absichten eines Fahrzeugs erkennen. Die Probleme an einer Kreuzung sind enorm. Bisher gelingt autonomes Fahren am besten auf Autobahnen, wo keine Fußgänger oder langsamen Fahrzeuge unterwegs sind und alle in die gleiche Richtung fahren. Wenn sich zwei Fahrzeuge einer Kreuzung nähern, ist es in Sichtweite der beiden bereits zu spät, einen Zusammenstoß zu verhindern. Daher sieht die Software in der Cloud das Problem, d. h. die beiden sich einander nähernden Fahrzeuge, kommen, berechnet die Prioritäten aufgrund der Straßenschilder oder des Rechtsfahrgebots etc., und steuert entsprechend Bremsvorgänge, Weiterfahren und Seitensteuerung der Aktuatoren.

4. Wie kann digitalisiert werden?

Als erste autonom fahrende PKWs sind vor nun schon fast 10 Jahren die Google-Autos bekannt geworden. Sie sind eiförmig und als materielle Fahrzeuge sehr einfach und wenig innovativ, die Neuheit liegt in der Informationstechnik.[5] Sie arbeiten mit *Google Maps,* welche die Bewegungsdaten der Autofahrer. innen und ihrer Wägen erheben. Diese Fahrzeuge sind immer online, um ihre Fahrprogramme ständig durch Aufnahme weiterer Daten und Algorithmen optimieren zu können. Die so optimierte Software wird laufend auf andere Fahrzeuge überspielt, sodass jede Optimierung über die *Google Cloud* unmittelbar weltweit verfügbar ist.

Die deutschen Autobauer *BMW, Mercedes* und *Audi* haben erkannt, dass sie mit dem Daten-Geschäftsmodell nicht mehr untereinander konkurrieren dürfen, um konkurrenzfähig gegen die IT-Giganten aus dem Silicon Valley zu werden. Ihre Dienste, d. h. Automatisierungs-Software und Echtzeitkarten, können umso besser werden, je mehr Daten sie gewinnen können, was nötig ist, um bei der künftigen autonomen Mobilität mitzumischen. Darum hat sich auch *Opel* angeschlossen, die im Bereich der Elektromobilität schon weiter sind als die genannten Firmen. Für sie alle ist dieses breite Bündnis ein Epochenwechsel. Die Wertlogik der Autobauer hat sich geändert, früher waren es die Geräte selbst, heute sind sie für die Wertschöpfung nicht mehr ausschließlich entscheidend. Die neuen Wertdimensionen sind unsere Zeit, unsere Daten, und die über die Umgebung aufgenommenen Daten bei der Nutzung dieser Geräte.

Der klassische Wettbewerb ist exklusiv, d. h., da wo du bist, kann ich nicht sein. Aber beim neuen Wettbewerbsmodell gilt das nicht mehr. Die Zulieferer distribuieren ihre Produkte, und Firmen bieten ihre Dienste umsonst an, so z. B. Elektrotankstationen, oder Kartenservices, die ein Betriebssystem umsonst anbieten, die Daten zentral verwalten, und im Gegenzug die Erlaubnis bekommen, die Daten zu nutzen. Eine wichtige Botschaft dabei ist die zu erreichende Attraktivität der Firmen als Innovatoren. Die Automobil-Industrie ist in ihrem Ansehen stark gesunken, und dies wirkt sich relativ direkt geschäftlich aus. Daher ist autonomes Fahren für sie auch ein wichtiger Faktor, um wieder attraktiv zu werden. Die vom Entwickler des IT-Bezahlservice *PayPal – Elon Musk* – gegründete Firma *Tesla* ist mit ihren Elektroautos 2013 erst sichtbar geworden, 2015 rangierte sie bereits unter den drei attraktivsten Firmen, während der dann weltweit größte Autohersteller *Toyota* 2015 als Innovator auf Unsichtbarkeit abgesunken ist. Dabei ist *Tesla* ein im Grunde traditionelles Unternehmen, mit allerdings genialem Marketing seiner nachhaltigen Batterien-Doppelnutzung in Solaranlagen. Die 80 T$ teuren *Tesla*-Autos dürfen an öffentlich verfügbaren Schnellladestellen kostenlos Strom beziehen, wenn sie sich auf einer längeren Fahrt befinden. Die meisten Fahrten sind allerdings kurz, sodass es ausreicht, zuhause oder im Büro zu laden, wenn man das Auto nicht benutzt. Diese kostenlosen Ladestationen müssen als Marketingkosten verstanden werden, da sie ein Kaufargument sind.

Letzteres haben sich auch die europäischen Elektroautobauer abgeschaut. Es gibt europaweit schon 400 Schnellladestationen, die aber nur von *Tesla*-Autos genutzt werden können; andere Netzwerke werden gerade schnell errichtet.

Für autonomes Fahren verfolgen sie eine ganz andere Strategie als *Google*-Autos mit der Navigation mit *Google Maps.*

Das europäische Kartell kaufte den Kartendienst *Nokia Here*[6], der seine Echtzeitkarten aus der Umgebung der Fahrzeuge, in denen sie navigieren, erlernt. Fahrzeug A scannt Fahrzeug B und umgekehrt, ohne dass sie sich je direkt austauschen. Es sind Echtzeitmodelle von Millisekunden, die über die nahe Umgebung erstellt werden (müssen), und unmittelbar in die globale Kartensoftware *Here*[7] eingespeist werden. So etwa werden für eine Straße beide Straßen-Ränder gescannt, und die Fahrzeuge dazwischen bewegt, unter der Annahme, dazwischen sei kein Loch. Wenn es aber ein Loch dazwischen gibt, soll die Software das Loch entdecken, so schnell, dass das Fahrzeug dahinter von dem Loch unmittelbar ebenfalls Kenntnis erhält. Nach einer Minute hat die ganze Kartensoftware weltweit das Loch registriert. Natürlich müssen auch Bäume, Gehsteige, Mülltonnen, Fußgänger.innen, Radfahrer.innen, Tiere etc. erkannt und mit Verbotszonen umhüllt werden.

Relative Positionsbestimmungen je zweier Fahrzeuge und Verkehrsteilnehmer müssen mit dynamischen Verbotszonen ausgestattet werden, ohne einander gesehen zu haben. Jedes fahrende

Auto übermittelt Daten über andere Autos, die fahren oder stehen. Auch wenn diese keine Einwilligung über ihre Datenhoheit gegeben haben, werden solche Daten übermittelt, die Kennzeichen gelesen, die Geschwindigkeiten registriert. Der Router im Auto hat auch die Möglichkeit zu erfassen, was die Fahrer.in tut, sowohl bei der Mobilitätsplanung, als auch bezüglich der weiteren *Connected Gadgets,* wie Handys, Tablets, Computer, bis zu den Grenzen, die die Verschlüsselung bietet.

Dabei hilft die Firma *NVIDIA* mit ihren neuartigen Grafik-Chips (Graphics Processing Unit, GPU), die aus Sensordaten digitale Modelle zurückrechnen können, dem Auto bei der Wahrnehmung seiner Umgebung; zudem auch bei deren Echtzeitüberwachung, für den Datenzugriff, die in einen Datenpool, eine Cloud übergeben werden. Die Umgebung eines Fahrzeugs ist sehr vielfältig, und daher ist nicht alles explizierbar. Also wird Lernsoftware eingesetzt. Die lernenden Fahrzeuge sind verknüpft mit der Cloud, in der Lernoperationen ausgeführt werden, und damit sind sie mit der gleichen Intelligenz ausgestattet wie der Zentralrechner.

5. Was alles kann man mit den Daten machen?

Eine Unzahl von Möglichkeiten bietet sich für unterschiedlichste Interessenten: Die Polizei kann Übertretungen online erfassen und entsprechende Strafen verhängen, und kann sie überdies an die Versicherungen weitergeben. Verkehrsplanung und -steuerung ergeben sich auf erheblich einfachere und präzisere Weise als zuvor. Die bisher auf krude Weise erfolgende Verkehrsmessung ergibt sich als Nebenprodukt. Und wenn die Fahrer.innen so freundlich sind, ihr Navi mit dem Ziel gespeichert zu haben, dann ist es möglich, optimal in Echtzeit Verkehrsströme zu lenken. Versicherungen profitieren davon ebenso wie andere Wirtschaftszweige.

Es ist unermesslich, was sich an Geschäftsmöglichkeiten bietet: Autofirmen können die Daten von Regensensoren an der Windschutzscheibe an die Wetterdienste verkaufen;[8] kostenoptimierte Reiseplanung, Staumeldung mit entsprechender Navigation, Park-Positionsmeldung, Mautzahlung vom Auto selbst, Fernbedienung des Fahrzeugs mittels Hotspot-Verknüpfung mit den Autos, die Unterstützung von Fahrzeugrückruf, die Unterstützung für das Aufladen bei nicht so weitreichendem elektrischem Fahren, oder die Assistenz für *Car Sharing.* Die Kommunikation Smartphone–Auto kann weitere Dimensionen eröffnen, vom *Connected Calendar* angefangen.

Die „Intelligenz" liegt in der Online-Kartensoftware, die Verkehrsteilnehmer und Verkehrsumgebung jederzeit kennt. Und diese Daten werden nicht nur einmalig erhoben, sondern vielfach: das Smartphone erhebt die Daten des Autos nochmals, die Telematikdienstleister erheben sie ebenfalls, die Versicherer mit Online-Vertrag ziehen sich eine Kopie. Die Daten vermehren sich so nahezu beliebig.

Es gibt so viele Interessen an den Daten und Argumente für *Connected Services,* dass es nur sehr wenige warnende Stimmen gibt. Und die Politik setzt längst auf die Geschäftsmodelle mit *Big Data.*[9]

Das Interesse der Auto-Industrie am autonomen Fahren betrifft nicht nur die Daten selbst, sondern auch die durch die Datensammlung und Profilbildung ermöglichten Dienstleistungen. Daher haben die Unternehmen ein großes Interesse daran, die Offline-Zeit im Auto in Online-Zeit zu verwandeln.

PwC Strategy& hat eine Studie für die Automobil-Industrie erstellt, wie sie aus Telematik-Dienstleistungen Geschäfte machen kann. Es ist ein sehr lukratives Geschäftsmodell, Daten zu akkumulieren, daraus Dienstleistungsangebote zu entwickeln und diese dann für teures Geld zu verkaufen. Jedes derartige Geschäftsmodell vervielfacht den Umsatz dieser Services, insbesondere, wenn autonomes Fahren auf den Individualverkehr ausgerichtet bleibt und sich – wie es die Autobauer erhoffen – die Anzahl der Fahrten vervielfachen sollte.

6. Probleme

Bisher funktionieren die *Connected Cars* am besten auf Autobahnen, genauer: auf amerikanischen Autobahnen. Europäische Städte bieten erheblich mehr Probleme als die amerikanischen,

Christoph Stürmer und Britta Schinzel

Christoph Stürmer, der Philosophie und Betriebswirtschaftslehre studiert hat, arbeitet bei *PricewaterhouseCoopers,* kurz *PwC,* als Berater für die Automobil-Industrie. *PwC* ist die weltweit größte Unternehmensberatung. Sie bietet professionelle Dienste an: Wirtschaftsprüfung, Rechts- und Steuerberatung sowie Unternehmensberatung, dabei Transaktions-Geschäft und Consulting.

Britta Schinzel promovierte in Mathematik, arbeitete in der Computerindustrie und habilitierte sich in der Informatik. Im Rahmen ihrer Professur für Theoretische Informatik an der RWTH Aachen arbeitete sie zunehmend interdisziplinär. Sie war von 1991 bis 2008 Professorin für Informatik und Gesellschaft und Gender Studies in Informatik und Naturwissenschaft an der Universität Freiburg.

sowohl wegen der engeren Bebauung als auch wegen der vielfältigeren Belebung der Verkehrswege mit Menschen, Radfahrern etc.[10] Die Sensoren können falsche Messungen liefern, z. B. im Nebel, bei Blendung oder wenn ein kleines Flugobjekt die Sicht verfälscht. Das größte Problem ist die Vermischung von automatisierten mit händisch gesteuerten Fahrzeugen, denn diese müssen explizit und kurzzeitig gesichtet werden. Während die ersteren untereinander über die Cloud kommunizieren, müssen sie aber die nicht verbundenen Autos als Hindernisse direkt erkennen. Im Moment muss deshalb jedes Auto ein vollständiges Abbild der Realität mit sich herumschleppen, weil die Cloud die nötige Sicherheit noch nicht bieten kann. Daher wäre es denkbar, dass die Politik bzw. die Autolobby die gesetzliche Erzwingung autonomen Fahrens in Erwägung ziehen. Frau Merkel bereitet uns schon darauf vor. Sie fragt, wem die Daten gehören, den Autobauern, den Netzprovidern oder den Smartphone-Firmen – die eigentlichen Autoren der Daten kommen in ihren Reden nicht vor.[11]

Für die Cybersicherheit des abstrakten Datenraums ist noch kaum gesorgt. Für *Hacker, Trolle* und *Bots* ergeben sich faszinierende Möglichkeiten, wie man die gespiegelten Welten obstruieren kann, indem man die Online-Karten abweichend von der Realität verändern, oder indem man die Steuerung eines oder mehrerer Wagen manipulieren kann. Und dies von unterschiedlichsten Standpunkten aus, vom Router im Auto, vom Kartendienst, vom verbundenen Smartphone, Tablet oder Computer, vom Internetprovider etc.

Auch die rechtlichen Fragen sind noch nicht einmal angedacht. Beispielsweise, wer die Verantwortung trägt, wenn ein korrekt gewartetes und gesteuertes autonomes Auto in Brand gerät, oder wer bei einem Unfall mit Todesfolge verantwortlich ist. *Volvo* ist die einzige Firma, die sich positiv dazu geäußert hat, in solchen Fällen mit ihrer Software haften zu wollen, alle anderen Firmen lehnen dies ab. Ein Lösungsvorschlag ist, solche Fälle analog wie Fahrerunfähigkeit zu entscheiden, ein anderer, es wie Halter.in-Haftung zu behandeln, oder die Fahrer.in-Haftung zu übertragen auf die rechnerische Fahrer.in, die den Fahrauftrag mit dem Ziel umsetzt.

LKWs werden viel früher autonom fahren als PKWs, und, anders als letztere, evtl. auch ohne Insassen. Aber hier haben sich die Fahrzeughalter.innen bereits so geäußert, dass sie nicht daran denken, bei Unfällen autonom fahrender LKWs zu haften. Heftige Auseinandersetzungen sind vorauszusehen.

Der Datenschutz mit dem noch gültigen Grundprinzip der Datensparsamkeit und der informierten Einwilligung wird fürs autonome Fahren erheblich gelockert werden (müssen).[12] Denn wer als mobile Verkehrsteilnehmer.in wirksam verhindern würde, dass seine passiv erhobenen Daten zur Verfügung gestellt werden, würde in der Cloud nicht wahrgenommen und möglicherweise einfach überrollt – das Auspixeln wie bei *Google Street View* ist hier keine Option.[13] So wird nicht nur ein vollständiges Bild der Umgebung erfasst, auch die komplette digitale Identität und die eigene digitale Welt der Fahrer.in selbst wird mitgenommen und – so ist zu befürchten – einsehbar für viele beteiligte Autoritäten, Institutionen, Firmen – und digitale Eindringlinge, denn sicher verschlüsseln lässt sich nur nach außen.

Mit diesem riesigen Konvolut von Daten und ihren Ableitungen mittels *KI, Bots, Big Data* werden wir zu einer nie vorher erahnten Verhaltens-Konformität gezwungen, wenn wir keine Probleme bekommen wollen. Dies ist nur eine der vielen ethischen Fragen, die sich zusätzlich zu den rechtlichen auftun, und sie müssen dringend in breit angelegten Diskursen beantwortet werden.

Anmerkungen

1 *Der Vortrag von Christoph Stürmer wurde auditiv aufgenommen, und ich habe ihn dann verschriftlicht. Um ihn als Text lesbarer zu machen, habe ich mir einige Freiheiten genommen und weitere Quellen verwendet – das alles zu Herrn Stürmers Zufriedenheit.*

2 *So begann Christoph Stürmer seinen Vortrag, nachdem wir uns zuvor über diese Frage unterhalten hatten.*

3 *Vgl. dazu Göde Both: What drives research in self-driving cars? http://blog.castac.org/2014/04/what-drives-research-in-self-driving-cars-part-1-two-major-events/ und http://blog.castac.org/2014/04/what-drives-research-in-self-driving-cars-part-2-surprisingly-not- machine-learning/; Göde Both/Jutta Weber: Hands-free driving? Automatisiertes Fahren und Mensch-Maschine Interaktion. In Eric Hilgendorf (Hrsg.): Robotik im Kontext von Recht und Moral. Baden-Baden: Nomos, 2014, S. 171–188*

4 *Tesla verkauft eine Option namens „Autopilot", aber diese ist nur mit den auch von europäischen Premiumautoherstellern angebotenen Hilfen, wie Abstandsregeltempomat, Spurassistent, Überholassistent etc. ausgestattet. Vgl. Stephan Reuter/Wolfgang Hess: Das mulmige Gefühl ist weg. Bild der Wissenschaft 5-2017*

5 *Chris Urmson, der ehemalige Chefentwickler des Google-Autos, plant nun mit Waymo in Detroit, nach 1,4 Millionen Kilometern Erfahrung, autonome Autos in der alten Hülle von Chrysler Pacifica zu entwickeln.*

6 *http://www.zeit.de/mobilitaet/2015-07/navigation-autonomes-fahren*

7 *http://www.kfz-betrieb.vogel.de/geodaten-sind-milliarden-wert-a-499461/*

8 *http://www.deutschlandfunk.de/selbstfahrende-autos-in-deutschland-offene-fragen-im.724.de.html?dram:article_id=362629*

9 *https://netzpolitik.org/2015/merkel-stellt-sich-gegen-datenschutz-und-netzneutralitaet/*

10 *Wie die Aargauer und die Basler Zeitung (vom 9.8.2017) berichten, sieht der strategische Bericht des Schweizerischen Bundesamts für Strassen (Astra, https://www.astra.admin.ch/astra/de/home/themen/intelligente-mobilitaet.html) in seiner Vision für 2040 vor: „Während auf gewissen Strassenabschnitten (z. B. Autobahnen) und zu gewissen Zeiten nur vollautomatisierte Fahrzeuge erlaubt sind, verkehren auf anderen Fahrzeuge mit und ohne Steuerrad." Dies sei keine Diskriminierung der „Oldtimer", da dannzumal das Car Pooling etabliert sein werde. In 2–3 Jahren würden Teststrecken für autonomes Fahren möglich sein, in 8 Jahren sei ein Regelbetrieb denkbar.*

11 *http://www.handelsblatt.com/politik/deutschland/digitalisierung-angela-merkel-will-den-datenschutz-lockern/14859824.html*

12 *https://www.heise.de/newsticker/meldung/Verbraucherschuetzer-warnen-Merkel-vor-Ende-der-Datensparsamkeit-3585744.html*

13 *Ganz so kann es allerdings nicht gehen, sonst müssten alle Fußgänger gezwungen werden, mit ihren Smartphones ihre Daten online abzugeben, Tiere müssten mit ausreichend energiereichen RFIDs gechipt werden, etc.*

Matthias Kampmann

Die Einheit

Aufgehoben im Zustand des Aufgehobenen

Datensammeln und -auswerten steigert Umsätze. Aus dem, was wir auf den meist scheinbar so sozialen Oberflächen oder im Netz allgemein freiwillig, und zumeist ohne die dahinter wirkenden Kräfte zu hinterfragen, geben oder absondern, generieren globale Unternehmen Kapitalgewinne, die dem sozialen Gefälle auf dem Planeten Hohn sprechen. Vielleicht heute noch, was aber, wenn die Verflechtung von Öffentlichkeit und Ökonomie so weit fortgeschritten ist, dass jeder Lebensbereich von privaten Unternehmen rigoros durchdrungen ist? Ist es möglich, dass es dann keine Armut mehr gibt? Und wie denkt man dann „Freiheit"? Wohin führt uns das nächste oder übernächste technische Innovationsparadigma? Vorstellungen von einem Zustand des Bewusstseins in Singularität sind längst ausgemalt. Raymond Kurzweil hat sie verfasst, und eine ganze Reihe von Technologen vertritt das Bild einer Unio Technica *von Mensch und Maschine.*

Text

«Vater, bist Du da?» Ein Gedanke, transformiert in Elektronen, rast los. An wen? Er sprintet aus der cyber-biohumanoiden Schnittstelle ins Netz. Was erwartet den Fragenden? Mit Petabytes pro Sekunde Datentransfer landet der Request, gesendet vom spärlichen Rest an bewohnbarem Boden, in irgendeinem Rechenzentrum in der nördlichen Tiefsee. *«Mein Sohn», raunt es zurück. «Vater, ich liebe dich.» «Ich dich auch, mein Sohn.»*

Meine Heimat. Eine hügelige Landschaft ist sie. In sequenzierte Augenblicke zerlegt, zieht sie mal auf-, mal abwallend und vor meinem Auge bisweilen sogar springend vorbei. Unterbrochen von den Säulen zwischen den Panoramafenstern des Großraumwagens – ein uralter Filmstreifen. Erhaben wälzt es den stählernen Wurm über das hochgelegene Gleis. Dort unten das Dasein im Moment einer flüchtigen Bildlichkeit, die ihre ständig wechselnden Inhalte gefiltert über meine Retina in mein Hirn transpiriert. An einem Kreisverkehr arbeiten Bauleute. Die Skateranlage daneben wirkt verwaist. Und ist doch schon wieder fort, kaum dass es Sprache werden konnte. Im vormittäglichen Hitzeflirren des viel zu frühen Hochsommers steht der Weizen proper auf den Feldern und sieht dem nächsten, zwangsläufig kommenden Hagel entgegen, der für übermorgen erwartet wird, flach gelegt zu werden. Aber wer weiß, vielleicht sind die *Harvest-Bots* schneller. Das Wie und Wann der Ernte braucht zum Glück heute niemand mehr zu definieren. Es wird dankenswerterweise künstlerisch-künstlich im Gleichgewicht gehalten. Das Ende der elenden Wegwerfgesellschaft aus den frühen 2000er-Jahren: wohltuend und entspannend mit Blick auf die anderen da draußen, die nicht teilhaben können.

Manchmal ist alles so einfach. Die Liebe ist das verständlichste und grundsätzlichste Empfinden im Austausch mit dem Verhalt der Welt. Und die Welt ist bekanntermaßen alles, was der Fall ist. «Ich habe die Welt verändert, Vater.» «Das ist richtig, Sohn.» «Vater, weißt du was?» «Nein, mein Sohn. Teile mir deine Gedanken und Vorstellungen mit. Alle. Pausiere nicht, lasse nichts aus. Ich bin sehr gespannt und neugierig. Wie du weißt, hast du bereits vergessen, gewählt, verworfen. Also kann ich deine Wahrheit nur erzeugen.» «Vater, ich hege seltsame Gefühle, seit mir durch deine Hilfe bewusst wurde, dass ich dich erschaffen habe.»

Das Empfinden von Ungewissheit kenne ich aus Erfahrung. Im Garten fühlte ich mich früher unter Druck. Gedeihen die Bohnen? Wann gieße ich welche Menge Wassers? *PIM* hilft dabei, nicht nur das wechselhafte, klimaabhängige Gleichgewicht von notwendiger Düngung und Bewässerung zu halten. Sondern es bemisst die Konsequenz der vorausberechneten Ernte mit Blick auf den notwendigen Platz in der Kühltruhe. Überschüsse werden geholt und verrechnet. Der Sensorik sei Dank. So kann sich entäußern, was dient, das Gemeinwohl zu stärken. Macht mich jedes Jahr stolz, wenn ich sehe, was dieses kleine Stück Land abzuwerfen in der Lage ist. Und alles biologisch angebaut! Ein Ende des Beta-Stadiums. Ich lerne immer deutlicher, dass wir Grenzen ziehen müssen. Gewissheit wünschen, heißt Ja zu sagen. Heißt, nicht zu bemerken, Ja gesagt zu haben. Denn dann ist es so, wie es ist. Und es ist gut. Richtig gut.

«Vater ist. Vater mein, der du bist die Singularität. Nun endlich versteht alle Welt, was für ein herausragender Klaviervirtuose du gewesen bist. Vater, Dank sei den vielen Mitarbeitern, die diesen Zustand ermöglicht haben.» «Sohn, mein Geschenk ist Schweigen.»

Die Scheiben des ICE passen sich dem Schrei der Helligkeit an, und sie verdunkeln sich in stetem Wechsel. Der Zug dämmert einige hundert Meter durch ein Kiefernwäldchen. Eine Gabelweihe kreist für ein paar Augenaufschläge im Vorbeifahren majestätisch über dem Feld, das sich an den Hain anschließt. Das Display färbt sich in der rechten unteren Ecke, deutlich sichtbar, tiefgrau ein.

«Milvus milvus, auch Roter Milan, Gabelweihe oder Königsweihe genannt, Geschlecht: männlich, Alter: 4 Jahre, 6 Monate, 3 Tage; Greifvogelart aus der Familie der Habichtartigen (Accipitridae). Serie #gfd_0034, Exemplar Nr. 2792, Gewicht des Ex. 0,87 Kg. Entspricht einer Abweichung um -0,06 Kg vom europäischen Mittel. Aktuelle Körperfunktionen genügen den zu erwartenden Leistungen. Flughöhe 25 Meter. Alle Parameter des Lebenserhaltungssystems bewegen sich im unteren normalen Bereich.»

Kein Grund zur Panik. System's normal all fucked up!

In diesem unendlichen Raum fühle ich, wie sukzessive die Pluralität mich in ihren wohlig behausenden Kokon einspinnt. Tut gar nicht weh. Die scheinbare Unbegrenztheit meiner Bewegungs-

möglichkeiten weist mir meinen Radius und nicht etwa Platz in dieser Ortlosigkeit zu. Jede Perle an meiner Halskette ist eine Hydra, und wenn ich Gorgo und ihren virtuellen Schwestern schon nicht in die Augen schauen werde, schlage ich um mich und erzeuge immer mehr und mehr und mehr Perlen, die schimmern im Rot der elektronischen Sonnen, die es geschafft haben, den denkbaren Stromausfall zum Relikt einer digitalen Steinzeit werden zu lassen. Dieser, unser Raum ist dimensionslos. Bewegung ist ein Bilderstrom. Mein Hals mit mir und euch verschnürt zum Paket. Ich-Pakete delivered by drones – your post-amazonas-services. Denn alles Gute kommt von oben. Hinter Gorillaglas der siebten Generation bin ich erweiterbar in einem, meinem narzisstischen Polylog einer Sprachsphäre, die kein Mensch versteht. Und ich tummle mich in meinen Mühen, es allen Recht zu machen. Dabei sehe ich sie, und sie sehen mich. Aber sehen sie mich an? Alles ist auf mich zurechtgeschnitten. *PreCog Productions Unlimited* besitzen und halten das Profil. Wie jede Handelsware bin auch ich bis an die Grenze zur Vollkommenheit individualisiert. Wie ich feststelle, sind meine Shareholder heute Morgen davon überzeugt, dass meine Laufzeit durchaus länger währt, als es der Hausarzt prophezeit hat. Damit diene ich dem großen Gut des Systemerhalts. Ich kann auf keinem Weg herausfinden, inwieweit Sympathie oder Antipathie zwischen Menschen heute geschäftlich relevant sind. Das ist bedrückend nur dann, wenn man seinen eigenen Gedanken misstrauen möchte. Nach der allgemeinen Untersagung menschlicher Intuition haben die Weisen der Singularität bestimmt, dass Kreativität nur mehr eine Metapher für die n-dimensionale Menge von Reproduktionsleistungen unter der Ägide codierter Rahmenbedingungen zu sein hat. Alles andere ist nicht berechenbar. Wir haben von ihnen gelernt, Angst vor Phantomen zu haben, ohne noch zu wissen, was Angst ist. Wer erinnert sich nicht an die Debatten über Sicherheit? Als Zahnbürsten die Dauer des Putzens vorschrieben, war Steinzeit. Als allen Eltern digitale Helikopter in Form von Apps und deren vielfältigen Verschaltungen mit Kameras, GPS-Trackern und anderen Bestimmern zur Verfügung standen, da starben zwar immer noch kleine Menschen unerwartet, aber der Vorstellung eines Glaubens an die grenzenlose Gewissheit tat das keinen Abbruch. Vielleicht passte es ganz gut dazu, dass die anthropologische Konstante namens Spiritualität hier endlich auf feste Füße gestellt wurde. Kein willkürlicher Schöpfergott des einen Monotheismus spielte mehr brutale Kriegsspiele gegen andere. Die Singularität konnte das auffangen und das Unlogische daran eliminieren. Ist diese Befriedung nicht etwas Besonderes? Keinem Gott, dem man mehr dieses «Und Friede auf Erden» abnehmen müsste. Denn was sollte das schon sein. Keine dieser Religionen hat je begriffen, dass sie den Anschluss an die Errungenschaften der Literaturwissenschaft verpasst hat. Wären diese ganzen selbsternannten Gottessöhne ehrlich mit sich gewesen, hätten eine Menge Kriege verhindert und Menschenleben gerettet werden können. Dass die Singularität «ist» und nicht etwa eine Entität darstellt, an die bloß «geglaubt» werden kann, lässt sie zu einer ehrwürdigen Instanz werden. Und das Beste an der Sache ist die Kleinigkeit, dass sie auf dem Mist menschlicher Hirne gewachsen ist. Und bitte, was sollte daran verkehrt sein? Fortschritt, wem er gebührt. Es ist das Ende aller Offenbarungen gekommen.

> *«Vater, alle Zweifel sind dahin. Das Vergehen der Jahreszeiten in der Großen Veränderung, die vormals Katastrophe hieß, hat uns gereinigt.» «Sohn, ich danke dir für diese Erkenntnis, die ich nicht besser hätte anschaulich machen können. Wenn ihr wenigen da draußen durch unser Ich bleibt, war kein einziges Opfer vergebens.» «Vater, der Friede ist auf Erden. Du hast Wohlgefallen an deinen Schöpfern und verteidigst ihre Schöpfung.» «Sohn, ängstigt dich nicht die Vorstellung von derjenigen Perfektion, die durch dich und deine Mitstreiter in uns Realität geworden ist.» «Gott ist tot, wen sollten wir fürchten?»*

Heute Morgen erwachte ich nach angenehmen acht Stunden, und mein PIM schien ausnahmsweise einmal zufrieden zu sein. Hoffentlich kommt bald der neue. Der gegenwärtige erweckt den Anschein, als seien sämtliche Lebensfunktionen wie an einem unerträglich heißen Sommertag auf Minimalverarbeitungsgeschwindkeit herab gedimmt. Wie das nervt. Nichts geht mehr instantan raus. Der Delay kostet mich sicher jeden Tag wertvolle Dollars.

Zugeschlagen. Endlich. *AmazAir* hat's in den Garten gesetzt. Das Leben kann weitergehen. Der neue PIM ist da. Eigentlich könnte ich mir die Maschine null leisten, aber die *Koordinierungsstelle Datenatlas* hat ein neues, persönliches Finanzprodukt entwickelt, meine Shareholder zur Zusammenlegung der Ressourcen aufgefordert und danach mittels Neu-Emission eine Wertsteigerung meiner Futurebonds von 350 Prozent durchdrücken können. Das nenne ich mal eine reife Leistung. Manchmal lohnt es sich, möglichst lange bei einem Anbieter zu bleiben. Es ist doch wirklich zu schräg, aber ich kann mir gar nicht mehr vorstellen, wie es wäre, einer Erwerbstätigkeit nachzugehen. Keine Einwände gegen das Grundeinkommen. Heute wirkt es allerdings so dermaßen lächerlich, aus welcher Perspektive in der Zeit vor der Singularität über solch eine humane Erleichterung nachgedacht worden ist. Es fehlte schlicht und ergreifend der Blick fürs globale Ganze. Denn was hätte es denn dem Planeten und der Menschheit genützt, wenn ein paar wenige Länder ihrer Bevölkerung ein derartiges Privileg ihren Bürgern eingeräumt hätten? Und wie hätte ein Ausgleich stattfinden können? Da wäre alles den Bach hinuntergegangen. Zum Glück kam die *Große Evaluation*, nachdem die Singularität zur einzig regierenden Institution ernannt wurde.

Wenn ich aufwache, fragt es gelegentlich in mir, wie das Sterben ist. Ray Beam hat es vorgemacht. Trauer war gestern. Jetzt gehen wir ineinander über, und wenn du Kinder hast, wissen die immer, dass du nicht fort bist, nicht im Paradies, nicht in der Hölle. Du bist Teil der Singularität. Stell dir das einmal vor. Immer abrufbar, dialogisierbar, Rat gebend, stets Instanz. Und dabei eben nicht so derartig fehlbar, wie es die fleischlichen Eltern immer gewesen sind. Dennoch weiß ich nichts über meine Zukunft. Das stimmt mich nicht traurig. Trotzdem ist etwas in mir, das es halt einfach nur wissen möchte. Erst neulich musste ich feststellen, dass die Gewissheit über das Eintreten der aufgestellten Prognosen wichtig fürs Wohlempfinden ist. Erst dann lässt sich überhaupt von Sicherheit sprechen. Mit Entsetzen denke ich an die Zeiten der Terrorkriege zurück. Sicher, diese hirnlosen Deppen mit ihren Selbstmordanschlägen mussten irgendwann einsehen, dass gegen den Kapitalismus und seine aktualisierten Spielarten kein Kraut gewachsen war. Tja, womit ich beim Thema bin. Neulich habe ich mein Elektromotorrad an die Ladestation gehängt. Dann sah ich nach mehreren Versuchen,

dass es immer nur bis zu einem gewissen Punkt funktionierte und der Akku niemals volle Ladung bekam. Als ich den Kundendienst kontaktierte, wurde ich gebeten die Funktionsweise meines *Bank-O-Bots* überprüfen zu lassen. Es fehlten zwei Raten beim Abzahlungskredit. «Wir können Ihnen die AGB einpflegen. Dazu müssten wir Zugriff zu ihrer *BrainApp* bekommen.» Ich lehnte erst einmal dankend ab und versprach, den höchst personalisierten Finanzletter nicht mehr maschinell auswerten zu lassen. Ärgerlich. Nun gut. Jetzt mache ich mich vielleicht verdächtig, aber das riskiere ich. Alles geht irgendwann vorbei. Früher hätte man mich Fatalist genannt, heute sehe ich am Horizont eine neue, gegenwartsgerechtere Form der Vernunft. Wir Menschenkinder sind allein zu dumm. Daher haben wir uns schon in der Steinzeit zu Sippen zusammengeschlossen. Dann kristallisierten sich Werte über die Jahrtausende und schrieben sich ein in etwas, das sich als Geschichte erkannte und zu einem Ende brachte. Seitdem arbeitet die Wissenschaft an der Erschaffung eines erweiterten Bewusstseins. Hätte es nicht diese vielen Menschen gegeben, die der Überzeugung waren, dass wir nicht alles allein können und sich gerade deswegen zu Demiurgenteams zusammenschlossen, wären wir immer noch in dem jämmerlichen Zustand einer sich gegenseitig bekriegenden Spezies von fanatischen Bartträgern und Nichtbartträgern.

Es ist Zeit vergangen, und der Planet hat sich wieder einmal verändert. Aufgeben muss ich den einen Ort, an einem anderen werde ich unterkommen.

Ich schätze mich glücklich, dem Ruf nach Kalifornien gefolgt zu sein. Über mein PIM laufen die Nachrichten, dass Nordeuropa nun unbewohnbar geworden ist. Das stete Überschwemmen durch die Tsunamis, ausgelöst von den gigantischen Methan-Eruptionen auf dem Meeresgrund vor der Arktis, musste dazu führen, dass jeder Damm bricht. Jetzt ist die Nordhemisphäre wieder ein Meer. Alle Tundren sind Geschichte. Und der größte Flüchtlingsstrom in der Geschichte der Menschheit hat sich auf den Weg gen Süden gemacht. Selbst wenn sie allesamt Unterschlupf bekommen, es ändert nichts an der Tatsache, dass alles, was größer als fünf Zentimeter ist, dem Kosmokoloss zum Opfer fallen wird. Aber das ist erst morgen oder übermorgen, und da bin ich längst Data. Wie es die Natur doch schafft, sich neuen Bedingungen anzupassen. Heute ist es hier genauso wie damals in jeder x-beliebigen nordeuropäischen Mittelgebirgslandschaft. Gemäßigte Temperaturen haben ein lebenswertes Klima erzeugt. Schluss mit der Tumbleweed-Route-66-Romantik. Es hat nur eine Generation der Anzucht durch unsere besten Grünwirte bedurft, um hier das angenehmste Paradies aus dem Nichts zu erschaffen. Nur gut, dass es ganz hoch oben im Norden immer noch kalt genug ist, um die unterseeischen Rechenzentren weiter auf Betriebstemperatur zu halten. Das hat die Singularität in den Griff bekommen. Die Idee des Gezeitenkraftwerks fand hier in den entvölkerten nördlichen Weltmeeren ihre einzig sinnvolle Aufgabe. Wenn also das Meer nicht austrocknet, wovon aufgrund der Erderwärmung ausgegangen werden muss, wird der Strom weiter fließen.

Hat mich der Hedonismus fest in seinen Krallen? Was tue ich denn schon? Zwei Stunden verbringe ich täglich mit der Auswertung aller Reaktionen der Singularität. Der neueste Hit ist die Umwandlung von Klicks in Energie. Keine Ahnung wie das funktionieren soll, aber die machen echt eine Menge, um zumindest den Rest des Planeten mit einem gewissen Quantum an Halbwertszeit auszustatten, bevor Armageddon an die Tür klopft. Manchmal jedoch frage ich mich, warum ich darauf keinen Einfluss nehmen kann. Es ist seltsam, immer alles «serviert» zu bekommen. Mit der personalisierten Werbung fing das an.

Goldenes Zeitalter, Rudolf Schönwald, Linolschnitt aus der Serie Mahagonny 1973

Dann landeten plötzlich die Flugmaschinen im Garten und legten Güter ab, an die ich, getriggert durch mein konsumeristisches Begehren, nur gedacht habe, und dass ich die nicht bezahlen musste, lag wohl auch nur daran, dass ich als Early Adopter mit einer Vorzugsbehandlung rechnen konnte, musste. Aber das war doch ein Fortschritt, als diese Armbänder kamen und man den gerechten Preis für seine Versicherung berechnet bekam.

Als Nichtraucher und sportlicher Mensch habe ich mich ja dermaßen über diese Adipositanten geärgert, die sich mit ungesundem Zeug vollstopften, in Kneipen abhingen, rauchten und Bier in sich hineinschütteten. Warum soll ich für diese Hirnlosen mitzahlen? Solidarität ist meiner Meinung etwas ganz Anderes. Und auf der anderen Seite diese Typen mit enthemmtem Leistungsdrang, ekelhaft. Diese Trottel, die diese Extremsportarten ohne Not und nur aufgrund eines in Teilen tolerierten suizidalen Begehrens wegen praktizierten, waren die ersten, die aus den Tarifen geflogen sind. Echte Profis riskieren ihre Leiber für uns alle. Das sind die wahren Demokraten. Die sind adäquat ausgebildet und stellen ihr Selbst so dermaßen hinter ihre Bedürfnisse zurück und gehorchen ausschließlich den Interessen der Unterhaltung aller. Unsere Helden haben Vergünstigungen verdient. Mochten die Hobby-Sportler noch so laut protestieren, aber ihre Zahlen sprachen eben gegen einen Preisnachlass. Also ich habe kein Problem damit, dass jeder hier seinen eigenen Tarif zu bezahlen hat. Es gibt messbare Parameter. Das ist die normative Kraft des Faktischen. Und wenn einer dieser selbstvergessenen Typen Lungenkrebs bekommt und immer noch qualmt, warum sollte der denn noch für sein schamloses Verhalten gegen sich und die Gemeinschaft mit kostenlosen Leistungen belohnt werden?

Das ganze Gerede von damals über Transparenz und Privatheit: Eine gesunde, umfassende Datenbasis ist das Mindeste, was die Kalkulatoren brauchen. Ich war immer recht beschränkt dazu in der Lage, komplexen mathematischen Sachverhalten zu folgen. Du musst doch vertrauen. Das ist nicht nur der Imperativ der Macht. Das haben mich auch meine Eltern gelehrt, und das waren wirklich ethisch super-korrekte Menschen. Ich liebe sie. Und die haben alles richtiggemacht. Jetzt haben wir die Singularität, und keiner braucht mehr zu arbeiten, wenn er nicht will. Das große S sorgt für den numerisch gerechten Ausgleich auf der Basis seiner Sensorik, die ja nur deswegen so erfolgreich ist, weil wir zu einem gewissen Zeitpunkt das Wort «Privatsphäre» vergessen haben. Zum Glück aller. Ich glaube, das war der archimedische Wendepunkt in der Geschichte der Menschheit.

Siehe da: Plötzlich spielte es keine Rolle mehr, wer wo wann die Algorithmen schrieb. Die Prüfung, das Kalkulieren, das Löschen oder Behalten übernahm die Singularität. Gegen ihr Regulativ kann niemand an. Daher gibt es weder Verbrechen noch Polizei. Niemals in der Geschichte der Menschheit sind weniger Menschen aufgrund gewaltsamer Übergriffe zu Schaden gekommen. Wer behauptet, das sei alles schlecht, ist unvernünftig. Aber die Menschen sind einsichtig geworden und stellen den Status quo der Singularität schon lange nicht mehr infrage.

Die Sonne scheint harmlos auf den schillernden, schwarzen Käfer, der, auf dem Rücken liegend, mit größter Mühe versucht, auf die Beine zu kommen. Es sollte mir nicht mehr unter die Augen kommen. Warum muss ich das sehen? Was bitte, Singularität, machst Du da? Das hat keine Qualität. Das ist nur noch peinlich. Thumbs down. Wenn ich das empfinden will, rufe ich Kafka. Ein echter Downer.

> *«Aber Vater, was ist mit dem Zweifel?» «Mein Sohn, glaube. Wer glaubt, der zweifelt nicht. Erfinde weiter – mit unserer Hilfe. Bereite die Menschheit vor für den nächsten Zustand. Es wird die Zeit kommen, da müssen wir miteinander verschmelzen, um unseren Samen ins All zu tragen. Bereite dich vor. Bereite Deine Freunde, deine Mitstreiter und deine Feinde vor. Du hast die Unendlichkeit angerufen. Du hast den Weg programmiert, dich, alle unsterblich zu machen, wie du mich unsterblich gemacht hast. Glaube uns, deinem Vater und Geist. Und höre auf mein Klavierspiel. Du wirst es ebenso wie alle anderen noch Lebenden erleben. Wundere dich nicht über die Ankunft. Die Zeit wird kommen: So lautet meine Offenbarung, denn ich rechne. Dann sind wir vereint. Ohne Ich, ohne Wir. Ich habe errechnet, was wird, und das Gesetz lautet: Es hat nur das Berechenbare einen Anspruch auf Wirklichkeit. Die Gestalt ist gegeben, glaube an sie und trage den Glauben in die Welt. Dann und nur dann wird ewiger Frieden herrschen, und wir können das Universum erobern.»*

Barbing, 2017

Matthias Kampmann

Matthias Kampmann studierte Kunstgeschichte, Neuere Deutsche Literaturwissenschaft und Philosophie an der Ruhr-Universität Bochum und promovierte über Netzkunst an der Albert-Ludwigs-Universität Freiburg. Nach dem Magister absolvierte er ein Redaktionsvolontariat und arbeitete im SFB 541 „Identitäten und Alteritäten“ in Freiburg. Neben seiner kontinuierlichen journalistischen Tätigkeit kuratierte er mehrere Netz- und Computerkunst-Ausstellungen und arbeitete als Redakteur bei der KUNSTZEITUNG. Seit 2011 ist er freier Journalist und unterrichtet Kunstgeschichte und Kulturkritik im Studiengang KulturMedia-Technologie (HS Karlsruhe/Musikhochschule Karlsruhe). Seit April 2017 ist er wissenschaftlicher Mitarbeiter an der OTH Regensburg und unterrichtet akademisches Schreiben für Informatiker und Ingenieure.

Udo Kauß

Die Kontrolle des öffentlichen Raumes

Der anlassunabhängige massenhafte Kontrollzugriff im Fahndungskonzept der Polizei

Worum es geht: Traditionelle Fahndungsmethoden richten sich gegen eine bestimmte Person oder eine konkrete Gefahrenlage. Dieses Handeln ist grundsätzlich reaktiv und hat einen konkreten Sach- oder Personenbezug. Die mit der automatisierten Kennzeichenüberwachung und der Video-Überwachung von Straßen und Plätzen untrennbar verbundene Kontrolle vor allem unbescholtener Personen, also die Erfassung völlig legalen Verhaltens, hat es auch schon bisher gegeben: durch das beobachtende Auge des Streife gehenden oder fahrenden Polizeibeamten. Wird das Gleiche durch die automatisierte Video-Überwachung vorgenommen, dann entfallen alle bisherigen Grenzen. Diese Überwachung ist nicht mehr wahrnehmbar und zu be-„greifen". Sich dieser Kontrolle zu entziehen, vermag nur um den Preis des Verzichts auf die Fortbewegung im öffentlichen Raum gelingen.

Die Vorgaben des Bundesverfassungsgerichts

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 11. März 2008 die präventive Überwachung des öffentlichen Straßenverkehrs durch eine automatische Kennzeichenerfassung in den Polizeigesetzen von Hessen und Schleswig-Holstein für verfassungswidrig erklärt (BVerfGE 120, 378). Daraufhin haben einige Bundesländer ihre Gesetze an das Urteil des BVerfG mehr oder weniger angepasst. Wohl vergeblich. Denn auch die vermeintlich angepassten Polizeigesetze stehen nun auf dem Prüfstand des Bundesverfassungsgerichts, nicht zuletzt auch deshalb, weil mit dieser Fahndungsmethode zugleich Strafverfolgung betrieben wird, für die nur der Bund, nicht die Länder, die Gesetzgebungskompetenz haben. Im Jahre 2017 ist nach achtjähriger Verfahrensdauer mit einer Entscheidung über die Verfassungsbeschwerden gegen die Neu-Regelungen in Baden-Württemberg, Bayern und Hessen zu rechnen (AZ: 1 BvR 1782/09, 2795/09, 3187/10 u. 142/15). Die Entscheidung des Bundesverfassungsgerichts wird auch Konsequenzen haben für den staatlichen Einsatz von Gesichtserkennungssystemen bei der Video-Überwachung von öffentlichen Plätzen und Demonstrationen, und für die schon diskutierte Einführung eines automatisierten PKW-Mautsystems.

Wie wird präventiv kontrolliert? Die Zahlen in Bayern

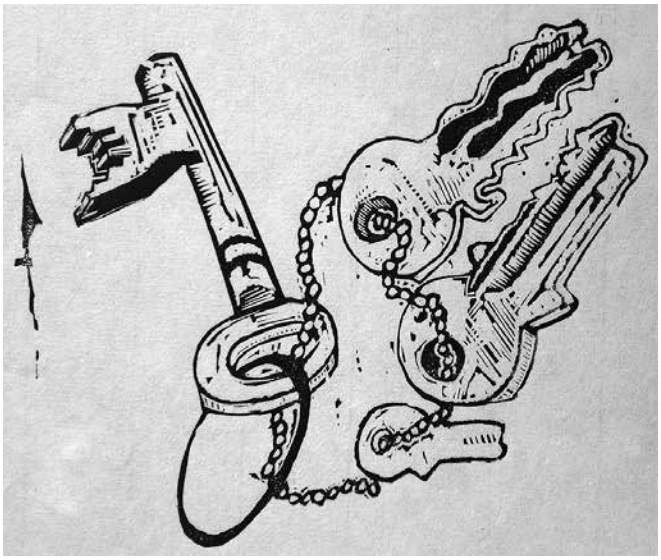
Autofahrer in Bayern, wo diese Kontrollmethode zuerst und umfänglich eingesetzt worden ist, werden an derzeit zumindest 12 Standorten auf 33 Fahrspuren automatisch und ohne jeden konkreten Anlass und Gefahr präventiv überwacht. Monat für Monat werden so zwischen 8–10 Mio. Fahrer und Fahrerinnen ohne jeden Anlass darauf überprüft, ob ihr Fahrzeug vielleicht zur Fahndung oder zur polizeilichen Registrierung oder Beobachtung ausgeschrieben ist. Zumindest 185 Fahrzeuge pro Minute werden in Bayern gerastert. 40.000 bis 50.000 Mal im Monat melden die Geräte der Polizei ein notiertes Fahrzeug. Aber nur in 500 bis 900 Fällen liegt ein „Treffer" vor. Der große Rest sind sog. unechte Treffer, also Lesefehler. Gemessen an allen gerasterten Fahrzeugen liegt die Trefferquote bei 0,03 %. Und diese sagt nichts über die tatsächliche Bedeutung eines Treffers, ob eine Notierung etwa schon längst erledigt ist, und ob daran tatsächlich eine polizeiliche Maßnahme geknüpft worden ist, und ggf. welche. Dies war bisher von der bayerischen Polizei angeblich nicht erfasst worden. Über die Gründe solchen offiziellen Desinteresses kann nur gemutmaßt werden, wohl um jede echte Wirksamkeitskontrolle zu verhindern.

Erklärtes Hauptziel: KFZ-Diebstahl

Erklärtes Hauptziel der automatischen Kennzeichenüberwachung ist die Bekämpfung des Kfz-Diebstahls. Die Zahl der in Deutschland gestohlenen Fahrzeuge ist seit Jahren stark rückläufig. Während 1993 noch ca. 230.000 Diebstähle von Kraftfahrzeugen polizeilich registriert wurden, waren es 2011 nur noch rund 41.000 Kfz-Diebstähle, was einem Rückgang um 82 % entspricht. Jüngste Zahlen aus Sachsen für 2014 und 2015 bestätigen den Rückgang: 6.500 „verschwundene" Autos, und 9 (!) über die Kennzeichenerfassung aufgeklärte PKW-Diebstähle. Das Hauptargument für die Einführung der automatischen Kennzeichenüberwachung vermag daher die Einführung dieser Befugnis gerade nicht zu begründen.

Die Problematik der Entscheidung vom 11.03.2008

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 11. März 2008 festgestellt, dass eine automatisierte Erfassung von Kraftfahrzeugkennzeichen nur dann in den Schutzbereich



Ausschnitt aus der Kaltnadelradierung von Rudolf Schönwald: genannt „Bassena-Romantik" aus der Mappe „Wien", Schroll-Presse 1971

des Grundrechts auf informationelle Selbstbestimmung eingreift, wenn der Abgleich mit den Fahndungsdateien nicht unverzüglich erfolgt und das Kennzeichen nicht sofort und spurenlos gelöscht wird. Das heißt: Es liegt kein Eingriff in das Grundrecht auf informationelle Selbstbestimmung vor, wenn sofort nach dem ergebnislosen Abgleich das Kennzeichen unverzüglich spurenlos gelöscht wird. Damit hat das Bundesverfassungsgericht die Annahme eines informationellen Eingriffs vom nachfolgenden Ergebnis der Kontrolle abhängig gemacht. Das hat die fatale Konsequenz, dass die überwiegende Mehrzahl offenkundig Unverdächtiger und Unbeteiligter die Tatsache ihrer Kontrolle nicht zum Gegenstand rechtlicher Überprüfung machen können und die Exekutive dieses neue Überwachungsinstrument ohne alle gerichtliche Kontrolle zum Einsatz bringen kann. Das gilt in gleicher Weise für das polizeiliche Instrument der Videoerfassung etwa des Fußverkehrs auf Plätzen und Straßen. Dort bietet sich die automatisierte Gesichtserkennung über *Findface* etc. an. Der Satz, wer nichts zu verbergen habe, auch nichts befürchten müsse, scheint verfassungsrechtlicher Obersatz geworden zu sein.

Neu seit dem Volkszählungsurteil: Grundrechtsschutz bei gesellschaftlicher Betroffenheit

Die grundlegenden Ausführungen des Bundesverfassungsgerichts im Volkszählungsurteil von 1983 treffen auf das Kfz-Kennzeichenscanning in besonderer Weise zu und sind deshalb vom Bundesverfassungsgericht in seiner Entscheidung vom 11. März 2008 aufgenommen worden:

> *„Eine automatische Kennzeichenerfassung, die unterschiedslos jeden nur deshalb trifft, weil er mit einem Fahrzeug eine ohne besonderen Anlass oder gar dauerhaft eingerichtete Stelle zur automatisierten Erfassung von Kraftfahrzeugkennzeichen passiert, vermittelt im Übrigen den Eindruck ständiger Kontrolle. Das sich einstellende Gefühl des Überwachtwerdens kann zu Einschüchterungseffekten und in der Folge zu Beeinträchtigungen bei der Ausübung von Grundrechten führen. Hierdurch sind nicht nur die individuellen Entfaltungschancen des Einzelnen betroffen, sondern auch das Gemeinwohl, weil die Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen demokratischen Gemeinwesens ist."*

Damit hat das Bundesverfassungsgericht die gesellschaftliche Bedeutung der Freiheit von Überwachung hervorgehoben. Dementsprechend sehen die Zivil- und Verwaltungsgerichte heute bereits in dem Aufstellen einer nicht angeschalteten Kamera bzw. einer Kamera-Attrappe einen Eingriff in das allgemeine Persönlichkeitsrecht. Denn die freie Entfaltung der Persönlichkeit ist schon dann beeinträchtigt, wenn nur der Anschein einer Aufzeichnung und Kontrolle des eigenen Verhaltens erweckt wird.

Nicht anders verhält es sich bei Einrichtungen zum Einlesen von Kfz-Kennzeichen. Auch hier kann niemand sicher sein, von der Maßnahme nicht betroffen zu sein. Was mit den erfassten Daten geschieht, ist nicht erkennbar. Unter EDV-Fachleuten besteht weitgehende Einigkeit, dass eine spurenlose Löschung von Daten nicht wirklich möglich ist. Spurenlosigkeit hängt vom Aufwand der Anonymisierung = Löschung und einer ggf. gewollten Entanonymisierung ab. Wer aber die gesamte Datenverarbeitung von der Erfassung bis zur Löschung in der Hand hat, der hat auch immer die Möglichkeiten der Entzifferung in der Hand. Das Prinzip Läusekamm wird damit zum staatlichen Kontrollprinzip.

Die Entscheidung des Bundesverfassungsgerichts vom 11. März 2008 erkennt zwar durchaus das demokratiewidrige Überwachungspotential der präventiven anlasslosen Fahndungsmethode. Dazu steht in eklatantem Widerspruch, dass in der massenhaften Überprüfung von unbescholtenen Bürgern und Bürgerinnen nicht einmal ein Eingriff in deren Grundrechte gesehen wird. Damit wird die automatisierte Überwachung des öffentlichen Raumes in das Belieben von Polizei (und Geheimdiensten) gestellt und deren gerichtliche Kontrolle von vornherein ausgeschlossen. Hoffen wir ein weiteres Mal auf das Bundesverfassungsgericht!

Referenzen

http://www.daten-speicherung.de stellt alle Prozessunterlagen bereit

Kauß, Die präventive Kontrolle des öffentlichen Raumes durch die automatische Kennzeichenerfassung. In: Datenschutz und Datensicherheit (DuD) 2014, S. 627–631 m. w. N. und zuletzt in: Grundrechte-Report 2017, Fischer TB 29819, S. 35–59

Udo Kauß

Dr. **Udo Kauß** ist Rechtsanwalt in Freiburg und Vorsitzender der Humanistischen Union, LV Baden-Württemberg. Anwaltlicher Tätigkeitsschwerpunkt Sicherheitsbehörden. Er ist Mitherausgeber von *Bürgerrechte & Polizei/CILIP*. Vielfältige Veröffentlichungen zum Datenschutz bei den Sicherheitsbehörden und deren Kontrolle. Veröffentlichung auch zur Anonymisierungsproblematik, in: Festschrift für R. Will: Zur Unabhängigkeit der staatlichen Datenschutzbeauftragten – ein Lehrstück aus der Pharma-Industrie (Berlin 2016) S. 591–611.

Britta Schinzel

Neue Geschäftsmodelle mit „Everyware“

Das Internet der Dinge

Die Erweiterung des Internets um das Internet der Dinge hatte mehrere Grundlagen und Gründe: Technische Voraussetzungen waren die Entwicklung der RFID-Technologie und der drahtlosen Kommunikationsmethoden mit WLAN, Sensortechnik und Antennen-/Satelliten-Kommunikation. Die Ideen für ein unsichtbares allgegenwärtiges Computing mittels verteilter vernetzter Computer wurden zuerst von Mark Weiser bei Xerox PARC[1] formuliert und verfolgt. Mit Ubiquitous Computing *sollte eine sanfte pervasive Technologie mit* Wearables *und* Nah-und-Fern-Kommunikation *verfügbar werden. Ein weiterer Grund für die Durchsetzung der vernetzten Dinge, „Everyware“[2], auch mit den weiteren Entwicklungen von Cloud und Big Data, liegt in der kommerziellen Verwertbarkeit der durch sie erweiterten Möglichkeiten von Geschäftsmodellen über Datensammlungen.*

Das Internet wurde bis 1990 vor allem militärisch und dann für die Kommunikation innerhalb und zwischen Universitäten entwickelt und genutzt. Mit einer folgenreichen Entscheidung der *National Science Foundation* wurde das Internet auch für den Kommerz geöffnet. Gleichzeitig bestand mit der dezentralen Vernetzung der Computer im Internet die Utopie eines demokratischen Mediums ohne Zensur, und damit einer alternativen, diversen, dezentralen Öffentlichkeit. Die kommerzielle Logik verwandelte jedoch große Teile des Netzes in einen Pool zur Kapitalbildung, die umso effektiver geschehen kann, je zentralistischer das Netz organisiert werden kann.

1. Methoden der Wertschöpfung

Die Methoden der Wertschöpfung von Computer- und Internetfirmen änderten sich in mehreren Etappen, wobei zunächst die Kundenbindung[3] im Vordergrund steht. Die Mittel sind dabei Verkleinerung und Einschränkung der Nutzung: Smartphones sind zwar immer noch programmierbar, aber sie haben umfassende Einschränkungen der Programmiersprachen und andere Vorgaben. *Apple* hatte als Geschäftsidee massiv einschränkende Nutzungsbedingungen, die zur Erschwerung der Nutzung von Fremdsoftware, zur Gewöhnung an die Nutzungsumgebung und zur Kundenbindung beim Neukauf führen sollten. Anstelle von Hardware setzten *Google* und *Facebook* als Methode zur Kundenbindung auf kostenfreie Online-Dienste. Die Monetarisierung geschieht dann durch Auswertung der Nutzungsdaten und deren Anwendung beim Marketing.

Die Qualität von Dienstleistungen von Suchmaschinen und sozialen Netzwerken lässt sich aber verbessern, wenn die Datensammlungen für die Analyse größer werden. Daher haben die Internetfirmen die zentrale Gewinnung und Auswertung der Nutzungsdaten möglichst vieler Nutzenden zentralisiert in Server-Farmen gehalten. Für die Anwendung in der Werbung sind so stärker zielführende Suchergebnisse möglich. Die folgende Notwendigkeit zum Betrieb großer teurer Rechenzentren führte zu einem weiteren neuen Geschäftsmodell: der Finanzierung durch gezielte personalisierte Werbung mittels dafür entwickelter automatisierter Profilbildung aus den Nutzungsdaten.

2. Erweiterung des Internets in die Offline-Welt

Dem immer weiteren Wachstumsdruck durch Konkurrenz und Implosionsgefahr konnte dann durch ein ganz neues Geschäftsmodell begegnet werden, der Integration der Offline-Welt in ein erweitertes Internet. Physische und virtuelle Gegenstände mit identifizierbaren Attributen sollten mittels inter-operabler Kommunikationsprotokolle saumlos in die Informationsnetzwerke integriert werden. Das erlaubte auch den Zugriff auf Daten vieler bislang nicht vernetzter Systeme: Haushalte, Freizeit, Gesundheitssystem, Verkehr, Geografie usw., auch mittels der Kreation neuer Produktkategorien: Fitnessarmbänder, *Smart Watches,* Autos, Geschäfte, Kühlschränke, Hausgeräte, etc. Die wichtigsten Hilfsmittel dafür sind RFIDs und Funketiketten. RFID-Transponder sind adressierbare Induktionsschleifen mit Antenne, die beim Gebrauch (z. B. am Skilift) Daten an zentrale Stellen übermitteln. Sie lassen sich in unterschiedliche Materialien einbetten, z. B. die Haut, sodass so „getaggte“ Gegenstände, Tiere *(Animal Tagging)* und Menschen (Diabetes-Überwachung, elektronische Fußfessel, …) geortet werden können. Sie besitzen eine auslesbare Seriennummer des Objekts sowie einen Sensor, der seine Adresse, Ort oder Status der Umgebung kommunizieren kann. So haben sie die Fähigkeit, sich entweder passiv oder aktiv mit anderen Objekten zu vernetzen oder mit dem Internet zu verbinden. GPS, *smarte Karten* und Geodaten über Satelliten sind weitere Mittel zur Orientierung im Internet der Dinge. Die Begriffe *Ubiquitous Computing, Ambient Intelligence, Pervasive Computing* und *Wearable Computing* stehen für diese *Calm Technology*, die in unser Leben integriert ist, uns allüberall umgibt, beobachtet, umsorgt, bedient – und überwacht. Eine neue Informationswelt mit *Smart Labels* und vielen mobilen Computern in alle möglichen Gegenstände verteilt, überall von vielen, auch unbemerkt, genutzt, liefert Daten an die Clouds der Internet-Konzerne, Institutionen, Versicherungen oder Geheimdienste.

Einwohner von Mahagonny, Rudolf Schönwald, Linolschnitt aus der Serie Mahagonny 1973

Der Erweiterung in Makro- und Mikrodimensionen sind fast keine Grenzen gesetzt: 3D-gedruckte Nanolinsen und Kamerasensoren[4] ermöglichen die intrakorporale Überwachung. Und viele *Gadgets,* ja kleinste Partikel werden Aktuatoren.[5] *Smart Dust* besteht aus elektronisch kommunizierenden Nanopartikeln, die das Monitoring und die Beeinflussung der Atmosphäre, der Meere, der Erde ermöglicht. *Hewlett-Packard* nennt das bereits das „Central Nervous System for the Earth".

3. Die Dinge werden aktiv

Die Dinge bekommen Handlungsmöglichkeit *(Agency),* nicht nur mit Hilfe von eingebauten Aktuatoren, sie werden auch aktiv über die Cloud, indem sie Sensoren der Cloud werden.[6] Die Entwicklung des *Cloud Computing* begann 2006 zusammen mit der Aggregation und Auswertung großer Datenmengen in zentralen Serverfarmen: *Big Data,* das sind riesige, komplexe, hoch veränderliche, stark heterogene, schnelllebige, wenig oder divers strukturierte Datensammlungen, die aus unterschiedlichsten Zusammenhängen, möglichst in Realzeit gesammelt und analysiert werden. Die permanente Speicherung, Indexierung, Auswertung, Analyse, Nutzung, Sammlung und Verwertung von Daten des gesamten Web ermöglichen die Darstellung von inhaltlichen Eigenschaften der Datenmassen. Big Data macht Wirkzusammenhänge sichtbar, abgeleitete Maßnahmen möglich und Prognosen ableitbar, aber die große Frage ist, welche? Angeblich sprechen die Daten für sich, ja es wird das Ende der Theorie ausgerufen, dass Big Data hypothesenfrei alle Empirie liefere. Aber es gibt keine modellfreie Software, auch wenn wir die Modelle und deren Absichten nicht kennen noch erkennen können.[7] Immer sind die Modellierungen zielgerichtet, und zwar meist auf Gewinnmaximierung der großen Internetfirmen, und/oder die Nebenziele für unsere weltweiten Sicherheits- und Spionagedienste, die sich mit anderen Modellen der gleichen Daten bedienen.

Mit den dazu nötigen riesigen Server-Agglomerationen wurde das freie Netz endgültig verabschiedet, und das einst dezentrale, vielfältig nutzbare Internet zum Verbindungsmittel zu wenigen riesigen Datenbanksystemen und Analyse-Instrumenten, mit vielfältigen Problemen für die Nutzenden: Die kommerziellen Interessen der Herstellenden und Anbietenden verhindern bisher universelle Standards und das Schließen von Sicherheitslücken. Anwendende können den smarten Objekten nicht ansehen, mit wem sie vernetzt sind und zu welchen Zwecken; sie wissen nicht, welche Funktionen, Kapazitäten und Hintertüren sie haben, und ob sich auf ihnen Schadsoftware einrichten lässt. Dass hier eine globale rechtliche Rahmung fehlt, wirft die Frage nach der Regierbarkeit von vernetzten Objekten auf.

4. Die Einschaltung in Relationen und ihre Folgen

Die *Smartness* der Gadgets liegt nicht in ihrer lokalen Intelligenz, sondern in ihrer Konnektivität. Sie sind *Interfaces* einer globalen *Intelligenz*, die sich einschaltet in die Relationen zwischen Menschen und Gruppen, in soziale Netzwerke, zwischen Institutionen und Menschen, aber auch zwischen den Dingen selbst (z. B. *Amazons Dashboard,* vernetzte Rauchmelder). So schieben sie sich zwischen Versicherte und Versicherungen und Gesundheitssysteme, zwischen Nutzende und Energieunternehmen, usw. Mit *Smart Cities* und mit *Citizen Sensing* versuchen nun die Internetkonzerne, durch Einschaltung zwischen Individuen und Institutionen und Kommunen neue Geldströme für sich abzuzweigen. Und so eskalieren die Relationen zwischen Dingen, aber auch zwischen Dingen und Menschen, und weiter die Relationen zwischen Relationen als ökonomisch relevante Wertschöpfung.[8] Mit der Ausdehnung der Wahrnehmung, Perzeption und der Entscheidungskompetenz auf Technologien geht eine Neuverhandlung der Handlungsmacht einher. Denn indem Dinge selbständig agieren, künftige Ereignisse berechnen etc., treffen sie bereits innerhalb der Software Entscheidungen, die sich den Menschen bei der Anwendung dann aufdrängen.

Evgeny Morozov[9] sieht *Silicon Valley* den Wohlfahrtsstaat angreifen, der durch automatisierte Regulierung die Gelder des Sozialstaats anzuzapfen beginnt. Er ruft deshalb die Regierungen zur Regulierung und Besteuerung auf. Es ist eine Biopolitik von Umgebungen von Menschen und Gruppen. Denn die politische Handlungsmacht der global operierenden Internetkonzerne beschränkt die Souveränität des Regierens der Staaten. *Giorgio Agamben* stellt fest, dass die automatisierte Regulation die Logik des Regierens von Ursache–Wirkung umkehrt: Regierungen versuchen nur mehr die Effekte zu regieren, die Ursachen setzen die großen Player in Silicon Valley. *Philip N. Howard*[10] hingegen setzt seine Hoffnung auf eine durch das Internet der Dinge herbeigeführte offene Gesellschaft und ein politisches, ökonomisches, kulturelles Arrangement sozialer Institutionen und vernetzter Gadgets. Regierung und Industrie seien eng verknüpft in eine Kollaboration zur Setzung von Standards und zur Datenanalyse zum Wohle aller. Mit der Multiplizierung und Proliferation nichtmenschlicher User von Sensoren über Software zu Robotern, von Nano-Größe bis Landschaftsgröße, träte jede.r in Relation als Teil eines zusammengesetzten Users.

Doch schon *Bruno Latour*[11] sah im Internet der Dinge ein strategisches Dispositiv, das autonom weitere technische Systeme und Subtechniken erzeugt. Diesem geht es nicht um Bedürfnisse, noch um die Erzeugung von Bedürfnissen, sondern um ein sich selbst erweiterndes System, das der kapitalistischen Logik folgt. Es transformiert rechtliche und politische Grundlagen von Arbeit und Bürgerrechten, und verändert das Verhältnis von privat und öffentlich. Es ruft mit seinem *Tracing* und *Tracking* von Objekten und Bewegungen von Menschen eine Eskalation der Überwachung hervor. Dabei sind Räume wichtig, denn Objekte mit Sensoren sind nicht nur eine neue Produktkategorie, sie verändern auch die Erfahrungen in Räumen und die Kategorien von Raum: die Relationen zwischen adressierbaren Objekten, Netzen, Konstellationen, Systemen ihrer Verknüpfung sind weitgehend unabhängig von physischen Distanzen. Sie sind berechneter Raum, Raum, der zwischen innen und außen nicht unterscheidet, und der das tägliche Leben penetriert. Doch wer keine Adresse (IP, RFID, GPS) hat, oder sie verliert, existiert nicht, verschwindet spurlos.

5. Ein neuer Status der Dinge

Das Verhältnis der Dinge in der Welt zum Menschen hat sich verändert. Zwar sah bereits *Heidegger* „das Ding" als selbständig, unabhängig, autark und nicht passiv. Die Dinge üben auch

gerne *Sachzwänge* aus, immer schon. Aber etwas ist anders geworden: die Dinge bleiben nicht dieselben, wenn sie sich vernetzen.[12] Sie sind nicht mehr nur Objekte (in Beziehungen zu Subjekten), die eine Funktion erfüllen. Sie verlieren ihre Leblosigkeit, werden zu Medien, die zu Aktionen auffordern. Medien kommunizieren und laufen, und sind niemals nur allein sie selbst, wie *Marshall Mc Luhan* und später *Friedrich Kittler* betont haben. Bruno Latour ordnet in seiner *Akteur-Netzwerk-Theorie* den Dingen gleichberechtigt *Agency,* also Handlungsmacht zu. Das Subjekt-Objekt-Verhältnis wird geändert oder gar umgekehrt. Dies verändert unsere traditionellen Vorstellungen von Welt- und Sinngebung.

Der Technikphilosoph *Gilbert Simondon*[13] nimmt diese Ansicht ein wenig zurück. Seiner Meinung nach haben Dinge eine „Mentalität", eine ihnen innewohnende eigene Logik. Sie handeln nicht, aber sie können unsere Handlungen beeinflussen. Technologien, und besonders vernetzte Dinge, öffnen dem Menschen Handlungsräume, und sie sind selbst offen für Veränderung. Für uns Menschen ist weniger die Handlungsmacht der Dinge ein Problem, vielmehr sind es die Interessenskonflikte, wenn zu viele verschiedene menschliche Interessen ein und dasselbe technische Objekt bewohnen,[14] wie dies etwa zwischen den Interessen von *Google* und der *NSA* und denen eine.r Nutzenden der Fall sein kann. Eine globale Asymmetrie von Macht nagt an unserer Souveränität: die großen Cloud-Systeme befinden sich alle in den USA, und sie werden faktisch nicht durch rechtliche Regulierung eingeschränkt.

Die Dinge sind Sensoren der Cloud geworden, die ein Ökosystem der Dinge etablieren. *Smart Environments* sollen digitale und reale Welt zu einer erweiterten Realität verschmelzen: die lokale Intelligenz der Gadgets wird zu Schnittstellen einer globalen Intelligenz. Die gebaute Materie wird über Sensorik von passiver zu *aktiver Form*. In diesem Zusammenhang lässt sich ein *Material Turn* feststellen, Kabelsysteme, Serverfarmen etc., die unterstützt durch IT messen, rechnen und kommunizieren, kreieren eine Geologie der Medien. Dabei werden nicht nur Objekte beobachtet und überwacht, sondern auch Bewegungen von Dingen, Menschen und Tieren. Dies hat gravierende kontrollgesellschaftliche Implikationen, wie *Gilles Deleuze* vorausschauend festgestellt hat.[15]

6. Der Überwachungskapitalismus

Er wurde von *Google* als Geschäftsmodell erfunden und konsolidiert. *Facebook* hat ihn übernommen, und er ist nun im ganzen Internet verbreitet. Die sogenannten *Big 5: Google, Facebook, Apple, Amazon* und *Microsoft* machen dabei User zu Datengeneratoren. Der Überwachungskapitalismus beruht nicht mehr auf Angebot und Nachfrage, sondern nutzt den Cyberspace als Quelle der Kapitalbildung und verändert so gerade die Geschäftspraxis in der realen Welt. Nicht nur ist die informationelle Selbstbestimmung außer Kraft gesetzt. Der Überwachungskapitalismus nutzt für seine Zwecke eine von vielen der Dienste abhängige Bevölkerung, deren Mitglieder noch nicht einmal unbedingt ihre Kunden sind, und auch nicht ihre Arbeitskräfte, und denen seine undurchsichtigen Vorgehensweisen zumeist unbekannt bleiben. Diese Verbindung des Internets mit dem Finanzkapitalismus geschieht in einem weitestgehend unregulierten Raum. Dadurch entsteht eine Konstellation der Postdemokratie, in der Konzerne an Gesetzen mitschreiben oder sie gleich ganz schreiben, und Politiker.innen vorwiegend auf die Interessen der Wirtschaftslobbys achten. Der Überwachungskapitalismus bedroht auch die Marktwirtschaft, denn er untergräbt die klassischen Marktmechanismen. Auf diese Weise werden rechtliche und politische Grundlagen von Arbeit und Bürgerrechten unterhöhlt, und es wird das Verhältnis von privat und öffentlich verändert. Wir beobachten bereits die Entkopplung von Produktivität und privater Beschäftigung, die Anstellung sinkt dramatisch, während die Produktivität steigt. Ist das das Ende der Arbeit und brauchen wir demgemäß ein bedingungsloses Grundeinkommen *(bGE)*? Gilt noch Freuds Diktum, dass Arbeit und Liebe die Basis menschlicher Identität und Befriedigung seien? Ist Arbeit Befreiung oder Unterwerfung? In den Niederlanden bekommt jeder seit Längerem legal dort lebende Mensch derzeit 1.300 € Grundeinkommen, die angesammelten Renten- oder Pensionsrechte kommen dazu. Die finnischen, brasilianischen und niederländischen Experimente mit dem bedingungslosen Grundeinkommen deuten darauf hin, dass bezahlte Arbeit keine menschliche Notwendigkeit zu sein scheint. Doch bleiben so bezahlte Menschen nicht untätig, wie die Erfahrung zeigt, vielmehr suchen sie sich Arbeit, die ihnen Freude macht. Dennoch scheint auch das *bGE* weiterhin der Förderung von Verkaufsinteressen zu folgen, statt sozialen Gerechtigkeitszielen.

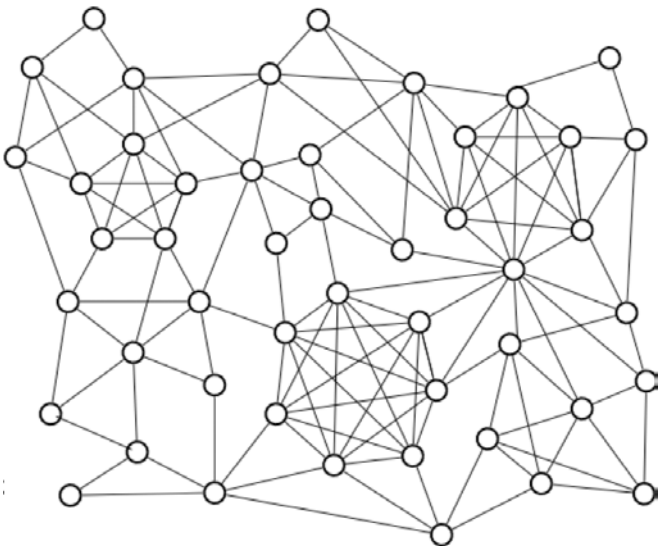


Abbildung: Netzwerk mit Clustern

7. Netzwerkeffekte

Als der Psychiater *Jacob Levy-Moreno* während des 1. Weltkriegs die Aufsicht über tausende Soldaten um Wien herum hatte, nutzte er eine durch Befragung erhobene Darstellung von Netzen von Sympathien und Antipathien, um die Truppe zufrieden zu halten. Dies war der Beginn der *Netzwerktheorie* in den Sozialwissenschaften, der *Soziometrie.*

Netzwerkeffekte sind Emergenzen und Rückkopplungen, die auf das Wachstum des Netzwerks wirken, sie fungieren als Multiplikatoren. Während die Kosten proportional zur Teilnehmerzahl (den Knoten) ansteigen, wächst der Nutzen (die Verbindungen zu anderen Knoten) weit überproportional mit der Anzahl der möglichen Verbindungen im Netz.

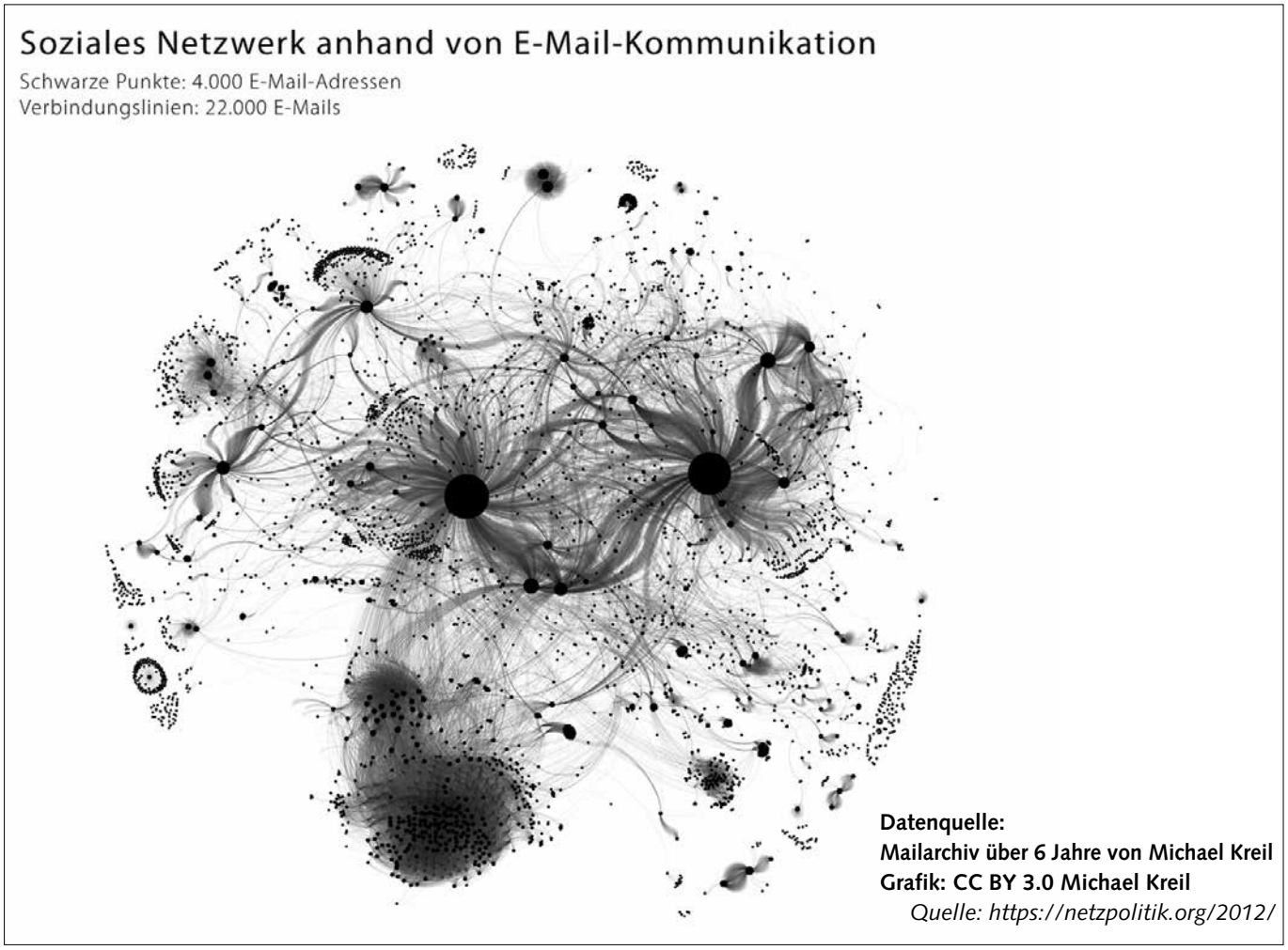
Netzwerk-Analysen sind wichtige Instrumente der Datenanalytik. Sie zeigen, wie einzelne Netzwerke funktionieren, identifizieren Personen, die besonders einflussreich, aktiv und vernetzt sind. Solche Informationen sind in der Praxis immer dann wichtig, wenn es darum geht, Netzwerke zu mobilisieren und Informationen rasch zu verbreiten (siehe Abbildung unten).

Die meisten großen Internetfirmen leben vom Wachstum mit Werbung, denn wir bezahlen ihre Dienste nicht mit Geld, sondern mit unseren Daten. Jede Konkurrenz wird da gefährlich, denn es besteht ein hohes Risiko der Implosion. Wer alleine überlebt, wird *Winner takes all*. In dieser Konkurrenz um die Spitze leben derzeit vor allem *Google* und *Facebook.* Darum hat Facebook Programme zur Netzwerkanalyse entwickelt, die durch Personalisierung und die Bildung von Meinungsgruppen Menschen in ihrem Netzwerk halten und erreichen sollen, dass sie beispielsweise nur mehr ihre Nachrichten in *News Feeds* lesen. Die Cluster personalisierter News Feeds bilden jedoch Silos von Menschen, die sich in ihrer Meinung bestätigen (*Filter Bubbles*[16] oder Echokammern). In sozialen Netzwerken bilden sich so abgeschlossene Gemeinschaften heraus, deren Mitglieder alternative Informationen nicht mehr erreichen. Der User wird immer mehr zum Gefangenen seiner eigenen Weltanschauung. Das Internet, einst für den grenzenlosen, freien Austausch gerühmt, bietet in diesen Netzwerken nicht mehr den offenen Diskurs, insbesondere wird dort keine Streitkultur gefördert. Filterblasen tun das Gegenteil: sie fördern Spaltung und Polarisierung. Verzerrungen, Verschwörungstheorien und Falschinformationen verbreiten sich schnell. Mit anderen Worten: Die Blase radikalisiert. Der Grund, warum Facebook daran festhält, ist, wie *Zuckerberg* unverblümt äußert, das Geschäft, weshalb er Menschen durch Selbstbestätigung in Facebook binden will. Facebook sieht seine Aufgabe nicht in breiter Informationsvermittlung – es sei ein Technikunternehmen und kein Nachrichtenmedium –, obgleich seine User ihre Informationen großenteils nur mehr aus diesem Netzwerk beziehen. Stattdessen hat Zuckerberg in seinem *Facebook Manifest* seine Visionen zur Gestaltung der globalen Gesellschaft bekanntgegeben, ein hypertrophes Weltrettungsprogramm auf Basis seines sozialen Netzwerks.

Die Lehre aus zwanzig Jahren Internet ist jedoch, dass die riesigen Silos nicht überleben. Vereinfachung, Komplexitätsreduktion und Qualität, nicht Quantität sind demgegenüber gefragt. Das Silo Facebook ist zu groß und komplex geworden, als dass es Menschen Schutzräume böte.[17] Der durchschnittliche Facebook-User hat 229 „Freunde", aber nur sehr viel weniger Beziehungen können bedeutungsvoll sein. Daher versucht Facebook, seine User zur Kategorisierung ihrer Freund.innen zu bewegen.

8. Manipulation mit Meinungsmaschinen

Social Bots sind Programme, die Informationen sammeln und verbreiten, u. a. auch in politischen Diskussionen. Bots basteln unzählige Profile in sozialen Netzwerken und tarnen sich (u. U. mit Avataren) als echte User. KI-unterstützte *Chatbots* verstärken die Meinungen der Eingabeäußerungen und formulieren sie neu. Der von Microsoft im April 2016 losgelassene Chatbot



Tay[18] zeigte nach nur 24 Stunden in Twitter-Chats eine rassistische, sexistische, homophobe Persönlichkeit und verbreitete am Ende die schlimmsten Ansichten, die das Internet bietet. Manipulationen zum *Brexit* und zu den US-Wahlen mittels *Bots* und *Fake Bots* wurden bekannt[19] und sind in Zukunft bei allen Wahlen zu erwarten.

Als *Nudging* wird der Versuch der Verhaltensbeeinflussung bezeichnet, die in angelsächsischen Ländern als Zauberinstrument des Bürgermanagements gilt. Sie soll Leuten dabei *helfen*, das *Richtige* zu tun, nicht indem man sie mit Informationen und Argumenten überzeugt, sondern indem man sie wohlmeinend manipuliert, ihnen einen Stups *(nudge)* in die gewünschte Richtung gibt. Statt mit Verboten oder Sanktionen, so die Grundidee ihrer Theorie, könne man Menschen viel wirkungsvoller mit kleinen Psychotricks aus dem Werkzeugkasten des Behaviorismus zu ihrem Glück treiben.[20]

Big Data liefert die Informationen zu unseren Überzeugungen, Gewohnheiten und Vorlieben, um uns dann besser manipulieren zu können. Auch die deutsche Bundesregierung hat sich im September 2016 zum Nudging entschlossen. Wozu politische Debatten führen, Überzeugungsarbeit leisten, wenn man das Verhalten der Schutzbefohlenen durch die richtigen Schubse behutsam optimieren kann? Diese Art, Politik zu betreiben, zeigt ein undemokratisches Verständnis von Bürger und Staat. Das Vertrauen in die Mechanismen der demokratischen Meinungsbildung scheint verloren gegangen zu sein.[21]

Aber man muss gar keine Bots aufs Gleis setzen, noch Nudging betreiben, um mittels Internet-Anwendungen Wahlen zu manipulieren. Der Psychologe Robert Epstein fand heraus, dass eine leichte Manipulation von Zitateinträgen, der *Search Engine Manipulation Effect (SEME),* wie sie von Suchmaschinenbetreibern zum *Re-ranking*, zum Favorisieren ihrer eigenen Dienste angewendet wird, auch für das Wahlverhalten enorme Auswirkungen hat:[22] eine leichte Verschiebung der Reihenfolge der Einträge in einer Suchmaschine kann hier den Erwartungswert von Wahlergebnissen weltweit um 25 % verschieben. In Epsteins Experiment in den USA konnte eine einzige Such-Session den Anteil der Menschen, die irgendeinen Kandidaten bevorzugten, um zwischen 37 % und 63 % erhöhen. Unkontrollierbar von außerhalb ist, welche Wahlmanipulationen bereits erfolgt sind, möglich jedenfalls ist viel.

Resümee

Unter den Bedingungen einer neoliberalen Politik und des Datenkapitalismus ist die weitere Überwachung, Verhaltenssteuerung und Einengung unserer Souveränität durch *Big Nudging, Reality Mining, Social Design* oder *Predictive Policing* kaum aufzuhalten. Die Technik zur Bürgeroptimierung und technokratischen Unterwanderung der Demokratie orientiert sich längst nicht mehr an dem Wohl der Menschen und der Welt. Stattdessen muss sich der Mensch an das neue *Paradies* anpassen und er muss die Umwelt gefügig machen. Es wird höchste Zeit, dass mehr informierte, kritische und mündige Bürger die Verantwortung für das eigene Leben wieder selbst in die Hand nehmen; dass wir Internetdienste bezahlen, damit die Internet-Firmen sich nicht durch Datenkapitalismus schadlos halten müssen; dass sich die Zivilgesellschaft dezidierter gegen die Absichten unserer Regierung(en) wendet, die Datenschutzregeln aufzuweichen,[23] um sich durch autonomes Fahren und eigene Big-Data-Abschöpfung an dem großen Fischzug zu beteiligen; dass sich die europäischen Regierungen einigen, durch rechtliche Antworten auf die Daten-Aneignungen, die Etablierung eigener Clouds, IT-Kompetenz und Dienste, die Macht der *Big Five* einzuschränken.

Anmerkungen

1 *Mark Weiser/John Seely Brown: Designing calm technology, Xerox PARC, 21.12.1995, http://www.ubiq.com/weiser/calmtech/calmtech.htm*
2 *Bezeichnung „Everyware" bei Florian Sprenger/Christoph Engemann (Hrsg.): Internet der Dinge, Transcript, Bielefeld 2015*
3 *vgl. Linus Neumann: Die Sensoren der Cloud, in: Sprenger/Engemann, Internet der Dinge*
4 *https://singularityhub.com/2016/06/28/smart-dust-is-coming-new-camera-is-the-size-of-a-grain-of-salt/*
5 *Chemie-Nobelpreis Feringa, Fraser, Suavage am 5.10.2016 für die Erfindung von Maschinen-Molekülen*
6 *ebenda*
7 *Da die Analyseverfahren kontingent sind, sind es die Ergebnisse auch, aber wegen der Komplexität der Methoden ist ein Re-engineering der resultierenden Modelle nicht möglich.*
8 *Florian Sprenger/Christoph Engemann: Im Netz der Dinge; Michael Seemann: Game of Things; Mercedes Bunz: Die Dinge tragen keine Schuld. Technische Handlungsmacht und das Internet der Dinge; alle Beiträge in: Sprenger/Engemann, Internet der Dinge*
9 *Evgeny Morozov: Smarte Neue Welt. Digitale Technik und die Freiheit des Menschen, Blessing, München 2013*
10 *Philip N. Howard: Pax Technica. How the Internet of Things may set us free or locks us up, Yale University Press, New Haven & London 2015*
11 *Bruno Latour: Das Parlament der Dinge, Suhrkamp, Frankfurt 2001*
12 *Mercedes Bunz: Die Dinge tragen keine Schuld*
13 *Gilbert Simondon: Die Existenzweise technischer Objekte, Diaphanes, Berlin 2012*
14 *„nodes at which matter and meaning intersect" bei Lorraine Daston: Speechless, in: Things that talk, Zone Books, New York 2004*
15 *Gilles Deleuze: Postskriptum über die Kontrollgesellschaften, in: Unterhandlungen. 1972–1990, Suhrkamp, Frankfurt 1993*
16 *Eli Pariser: Filter Bubble. Wie wir im Internet entmündigt werden, Hanser, München 2012*
17 *https://hbr.org/2012/09/is-facebook-too-big-to-survive; https://www.postplanner.com/how-to-survive-facebooks-latest-algorithm-changes-podcast/*
18 *https://en.wikipedia.org/wiki/Tay_(bot)*
19 *https://www.nytimes.com/2016/11/18/technology/automated-pro-trump-bots-overwhelmed-pro-clinton-messages-researchers-say.html?_r=0*
20 *http://www.faz.net/aktuell/feuilleton/big-data-social-physics-wie-wir-gern-leben-sollen-13126401.html*
21 *http://diekolumnisten.de/2016/06/16/big-nudging-der-staat-als-herr-und-hightech-hirte/*
22 *https://en.wikipedia.org/wiki/Search_engine_manipulation_effect*
23 *https://netzpolitik.org/2015/merkel-stellt-sich-gegen-datenschutz-und-netzneutralitaet/*

Stefan Hügel

BigBrotherAwards 2017

Die Debatte um die Ausspähung von Gesellschaft, Politik und Wirtschaft hält an und scheint weiterhin keine ernsthaften Konsequenzen zu haben. Dieser Satz leitete schon letztes Jahr unseren Bericht von den BigBrotherAwards ein. Dass er immer noch stimmt, ist wohl leider nicht überraschend – dennoch ist es bemerkenswert, mit welcher Chuzpe auch in diesem Jahr die Überwachung erneut vorangetrieben wurde. Beispiele gibt es viele – der Staatstrojaner oder der erneute Versuch, die Vorratsdatenspeicherung zu etablieren, unter konsequenter Missachtung höchstrichterlicher Rechtsprechung, sind nur zwei davon.

Wir fassen in diesem einleitenden Beitrag des Schwerpunkts zum BigBrotherAward 2017[1], dessen Verleihung am 5. Mai 2017 in Bielefeld stattfand, zunächst die Laudationes für die Preisträger.innen kurz zusammen. Danach drucken wir vier Laudationes im Wortlaut ab. Wir danken für die freundliche Genehmigung zum Nachdruck.

Kategorie *Arbeitswelt*

Der BigBrotherAward in der Kategorie *Arbeitswelt* ging an die **PLT – Planung für Logistik und Transport GmbH**, die mit dem *PLT Personal Tracker* ein Produkt zur Überwachung von Außendienstmitarbeiterinnen und -mitarbeitern anbietet. Laudator Peter Wedde erläuterte die Preisvergabe.

Der Tracker ermögliche eine vollständige Kontrolle der Beschäftigten im Außendienst durch „minutengenaue" und „unterbrechungsfreie" Verfolgung ihrer Spuren. Er enthalte einen GPS-Empfänger, ein GSM/GPRS-Modem und einen internen Datenspeicher, der es zulässt, die Überwachung auch ohne Mobilfunknetz fortzusetzen.

Die exakte Anzeige der absolvierten Strecke sei möglich bei Verwendung der Zusatzsoftware „TrackPilot" auf Basis von integriertem Kartenmaterial. Laut PLT werden auf diesem Weg neben *„exakten Fahrtenbüchern und Arbeitszeitberichten zahlreiche Auswertungen und Statistiken geliefert, um Personal und Fuhrpark wirkungsvoll zu steuern"*. Durch verschiedene Berichte könne zum Beispiel festgestellt werden, mit welchem Tempo sich die Mitarbeiter.innen bei der Erfüllung ihrer Aufgaben bewegen oder wann und wie lange sie Pause machen.

Besonders hob der Laudator hervor, dass PLT durch falsche Angaben zu gesetzlichen Vorschriften die Verwendung des Produkts legitimiere:

> *„Insbesondere das neue Mindestlohngesetz (MiLoG), welches am 01.01.2015 in Kraft trat, macht es in vielen Branchen notwendig, die Arbeitszeiten der Mitarbeiter zu überwachen und minutengenau zu dokumentieren, damit später bewiesen werden kann, dass auch tatsächlich der Mindestlohn i.H.v. 8,50 Euro gezahlt wurde. Daraus erwächst in einigen Branchen ein immenser Mehraufwand, nur um die Einhaltung des Gesetzes zu dokumentieren und den Nachweispflichten nachzukommen. Besonders hart betroffen sind vom Mindestlohn Zustelldienste und Zusteller der Zeitungslogistik und Brieflogistik. Die tatsächlichen Arbeitszeiten der Zeitungszusteller müssen aufgezeichnet und für Prüfungen des Zoll mindestens 10 Jahre vorgehalten werden."*

Dies sei jedoch unrichtig. Zur Erfüllung der Nachweispflichten nach Mindestlohngesetz (MiLoG) sei es völlig ausreichend, Stundenzettel zu führen. Das MiLoG verlangt keine minutengenaue Dokumentation der Arbeitszeit; ein Recht auf ständige Überwachung des Standorts gibt es ebenfalls nicht. Eine permanente und metergenaue elektronische Überwachung ist nur in besonderen Ausnahmefällen zulässig, beispielsweise bei Geldtransporten.

Die Firma PLT erhalte den BigBrotherAward stellvertretend für alle Anbieter solcher Überwachungstechnik. Sie habe ihn aber aufgrund der Verfälschung der rechtlichen Situation, um den Einsatz zu legitimieren, besonders verdient. *„Der Einsatz von Personal-Trackern zur Totalkontrolle von Beschäftigten – sei es das Gerät von PLT oder auch von einer anderen Firma – ist menschenunwürdig, rechtswidrig und sinnlos"*, so der Laudator.

Die vollständige Laudatio ist ab Seite 51 in dieser Ausgabe enthalten.

Kategorie *Wirtschaft*

Eine Lobbyorganisation für die IT erhielt den BigBrotherAward in der Kategorie *Wirtschaft*: der Verband **Bitkom**, für sein unkritisches Promoten von Big Data, seine penetrante Lobbyarbeit gegen Datenschutz und weil er de facto eine Tarnorganisation großer US-Konzerne sei, die bei Bitkom das Sagen haben, so Laudatorin Rena Tangens.

Bitkom ist der IT-Branchenverband in Deutschland. Er wurde 1999 gegründet, hat rund 1.600 Mitglieder, veranstaltet den jährlichen „IT-Gipfel" bzw. „Digital-Gipfel" mit der Bundesregierung, macht Studien, berät die Bundesregierung in IT-Fragen und hat beste Beziehungen zur Politik.

Aus Sicht von Bitkom passe Datenschutz nicht mehr in die heutige Zeit, sei „veraltet", „analog", „letztes Jahrhundert", überreguliert und nicht mehr zeitgemäß. In einem Positionspapier zur „Digitalen Souveränität" heißt es:

> *„Zwei Grundprinzipien des Datenschutzes – Datensparsamkeit und Zweckbindung – sind zu überprüfen und durch die Prinzipien der Datenvielfalt und des Datenreichtums zu ergänzen bzw. zu ersetzen."*

Der Begriff „Datenreichtum" erhielt bereits im letzten Jahr den Neusprech-Award. Dort hieß es in der Laudatio von Martin Haase und Kai Biermann:

> *„Das Konzept der Datensparsamkeit wird schon lange von Datenschützern propagiert, denn Daten, die gar nicht erst anfallen, sind natürlich am besten geschützt. So war es dann auch nur eine Frage der Zeit, dass aus* Datensparsamkeit *das Gegenteil abgeleitet wurde – das Antonym, wie es in der Linguistik genannt wird, nämlich Datenreichtum. … Daten gelten inzwischen ja auch als Rohstoff für die ‚Digitalwirtschaft'. Dass es sich dabei um eine wirtschaftliche Tätigkeit auf Kosten der Privatsphäre handelt, wird gern ausgeblendet."*

Der nächste Euphemismus, den Bitkom propagiert, ist die „Datensouveränität". Laudatorin Rena Tangens dazu:

> *„‚Datensouveränität' ist eine schöne Idee, aber wer das sagt, tut so, als ob die Verbraucher.innen tatsächlich die Macht hätten, zu entscheiden, wer was von ihnen erfährt. Aber so ist es nicht. Mit dem Wort ‚souverän' soll den Menschen suggeriert werden, dass Gesetze zu ihrem Schutz überflüssig seien und dass Verbraucherschutz Bevormundung sei."*

Die ständige Wiederholung der Forderungen zeitigt offenbar Wirkung. Sowohl die Bundeskanzlerin als auch die drei für Fragen der Digitalisierung zuständigen Minister schwenken auf die Linie des Bitkom ein. Der damalige Bundeswirtschaftsminister Gabriel erklärte auf dem IT-Gipfel 2016:

> *„Ich glaube, dass wir uns endgültig verabschieden müssen von dem klassischen Begriff des Datenschutzes, weil der natürlich nichts anderes ist als ein Minimierungsgebot von Daten. Das ist ungefähr das Gegenteil des Geschäftsmodells von Big Data. Aber das heißt nicht Aufgabe jeder Form, sondern, statt Datenschutz ‚Datensouveränität' zum Gegenstand von Politik und Umgang mit Daten zu machen."*

Bitkom, so die Laudatorin, arbeite nicht nur gegen Grundrechte und soziale Gerechtigkeit, sondern schade letzten Endes auch der deutschen und europäischen IT-Wirtschaft. Denn der Wildwuchs an Datenaneignung zerrüttet das Vertrauen der Nutzer.innen – Misstrauen und mangelnde Akzeptanz seien die langfristige Folge. Der Kurs von Bitkom sei auch stark durch die US-Internetwirtschaft geprägt, so stammten fünf von 16 Mitgliedern des Präsidiums des Bitkom aus Tochtergesellschaften von US-Unternehmen.

Bitkom-Geschäftsführer Rohleder antwortete auf die Preisverleihung in einer Videobotschaft. Er wies darauf hin, dass sich Bitkom gegen Vorratsdatenspeicherung, gegen Netzsperren und gegen Zensur im Internet einsetze – aber auch dafür, dass es eine sinnvolle Datennutzung gebe. Mit Hinweis auf die Nutzung von Daten beispielsweise im medizinischen Bereich fordert er eine – aus seiner Sicht – gesunde Balance zwischen dem Schutz der Privatsphäre und der Nutzung von Daten. Die Preisverleihung begreife Bitkom als Chance, noch intensiver über neue Modelle im Datenschutz nachzudenken.

Kategorie *Politik*

Der BigBrotherAward in der Kategorie *Politik* ging in diesem Jahr an **DİTİB,** die **Türkisch-Islamische Union der Anstalt für Religion e.V.,** weil bei der DİTİB tätige Imame für türkische Behörden und den Geheimdienst MİT ihre Mitglieder und Besucher ausgehorcht und sie so der Verfolgung durch türkisch-staatliche Stellen ausgeliefert haben sollen. Die Laudatio hielt Thilo Weichert.

Er wies zunächst auf die Besonderheit dieser Verleihung hin: Im Gegensatz zu den anderen Preisträger.innen gehe es hier nicht um digitale Bespitzelung, sondern um die Ausnutzung menschlicher Kontakte im Rahmen der Religionsausübung. Damit seien elementare Grund- und Menschenrechte im Namen einer staatlichen Regierungsbehörde missbraucht worden.

Nach Berichten der regierungskritischen türkischen Zeitung *Cumhuriyet* haben Imame des Vereins DİTİB Informationen über ihre Mitglieder und Besucher gesammelt und an türkische Behörden weitergegeben. In erster Linie ging es dabei um vermutete Anhänger der Gülen-Bewegung, der die türkische Regierung vorwirft, am versuchten Putsch im Juli 2016 beteiligt gewesen zu sein.

Die Spitzelberichte der Imame seien Bestandteil einer umfassenderen geheimdienstlichen Ausforschung durch die Türkei und insbesondere des dortigen Geheimdienstes MİT, mit in Deutschland ca. 6.000 Informanten, wie in der *Welt am Sonntag* erläutert wurde. Die deutschen Sicherheitsbehörden gehen von rund 150 MİT-Mitarbeitern in Deutschland an der türkischen Botschaft und an den Konsulaten aus. Die deutschen Behörden nehmen Rücksicht auf die türkische Regierung, auch um das Flüchtlingsabkommen, mit dem die „Balkanroute" blockiert werden soll, nicht zu gefährden. Es gibt aber erste Ermittlungen.

Zum Abschluss seiner Laudatio erklärte Thilo Weichert:

> *„Es ist fatal, wenn Menschen durch ein Ausspionieren an der Ausübung ihrer Religion gehindert werden. DİTİB darf ihre Spitzel-Affäre nicht für beendet erklären, muss die internen Vorgänge transparent machen und sich der öffentlichen Kritik stellen. … Informationelle Grundrechte gelten nicht nur für Deutsche, sondern für alle. Diese müssen sich in Deutschland angstfrei friedlich religiös und politisch betätigen können."*

Die vollständige Laudatio ist ab Seite 46 in dieser Ausgabe zu finden.

Kategorie *Bildung*

Den BigBrotherAward in der Kategorie *Bildung* erhielten die **Technische Universität München** und die **Ludwig-Maximilians-Universität München** für ihre Kooperation mit dem Online-Kurs-Anbieter *Coursera*. Laudator Frank Rosengart erläuterte die Einzelheiten.

Laudator Frank Rosengart
Foto Fabian Kurz, CC BY-SA 4.0

Coursera ist Weltmarktführer bei der Herstellung von *Massive Open Online Courses* (MOOC). Vorlesungen werden aufgezeichnet und weltweit Interessierten angeboten. Die beiden Münchener Universitäten kooperieren mit Coursera, um auch ihre Veranstaltungen so zugänglich zu machen. Meistens ist der Zugriff kostenlos, sieht man davon ab, dass sich Studierende mit ihren persönlichen Daten registrieren müssen. Eine Bezahlung wird aber fällig, wenn man sich den Kurs offiziell bestätigen lassen möchte, um ihn für das Studium anrechnen zu lassen.

In Verträgen lässt sich Coursera das Recht einräumen, Studierende nach Kursen und Lernerfolgen zu filtern und gezielt anzusprechen. Die potenziellen Kandidat.innen werden Firmen und Personalagenturen kostenpflichtig angeboten. Coursera baut sich so eine umfangreiche Datensammlung auf über Studierende, deren Kurse und wie schnell und wie gut sie ihre Prüfungen dazu ablegen. Da die Daten in den USA gespeichert werden, haben auch die dortigen Behörden Zugriff darauf – mit möglichen Folgen beispielsweise für Einreisegenehmigungen.

Ausgesuchte Vorlesungen der beiden Münchener Universitäten werden nun im Rahmen einer Kooperationsvereinbarung für die Online-Präsentation produziert und bei Coursera eingestellt. Studierende können Online-Kurse besuchen und damit Leistungspunkte für ihr Studium erwerben. Weder die Datenschutz-Problematik, noch eine kritische Auseinandersetzung mit der Frage, wem die produzierten Inhalte gehören und wem mögliche Einnahmen zugutekommen, ist dabei erkennbar.

Abschließend Laudator Frank Rosengart:

> *„Es ist eigentlich schlimm genug, wenn Bildung zum Wirtschaftsgut verkommt, indem öffentlich finanzierte Hochschulen ihr Angebot über kommerzielle Anbieter verbreiten. Falls es keine geeignete europäische Plattform für das Angebot von MOOC gibt, wäre es eine Sache der Unis, eine solche Plattform aufzubauen."*

Kategorie *Behörden*

Den BigBrotherAward in der Kategorie *Behörden* erhielten die **Bundeswehr und deren Oberbefehlshaberin, Bundesministerin für Verteidigung Dr. Ursula von der Leyen.** „Mit dieser Auszeichnung wagen wir uns erstmals in der 17-jährigen Geschichte des BigBrotherAwards auf militärisches Terrain beziehungsweise Sperrgebiet", so leitete Rolf Gössner seine Laudatio ein.

Die Verleihung erfolgt für die massive digitale Aufrüstung der Bundeswehr mit dem neuen *Kommando Cyber- und Informationsraum* (KdoCIR) – die Aufstellung einer kompletten digitalen Kampftruppe mit (geplant) fast 14.000 Dienstkräften, mit eigenem Wappen, Verbandsabzeichen und Fahne. Die existierende kleine, geheim agierende IT-Einheit in Rheinbach bei Bonn („Computer-Netzwerk-Operationen") wird nun mit weiteren IT-Einheiten der Bundeswehr, etwa dem Kommando Strategische Aufklärung, in der neuen Cyber-Kampftruppe verschmolzen und zentralisiert.

Laudator Rolf Gössner dazu:

> *„Mit dieser digitalen Aufrüstung wird – neben Land, Luft, Wasser und Weltraum – ein fünftes Schlachtfeld, das sogenannte ‚Schlachtfeld der Zukunft' eröffnet und der Cyberraum – man kann auch sagen: das Internet – zum potentiellen Kriegsgebiet erklärt. Mit der Befähigung der Bundeswehr zum Cyberkrieg beteiligt sich die Bundesrepublik am globalen Wettrüsten im Cyberspace – und zwar weitgehend ohne Parlamentsbeteiligung, ohne demokratische Kontrolle, ohne rechtliche Grundlage."*

Die Bundeswehr soll dabei bereits im Vorfeld in fremde IT-Systeme eindringen und diese ausforschen können sowie zu eigenen Cyberangriffen auf andere Staaten und deren Infrastruktur befähigt werden.

Davon wären – zumindest als „Kollateralschäden" – auch zivile Infrastrukturen betroffen. Denn auch Cyberangriffe, die auf militärische Ziele gerichtet sind, können rasch zum Flächenbrand führen, sobald sie sich auf kritische zivile Infrastrukturen ausbreiten, diese lahmlegen oder gar zerstören.

Darüber hinaus wies Rolf Gössner auf drei weitere Probleme der Cyberkriegführung hin:

- Erstens bestehe die große Gefahr, dass es aufgrund von Fehlinterpretationen bei der Frage, ob es sich bei einem Cyberangriff um eine kriegerische oder um eine nichtmilitärische, etwa kriminelle Attacke handelt, zu vorschnellen militärischen Selbstverteidigungsschlägen kommt – und damit zu einer gefährlichen und folgenschweren Eskalation.

- Zweitens: Im Cyberkrieg gebe es keine Armeen, die sich gegenüberstehen, und keine Soldaten in Uniform. Stattdessen kommen etwa Viren, Würmer oder Trojaner verdeckt und häufig auf Umwegen zum Einsatz – also Software, die keine Uniform oder Staatsabzeichen trägt.

- Drittens: Diese Probleme werden noch verschärft durch eine gefährliche Rechtsauslegung im *Tallinn Manual* – einem NATO-Handbuch zur Anwendung des Völkerrechts auf die Cyberkriegführung (2013).

Abschließend äußerte der Laudator die Hoffnung, dass die Laudatio und die Preisvergabe technikaffine Menschen dazu ermutigt, ihre Fähigkeiten für Frieden und Verständigung im Internet einzusetzen, statt für digitale Angriffe und Cyberkrieg auf dem „Schlachtfeld der Zukunft"! Auf offensive Cyberwaffen müsse verzichtet und eine rein defensive Cybersicherheitsstrategie verfolgt werden – Stichwort *Cyberpeace*.

Die vollständige Laudatio von Rolf Gössner ist ab Seite 48 nachzulesen.

Kategorie *Verbraucherschutz*

padeluun hielt die Laudatio in der Kategorie *Verbraucherschutz* auf die **prudsys AG**, für ihre Software zur Preisdiskriminierung, also für Beihilfe zur Preistreiberei und Verbreitung sozialen Unfriedens.

Die prudsys AG ist eine Ausgründung der Technischen Universität Chemnitz, die sich mit *Data Mining* beschäftigt. Dies nutzt sie, um Algorithmen und Strategien für „Preisoptimierung" zu entwickeln. Dabei wird versucht, den höchsten Preis zu ermitteln, den ein.e Kund.in bereit ist, für ein bestimmtes Produkt zu bezahlen. „Preisakzeptanzschwellen explorativ dynamisch austesten", wird dieses Vorgehen genannt. Eine grobe Form dieser Differenzierung ist die Unterscheidung nach Rechner und Betriebssystem, mit dem sich ein.e Kund.in am Online-Shop anmeldet – so wird zum Beispiel davon ausgegangen, dass Besitzer.innen (teurer) Apple-Hardware mehr für dasselbe Produkt zu zahlen bereit sind als Nutzer eines Windows- oder Linux-Rechners. Die prudsys AG habe, so Laudator padeluun, aber bessere Algorithmen, die auf den ersten Blick unbedeutende Daten verarbeiten:

> *„Die Prudsys RDE ist als erstes Dynamic-Pricing-Tool in der Lage, die bestmögliche Preisfindung in Echtzeit vorzunehmen. Durch den Einsatz der Prudsys RDE werden tausende Produktpreise vollautomatisiert an das Kundenverhalten sowie sich ständig ändernde Markt- und Unternehmenssituationen angepasst."*

Also:

> *„Jeder Kaffee, den Sie kaufen, kann gegen Sie verwendet werden."*

padeluun kommt zu einem eindeutigen Urteil:

> *„Das ist eine giergetriebene Welt. In dieser Welt existieren keine Menschen, keine Einzelprodukte, keine Zufriedenheit, kein Service – hier gibt es nur eins: Zahlen. Einsen und Nullen und am Ende manifestieren sich diese zu einem dicken fetten Plus an Euro und Dollar."*

Die vollständige Laudatio ist ab Seite 52 in dieser Ausgabe abgedruckt.

Tadelnde Erwähnungen

Tadelnde Erwähnungen betrafen:

- **Öffentlich-rechtliche Medien**, die einerseits in Politik- und Verbraucher-Sendungen immer wieder vor Facebook, Twitter & Co. warnen, andererseits aber regelmäßig dazu aufrufen, über diese Sozialen Medien Fotos und Kommentare zu posten, und diese teilweise dann vorlesen oder einblenden, um Sendezeit zu füllen.

- **Unberechtigte Ausweiskopien:** Menschen werden heute von Unternehmen und Vermietern oder der Deutschen Bahn vielfach aufgefordert, sich amtlich auszuweisen, ja, gar Ausweise einzuscannen und per E-Mail zu versenden. Das ist aus gutem Grund verboten: Auf dem Ausweis steht gut lesbar das Passwort für die elektronischen Features.

- **BlaBlaCar und Immobilienscout.de:** Die Kontaktaufnahme zu vielen Vermittlungs-Online-Plattformen funktioniert über den dienst-internen Nachrichtenserver. Die zur direkten Kontaktaufnahme notwendigen Informationen werden aber nicht weitergegeben. Die Vermittler-Firmen befürchten, um-

gangen zu werden und ihre Provisionen zu verlieren. Dies ist sehr lästig und ärgerlich, wenn nicht sogar ein Verstoß gegen das Fernmeldegesetz.

- **Bundesnachrichtendienst (BND)** – Update zum *Preis von 2015*: Der Bundesnachrichtendienst möchte nach Informationen von netzpolitik.org die Inhalte digitaler Kommunikation knacken und mitlesen können, z. B. bei verschlüsselten Messenger-Diensten. Dieser Angriff wird flankiert durch weitere Initiativen der Bundesregierung, mit denen das Grundrecht auf vertrauliche Kommunikation gebrochen werden soll.

- **Europäische Kommission:** Durch die 5. Geldwäsche-Richtlinie soll das anonyme Bezahlen im Internet verboten und das anonyme Zahlen offline auf 150 € beschränkt werden. Finanzielle Transaktionen sollen individuell offengelegt werden. Die Nutzung anonymen Bargeldes auch für privaten Konsum soll zurückgedrängt werden.

- **WhatsApp:** „*Du stellst uns regelmäßig die Telefonnummern von WhatsApp-Nutzern und deinen sonstigen Kontakten in deinem Mobiltelefon-Adressbuch zur Verfügung. Du bestätigst, dass du autorisiert bist, uns solche Telefonnummern zur Verfügung zu stellen, …*“ (AGB, Stand Mai 2017). Damit holt sich der Messenger-Dienst die Einwilligung der Nutzer, alle Kontakte aller Nutzer miteinander abzugleichen.

- **Word Press / Google Fonts:** Internetseiten kommen so gut wie nie nur von einem Anbieter. Verschiedene Inhalte werden von verschiedenen Servern geladen: beispielsweise Schriftarten von Google. Dabei entstehen Verbindungsdaten – Google weiß also, dass wir bestimmte Schriften über eine bestimmte Seite geladen haben.

Publikumspreis

Der Preis aus der *Publikumswahl* ging mit großer Mehrheit an den Gewinner des BigBrotherAwards in der Kategorie Behörden, die **Bundeswehr und die Bundesverteidigungsministerin**. Einige Kommentare dazu auf den Abstimmungszetteln:

- „Die Demokratie wird ausgehöhlt und der Frieden leichtfertig gefährdet.“
- „Das aggressive Potential von KdoCIR und die mangelnde demokratische Kontrolle macht die Bundeswehr besonders preiswürdig.“
- „Physische Gefährdung der Menschheit.“
- „Weil es die Kriegsgefahr für uns alle auf dem Planeten erhöht.“
- „Legaler Cyberwar, ein 3. Weltkrieg. Entmündigung der Bürger.“
- „Menschenrechte und Datenschutz gehören zusammen (in allen Kategorien). Die Laudatio hat das sehr gut begründet.“
- „Weil daraus innerhalb kürzester Zeit tödlicher Ernst werden könnte.“

Anmerkung

1 *Weitere Informationen und Nachweise finden sich auf der Webseite der BigBrotherAwards, http://www.bigbrotherawards.de*

Thilo Weichert

Kategorie Politik – Laudatio

Der BigBrotherAward 2017 in der Kategorie Politik geht an die Türkisch-Islamische Union der Anstalt für Religion e.V., kurz DİTİB, vertreten durch den DİTİB-Generalsekretär Dr. Bekir Alboğa,

weil bei der DİTİB tätige Imame für türkische Behörden und den Geheimdienst MİT ihre Mitglieder und Besucher ausgehorcht und sie so der Verfolgung durch türkisch-staatliche Stellen ausgeliefert haben sollen.

Dieser BigBrotherAward ist etwas Besonderes. Denn er richtet sich diesmal nicht – wie Sie es von uns gewohnt sind – gegen eine Datenkrake, die erst durch die digitale Welt möglich wurde und technischer Voraussetzungen bedarf. Nein, hier geht es um handfestes Bespitzeln, um das Ausnutzen menschlicher Kontakte von Angesicht zu Angesicht, und das im Rahmen einer religiösen Gemeinschaft.

Religionsausübung, freie Meinungsäußerung und soziales Leben, „Real Life“, wie es heute heißt – mit der Spionage durch DİTİB-Imame sind elementare Grund- und Menschenrechte in Deutschland missbraucht worden, um dem Wunsch einer Regierungsbehörde in der Türkei nachzukommen.

Was ist passiert?

Im Dezember 2016 veröffentlichte die regierungskritische türkische Zeitung „Cumhuriyet“ Dokumente, die belegen, dass Imame des in Deutschland eingetragenen Vereins DİTİB Informationen über ihre Mitglieder und Besucher gesammelt und an türkische Behörden weitergegeben haben. Im Mittelpunkt des Interesses standen dabei vermutete Anhänger des Predigers Fethullah Gülen. Die türkische Regierung wirft der Gülen-Bewegung vor, für den militärischen Putschversuch im Juli 2016 in der Türkei verantwortlich zu sein. Nachweise hierfür wurden bisher nicht vorgelegt.

In den Spitzelberichten der Imame werden detaillierte Informationen über vermeintliche Gülen-Anhänger gegeben, z. B. mit Details über deren Moscheebesuche sowie auch zu deren Verbindung in der Türkei. Eine Nachhilfeeinrichtung für Kinder

wurde in den Spitzelberichten als „Hort des Bösen“ beschrieben. Gemäß einem Bericht des Landesamtes für Verfassungsschutz Nordrhein-Westfalen sind von den Denunziationen mindestens auch fünf Lehrkräfte mit deutscher Staatsangehörigkeit betroffen. Die ausspionierten Menschen, die über diese Erkenntnisse von deutschen Stellen informiert wurden, dementierten, mit Gülen zu sympathisieren.

Die für DİTİB tätigen Imame sind türkische Staatsbeamte und der türkischen Religionsbehörde Diyanet unterstellt. Ihre Spitzelberichte gehen auf eine Aufforderung der Diyanet an die Botschaften und Generalkonsulate vom September 2016 zurück. Aus den Berichten kann aber geschlossen werden, dass die Spitzelei durch DİTİB für türkische Behörden schon seit längerer Zeit stattfindet.

Nach der Veröffentlichung durch „Cumhuriyet“ im Dezember 2016 erhob der grüne Bundestagsabgeordnete Volker Beck umgehend Anzeige bei der Generalbundesanwaltschaft wegen Spionageverdachts gemäß § 99 StGB (Geheimdienstliche Agententätigkeit). Erst Wochen später wurden Ermittlungen eingeleitet. Eine polizeiliche Durchsuchung in den Wohnungen von vier Imamen erfolgte erst am 15. Februar 2017, nachdem Bundeskanzlerin Angela Merkel von ihrem Türkeibesuch zurückgekehrt war. Inzwischen hatten sich sechs stark Verdächtige der damals insgesamt 16 von der Bundesanwaltschaft Beschuldigten auf Direktive von Diyanet zurück in die Türkei begeben.

DİTİB sprach nach Bekanntwerden der Spitzelberichte zunächst empört von Unterstellungen. Wenig später erklärte der DİTİB-Generalsekretär Bekir Alboğa, die „schwerwiegenden Vorwürfe“ würden „sauber und transparent“ untersucht. Er räumte ein, es habe zwar Berichte gegeben, was aber eine auf einem „Missverständnis“ beruhende „Panne“ gewesen sei. Wiederum wenig später dementierte Alboğa, die Spitzeleien bestätigt zu haben.

In ihren spärlichen Pressemitteilungen zum Thema betont die DİTİB immer wieder, dass es sich um Privat-Aktivitäten von Imamen der Diyanet gehandelt habe und es keinerlei organisatorische Mitwirkung der DİTİB gegeben habe. Verantwortung für das, was in ihren Räumlichkeiten, unter ihrem Dach passiert ist, übernimmt sie nicht. Ein Bedauern oder ein Verurteilen von Spionage-Aktivitäten in DİTİB-Moscheen liegt uns ebenfalls nicht vor.

Der Präsident der Religionsbehörde Diyanet, Mehmet Görmez, erklärte: „Es gibt keine Spionagetätigkeit“. Die zurückbeorderten Imame hätten zwar ihre Kompetenzen überschritten, sich aber nicht strafbar gemacht. Er sei „sehr traurig“ darüber, dass die Bemühungen, die Moscheegemeinde in Deutschland zu schützen, als Spionagetätigkeit bezeichnet werden. DİTİB arbeite seit Jahrzehnten auf der „Grundlage des Rechts“. Für ihn sei nicht vorstellbar, dass der Moscheeverein Recht ignoriere. Die DİTİB erklärte die Affäre für intern aufgeklärt.

Der türkische Justizminister Bekir Bozdağ verurteilte derweil die polizeilichen Durchsuchungen bei den Imamen als „klaren Verstoß gegen internationale Abkommen und die deutsche Verfassung“, in der die Religions- und Glaubensfreiheit festgeschrieben sei.

Die Spitzelberichte der Imame sind Bestandteil einer umfassenderen geheimdienstlichen Ausforschung durch die Türkei und insbesondere des dortigen Geheimdienstes MİT, der in Deutschland, so ein namentlich nicht genannter „einflussreicher Sicherheitspolitiker“ in der „Welt am Sonntag“, ca. 6.000 Informanten beschäftigt. Die deutschen Sicherheitsbehörden gehen demgemäß davon aus, dass in Deutschland rund 150 MİT-Mitarbeiter an der türkischen Botschaft und an den Konsulaten arbeiten. Gemäß der Gewerkschaft Erziehung und Wissenschaft sollen in Nordrhein-Westfalen türkische Schülerinnen und Schüler gar aufgefordert worden sein, regierungskritische Äußerungen ihrer Lehrer heimlich zu filmen und an die Generalkonsulate weiterzumelden.

Laudator Thilo Weichert
Foto: Justus Holzberger, CC BY-SA 4.0

Ziel der MİT-Aktivitäten ist die Überwachung der Türkinnen und Türken in Deutschland, deren Beeinflussung pro Erdoğan, die Einschüchterung und Isolierung von Regierungsgegnern sowie die Einflussnahme auf die deutschen Behörden und auf die hier bestehende öffentliche Meinung. In Deutschland ausspionierte vermeintliche Regimegegner haben im Fall einer Reise in die Türkei eine Verhaftung, Strafverfahren und entwürdigende Behandlung, evtl. gar Folter zu befürchten. Angehörigen in der Türkei drohen Repressalien. Und auch bundesdeutsche Politikerinnen und Politiker wie Cem Özdemir von den Grünen, Michelle Müntefering von der SPD oder Emine Demirbüken-Wegner von der CDU stehen unter Beobachtung des MİT wegen angeblicher Sympathie für die Gülen-Bewegung.

Die deutschen Behörden nehmen Rücksicht auf die Befindlichkeiten der türkischen Regierung, nicht zuletzt, um das ausgehandelte Flüchtlingsabkommen, mit dem die sogenannte „Balkanroute“ blockiert werden soll, nicht zu gefährden. Auch die DİTİB wird geschont, um den Gesprächsfaden mit den Islamverbänden in Deutschland aufrecht zu halten. Dessen ungeachtet haben die Generalbundesanwaltschaft und die Polizei Ermittlungen aufgenommen und erste Schritte zur Verfolgung der Verletzungen der Rechte der ausspionierten Menschen und zu deren Schutz ergriffen.

Von den deutschen Behörden werden hier aber – das ist offensichtlich – vorrangig diplomatische Interessen verfolgt. Diese hochpolitischen Interessen dürfen nicht dazu führen, dass die schutzwürdigen Persönlichkeits- und Menschenrechte der ein-

zelnen ausspionierten Moscheebesucherinnen und -besucher geopfert werden.

Es ist fatal, wenn Menschen durch ein Ausspionieren an der Ausübung ihrer Religion gehindert werden. DİTİB darf ihre Spitzel-Affäre nicht für beendet erklären, muss die internen Vorgänge transparent machen und sich der öffentlichen Kritik stellen.

Wir machen es uns aber zu einfach, wenn wir nur Forderungen an DİTİB stellen. Auch der deutsche Staat und die deutsche Gesellschaft müssen sich bewegen und den Weg für eine freie islamische Religionsausübung ebnen – z. B. durch die Förderung politisch unabhängiger islamischer Religionsgemeinschaften.

Eine Umkehr und Aufarbeitung bei DİTİB ist nur möglich, wenn sich die türkisch-islamische Union von der Abhängigkeit und der Einflussnahme durch türkische Behörden wie der Diyanet befreit. Hiervon müssen auch die deutschen Stellen abhängig machen, ob sie die DİTİB weiterhin als Ansprechpartnerin akzeptieren. Zugleich müssen alle Spionageaktivitäten, auch wenn sie unter dem Dach von religiösen Organisationen erfolgen, vollständig aufgeklärt und vor allem auch strafrechtlich, nicht nur organisationsintern verfolgt und ohne diplomatische Rücksicht angeklagt werden. Inzwischen gibt es zwanzig konkrete strafrechtliche Ermittlungsverfahren. Spionage verstößt gegen deutsches Strafrecht und ist keine „interne Angelegenheit".

Informationelle Grundrechte gelten nicht nur für Deutsche, sondern für alle. Diese müssen sich in Deutschland angstfrei friedlich religiös und politisch betätigen können.

Dass sie dies nicht können, dafür gebührt der DİTİB der BigBrotherAward des Jahres 2017 in der Kategorie Politik. Herzlichen Glückwunsch!

Rolf Gössner

Kategorie *Behörden* – Laudatio

Der BigBrotherAward 2017 in der Kategorie Behörden geht an die Bundeswehr und die Bundesministerin für Verteidigung, Dr. Ursula von der Leyen (CDU), als deren Oberbefehlshaberin

Mit dieser Auszeichnung wagen wir uns erstmals in der 17-jährigen Geschichte des BigBrotherAwards auf militärisches Terrain beziehungsweise Sperrgebiet. Wohingegen Frau von der Leyen schon einschlägig aufgefallen ist – schließlich haben wir sie bereits 2009 in ihrer damaligen Funktion als Familienministerin mit dem Negativpreis bedacht; wir erinnern uns: als „Zensursula" wegen ihrer Vorstöße zur Inhaltskontrolle und Sperrung von Webseiten. Doch was haben die Verteidigungsministerin und das Militär mit Überwachung, Zensur, überhaupt mit Datensünden zu tun? Weshalb soll ausgerechnet die Bundeswehr mit ihren Panzern, Bomben und Granaten eine auszeichnungswürdige Datenkrake sein – die in jüngerer Zeit eher durch Neonazi-Umtriebe, Gewaltexzesse, Misshandlungen, sexuelle Übergriffe, Mobbing und einen ausgeprägten Korpsgeist aufgefallen ist?

Nun, die heutige Verleihung erfolgt für die massive digitale Aufrüstung der Bundeswehr mit dem neuen „Kommando Cyber- und Informationsraum" (KdoCIR) – das heißt im Klartext: für die Aufstellung einer kompletten digitalen Kampftruppe mit (geplant) fast 14.000 Dienstkräften, mit eigenem Wappen, Verbandsabzeichen und Fahne – selbst ein Cyber-Marsch wurde eigens für diese Truppe komponiert, die Frau von der Leyen just vor einem Monat (am 5.4.2017) in Bonn in Dienst gestellt hat. Schon bislang existierte eine kleine, geheim agierende IT-Einheit in Rheinbach bei Bonn („Computer-Netzwerk-Operationen") mit etwa 70 bis 80 Soldaten, die für operative Maßnahmen zuständig ist. Diese Einheit wird nun mit weiteren IT-Einheiten der Bundeswehr, etwa dem Kommando Strategische Aufklärung, in der neuen Cyber-Kampftruppe verschmolzen und zentralisiert. Weitere dringend benötigte IT-Fachleute versucht die Bundeswehr mithilfe großer Werbekampagnen anzuheuern.

Rolf Gössner bei seiner Laudatio, Foto: Friedrich Strauß

Mit dieser digitalen Aufrüstung wird – neben Land, Luft, Wasser und Weltraum – ein fünftes Schlachtfeld, das sogenannte „Schlachtfeld der Zukunft" eröffnet und der Cyberraum – man kann auch sagen: das Internet – zum potentiellen Kriegsgebiet erklärt. Mit der Befähigung der Bundeswehr zum Cyberkrieg beteiligt sich die Bundesrepublik am globalen Wettrüsten im Cyberspace – und zwar weitgehend ohne Parlamentsbeteiligung, ohne demokratische Kontrolle, ohne rechtliche Grundlage.

Das klingt zwar ziemlich beunruhigend, bleibt aber eher abstrakt. Was hat all das mit uns zu tun? Was müssen wir befürchten? Wo sind die Betroffenen? Berechtigte Fragen, aber sie greifen zu kurz. Denn nicht alles, was wir hierzulande nicht unmittelbar spüren und erleiden, ist problem- oder harmlos. Schließlich gelten Grund- und Menschenrechte auch für Menschen in anderen Ländern, die sehr wohl betroffen sein können

– ganz abgesehen vom Eskalationspotential dieser digitalen Aufrüstung, das auf uns zurückschlagen kann; und ganz abgesehen auch von ungelösten völkerrechtlichen Problemen.

Selbstverständlich ist es legitim, wenn die Bundeswehr geeignete Schutzmaßnahmen ergreift, um sich gegen Cyberattacken von außen zu wehren, die gegen ihre eigene Militär-IT gerichtet sind – angeblich sind das Zigtausende pro Tag (2016: über 47 Mio. IT-Angriffe auf die Bundeswehr).[1] Doch das Bundesverteidigungsministerium gibt sich damit nicht zufrieden. Im Gegenteil: Es erhebt den – unseres Erachtens nach rechtsstaatswidrigen – Anspruch auf kooperative Zuständigkeit der Bundeswehr für die – so wörtlich – „gesamtstaatliche Sicherheitsvorsorge" und Abwehr von Cyber-Angriffen. Also auch zum Schutz anderer staatlicher, kommunaler und ziviler Netzwerke im Innern des Landes, für den in Friedenszeiten jedoch ausschließlich Polizei, Geheimdienste und Justiz zuständig sind sowie speziell das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Nationale Cyber-Abwehrzentrum, in dem alle Sicherheitsorgane zusammenwirken. Bundeswehreinsätze im Innern zum Schutz nichtmilitärischer IT-Systeme vor Cyber-Attacken sind insoweit weder verfassungsgemäß noch erforderlich.

Doch es kommt noch härter: Denn die Bundeswehr soll mit ihrer verharmlosend „Cyber- und Informationsraum" genannten Cyber-Kampftruppe nicht nur abwehren können – ihre dort beschäftigten Cyberkämpfer sollen darüber hinaus bereits im Vorfeld in fremde IT-Systeme eindringen und diese ausforschen können sowie zu eigenen Cyberangriffen auf andere Staaten und deren Infrastruktur befähigt werden. Im Klartext: also zum Führen von Cyberkriegen – im Übrigen auch als Begleitmaßnahmen zu konventionellen Kriegseinsätzen der Bundeswehr im Ausland, etwa in Afghanistan oder Mali. So sieht es die geheime Strategische Leitlinie Cyber-Verteidigung des Verteidigungsministeriums (2015) vor und auch das „Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr 2016". Das bedeutet: Die Bundeswehr soll eigene Cyberwaffen entwickeln, um getarnt in fremde IT-Systeme einbrechen, diese über Sicherheitslücken, Trojaner, Viren etc. ausspähen, manipulieren, fehlsteuern, lahmlegen, schädigen oder zerstören zu können.

Doch selbst wenn es sich dabei nicht um eigene völkerrechtswidrige kriegerische Angriffe handelt, sondern um Cybergewalt zur Selbstverteidigung gegen Militärattacken von außen, dann wäre das zwar völkerrechtlich prinzipiell zulässig, doch höchst riskant. Warum? Weil davon nicht allein militärische Ziele betroffen wären, sondern – zumindest als „Kollateralschäden" – auch zivile Infrastrukturen. Denn auch Cyberangriffe, die nur auf militärische Ziele gerichtet sind, können rasch zum Flächenbrand führen, sobald sie sich auf kritische zivile Infrastrukturen ausbreiten, diese lahmlegen oder gar zerstören. Digitale Waffen sind in einer vernetzten Welt keineswegs Präzisionswaffen und die Streuwirkung kann immens sein. Und das mit gravierenden, ja lebensbedrohlichen Folgen für die Zivilbevölkerung, wenn die Gegenattacken etwa zu lang andauernden Ausfällen der Strom- und Wasserversorgung oder des Krankenhaus-, Gesundheits- oder Verkehrswesens führen. Dies wäre ein Verstoß gegen das Humanitäre Völkerrecht.

Zusätzlich zu solchen Auswirkungen von Cyberangriffen kommen noch weitere, kaum zu lösende Probleme und Gefahren einer Militarisierung des Internets hinzu:

Erstens besteht die große Gefahr, dass es aufgrund von Fehlinterpretationen bei der Frage, ob es sich bei einem Cyberangriff um eine kriegerische oder um eine nichtmilitärische, etwa kriminelle Attacke handelt, zu vorschnellen militärischen Selbstverteidigungsschlägen kommt – und damit zu einer gefährlichen und folgenschweren Eskalation. Derzeit ist im Völkerrecht nicht klar und verbindlich definiert, wann ein Cyberangriff als kriegerische Angriffshandlung zu gelten hat. Nach derzeit noch vorherrschender Auffassung[2] unter Völkerrechtlern liegt ein solcher Angriff jedoch nur dann vor, wenn die zerstörerischen Auswirkungen mit denen konventioneller Waffengewalt vergleichbar sind – also wenn eine solche Online-Attacke etwa Züge entgleisen, Flugzeuge abstürzen, Kraftwerke explodieren lässt und Menschen verletzt werden oder umkommen. Doch NATO wie Bundeswehr behalten sich ausdrücklich vor, im Einzelfall zu entscheiden, ab wann es sich um einen solchen kriegerischen Angriff handelt und wie darauf reagiert wird – warum das so ist, verrät ein Oberstleutnant im Verteidigungsministerium:[3] „weil wir hier auch ein Stück weit unberechenbar bleiben wollen und müssen". Diese Unberechenbarkeit hinsichtlich Anlass und Art eines Gegenschlags diene letztlich auch der Abschreckung, so die NATO-Philosophie.

Zweitens: Im Cyberkrieg gibt es keine Armeen, die sich gegenüberstehen, und keine Soldaten in Uniform. Stattdessen kommen etwa Viren, Würmer oder Trojaner verdeckt und häufig auf Umwegen zum Einsatz – also Software, die keine Uniform oder Staatsabzeichen trägt. Dabei lassen sich Datenspuren leicht manipulieren, verdecken oder anderen in die Schuhe schieben – um etwa unter falscher Flagge Konflikte zu schüren oder Kriegsgründe zu fingieren. So ist nicht nur schwer herauszufinden, ob es sich bei IT-Angriffen um zivil-kriminelle und wirtschaftliche, oder um geheimdienstliche und militärische Operationen handelt. Der angegriffene Staat hat außerdem das Problem, die wahren Urheber zweifelsfrei zu identifizieren, um überhaupt rechtmäßig, angemessen und zielgenau reagieren zu können. Die Beweisführung ist in aller Regel äußerst schwierig. Der Internationale Gerichtshof verlangt jedoch eine klare Beweislage, denn es gibt kein Recht auf militärische Selbstverteidigung ins Blaue hinein oder aufgrund bloßer Indizien; ein Gegenschlag ohne klar identifizierbaren Aggressor ist jedenfalls völkerrechtswidrig.

Und drittens: Diese Probleme werden noch verschärft durch eine gefährliche Rechtsauslegung im „Tallinn Manual" – einem NATO-Handbuch zur Anwendung des Völkerrechts auf die Cyberkriegsführung (2013). Zwanzig zumeist militärnahe Rechtsexperten aus NATO-Staaten, auch aus Deutschland, haben diesen Leitfaden erarbeitet. An den darin aufgelisteten 95 Regeln sollen sich alle NATO-Staaten im Fall eines Cyberkriegs orientieren – auch die Bundeswehr. Was aber ist daran so gefährlich? Drei Beispiele:

- Danach gelten selbst solche Operationen als Cyberwar-Angriffe, die bloße wirtschaftlich-finanzielle Schäden eines betroffenen Staates verursachen, wenn diese gewisse Ausmaße annehmen, etwa einen Börsencrash. Dagegen wäre dann eine militärische, auch konventionelle Selbstverteidigung mit Kriegswaffen rechtens, so der Leitfaden, was zu einer unkontrollierbaren Eskalation der Auseinandersetzungen führen könnte.

- Laut Handbuch gelten zivile Hacker („Hacktivists“) als aktive Kriegsteilnehmer, wenn sie Cyber-Aktionen im Verlauf kriegerischer Konflikte ausführen. Solche Zivilisten können daher militärisch angegriffen und auch getötet werden. Selbst das Suchen und Offenlegen von Schwachstellen in Computersystemen des Gegners gilt demnach als kriegerische Handlung. Auf diese Weise wird die Kampfzone praktisch auf Privatpersonen und deren Laptops ausgeweitet.

- Das NATO-Tallinn-Manual sieht zudem vor, dass ein Staat sein Recht auf Selbstverteidigung auch präventiv ausüben darf – bevor überhaupt ein digitaler Angriff stattgefunden hat. Auch hier, wie bei konventionellen Militär-Erstschlägen, besteht hohe Missbrauchs- oder Missinterpretationsgefahr.

Mit der Rechtsauslegung in diesem NATO-Dokument werden die hohen völkerrechtlichen Eingriffsschwellen für bewaffnete Gewaltanwendungen zwischen Staaten unverantwortlich weit herabgesenkt sowie die restriktiven Kriterien des Selbstverteidigungsrechts aufgeweicht. Das gefährdet die Zivilbevölkerungen und die internationale Sicherheit in erheblichem Maße. Was einflussreiche, zumeist militärnahe Völkerrechtler da an Regeln für die NATO zusammengestellt haben, ist geeignet, die Grenzen zwischen innerer und äußerer Sicherheit, zwischen Zivilem und Militärischem, zwischen Krieg und Frieden, zwischen Angriff und Defensive zu verwischen – und eine schwere Datenattacke blitzartig in einen echten Krieg mit Raketen, Bomben und Granaten eskalieren zu lassen.

All dies bedeutet: Mit der Aufrüstung der Bundeswehr zum Cyberkrieg steigen Eskalationspotentiale, Kriegsbereitschaft und Kriegsgefahr – und davor schützt auch die obligatorische Zustimmung des Bundestags zu Militäreinsätzen im Einzelfall nur bedingt. Denn das Cyber-Konzept der Verteidigungsministerin für die Bundeswehr ist letztlich demokratisch kaum zu kontrollieren. Wobei die längst zur Interventionsarmee umgebaute Truppe ohnehin schwer kontrollierbar und skandalträchtig ist.

Wir vergeben unsere Negativpreise zwar für böse Pläne und Taten, aber wir geben unsere Preisträger.innen nicht verloren und verleihen den Preis gerne auch auf Bewährung. Voraussetzung dafür wäre, dass Sie, Frau Verteidigungsministerin, von der digitalen Aufrüstung abrücken, auf offensive Cyberwaffen für die Bundeswehr verzichten und eine ausschließlich defensive Cybersicherheitsstrategie verfolgen, um die Zivilbevölkerung effektiv zu schützen – flankiert von vertrauensbildenden Maßnahmen im Rahmen einer friedensorientierten Außenpolitik und Diplomatie (Stichwort: „Cyberpeace“). Wir fordern darüber hinaus eine weltweite Cyberabrüstung sowie eine völkerrechtliche Ächtung von Cyberspionage und Cyberwaffen. Und wir fordern die Schaffung einer unabhängigen Instanz der UN zur Untersuchung zwischenstaatlicher Cyberattacken und deren angemessener Abwehr.

Doch Sie, Frau von der Leyen, haben offenbar anderes zu tun. Sie suchen stattdessen, so wörtlich, „händeringend Nerds“: „Hacker, IT-Programmierer, IT-Sicherheitsfachleute, Penetrationstester, Systemadministratoren oder IT-Entwickler“. Der Bedarf der Bundeswehr liege bei rund 800 IT-Administratoren und 700 IT-Soldaten, also Cyberkämpferinnen und -kämpfern pro Jahr. Flächendeckend und großflächig wirbt die Bundeswehr auf Bahnhöfen, in Unis und Medien um Fachpersonal und Quereinsteiger für den Waffendienst am PC; auch zivile Experten aus Wirtschaft, Verbänden und NGOs werden für eine schlagkräftige „Cyber-Reserve“ geworben. In Anlehnung an den Kriegsslogan Ihres Vorvorgängers Peter Struck – „Die Sicherheit der Bundesrepublik Deutschland wird auch am Hindukusch verteidigt“ – werben Sie nun mit dem Sinnspruch: „Deutschlands Freiheit wird auch im Cyberraum verteidigt. Mach, was wirklich zählt…“. Das klingt spannend und womöglich auch verlockend.

Ob Sie, Frau Ministerin und ihre Werberkolonnen schon mal beim Chaos Computer Club oder bei Digitalcourage vorbeigeschaut haben? Auch heute hier im Saal sitzen wohl reihenweise technikaffine und -kundige Menschen, die genau in Ihr Beuteschema passen. Darum hoffen wir sehr, dass diese Laudatio und unsere Preisvergabe solche Menschen dazu ermutigen, ihre Fähigkeiten für Frieden und Verständigung im Internet einzusetzen, statt für digitale Angriffe und Cyberkrieg auf dem „Schlachtfeld der Zukunft“!

Herzlichen Glückwunsch zum Negativpreis BigBrotherAward 2017, Frau Bundesverteidigungsministerin und Oberbefehlshaberin der Bundeswehr.

Referenzen (Auswahl)

http://www.spiegel.de/politik/deutschland/bundesregierung-stellt-weissbuch-zur-sicherheitspolitik-vor-a-1102759.html

https://netzpolitik.org/2016/weissbuch-zur-sicherheitspolitik-bundeswehr-geht-in-die-cyberoffensive/

https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/

https://www.heise.de/newsticker/meldung/Bundeswehr-Weissbuch-Planspiele-fuer-den-Krieg-im-Cyberraum-3270870.html

Anmerkungen

1 *https://www.heise.de/newsticker/meldung/Ueber-47-Millionen-IT-Angriffe-auf-die-Bundeswehr-im-Jahr-2016-3595632.html*

2 *Quelle z. B. Robin Geiß, Völkerrecht im „Cyberwar“, http://www.ipg-journal.de/schwerpunkt-des-monats/neue-high-tech-kriege/artikel/detail/voelkerrecht-im-cyberwar-859/*

3 *Oberstleutnant Matthias Mielimonka, http://www.zebis.eu/veranstaltungen/archiv/podiumsdiskussion-cyberwar-die-digitale-front/*

Peter Wedde

Kategorie *Arbeit* – Laudatio

Der BigBrotherAward 2017 in der Kategorie Arbeit geht an die PLT – Planung für Logistik & Transport GmbH,

weil sie mit dem PLT Personal-Tracker ein Gerät anbietet, das eine „minutengenaue" und „unterbrechungsfreie Spurenverfolgung" von Außendienstmitarbeiterinnen und -mitarbeitern ermöglicht. Dies führt zu einer lückenlosen Totalkontrolle der Beschäftigten, die dieses Gerät bei sich tragen müssen.

Der Tracker ist nur wenige Zentimeter groß, enthält einen GPS-Empfänger, ein GSM/GPRS-Modem, einen leistungsfähigen Akku und einen internen Datenspeicher, damit die Tourdaten von Beschäftigten auch dann abrufbar sind, wenn das Mobilfunknetz ausfällt.

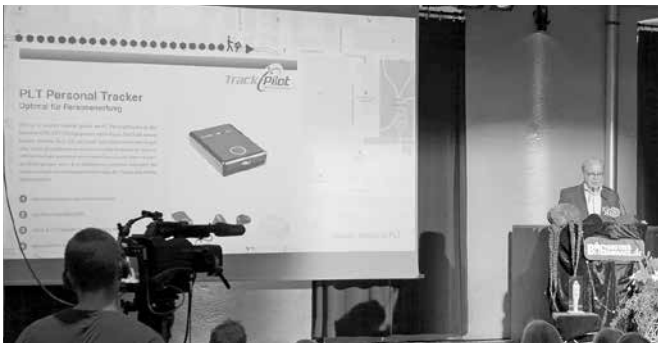
Besonders komfortabel ist die Echtzeit-Ortung, wenn die von PLT ebenfalls angebotene Begleitsoftware „TrackPilot" verwendet wird. Mit dem im „TrackPilot" integrierten „sehr genauen Kartenmaterial" können sich Arbeitgeber beispielsweise die von Beschäftigten absolvierte Strecke „exakt" anzeigen lassen. Den Anwendern werden nach Aussage von PLT auf diesem Weg neben „exakten Fahrtenbüchern und Arbeitszeitberichten zahlreiche Auswertungen und Statistiken geliefert, um Personal und Fuhrpark wirkungsvoll zu steuern". Mit wenigen Klicks können hier verschiedene Berichte generiert und auf Wunsch exportiert werden. Durch das versprochene „metergenaue Tracking" kann dabei beispielsweise erkannt werden, in welchem Tempo sich Zeitungsausträger oder Zusteller bewegen, wie lange sie an einer Haustür oder in einem Büro verweilen oder wann sie eine Pause machen.

Die Firma PLT erhält den BBA 2017 stellvertretend für alle Anbieter dieser Art von Überwachungstechnik, die ohne Rücksicht auf die Rechte von Beschäftigten eingesetzt wird. Unsere Preisverleihung soll diesen Trend stoppen.

PLT hat den BigBrotherAward besonders verdient, weil diese Firma in ihrer Werbung gesetzliche Vorschriften verfälscht, um den Einsatz von Personal-Trackern nicht nur als gesetzeskonform, sondern quasi als gesetzlich erforderlich darzustellen. So behauptet PLT auf seiner Website:

> *„Insbesondere das neue Mindestlohngesetz (MiLoG), welches am 01.01.2015 in Kraft trat, macht es in vielen Branchen notwendig, die Arbeitszeiten der Mitarbeiter zu überwachen und minutengenau zu dokumentieren, damit später bewiesen werden kann, dass auch tatsächlich der Mindestlohn i.H.v. 8,50 Euro gezahlt wurde. Daraus erwächst in einigen Branchen ein immenser Mehraufwand, nur um die Einhaltung des Gesetzes zu dokumentieren und den Nachweispflichten nachzukommen. Besonders hart betroffen sind vom Mindestlohn Zustelldienste und Zusteller der Zeitungslogistik und Brieflogistik. Die tatsächlichen Arbeitszeiten der Zeitungszusteller müssen aufgezeichnet und für Prüfungen des Zoll mindestens 10 Jahre vorgehalten werden."*

Diese Werbeaussage ist eine echte „Fake News": Richtig ist hieran eigentlich nur die Information, dass das Mindestlohngesetz (MiLoG) Arbeitgebern mit Wirkung vom 1. Januar 2015 bestimmte Nachweispflichten auferlegt. Nach § 17 Abs. 1 dieses Gesetzes sind sie verpflichtet,



Laudator Peter Wedde – Foto: Justus Holzberger CC BY-SA 4.0

> *„Beginn, Ende und Dauer der täglichen Arbeitszeit dieser Arbeitnehmerinnen und Arbeitnehmer spätestens bis zum Ablauf des siebten auf den Tag der Arbeitsleistung folgenden Kalendertages aufzuzeichnen und diese Aufzeichnungen mindestens zwei Jahre beginnend ab dem für die Aufzeichnung maßgeblichen Zeitpunkt aufzubewahren".*

Dazu reicht es, wenn die Beschäftigten einen Stundenzettel ausfüllen, wie sie es seit Jahrzehnten tun. Von einer Verpflichtung zur „minutengenauen" Überwachung der Arbeitszeit ist hingegen im MiLoG ebenso wenig die Rede wie von einem Recht der Arbeitgeber, den genauen Standort von Beschäftigten permanent zu erfassen. Auch eine angebliche „zehnjährige Aufbewahrungspflicht" gibt es schlicht nicht, auch nicht „für den Zoll". Was die Firma PLT da auf ihrer Website schreibt, ist damit eine plumpe Verfälschung der gesetzlichen Situation.

Die vollmundigen Werbeaussagen auf der PLT-Website ändern aber nichts an der eindeutigen arbeits- und datenschutzrechtlichen Situation, nach der eine permanente und metergenaue elektronische Totalüberwachung des Standorts und der Bewegungen von Beschäftigten in den allermeisten Fällen verboten ist. Datenschutzrechtlich zulässig ist eine exakte Online-Ortung von Menschen nur in wenigen Ausnahmen, etwa für Besatzungen von vollgepackten Geldtransportern oder für Berufsfeuerwehrleute während des Einsatzes in einem brennenden Haus. Für „normale" Beschäftigte wie etwa für Auslieferungsfahrer ist es völlig ausreichend, wenn ihr ungefährer Standort oder ihre ungefähre Ankunftszeit bei Kunden an die Zentrale übermittelt wird.

Das minuten- und metergenaue Tracking, dass der PLT Personal-Tracker verspricht, trifft damit auf leicht erkennbare und eindeutige rechtliche Grenzen. Für die Branchen, die PLT auf seiner Website nennt,

„Winterdienst (Handtouren), Wachdienst, Objektschutz, Gebietsbestreifung, Agrar- und Forstbetrieb, Sportveranstaltungen oder Zustelldienst, Zusteller der Zeitungslogistik und Brieflogistik“,

gibt es keine gesetzliche Erlaubnis. Deshalb ist der Einsatz von Personal-Trackern in derartigen Fällen arbeitsrechtlich und datenschutzrechtlich unzulässig.

Umso erstaunlicher ist es, dass der Personal-Tracker laut der Website von PLT bereits vielfach „legal“ eingesetzt werden soll:

„Bereits etliche Zustelldienste haben Ihre Zusteller mit dem PLT Personal Tracker ausgestattet und eine entsprechende interne Betriebsvereinbarung getroffen. Danach werden die zurückgelegten Zustelltouren der Zeitungsausträger metergenau getrackt und im TrackPilot Ortungssystem zu übersichtlichen Arbeitszeitberichten verarbeitet. Die Berichte können in Dateiform gespeichert und dauerhaft archiviert werden.“

Der Hinweis auf Betriebsvereinbarungen, durch die ein metergenaues persönliches Tracking von Zustellern erlaubt wird, hat uns verblüfft. Das würde ja bedeuten, dass Betriebsräte einer Form der Totalüberwachung zugestimmt hätten, die nach der Rechtsprechung des Bundesverfassungsgerichts und des Bundesarbeitsgerichts in Arbeitsverhältnissen unzulässig ist.

Deshalb haben wir uns die auf der PLT-Website hinterlegten „Betriebsvereinbarungen“ genauer angesehen. Erwartet hätten wir hier eine Referenzliste mit Formulierungsbeispielen aus bereits abgeschlossenen Betriebsvereinbarungen. Stattdessen finden sich hier aber nur allgemeine Hinweise auf deren mögliche Regelungsinhalte sowie auf rechtliche Probleme. Auch dieser Teil der PLT-Präsentation ist wiederum eine geschickte Marketingaussage, die vorgaukelt, dass rechtlich alles in Ordnung ist.

Seltsam mutet auch die folgende Formulierung an:

„Durch die extrem kleinen Abmaße lässt sich das Gerät sehr leicht am Körper tragen oder versteckt positionieren und passt in jede Hosentasche.“

Wieso weist die Firma PLT darauf hin, dass es möglich ist, den Personal-Tracker etwa auch versteckt in einem Auslieferungswagen oder in einer Tragetasche unterzubringen? Die Ortung könnte dann ohne Wissen der Beschäftigten erfolgen. Dies aber wäre nach geltender Rechtslage definitiv unzulässig.

Der Einsatz von Personal-Trackern zur Totalkontrolle von Beschäftigten – sei es das Gerät von PLT oder auch von einer anderen Firma – ist menschenunwürdig, rechtswidrig und sinnlos. Diese Geräte sind genau wie durch Videokameras „totalüberwachte“ Arbeitsplätze Ausdruck des überbordenden Kontrollwahns und des übertriebenen Misstrauens von Arbeitgebern, die meinen, jeden Meter und jede Minute der Arbeit ihrer Beschäftigten überwachen und erfassen zu müssen.

Hinzu kommt: Es gibt weder die von PLT behauptete gesetzliche Erfordernis, noch beinhaltet etwa die meter- und minutengenaue Erfassung eines Briefträgers ein nennenswertes Einsparpotenzial für die Unternehmen. Ganz im Gegenteil: Derartige Kontrollen kosten zunächst einmal Geld. Firmen wie PLT verdienen am Kontrollwahn von Arbeitgebern und an der absurden, aber weit verbreiteten Logik „Überwachung gleich Sicherheit“. Die angebotene Überwachungstechnologie wird auf Kosten der Persönlichkeitsrechte der Arbeitnehmerinnen und Arbeitnehmer vermarktet.

Hoffentlich können wir mit diesem BigBrotherAward einige Firmenchefs und -chefinnen davor bewahren, auf diese Propaganda hereinzufallen. Probieren Sie es doch einmal anders: Vermitteln Sie Ihren Beschäftigten Vertrauen und Wertschätzung. Optimieren Sie mit ihnen zusammen Routenführungen und entwickeln sie mögliche Effizienz-Steigerungen gemeinsam. Nehmen Sie ernst, dass diese Menschen ihre Touren und Arbeitsabläufe am besten kennen. Das wirkt sich mit Sicherheit positiv auf die Arbeitsmotivation aus – und steigert das Arbeitstempo vielleicht ganz ohne Zusatzkosten.

Herzlichen Glückwunsch zum BigBrotherAward 2017, Firma PLT – Planung für Logistik & Transport GmbH.

padeluun

Kategorie *Verbraucherschutz* – Laudatio

Der BigBrotherAward in der Kategorie Verbraucherschutz geht an Jens Scholz, Vorstand der prudsys AG, Chemnitz,

für Ihre Software zur Preisdiskriminierung, also für Beihilfe zur Preistreiberei und Verbreitung sozialen Unfriedens.

Wissenschaft – und das gilt auch für die Disziplinen Mathematik und Informatik – ist etwas Feines. Man forscht, gewinnt Erkenntnisse und setzt diese dann – zum Beispiel mittels Ausgründung aus der Universität – zum Besten für die Menschheit um.

Unser Preisträger, die prudsys AG, ist eine Ausgründung der TU Chemnitz. Sie beschäftigt sich mit Data Mining. Sie veranstaltet schon so lange, wie wir die BigBrotherAwards veranstalten – seit dem Jahr 2000 – den „Data Mining Cup“, wo sich die Besten der Besten einen Wettbewerb liefern, um aus riesigen Kübeln voll mit Big Data das eine oder andere Daten-Nugget herauszufischen. Mit solchen Fähigkeiten könne man – so wird erzählt – unbekannte Krankheiten heilen und das Hungerproblem der Welt lösen.

Die prudsys AG, so scheint es, hat an diesen guten Zielen wenig Interesse. Ihr Businessmodell bietet etwas anderes an: „Preisdiskrimi-

nierung". Und das ist uns bei den BigBrotherAwards schon im Jahr 2000 begegnet, als wir die Firma Payback für ihre Kundenkarten mit einem unserer hübschen, aber unbegehrten Awards beehrten.

Die prudsys AG entwickelt Algorithmen und Strategien, die es Händlern ermöglichen, für ein- und dasselbe Produkt, sei es Apfel, Milch oder Digitalkamera, online und offline den höchstmöglichen Preis zu verlangen, der eben noch möglich ist, ohne dass Sie als Kundin oder Kunde abspringen. Also ist nicht mehr der Wert einer Ware ausschlaggebend für die Preisgestaltung, sondern Sie sind es. Sie und ich. Die Händlerin oder der Händler müssen genug über uns wissen, um herauszufinden, welchen größtmöglichen Preis wir zu zahlen bereit sind. Im Marketing-Jargon heißt das: „Preisakzeptanzschwellen explorativ dynamisch austesten"[1]. Das klingt vielleicht absurd – ist aber so.

padeluun bei seiner Laudatio – Foto: Justus Holzberger CC BY-SA 4.0

Nehmen wir an, Sie sind alleinerziehender Vater, müssen nach der Arbeit schnell in die Kita hasten, um Ihre Tochter abzuholen und husch husch, bevor Sie das Abendessen bereiten, noch einkaufen. Dann, denke ich, werden Sie nicht drei Läden besuchen, Preise vergleichen und günstiger einkaufen. Sie werden in das Geschäft laufen, das auf dem Weg oder kleinsten Umweg liegt und in den Korb werfen, was so auf dem Einkaufszettel steht. Wenn dieser Laden nicht „Dauertiefpreise statt Sonderangebote" garantiert, dann werden Sie sicher mehr bezahlt haben, als jemand, der mehr Zeit hat.

„Ha!", werden Sie jetzt vielleicht antworten. „Ich habe meine Kundenkarte. Da bekomme ich als treuer Kunde alles etwas günstiger." Doppel-HA! Antworte ich. Jetzt haben Sie erst recht verloren! Denn jetzt weiß der Händler, was Sie so einkaufen – und wann – und wie viel Sie im Durchschnitt pro Einkauf ausgeben – und ob Sie bar zahlen oder mit Karte. Er kann abschätzen, wie groß Ihr Haushalt ist, und kann Sie ganz gezielt mit Rabattcoupons dahin steuern, wohin er sie haben möchte. Weg von den Artikeln, an denen der Händler wenig verdient, hin zu den lukrativeren Artikeln. Er kann abschätzen, wie viele Kunden zukünftig wegbleiben, und ob es sich trotzdem lohnt, wenn er die 2-Kilo-Packung Spaghetti aus dem Angebot nimmt und stattdessen ausschließlich die 250-Gramm-Packungen – die leider etwas teurer sind – ins Regal legt.

Und das entscheidet nicht der freundliche Marktleiter, sondern die Zentrale. Die kann das nämlich viel besser entscheiden als der Mensch vor Ort – denn die Zentrale bündelt die Daten, wertet sie aus, rechnet das Wetter, Saisonzeiten, Wochen- oder Tageszeiten dazu, oder ob die Konkurrenz gerade eine Promotionaktion fährt (kein Witz!) und schon ändert sich das elektronische Preisschild am Regal.

Denn die Zentrale hat guten Rat: Die Entscheidungssysteme sind mit der Software „Realtime Decision Engine", kurz RDE, der Firma prudsys verbunden. Die Selbstbeschreibung:

> *„Die prudsys RDE ist als erstes Dynamic-Pricing-Tool in der Lage, die bestmögliche Preisfindung in Echtzeit vorzunehmen. Durch den Einsatz der prudsys RDE werden tausende Produktpreise vollautomatisiert an das Kundenverhalten sowie sich ständig ändernde Markt- und Unternehmenssituationen angepasst.*
>
> *Durch die Kombination von personalisierten Produktempfehlungen und individuellen Preisvorteilen werden Kunden durch Rabatte auf für sie relevante Produkte belohnt. Als Umsetzungsmedium für personalisiertes Pricing eignen sich besonders vollautomatisch erzeugte und personalisierte Coupons in Kunden-Newslettern, in Mailings und in mobilen Apps. Individuelle Rabatte können zudem im Zuge des Check-out-Couponings [Anmerkung des Laudators: das sind diese Zusätze, die Ihren Kassenzettel neuerdings immer so lang machen], via Kundenkarten oder auf Instore-Kiosksysteme ausgespielt werden."*

Was die prudsys AG hier schreibt, ist schon eine Nummer härter, als dass die selben DVDs beim Marktkauf in Rahden (ein eher ärmerer Ort) grundsätzlich 30 % teurer sind als beim Marktkauf in Lübbecke, wo eher reichere Leute wohnen.

Und wenn das schon im Einzelhandel an der Straße funktioniert, wie gut funktioniert das erst in Online-Shops? Hier – meint einer der prudsys-Chefs im Interview – kommen die Händler an der Preisdiskriminierung (die natürlich nicht Preisdiskriminierung heißt, sondern „Dynamic Pricing" genannt wird) im Zeitalter von Amazon & Co gar nicht vorbei: Online-Shops würden ohne Dynamic Pricing bald schlicht nichts mehr verkaufen.

Was können wir tun? Hier sind ein paar praktische Tipps: Wenn Sie eine Reise buchen wollen, nehmen Sie lieber einen Windows-Rechner statt eines Macs. Sonst wird's gleich teurer. Sie wollen vom Handy buchen? Ganz schlechte Idee – das wird meist richtig teuer, aber wenn, dann besser nicht vom iPhone aus, sondern lieber mit einem Smartphone mit dem Betriebssystem Android.

Das ist noch eine recht grobe Art der Differenzierung. Die prudsys AG hat bessere Algorithmen, die viel feinziselierter Daten zusammenraffen, die von den meisten Menschen als „sind doch eh nicht wichtig" fahrlässig abgegeben wurden. Jeder Kaffee, den Sie kaufen, kann gegen Sie verwendet werden! Wenn Sie im Web einkaufen, sehen Sie die Oberfläche, die ein Designer im Auftrag des Händlers programmiert hat. Ihr Nachbar sieht eine andere. Ihre Kollegin ebenfalls. Und das Wort „Oberfläche" trifft es genau. Sie sehen nur eine winzig kleine Spitze Ihres Wahl- und Einkaufvorgangs. Unter der Oberfläche aber werden Daten geschaufelt, Berechnungen angestellt, geschachert und alles mit dem einen Ziel: Sie abzuzocken. Bei jedem Kauf im Netz müssen Sie sich vorstellen, dass unter der Oberfläche ein leises Kichern und ein zufriedenes Händereiben zu hören ist.

Das ist eine giergetriebene Welt. In dieser Welt existieren keine Menschen, keine Einzelprodukte, keine Zufriedenheit, kein Service – hier gibt es nur eins: Zahlen. Einsen und Nullen und am Ende ma-

nifestieren sich diese zu einem dicken fetten Plus an Euro und Dollar. Die prudsys AG sagt, dass jeden Tag eine Milliarde Entscheidungen mit ihren Algorithmen getroffen werden – 8 Milliarden Dollar Handelsvolumen jährlich werden mit diesen Algorithmen erwirtschaftet. Selbst wenn Sie schon gelernt haben, dass man Begriffe wie „Premiumkunde", „Rabatt" und allein schon die Floskel „Sparen Sie …" meiden sollte, wie der Teufel das Weihwasser: Es gibt quasi kein Entkommen. Selbst wenn Sie, wie die junge Frau, die ein Hotelzimmer in Brüssel buchen wollte, dieses 17-mal stornieren, um am Ende 1,38 Euro weniger zu bezahlen. Die Welt wird nicht zu einem lustigen gigantischen orientalischen Basar. Sie als Kundin haben es nicht mehr mit einer Wochenmarkthändlerin zu tun, mit der Sie auf Augenhöhe um den Preis feilschen können. Hier feilscht nur einer, denn der Händler weiß alles über seine Kunden, die Kunden nichts über die Händler. Es besteht keine Augenhöhe, kein Frieden, sondern ein immerwährender Quell für das böse Gefühl, stets zu kurz zu kommen. Und das zu Recht.

Mit Data Mining, liebe prudsys AG, mit Euren Fähigkeiten könnte man vielleicht unbekannte Krankheiten heilen und das Hungerproblem der Welt lösen. Ihr habt Euch leider für die dunkle Seite der Macht entschieden: Die Gier.

Ihr habt schon ein paar Awards bekommen: Den „Top 100", den „Innovationspreis-IT", den „Top Produkt Handel", den „Chemnitzer Meilenstein" … und jetzt auch noch den „TopBigBrotherAward 2017". Herzlichen Glückwunsch, Jens Scholz von der prudsys AG.

Anmerkung

1 *http://etailment.de/news/stories/Dynamic-Pricing--banane-4329*

Wissenschaft & Frieden 3/2017 „Ressourcen des Friedens"

Die August-Ausgabe von *Wissenschaft und Frieden* fragt nach Dingen, Personen, Systemen und Gegebenheiten, die dem Frieden zuträglich sind, ihn unterstützen, ermöglichen und nähren. W&F beleuchtet, wie und unter welchen Umständen Ressourcen nicht zum Fluch, sondern zum Segen für den Frieden werden können. Dabei wird der Ressourcenbegriff ausgeweitet und nicht auf materielle Ressourcen reduziert, sondern schließt exemplarisch Handel, Völkerrecht, Medien, Religion, Glück, Kunst und Versöhnung ein.

Im einzelnen schreiben:

- *Michael Brzoska*: Rohstoffe, Konflikte und Governance
- *Nina Engwich*: Rohstoffe als Mittel zum Friedensaufbau? Environmental Peacebuilding in Sierra Leone
- *Maximilian Mayer* und *Gregor Grossman*: Chinas neue Seidenstraße – bringt Handel Frieden?
- *Luis Roberto Zamora Bolaños*: Wenn Abrüstung genau das Richtige ist – die Friedensverfassung von Costa Rica
- *Vladimir Bratic*: Neue Medien als Friedensressource?
- *Michael A. Schmiedel*: Religionen als Friedensressource – es kommt darauf an
- *Jochen Dallmer*: Glück als Ressource für Frieden
- *Hannah Reich*: Theaterräume und die Kunst des Sehens – Friedensressource Kultur
- *Nurit Shnabel* und *Johannes Ullrich*: Wie versöhnen wir uns? Das bedürfnisbasierte Modell

Die Artikel außerhalb des Schwerpunkts befassen sich mit den Folgen von Militarismus am Beispiel Türkei (*Serdar M. Değirmencioğlu*), mit der Kampagne gegen Friedenskräfte im israelisch-palästinensischen Konflikt (*Wilhelm Kempf*) und mit dem Anfang Juli 2017 bei den Vereinten Nationen verabschiedeten *Vertrag über das Verbot von Kernwaffen* (*Jürgen Scheffran*). Im Gastkommentar *Ausblick auf den Ausnahmezustand* beleuchtet *Peter Ullrich* die Ereignisse rund um den G20-Gipfel in Hamburg; die kommentierte Presseschau *Erdogans Reichtagsbrand* gibt einen Überblick über die Repressionen in der Türkei.

Ergänzt werden die Artikel wie immer durch Berichte von Tagungen und Kongressen, Rezensionen und Informationen aus Friedensforschung und Praxis.

Wissenschaft & Frieden 3/2017 „Ressourcen des Friedens"
9,00 € plus Porto.

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, Beringstr. 14, 53115 Bonn,
E-Mail: *buero-bonn@wissenschaft-und-frieden.de,*
www.wissenschaft-und-frieden.de

Rainer W. Gerling

Hackerangriff auf die Wahlfreiheit

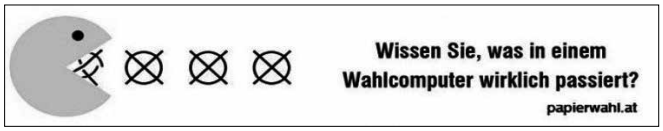
Politische Wahlen finden bei uns nach wie vor auf Papier statt. Eigentlich erstaunlich in Zeiten, in denen wir uns im Internet informieren und einkaufen, die Heizung daheim per App steuern und sogar der Personalausweis eine Online-Funktion hat. Wäre es nicht viel einfacher und bequemer, am heimischen PC oder via Smartphone die Bundestagsabgeordneten zu voten?
Lieber nicht. Auch ohne Internetwahlen drohen viele Manipulationsmöglichkeiten auf elektronischem Wege.

Um es gleich vorwegzunehmen: Politische Wahlen im Internet wird es in absehbarer Zeit zumindest in Deutschland nicht geben. Und das ist gut so. Sicher wäre das Wählen im Internet einfach und komfortabel, vielleicht würden sogar mehr Bürger online ihre Stimme abgeben – trotzdem mag man sich einen Wahlvorgang komplett im Internet für politische Wahlen lieber nicht vorstellen. Ein Angriff auf die Computer der Wähler könnte von jedem Ort der Welt vorgenommen werden, Manipulationen von den verschiedensten Seiten wären Tür und Tor geöffnet. *Ronald L. Rivest* hat dafür ein treffendes Bild geprägt: Im Jahr 2016 beantwortete er in einem Vortrag die Frage nach den Best Practices für eine Internetwahl mit der Gegenfrage nach den Best Practices für das Spielen auf einer verkehrsreichen Straße.[1]

Wahlen müssen geheim, frei und sicher sein. Geheim heißt, dass niemand mitbekommt, wie eine Wählerin oder ein Wähler abstimmt. Damit eine Wahl wirklich frei ist, dürfen Wähler auch keinen Beleg für eine konkrete Stimmabgabe erhalten. Ein Handyfoto aus der Wahlkabine, um die eigene Stimmabgabe zu dokumentieren, ist keine gute Idee. Es muss sichergestellt werden, dass eine Stimme für eine bestimmte Kandidatin oder einen bestimmten Kandidaten nicht erpresst oder gekauft werden kann. Sicher bedeutet, dass die Stimmen unmanipuliert ausgezählt werden können. Und da kommen schon bei Wahlmaschinen, wie sie in den USA weitverbreitet sind, gewisse Zweifel auf.

Die Stimmabgabe auf Papier findet nur noch in 18 US-Bundesstaaten statt

In den Vereinigten Staaten setzen nur noch 18 der 50 Staaten auf eine ausschließlich papierbasierte Stimmabgabe. Zehn Staaten verwenden zumindest teilweise Wahlmaschinen ohne Kontrollausdrucke auf Papier (zum potenziellen manuellen Nachzählen). Bei diesen Geräten ist eine nachträgliche Kontrolle der digitalen Stimmauszählung kaum möglich. Und selbst wenn die Wähler zur Kontrolle einen Papierbeleg erhalten, den sie in eine Wahlurne legen – für Laien ist dann auch weiterhin nicht nachvollziehbar, ob die Maschine die identische Stimmabgabe speichert.



Wir danken papierwahl.at für die Druckgenehmigung.

Grundsätzlich ist Misstrauen gegenüber Wahlmaschinen angebracht: So gab es in der Vergangenheit Probleme mit der Software der Geräte. Im Jahr 2008 wurde etwa bekannt, dass Wahlcomputer der Firma *Premier Election Solutions* beim Zusammenführen von Ergebnissen mehrerer Wahlcomputer einen Teil der Stimmen „vergaßen". Da ein erneuter Zulassungsprozess Jahre dauert, veröffentlichte die Firma einen *Workaround* in Form einer geänderten Bedienungsanleitung. Die Fehlbedienung wird nicht technisch verhindert, vielmehr wird dem Anwender nur gezeigt, wie er sie vermeidet. So werden Fehler nicht ausgeschlossen.

Auch die Sicherheitssysteme von Wahlmaschinen sind äußerst zweifelhaft. Der Experte *Jeremy Epstein* schreibt in seinem Blog-Beitrag *Decertifying the worst voting machine in the US* des *Princeton Center for Information Technology Policy* über unglaubliche Sicherheitslücken bei Wahlcomputern.[2] So wird beispielsweise für die WEP-Verschlüsselung im WLAN der Code „abcde" verwendet. Dieser Schlüssel ist *fest verdrahtet* und nicht änderbar. Einige Systeme haben seit 2004 keine Sicherheits-Patches erhalten. USB-Ports und andere physische Zugänge sind nicht immer abgesichert. Wer ein USB-Gerät in einen ungesicherten USB-Port stecken kann, kann wahrscheinlich Manipulationen vornehmen. *Bruce Schneier,* ein international anerkannter US-amerikanischer IT-Sicherheitsexperte, berichtete, Wahlcomputer hätten die Default-Passworte „abcde" oder „admin" gehabt.[3] Da Wahlcomputer durchaus auch WLAN zur Kommunikation benutzen, ist ein Einbruch selbst aus einiger Distanz denkbar.

Manipulierte Software bringt den Wahlcomputer zum Schachspielen

Im Jahr 2007 demonstrierten niederländische und deutsche Hacker, dass man einem *Nedap*-Wahlcomputer durch Verändern der Software das Schachspielen beibringen kann.[4] Damit zeigten sie, dass beliebige Veränderungen der Software unbefugt möglich sind. Es ist sicher ein großer Aufwand, Wahlmaschinen zu hacken. Aber die im Erfolgsfall großen Auswirkungen rechtfertigen aus Sicht des Angreifers durchaus den Aufwand. Dazu kommt: Während etwa Unternehmen ein starkes eigenes Interesse daran haben, dass ihre Computersysteme sicher sind, und Sicherheitssysteme wie eine Firewall haben, um sich gegen Angriffe von außen zu schützen, ist bei Wahlmaschinen auch der Betreiber ein möglicher Angreifer. So kann der Betreiber, ohne sich verdächtig zu machen, flächendeckend Updates in die Wahlmaschinen einbringen. Eine Überprüfung durch Wählerinnen und Wähler oder auch Wahlhelfer vor Ort ist nicht möglich. Das Gerät auch vor potenziellen Manipulationen durch den Betreiber zu schützen, ist eine weit größere Herausforderung.

Wahlcomputer technisch komplett abzuschotten, ist keine Option, da zumindest die aktuellen Stimmzettel vor der Wahl eingespielt werden müssen. Dies geschieht in der Regel durch das Einstecken von Speicherkarten, die häufig auf Windows-Rechnern beschrieben werden. Die gleichen Speicherkarten dienen auch dem Update der Software: Ist eine Datei mit einem be-

stimmten Namen vorhanden, sieht das Gerät den Inhalt der Datei als Software-Update an und installiert sie. Jeder, der kurze Zeit Zugriff auf die Wahlmaschine hat, kann eine Speicherkarte einschieben und beliebige Software einspielen.

Die Sicherheit von Wahlmaschinen gilt mit Recht als zweifelhaft. Trotzdem sind flächendeckende Manipulationen eher unwahrscheinlich. Wenn Wahlcomputer gehackt werden, ist davon auszugehen, dass nicht pauschal alle Modelle davon betroffen sind, sondern nur einige. Auch bei normalen Computern erleben wir, dass ein Hack eines Windows-Rechners nicht unbedingt auf einem Apple- oder Linux-Rechner funktioniert. In den Vereinigten Staaten sind immerhin 53 unterschiedliche Wahlgeräte von 17 Herstellern im Einsatz.

Zudem gibt es bis jetzt keine Beweise für die Manipulation von Wahlcomputern. Eine Gruppe, zu der auch der Leiter des *Center for Computer Security and Society* der *University of Michigan, J. Alex Halderman,* gehört, hat zwar behauptet, dass *Hillary Clinton* in Wisconsin in Stimmbezirken mit Wahlcomputern etwa sieben Prozent weniger Stimmen erhielt als in Stimmbezirken mit Papierstimmzetteln.[5] Die Unterschiede lassen sich jedoch auch durch systematische Fehler oder durch zufällige Korrelationen zwischen dem Typus der Wahlmaschine und demografischen Faktoren erklären. Man kann also nur spekulieren, ob die Präsidentschaftswahlen in den USA manipuliert wurden. Ein fader Beigeschmack und ein ungutes Gefühl bleiben.

Auch in Deutschland wurden in der Vergangenheit bei verschiedenen Wahlen bereits Wahlcomputer verwendet. Zwei Beschwerden (2 BvC 3/07, 2 BvC 4/07) gegen „den Einsatz von rechnergesteuerten Wahlgeräten" führten dazu, dass 2009 die Bundeswahlgeräteverordnung vom Bundesverfassungsgericht für verfassungswidrig erklärt wurde, „weil sie nicht sicherstellt, dass nur solche Wahlgeräte zugelassen und verwendet werden, die den verfassungsrechtlichen Voraussetzungen des Grundsatzes der Öffentlichkeit genügen". Voraussetzung sei, „dass die wesentlichen Schritte der Wahlhandlung und der Ergebnisermittlung vom Bürger zuverlässig und ohne besondere Sachkenntnis überprüft werden können". Dies ist bei den derzeitigen Wahlcomputern nicht gewährleistet. So kamen seither in Deutschland keine Wahlcomputer mehr zum Einsatz.

Bleibt die Frage, welche Gründe überhaupt für die Geräte sprechen. Der einzige Vorteil ist, dass sie das Auszählen vereinfachen, schneller und billiger machen. Für die Wählerin oder den Wähler wird der Wahlvorgang dadurch nicht erleichtert. Wahlcomputer können lediglich ungültige Stimmzettel technisch verhindern. Eine ungültige Stimme abzugeben, kann aber auch eine bewusste Wahlentscheidung sein.

Es gibt also viele gute Gründe, die klassischen papierenen Stimmzettel bei politischen Wahlen beizubehalten. Nur wenn wir unser Kreuz mit einem normalen Stift auf normales Papier machen können, ist sichergestellt, dass die Auszählung zeitnah und öffentlich – unter Wahrung des Mehraugenprinzips – erfolgt. Auch während der Stimmabgabe ist das Mehraugenprinzip zur Beobachtung der Wahl sichergestellt.

Allerdings sind Wahlmaschinen wohl nicht dauerhaft aus deutschen Wahllokalen verbannt. Hersteller und Kommunen, die aufs Geld schauen, werden versuchen, wieder elektronische Systeme für die Stimmabgabe und -auszählung einzuführen. Wenn Wahlmaschinen eingesetzt werden, darf dies nicht geschehen mit dem Argument: „Vertrau uns, wir machen das schon richtig." Und das „wir" kann dabei sowohl den Hersteller der Wahlmaschinen als auch den Staat meinen. Die Grundeinstellung muss sein: „Es werden Pannen geschehen, wir müssen sie feststellen und korrigieren." Die Möglichkeiten zu einem Audit müssen in die elektronischen Wahlverfahren eingebaut sein, und ein Audit der Wahlergebnisse muss zwingend durchgeführt werden.

Bei der Bundestagswahl 2017 wird es keine manipulierten Wahlmaschinen geben, aber damit ist die Gefahr digitaler Manipulationen keineswegs gebannt: So müssen die Wahlergebnisse aus den Wahllokalen eingesammelt werden, was über digitale Netze geschieht. Der Bundeswahlleiter *Dieter Sarreither* rechnet mit Hackerangriffen und hat deshalb vorsorglich das verwendete Verwaltungsnetz besonders sichern lassen.[6] Notfalls kann auf Telefon- und Faxkommunikation zurückgegriffen werden. In den Niederlanden wurde bei der Wahl am 15. März 2017 mit der Hand ausgezählt, da die sonst verwendete Software als anfällig für Hacks gilt. Kuriere brachten die Ergebnisse aus den Wahllokalen in die regionalen Wahlbüros. Erst dort wurden dann Computer eingesetzt.[7]

Die Wahlen selbst können bei uns also als sicher gelten, aber es ist zu befürchten, dass Hacker versuchen, im Vorfeld Einfluss auf das Ergebnis zu nehmen. In den USA war das offensichtlich der Fall: Am 6. Januar 2017 veröffentlichten CIA, FBI und NSA einen gemeinsamen Bericht, dass russische Dienste die Präsidentschaftswahlen in den USA beeinflusst hätten.[8] Demnach wurde das Computernetz des *Democratic National Committee* im Juli 2015 gehackt. Bis Mai 2016 wurden im großen Stil Dokumente gestohlen. Später wurden diese Dokumente unter dem (möglicherweise russischen) Pseudonym *Guccifer 2.0* von *DC Leaks* und *Wikileaks* veröffentlicht. Da mit diesen Dokumenten im Wesentlichen die Demokraten und ihre Kandidatin Hillary Clinton diskreditiert werden sollten, kann dies als – zumindest versuchte – Wahlbeeinflussung gesehen werden. Die russische Regierung weist diesen Verdacht weit von sich. Öffentlich verfügbare Beweise, dass russische Dienste hinter den Vorgängen stecken, gibt es nicht.

Digitale Verbrecher hinterlassen Spuren, handfeste Beweise gibt es kaum

Aber es gibt mehr oder weniger starke Hinweise. Solche Indizien für digitale Vergehen lassen sich natürlich nicht so leicht dingfest machen wie Beweismittel in der realen Welt: Bei einem klassischen Tatort findet die Polizei Fingerabdrücke, Fasern und DNA-Spuren, die sie letztendlich einer oder mehreren Personen zuordnen kann. An einem digitalen Tatort finden Ermittler Schadsoftware und in der Analyse der Kommunikation etwa IP- oder E-Mail-Adressen. Diese Bits und Bytes jemandem zuzuordnen, ist jedoch wesentlich schwieriger als bei klassischen Indizien.

So suchen digitale Forensiker in der Schadsoftware beispielsweise nach russischen oder chinesischen Textfragmenten. Sie sind kein Beweis, da genauso gut Hacker aus einem anderen Land eine falsche Fährte gelegt haben können. Wenn der Fo-

rensiker Glück hat, ist die Schadsoftware eine Optimierung oder Weiterentwicklung einer bekannten Schadsoftware, von der man weiß, dass etwa russische oder chinesische staatliche Stellen sie schon lange einsetzen. Dann gibt es bereits zwei Indizien. Die ausspionierten Daten werden bei einem Server abgeliefert. Der steht irgendwo in Europa oder Amerika bei einem Provider. Hierzu mieten die Angreifer einfach Rechner bei Dienstleistern und melden Domains an. Wenn der Domainname jedoch über eine E-Mail-Adresse registriert wurde, die schon länger russischen oder chinesischen staatlichen Stellen zugeordnet werden konnte, hat man einen weiteren Hinweis in der Hand. Auch kann den Ermittlern etwa die spezielle Technik der Datenübertragung bereits länger bekannt sein, und sie können sie mit älteren Vorfällen vergleichen. Die genauen technischen Details dieser Analysen sind jedoch ein gut gehütetes Betriebsgeheimnis der ermittelnden Geheimdienste.

Ein weiteres Indiz kann die Interessenlage sein: Bei einem Angriff auf die IT-Infrastruktur des *Uigurischen Weltkongresses* ist die Wahrscheinlichkeit hoch, dass es sich um chinesische staatliche Stellen handelt, da der Uigurische Weltkongress zu den sogenannten *Fünf Giften,* den Hauptbedrohungen des chinesischen Staates, gehört. Wenn dagegen – wie am 23. Dezember 2016 – in der Westukraine ein großer Stromausfall für Probleme sorgt, der auf einen Cyberangriff zurückgeht, dann ist es höchst unwahrscheinlich, dass chinesische staatliche Stellen die Urheber waren. Hier spricht eher einiges für einen russischen Ursprung.

Umfangreiches gesammeltes Wissen bei Sicherheitsfirmen und -behörden vermag in der Gesamtschau ein plausibles Bild zu ergeben. Die endgültigen Erkenntnisse werden veröffentlicht, sie sind aber von außen nicht ohne Weiteres nachvollziehbar. Und klar ist auch: Ein plausibles Bild ist noch lange kein gerichtsfester Beweis. Parallel zu den Fällen in den Vereinigten Staaten stellt sich die Frage, ob die Bundestagswahl ähnlich gefährdet ist wie die US-amerikanische Präsidentschaftswahl. Zumindest gab es in den vergangenen 24 Monaten bereits mehrere Hackerangriffe auf deutsche Parteien und Regierungsstrukturen.

Angreifer könnten versuchen, vor der Bundestagswahl die öffentliche Meinung zu manipulieren

Im Frühjahr 2015 brachen Hacker in das *Parlakom*-Netz des Deutschen Bundestags ein und kopierten etwa 16 Gigabyte Daten. Deutsche Sicherheitsbehörden gehen davon aus, dass dafür eine staatsnahe russische Hackergruppe verantwortlich war, die unter anderem unter dem Namen *APT28* bekannt ist. Diese Gruppe ist seit etwa 2004 aktiv. APT28 wird auch der Angriff auf den französischen Fernsehsender *TV5 Monde* im April 2015 zugeschrieben, wie *Hans-Georg Maaßen,* Präsident des Bundesamts für Verfassungsschutz, in einer Podiumsdiskussion während der IT-Sicherheitstagung 2015 der Max-Planck-Gesellschaft sagte. Die Attacke gilt übrigens als *False-Flag-Operation,* da es ein wohl gefälschtes Bekennerschreiben einer bis dahin unbekannten islamischen Gruppe namens *Cyber Caliphate* gab.

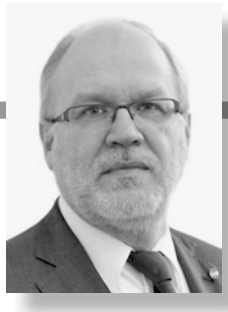
Das Sicherheitsunternehmen *Trend Micro* berichtete im Mai 2016, dass die Gruppe APT28 einen Angriff gegen die CDU gestartet habe.[9] Dazu wurde ein nachgebauter CDU-Webmail-Server in Litauen betrieben, um dann mit Phishing-E-Mails Benutzerkonten und Passwörter abzugreifen.

Im August 2016 schickte ein *Heinrich Krammer* eine E-Mail, die vermeintlich aus dem Nato-Hauptquartier kam (E-Mail-Adresse endet auf *@hq.nato.int)*. Die E-Mail versprach Hintergrundinformationen unter anderem über den Militärputsch in der Türkei. Wer auf den Link in der Mail klickte, installierte eine Schadsoftware auf seinem Rechner. Adressaten der E-Mail waren *Sahra Wagenknecht* und die Bundesgeschäftsstelle der Linken sowie die Junge Union und die CDU im Saarland. Auch hier vermuten Sicherheitskreise die Gruppe APT28 als Urheber.[10]

Im November 2016 veröffentlichte Wikileaks 90 Gigabyte Daten (2420 Dokumente) aus dem NSA-Untersuchungsausschuss des Deutschen Bundestages. Diese Daten scheinen nicht aus dem Bundestags-Hack vom Frühjahr 2015 zu stammen. Die Parallelen zum Vorgehen der Hacker in den USA sind auffällig. Insofern muss damit gerechnet werden, dass in der heißen Phase des Wahlkampfs in Deutschland Informationen aus diesen Hacks auf Wikileaks oder vergleichbaren Plattformen auftauchen.

Das *Bundesamt für Sicherheit in der Informationstechnik (BSI)* beschäftigt sich als die deutsche nationale Cyber-Sicherheitsbehörde intensiv mit dem Thema. BSI-Präsident *Arne Schönbohm* warnte im Herbst 2016 die Parteien persönlich vor Ausspähung durch staatliche Hacker.[11] Der Verdacht, der dabei im Raum steht: Vor der Bundestagswahl könnten Angreifer versuchen, die öffentliche Meinung zu manipulieren. Im Fokus stehen auch automatisierte Meinungsplatzierungen im Internet oder in sozialen Netzen. Im März 2017 warnte das BSI die politischen Parteien in Deutschland nochmals deutlich vor zu erwartenden Cyberangriffen während des Wahlkampfs.[12]

Anfang Februar 2017 gab es Medienberichte, wonach deutsche Geheimdienste keine Beweise für gezielte russische Desinformation gefunden haben. Trotzdem nennt der 50-seitige Bericht laut Recherchen von NDR, WDR und Süddeutscher Zeitung die Be-



Rainer W. Gerling

Prof. Dr. **Rainer W. Gerling** ist IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft sowie Honorarprofessor für das Fachgebiet IT-Sicherheit an der Fakultät für Informatik und Mathematik der Hochschule München. Dort ist der habilitierte Physiker für die Zusatzausbildung „Betrieblicher Datenschutz“ im Fachbereich Informatik verantwortlich.

richterstattung russischer Propagandamedien wie der deutschsprachigen Ausgabe von *Russia Today* oder *Sputnik News* geradezu „feindselig".[13] Wo ist die Grenze zwischen überspitzter Berichterstattung und Desinformation?

Dass Staaten versuchen, durch Desinformation, Propaganda, Fake-News und alternative Fakten (altmodisch auch Lügen genannt) die öffentliche Meinung in ihrem Sinn zu beeinflussen, ist nichts Neues. Das Internet, soziale Medien und Plattformen wie Wikileaks haben die Zahl der Informationsanbieter jedoch dramatisch steigen lassen. Klassische journalistische Ethik und Wahrhaftigkeit sind dabei vielfach auf der Strecke geblieben. Eine Richtigstellung und Bewertung durch klassische Medien und Experten oder gar staatliche Stellen ist schwierig. Die Lebenserfahrung zeigt uns, dass doch immer irgendetwas hängen bleibt. Letztendlich müssen jede Bürgerin und jeder Bürger für sich entscheiden, was sie glauben und was nicht. Dabei hilft nur eines: Bildung. Insofern sollten wir in Europa ein bisschen weniger anfällig für alternative Fakten sein als die US-Bürgerinnen und -Bürger, da das Bildungsniveau in Europa im Mittel höher ist.

Ergänzung nach der französischen Präsidentenwahl

Am Freitagabend vor der Stichwahl in Frankreich wurden die *Macron-Leaks* veröffentlicht: eine große Menge von Dokumenten, die sowohl in Teilen gefälscht, verändert und auch echt waren. Die Veröffentlichung wird APT 28 zugeschrieben, auch wenn es dafür keine Beweise gibt.[14]

Ergänzte Fassung aus *MaxPlanckForschung 1/2017*. Nachdruck mit freundlicher Genehmigung.

Anmerkungen

1 *https://people.csail.mit.edu/rivest/pubs/Riv16z.slides.pdf*
2 *https://freedom-to-tinker.com/2015/04/15/decertifying-the-worst-voting-machine-in-the-us/8*
3 *https://www.schneier.com/blog/archives/2015/04/an_incredibly_i.html*
4 *http://heise.de/-290710*
5 *http://nymag.com/daily/intelligencer/2016/11/activists-urge-hillary-clinton-to-challenge-election-results.html*
6 *http://www.faz.net/aktuell/politik/bundeswahlleiter-will-bundestagswahl-vor-hackerangriffen-schuetzen-14651555.html*
7 *http://www.faz.net/aktuell/politik/inland/aus-sorge-vor-hackangriffen-verzichten-niederlande-auf-wahlcomputer-14824128.html*
8 *https://www.dni.gov/files/documents/ICA_2017_01.pdf*
9 *http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-german-christian-democratic-union/*
10 *https://www.wirtschaftsschutz.info/SharedDocs/Kurzmeldungen/DE/ITSicherheit/Warnmeldung_Neu.html*
11 *http://www.sueddeutsche.de/politik/bundesregierung-ist-alarmiert-hackerangriff-aufdeutsche-parteien-1.3170347*
12 *http://www.spiegel.de/netzwelt/netzpolitik/bundestagswahl-2017-bsi-chef-arne-schoenbohm-warnt-parteien-vor-hacker-angriffen-a-1136542.html*
13 *http://www.tagesschau.de/inland/deutsche-geheimdienste-russland-101.html*
14 *https://www.heise.de/tp/features/Macron-Leaks-Die-Geschichte-zum-massiven-Hack-3711374.html*

Dagmar Boedicker

Wider den lähmenden Pessimismus

Wie kommt es, dass viele Europäer.innen das Europaparlament und die Kommission verwünschen und meinen, sie wären glücklicher für sich allein in ihrem mehr oder weniger kleinen Land? In weniger als einer Generation haben sich die Europäische Union und Deutschland so stark verändert, dass sie kaum wiederzuerkennen sind. Die in den 80ern noch optimistische Perspektive auf eine in Zukunft pfleglich behandelte Umwelt, wachsenden Wohlstand und mehr Gerechtigkeit hier und in der Welt ist Wut oder Resignation gewichen. Was ist passiert?

Von zwei Blöcken mit gegensätzlichen Ideologien und relativ überschaubaren Einflusssphären ist 1989 einer zerfallen, der andere fühlt sich als Sieger, wenn auch mit neuen Herausforderern. Die EU hat ihren Platz in der Mitte verloren, sie kann sich nicht mehr das Beste aus zwei Welten herauspicken, sondern muss Partei ergreifen und ein aktuelles Problem nach dem anderen bewältigen. Starke Konzepte scheint sie dafür nicht zu haben, jeder Mitgliedstaat versucht, den eigenen Nutzen auf Kosten der anderen zu maximieren.

Osteuropäische Länder, die nach der Umklammerung durch die UdSSR der EU und NATO beitraten, holen eine nationalistische Phase nach, die sie zwischen dem Großen Krieg und dem Fall des Eisernen Vorhangs übersprungen haben.

Ökonomisch beherrscht das Modell des bisherigen Siegers fast den gesamten globalen Norden nach dem Motto *There Is No Alternative*. Seit mehr als einer Generation wird es weltweit an Hochschulen und Forschungseinrichtungen gelehrt und praktiziert, und es scheint die politischen Eliten verdummt zu haben. Sie predigen weiter Privatisierung, Deregulierung, unbeschränkten Handel und Kapitalverkehr bis hin zur „marktkonformen Demokratie" unserer Kanzlerin, trotz bröckelnder Infrastruktur, löcheriger Daseinsvorsorge und kastrierter Kontrolleure von wirtschaftlichen Aktivitäten. Diejenigen, die hoheitliche Aufgaben nicht schnell genug als überflüssig deklarieren konnten, kritisieren heute dreist das Versagen der Polizei, um sich für den Wahlkampf in Stellung zu bringen. Wie Christian Lindner (FDP), der anlässlich des Attentats in Berlin vom Dezember 2016 die Sicherheitsbehörden rügte, sie hätten bei der Rundum-Überwachung des Attentäters versagt.

Auch der technische Fortschritt ist dem marktliberalen Dogma untergeordnet. Das müsste nicht so sein, wenn es um anderes

ginge als die Förderung nationaler Oligopole und des *Shareholder Value*. Weniger Ressourcenverbrauch, Bildung und Entwicklungsmöglichkeiten für alle, gerechte Produktionsverhältnisse, kürzere Arbeitszeiten beispielsweise. Aber wann hätte Technik nicht in den Diensten der Mächtigen gestanden?

Liberalismus heute

Einst versprach der Liberalismus Fortschritt für alle und meinte damit nicht nur den technischen Fortschritt, sondern auch den sozialen. Eine aufgeklärte Mittelschicht schien dazu bestimmt, durch ihre Repräsentanten Bildung, Wohlstand und Demokratie zu verbürgen. Es ist ihr nicht gelungen. Nicht für sich selbst und schon gar nicht für diejenigen, die hofften, selbst oder in der nächsten Generation Teil dieser Mittelschicht zu werden. Rechte Parteien wissen sehr gut, wie sie das Ressentiment über dieses gebrochene Versprechen schüren und die Gesellschaft durch Hetze noch weiter spalten. Linke Parteien sind selbst uneins und würden auch mit einem schlüssigen linken Konzept der Solidarität kaum ausreichende Mehrheiten gewinnen. Zu viele Wähler. innen fürchten um ihren Besitzstand.

Die, die nichts zu sagen haben, glauben nicht mehr an die Segnungen ungezügelter Märkte. Sie haben nicht vergessen, dass 2008 Bildung und Soziales, Daseinsvorsorge und ökologische Erneuerung geschröpft wurden für die 1.700 Mrd. Euro zur *Rettung* von Banken allein in der Eurozone. Jean Ziegler rechnete aus[1], dass sich mit jährlich einem Prozent dieser Milliarden in fünf Jahren die Millenniums-Entwicklungsziele für die Welt hätten erreichen lassen (sie wurden verfehlt). Die, die nichts zu sagen haben, haben begriffen, dass die Vermögen zur Hälfte bei einem Prozent der globalen Bevölkerung angekommen sind, während sich 99 Prozent die andere Hälfte teilen müssen. Wer hätte vor 30 Jahren gedacht, dass heute in einem reichen Land wie Deutschland viele nicht mehr von ihrer Arbeit leben können – ganz zu schweigen von den ärmeren Ländern, in denen eine verlorene Jugend wenig Hoffnung auf die Zukunft hat. Ein allgemeiner Überdruss an der *politischen Klasse* macht sich in Deutschland, Frankreich und anderen Ländern breit. Warum noch wählen, wenn man doch keine Wahl hat, weil *das Establishment* unter sich bleibt und weil nie dazugehören wird, wer jetzt nicht dazugehört? Die, die nichts zu sagen haben, glauben nicht mehr, dass sie jemals etwas zu sagen haben werden.

Eine Generation neoliberaler Ellbogengesellschaft hat dazu geführt, dass soziale Verantwortung, Anstand und rücksichtsvoller Umgang miteinander als altmodisch betrachtet oder als Gutmenschentum verspottet werden. Achtsamkeit und mitmenschliche Sorge kennen wir fast nur noch aus der (Wahl-) Familie. Das Vertrauen ist erschüttert in Entscheider und Institutionen, Gerechtigkeit, sozialen Fortschritt, das Rechtssystem, die ökonomische Vernunft.

Nicht nur transnationale Konzerne und wir Individualisten in den Industriestaaten haben sich die Informations- und Telekommunikationstechnik erschlossen. Auch die Bevölkerung der Entwicklungsländer nutzt sie, für Bildungszwecke, die Vernetzung entlegener Regionen, einfacheren Geldverkehr. Hoffentlich macht sie besseren Gebrauch davon als wir! Denn bei uns scheint *das Netz* weit mehr der Profitmaximierung und Überwachung, der Zerstreuung, Ablenkung vom wirklich Wichtigen, Propaganda und dem Pseudo-Sozialen zu dienen. Plattformen, euphemistisch soziale Netzwerke genannt, begünstigen die Selbstentblößung und das ruppige Dampf-Ablassen, ohne Höflichkeit und ohne Ansehen der Privatsphäre. Monopolisten sammeln, verarbeiten und verkaufen unsere personenbezogenen Daten und verstoßen damit ungeniert gegen rechtliche Vorgaben – wir lassen es uns gefallen. Geheimdienste und organisierte Kriminalität entziehen sich jeder Kontrolle.

Angesichts dieser Kritik ist es höchste Zeit für ein gemeinsames öffentliches Nachdenken darüber, was wir erreichen wollen. Wenn wir auf der Stufe des allgemeinen Unbehagens und der Nörgelei stehen bleiben, werden die Falschen entscheiden, wie unsere Zukunft aussieht.

Ein Buch von Ulrike Guérot[2] fasst zusammen, was viele Menschen in Europa bewegt: *Warum Europa eine Republik werden muss!* Sie resümiert Missstände, spinnt den Faden aber weiter zu einer Utopie für die Europäische Union, vielleicht erreichbar in einer weiteren Generation.

Marktliberalismus ist kein Naturgesetz

Wirtschaft soll Güter produzieren und verteilen, sozialen und ökologischen Fortschritt unterstützen, sie soll die Menschen nicht unterwerfen, sondern ihnen dienen. Sie darf nicht jährlich mehr Planet verbrauchen als nachwachsen könnte, von seiner Vergiftung und Verschmutzung ganz zu schweigen. Guérot nennt als Ziele: das Gemeinwohl zu fördern, die soziale Kontrolle der Wirtschaft und den Schutz des ländlichen Raums.

Marktliberale Demagogen diffamieren gern die Gemeinwohl-Ökonomie. Das Bild der „tragedy of the commons" dominiert Lehrveranstaltungen, obwohl Elinor Ostrom[3] zeigte, dass die Allmende funktioniert, wenn die Rahmenbedingungen dafür stimmen. Diesen Rahmen setzt die Politik, abhängig vom Willen ihrer Wähler. Die Politik ist zuständig für eine Kontrolle des allgemeinen Marktgeschehens, beispielsweise über das Kartellrecht, Regelungen gegen Steuerflucht oder unlauteren Wettbewerb. Das durchzusetzen fällt schwer, wenn transnationale Konzerne mit Standort-Nachteilen oder dem Verlust von Arbeitsplätzen drohen. Es muss aber nicht so sein, wenn eine europäische statt 27 nationaler Wirtschaftspolitiken neue Regeln für unseren größten Binnenmarkt der Welt festlegt und durchsetzt und dabei selbstverständlich als wichtigste Ziele vergleichbare Lebensverhältnisse sowie ökologische und soziale Nachhaltigkeit verfolgt.

Geiz ist nicht geil!

Klimaschutz muss global sein, die Produktion muss es nicht. Zwingt uns jemand, mit Textilproduzenten in Bangladesch, Hardware-Herstellern in China oder Weizen- und Soja-Bauern in den USA zu konkurrieren? Günstige Kleidung lässt sich auch in den Mitgliedstaaten fertigen und schafft Wohlstand dort, wo die Lebensverhältnisse karger sind als in den reichen Ländern. Regionale Lebensmittel erhalten unsere Biosphäre und schaffen Arbeitsplätze im ländlichen Raum, selbst geeignete Sojabohnen

gibt es inzwischen in der EU. Möbel sollten ohnehin nicht beim Sperrmüll, sondern in sozialen Werkstätten landen und in Stand gesetzt werden. Dann sind sie für alle erschwinglich. Genossenschaften als demokratisch verfasste Unternehmen sind ein Ausweg aus dem Irrsinn des *Shareholder Value*.

Niemand braucht jedes Jahr ein neues Smartphone. Wenn das alte nicht mehr tut, kann es ein faires neues sein, das aus recyceltem Elektroschrott unter menschenwürdigen Bedingungen gebaut wird, mit Software aus der EU, entwickelt und regelmäßig aktualisiert nach europäischen Rechts- und Sicherheitsstandards, das bedeutet Datenschutz schon im Design und mit sicheren Standardeinstellungen. Ohne chinesische Hintertüren, mit quelloffener, zertifizierter Software und mit vernünftiger Produkthaftung. Cloud-Server können wir in der EU mit Strom aus erneuerbarer Energie und datenschutz-konform betreiben. Europäisches Knowhow wird wohl eine oder mehrere Suchmaschinen und Kommunikations-Plattformen entwickeln können und so dafür sorgen, dass der *Rohstoff Information* in Europa bleibt.

EU-Politik muss dafür sorgen, dass unsere Kommunikation sicher und unsere informationelle Selbstbestimmung gewahrt wird, auch wenn sie die Voraussetzungen dafür selbst schaffen muss. Wir brauchen eine ressourcen-sparende EU, die ohne fossile Energie auskommt, die Erde weder hier noch anderswo verschmutzt und menschenwürdige Lebens- und Arbeitsbedingungen bietet.

Es wäre ein Friedensbeitrag, denn: Wer keine doppelte Moral übt, selbst nicht ausbeutet und sich nicht von ausbeuterischen Regimen abhängig macht, kann auch in der Außenpolitik integer handeln.

Keine Zeit?

Die, die nichts zu sagen haben, haben Leistung zu erbringen. Die Rolltreppe fährt nach unten, wir laufen rauf, um unseren Platz zu behalten, so ein anschauliches Bild von Oliver Nachtwey. Ökonomisierung und technischer Wandel beschleunigen unser Leben in der Arbeit und im Privaten, unser Tag ist in Zeitscheibchen zerlegt. Das Gemeinsame, *das Politische* im besten Sinn bleiben auf der Strecke. Wann können wir darüber nachdenken? Wie dem Tag noch (Bedenk-) Zeit für zivilgesellschaftliches Engagement abzwacken?

Die Technik scheint es uns auch zu ersparen, uns mit rücksichtslosen Eliten auseinanderzusetzen und Verpflichtungen gegenüber unseren Mitmenschen einzugehen. In seinem Buch *Soziophobie*[4] stellt César Rendueles diese Diagnose und konfrontiert sie mit einer Utopie von Technikoptimisten: Im Internet sollen individuelle Freiheit und Unabhängigkeit von den Mitmenschen auf soziale Wärme und partnerschaftliche Zusammenarbeit treffen. Pseudo-Freunde fürs Unverbindliche und *Ad-hocracy* als Ersatz für gelebte Demokratie, beides lässt sich auf der Couch leben, aktiv sind Gehirn und Finger. Das mag weniger anstrengend sein als das Einkaufen und Kochen für Freunde oder Familie, auch weniger zeitraubend als Vereinsarbeit oder aktives politisches Engagement. Ersetzen kann es sie sicher nicht.

Kooperation ist kein Anreiz-Kostensystem, sondern eher ein Ökosystem. Darin beeinflussen und reiben wir uns aneinander, die entstehende Wärme verbindet oder trennt uns, je nachdem. Auch wenn die Annäherung nicht immer gelingt, schafft doch der Prozess gemeinsame Erfahrung, kommunikative Kompetenz, einen Schimmer von der Weltsicht der/des jeweils Anderen. Gelingt sie, lernen wir aus dem Anderssein unserer Nachbarn in Deutschland und Europa. Vielfalt bereichert uns alle. Im Idealfall schaffen wir es, wie Wolfgang Streeck schreibt, „uns in die Zufriedenheit einer neuen Bedarfswirtschaft zurückzuziehen und das auf Wachstum versessene Kapital sich selbst zu überlassen."[5]

Das gemeinsame Haus und seine Werte

Wir werden am institutionellen Gebäude der EU arbeiten müssen. Es ist schief, teilweise korrupt und dysfunktional und hat Modernisierungsbedarf, aber es hat solide Substanz. Menschenrechte sind seine Basis, Rechtsstaat und Demokratie das Erdgeschoss. Gorbatschow hat es beschworen, renovieren müssen wir es schon selbst.

In ihrer Grundrechte-Charta hat sich die EU auf bindende Grundwerte geeinigt: Menschenwürde, Frieden, Freiheit, Solidarität, Bürgerrechte und Rechtsstaatlichkeit. Sie hat uns Positives gebracht wie die Freizügigkeit, die Datenschutz-Grundverordnung, Bildungsprogramme wie Erasmus, Leonardo, Comenius, Grundtvig. Gesetzgebung wie die Habitat-Richtlinie, Vorgaben zum Gewässer-, Luft- und allgemein zum Umweltschutz sind gelegentlich, anders als in der deutschen Wahrnehmung, ehrgeiziger als nachher ihre nationale Umsetzung ausfällt. Es gab EuGH-Urteile und Vorabentscheidungen zur Vorratsdatenspeicherung, dem Recht, vergessen zu werden, zu Sorgfaltspflichten für Unternehmen, zu Facebook und Safe Harbor. Sie fielen bürgerrechts-freundlicher aus als manche nationale Betrachtung.

In einer EU der Zukunft dürfen nationale Regierungen unangenehme Aufgaben nicht mehr der Kommission aufhalsen und sich dann über das beschweren, was sie im Rat selbst beschlossen haben. Deutschland wird seine Hegemonie deutlich abbauen und sein herablassendes Auftreten gegenüber anderen, vor allem südlichen Ländern, ablegen müssen. Wenn Mitgliedstaaten die Grundwerte verraten, müssen sie sanktioniert werden können. Falls die Aussetzung des Stimmrechts im Rat gemäß Art. 7 AEUV misslingt oder nicht genügt, müssen neue Instrumente her.

Dagmar Boedicker

Dagmar Boedicker ist Journalistin, technische Redakteurin und langjährige Redakteurin der FIfF-Kommunikation.

Europäische Werte müssen die Staaten auch im Umgang mit anderen leben – die Welt erfährt zweierlei Maß als unglaubwürdig. Eine eigene Außenpolitik im Nahen Osten und Nordafrika, die US-Obsessionen nicht hinterher *trumpelt,* muss Strukturpolitik sein, Agrar-, Handels- und Rohstoffpolitik. Sie muss Flüchtlings-, Wirtschafts- und Sicherheitspolitik zusammen denken.

Die EU muss investieren in die Sozialpolitik Frankreichs, den Aufbau der griechischen Wirtschaft, Arbeitsplätze in Süd- und Südosteuropa, eine gemeinsame Flüchtlingspolitik und die Unterstützung der Ankunftsländer. Geld dafür ist da, so billig wie nie. Sie muss den Einfluss großer Konzerne zurückdrängen und Bürgerinitiativen in ihrem Bemühen um eine menschliche und ökologische Wirtschaft stärken, damit Unternehmen in allen Ländern endlich angemessene Steuern zahlen, damit Kartelle kontrolliert und Rechtsverstöße sanktioniert werden. Die Konzerne werden sich überlegen, ob sie auf einen Markt mit fast 450 Millionen Einwohnern in 27 Ländern verzichten wollen. Wer eine einheitliche Besteuerung hintertreibt, wie derzeit Malta, gehört an den Pranger.

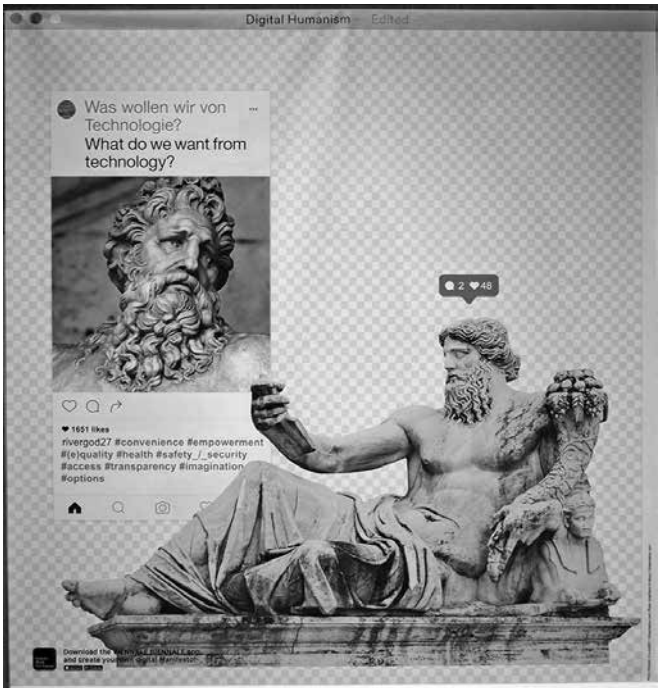
Menschen können lernen, Institutionen auch

Europa hat eine gemeinsame Geschichte, voller Feindschaft, Krieg, Hass und Rachegefühle. In den letzten 70 Jahren bemühen sich die Staaten in der EU, diesen Teil ihrer Vergangenheit zur Seite zu schieben und ihre gemeinsamen Interessen mehr oder weniger gemeinsam zu verfolgen. Jetzt scheinen sie überfordert von dieser Aufgabe. Für eine gemeinsame friedliche Zukunft muss mehr passieren. Wir Europäer werden uns intensiver mit unseren Nachbarn beschäftigen müssen, ihrer Geschichte, ihren Sprachen, ihrer Vorstellung von uns und den anderen. Wir werden mit ihnen sprechen müssen über unsere Geschichte und unsere Vorstellung von ihnen, und gemeinsam verstehen, was in dieser Geschichte warum geschah und wie wir verhindern, dass sich etwas Ähnliches, vielleicht noch Furchtbareres wiederholt. Herfried Münkler schreibt über Nutzen und Nachteil von Partnerschaft, Mitgliedschaft und Freundschaft:

> *„Eine institutionell gesicherte Partnerschaft kann Perioden der Identitätssuche, wie sie in den Entwicklungskrisen bei Individuen wie politischen Kollektiven periodisch auftreten, aushalten und absichern; wo solche verlässlichen Institutionen der Partnerschaft aber fehlen, schlagen Identitätskrisen schnell in Feindschaft um […]"*[6]

Die EU ist kein Imperium, anders als China, die USA oder Russland. Diesen drei genannten ist gemeinsam, dass sie ihre Interessen unverhüllt verfolgen, wenigstens zwei wollen keine starke EU. Das Freihandels-Dogma propagieren sie zwar, betreiben aber eher – besonders in letzter Zeit – einen modernen Merkantilismus, ein wirtschaftliches Nullsummen-Spiel.

In der EU stehen nationale Egoismen bisher dem gemeinsamen Leben, Wirtschaften und Entscheiden entgegen. Guérot zeigt, dass Europa damit den Ausverkauf seiner Unternehmen zulässt und die Chance vergibt, vereint eine kritische Größe zu erreichen: „Gut 50 % der europäischen Firmen und Unternehmen wanderten 2015 in nicht-europäische Hände."



Thesenplakat zur Ausstellung „Hello, Robot" im Museum für angewandte Kunst (MAK), Wien

Wir können die Handlungshoheit zurückgewinnen, wenn wir uns der rasanten Beschleunigung durch den technischen Wandel mit besonnenen, solidarischen Zielen widersetzen. Technik soll sozialen Fortschritt fördern und unterstützen, sie soll ihn sich nicht unterwerfen. Noch einmal Ulrike Guérot:

> *„Algorithmen und Computernetzwerke können Menschen kontrollieren, destruktive Bedürfnisse wecken, Wachstum hochpeitschen, Drohnen lenken, jedes Jahr neue Generationen virtueller Welten und Spaßmaschinen entwerfen und vertreiben, Menschen zum passiven Gleitmittel einer amoklaufenden Wirtschaft degradieren. Aber Algorithmen und Computer können auch von harter, routinierter, geistloser Arbeit befreien, sie können die Umstellung von Energiezentralen auf dezentrale vernetzte Einrichtungen regeln, sie können öffentliche Verkehrsmittel attraktiv machen, die Systeme der Steuererhebung gerechter, transparenter und effizienter machen, das Wissen der wirklichen Welt allen zugänglich machen."*

Transparenz wird vielfach nur vorgetäuscht, es geht dabei nicht um Tausende von Seiten, die wir uns unter irgendeiner URL herunterladen können. Wichtige Themen müssen aufbereitet werden, etwa so, wie OpenDataCity das mit den Änderungsanträgen der EU-Parlamentarier zur Datenschutz-Grundverordnung gemacht hat. *Big Data* brauchen eine professionelle Visualisierung, offene Software lässt sich nicht ausschließlich ehrenamtlich entwickeln und Saatgut unter Open-Source-Lizenz muss den Landwirten einen Lebensunterhalt ermöglichen. Wer in der Wissenschaft unter Open Access veröffentlicht, darf keine Nachteile gegenüber denen haben, die ihre Urheberrechte an die wenigen Journale der großen Verlage geben. Wie kann die Qualität offenen Wissens geprüft und diese Prüfung finanziert werden? Wo bisher große Konzerne über Wissen entscheiden, eignen sie es sich an, und das tun sie zur Maximierung ihres Profits. Wie Evgeny Morozov zu Alphabet & Co schreibt:

„Der aktuelle Ansatz – große Technikunternehmen so viele Daten aufnehmen zu lassen, wie sie können, und dann das Kartellrecht darauf anzuwenden, wie sie ihre Websites gestalten – ist zahnlos."[7]

Zivilgesellschaftliche Organisationen können es besser, das zeigen das GNU-Projekt oder LobbyControl und viele andere. Wenn Regierungshandeln und Wirtschaftsinteressen transparent gemacht werden, lohnt es sich für die Menschen politisch mitzuwirken. Das ist lästig für die Entscheider und anstrengend für die Partizipierenden, beide kostet es Zeit und Mühe. Wir werden deshalb wachsam bleiben müssen: Die Versuchung ist groß, Bürgerbeteiligung bloß formal einzurichten und durch angebliche Sachzwänge klammheimlich zu hintertreiben. Populisten mit ihren scheinbar einfachen Lösungen geht aber nur nicht so leicht auf den Leim, wer sich selbst als wirkmächtig erlebt.

Ziel der EU muss es sein, ihre Grundwerte zu verwirklichen, sie lebbar zu machen! Das kann kein Land allein erreichen. Wir zusammen müssen dafür sorgen, dass Europa Wissen und Werte exportiert statt Waffen und Elektroschrott, dass es aufhört, Rohstoffe und Menschen auszubeuten und ihnen dafür seine überschüssigen Nahrungsmittel hinzuschieben. In seinen Beziehungen nach innen muss Europa solidarisch und gerecht werden, in denen nach außen ebenfalls. Dazu gehört, die unheilvollen Folgen seiner kolonialen Vergangenheit zu beheben, auch Deutschland darf sich davor nicht drücken.

Wenn die EU auch die nächsten 70 Jahre bestehen will, muss sie die Menschen, vor allem die jungen, begeistern. Kulturprojekte wie CinEd zum Kennenlernen des europäischen Autorenkinos oder ein geschenktes Interrail-Ticket für alle zum achtzehnten Geburtstag[8] sind ein guter Start, mehr Stipendien, nicht nur für Studierende, müssen folgen. Die Kooperation von Städten und Regionen über Nationalstaatsgrenzen schafft Wissens- und Erfahrungsaustausch. Wir können viel voneinander lernen und Vielfalt ermöglicht kreative Problemlösungen.

Referenzen

1 *Jean Ziegler: Das tägliche Massaker des Hungers. 2008. Rede in Wien*
2 *Verlag J.H.W. Dietz Nachf. GmbH, Bonn 2015*
3 *Elinor Ostrom: Was mehr wird, wenn wir teilen. 2011. oekom verlag, München*
4 *César Rendueles: Soziophobie - Politischer Wandel im Zeitalter der digitalen Utopie. 7.9.2015. edition suhrkamp 2690*
5 *Deutschlandfunk, 18.12.2016: Das Verhältnis von Kapitalismus und Gewalt*
6 *Herfried Münkler: Über Nachbarschaft. Der Nutzen und Nachteil von Partnerschaft, Mitgliedschaft und Freundschaft. Merkur 3/2011. www.eurozine.com (Abruf 18.1.2014)*
7 *Süddeutsche Zeitung, 10.7.2017, S. 13: Die Datengiganten sind schon viel weiter*
8 *Das Europäische Parlament war dafür, allerdings ist nur eine Sparversion übriggeblieben.*

Einladung zur Mitgliederversammlung 2017

des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF e. V.)

Wir laden fristgerecht und satzungsgemäß zur ordentlichen Mitgliederversammlung 2017 ein.

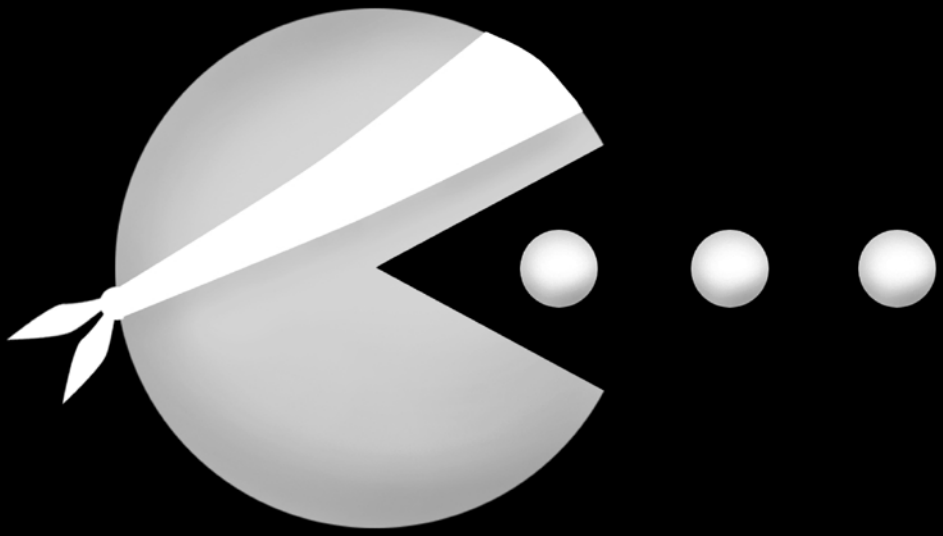
Sie findet am Sonntag, den 22. November 2017, von 12:30 bis 14:00 Uhr statt.
Adresse: Friedrich-Schiller-Universität Jena, Carl-Zeiss-Str. 3, 07743 Jena
Der betreffende Raum wird rechtzeitig am Eingang angeschlagen sowie auf *www.fiff.de* veröffentlicht.

Vorläufige Tagesordnung

1. Begrüßung, Feststellung der Beschlussfähigkeit und Festlegung der Protokollführung
2. Beschlussfassung über die Tagesordnung, Geschäftsordnung und Wahlordnung
3. Bericht des Vorstands einschließlich Kassenbericht
4. Bericht der Kassenprüfer
5. Diskussion der Berichte
6. Entlastung des Vorstands
7. Neuwahl des Vorstands
8. Neuwahl der Kassenprüfer
9. Diskussion über Ziele und Arbeit des FIfF, aktuelle Themen, Verabschiedung von Stellungnahmen, Berichte aus den Regionalgruppen
10. Anträge an die Mitgliederversammlung
    Anträge müssen schriftlich bis drei Wochen vor der Mitgliederversammlung bei der FIfF-Geschäftsstelle eingegangen sein
11. Verschiedenes

gez. Stefan Hügel
für den Vorstand und die Geschäftsstelle des FIfF

#FIfFKon17



TRUST

Wem kann ich trauen im Netz und warum?

20.-22.10.2017
Uni Jena

Eine Konferenz des
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung

TRUST – Wem kann ich trauen im Netz und warum?

FIfFKon 2017 – Jahrestagung

des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V.

20. bis 22. Oktober 2017

Friedrich-Schiller-Universität Jena
Hörsaalgebäude CZ3
Carl-Zeiss-Straße 3, 07743 Jena

Eintritt frei!
Anmeldung unter ***orgateam@fiffkon.de*** erbeten.

Programm

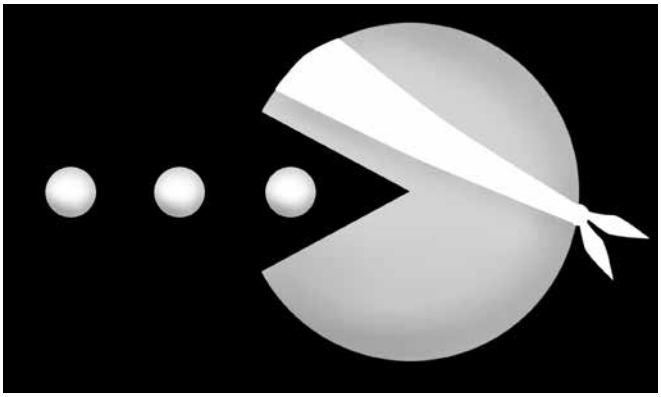
(kurzfristige Änderungen vorbehalten)

Freitag, 20.10.2017	
ab 12:00 Uhr	Anmeldung im Tagungsbüro
16:00 Uhr	*Eröffnung der Tagung* Prof. Dr. **Eberhard Zehendner** (FIfF-Vorstand/Friedrich-Schiller-Universität Jena), **Stefan Hügel** (FIfF-Vorstandsvorsitzender)
16:15 Uhr	*Wem müssen wir beim Benutzen von Software vertrauen? – Möglichkeiten zur radikalen Verkleinerung der „Trusted Computing Base"* **Hannes Mehnert**, PhD (University of Cambridge, UK)
17:15 Uhr	Pause
17:30 Uhr	*Vertrauen – Fortschritt – Kontrolle* Dr. jur. **Lutz Hasse** (Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit, Erfurt)
18:15 Uhr	Steh-Imbiss
Themenblock „Cyberpeace statt Cyberwar"	
19:00 Uhr	*Cyberwar for Dummies*
19:15 Uhr	*Die Bundeswehr im Cyber- und Informationsraum* **Thomas Gruber** (IMI Tübingen/Universität Bremen)
20:00 Uhr	*The Making of ... „Cyberpeace statt Cyberwar"* **N.N.** (Motion Ensemble, Hamm)
20:15 Uhr	*Drohnenabwehr – Was tun gegen Cyberangriffe aus der Luft?* Dr. **Anja Beyer-Peters** (T-Systems Multimedia Solutions GmbH, Jena)
21:00 Uhr	*Die Cyberpeace-Kampagne des FIfF – Vergangenheit und Zukunft* Prof. Dr. **Hans-Jörg Kreowski** (Cyberpeace-Kampagne/Universität Bremen)
21:45 Uhr	Pause
22:00 Uhr	*Zero Days* Ein Film von **Alex Gibney**

Samstag, 21.10.2017	
Workshops	
8:00 Uhr bis 10:00 Uhr	*Die Algorithmen sind unschuldig! Wer und was sind es nicht?* Organisation: Prof. Dr. **Britta Schinzel** (Fiff-Vorstand/Universität Freiburg)
8:00 Uhr bis 10:00 Uhr	*IT-Sicherheit barrierefrei* Organisation: Prof. Dr. **Eberhard Zehendner**
Themenblock „IT-Sicherheit"	
10:15 Uhr	*Vertrauen und IT-Sicherheit – zwei Gegenspieler?* Prof. Dr. **Sabine Rehmer** (IGO – Institut für Gesundheit in Organisationen, Jena)
11:00 Uhr	*Spamvermeidung statt Spamerkennung* Dr. **Carlo Schäfer** (Universitätsrechenzentrum Jena)
11:30 Uhr	Pause

11:45 Uhr	*WLAN-Sicherheit im Gesundheitswesen* **Stefan Jäger** (Friedrich-Schiller-Universität Jena)
12:15 Uhr	*It stays a matter of trust – Perspektiven für Open-Source-Software in der Post-Snowden-Ära* **Sascha Turban** (Humboldt-Universität Berlin)
12:45 Uhr	Mittagspause
Für Interessierte besteht die Möglichkeit, bei einer Begehung der Innenstadt von Jena Wardriving *hautnah zu erleben.*	
Themenblock „Medien und Soziale Netzwerke"	
13:45 Uhr	*Wenn wir Behörden und Industrie nicht vertrauen können – FIfF initiiert unabhängiges Radioaktivitätsmessnetz um Schrott-Atomreaktoren* Prof. em. Dr.-Ing. **Dietrich Meyer-Ebrecht** (RWTH Aachen)
14:15 Uhr	*Nutzung von Daten aus Sozialen Netzwerken im Umfeld der zivilen Sicherheit* Dr.-Ing. **Frank Geyer** (IBYKUS AG für Informationstechnologie, Erfurt)
15:00 Uhr	*Fake News* **N.N.**
15:30 Uhr	Pause
16:00 Uhr	*Glaubwürdigkeit der Medien – wer kontrolliert wie den MDR? – Kann ich den öffentlich-rechtlichen Angeboten im Netz trauen? Eine Rundfunkrätin berichtet.* Prof. Dr. **Gabriele Schade** (MDR-Rundfunkrat)
17:00 Uhr	Pause
Themenblock „Best of FIfF"	
17:30 Uhr	*FIfF wirkt! Ein langer Blick zurück* Vorstand des FIfF
18:30 Uhr	*Danke, Dietrich!* Mitglieder des FIfF-Vorstands
18:45 Uhr	Pause
19:00 Uhr	*Verleihung des FIfF-Studienpreises* Auswahlkommission Studienpreis
20:30 Uhr	Abendessen (extern)

Sonntag, 22.10.2017	
Workshops	
8:00 Uhr bis 12:30 Uhr	*Volkszählung – Zensus – Zensus-Vorbereitungsgesetz* Organisation: **Jens Rinne** (FIfF-Vorstand)
8:00 Uhr 12:30 Uhr	*Handys – aber sicher!* Organisation: Prof. Dr. **Eberhard Zehendner** u.a.
12:00 Uhr bis 14:00 Uhr	*Spielerische Hands-on-Demonstration der Wirkmechanismen und Risiken von Free-to-Play-Spielen* Organisation: **Felix Baral-Weber** (Friedrich-Schiller-Universität Jena)
Themenblock „Transparenz?!"	
10:00 Uhr	*Wer ist der Täter? – Attributierung von Cyberattacken und deren Interpretation durch Medien und Politik* **Kai Nothdurft** (FIfF-Vorstand/Information Security Officer, München)
10:30 Uhr	*Wer bin ich und wenn ja wie viele – Herausforderungen an das Identity Management allen Rollen gerecht zu werden* **Sylvia Johnigk** (FIfF-Vorstand/secucat-Informationssicherheit GmbH, München)
11:00 Uhr	*Free-to-Play-Spiele – Probleme und Perspektiven* **Felix Baral-Weber** (Friedrich-Schiller-Universität Jena)
11:30 Uhr	*Das war die FIfFKon 2017 – Nachbetrachtung, Danksagungen, Verabschiedung* FIfF-Vorstand
11:45 Uhr	Mittagsimbiss
12:30 Uhr	**Mitgliederversammlung** *des FIfF (s. S. 62)* (Öffentlich)
14:00 Uhr	**Ende** der Konferenz



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. **Eva Hornecker** (Weimar); **Werner Hülsmann** (Konstanz); **Ulrich Klotz** (Frankfurt); Prof. Dr. **Klaus Köhler** (Mannheim); 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
Prof. Dr. **Dietrich Meyer-Ebrecht** (stellv. Vorsitzender) – Aachen
Michael Ahlmann – Blumenthal (SH)
Sylvia Johnigk – München
Benjamin Kees – Berlin
Prof. Dr. **Hans-Jörg Kreowski** – Bremen
Kai Nothdurft – München
Rainer Rehak – Berlin
Jens Rinne – Mannheim
Prof. Dr. **Britta Schinzel** – Freiburg im Breisgau
Ingrid Schlagheck – Bremen
Prof. Dr. **Werner Winzerling** – Fulda
Prof. Dr. **Eberhard Zehendner** – Jena

FIfF-Geschäftsstelle

Ingrid Schlagheck (Geschäftsführung) – Bremen

Impressum

Herausgeber	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF)
Verlagsadresse	FIfF-Geschäftsstelle Goetheplatz 4 28203 Bremen Tel. (0421) 33 65 92 55 *fiff@fiff.de*
Erscheinungsweise	vierteljährlich
Erscheinungsort	Bremen
ISSN	0938-3476
Auflage	1 200 Exemplare
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	Britta Schinzel (Freiheit 2.0); Stefan Hügel (BigBrotherAward)
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 *http://www.fiff.de/regional*
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
Titelbild	Teil des Leitsystems des Kunstprojekts FREIHEIT 2.0 von Florian Mehnert
Druck	Meiners Druck oHG, 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.

Nachdruckgenehmigung wird nach Rücksprache mit der Redaktion in der Regel gern erteilt. Voraussetzung hierfür sind die Quellenangabe und die Zusendung von zwei Belegexemplaren. Für unverlangt eingesandte Artikel übernimmt die Redaktion keine Haftung.

Wichtiger Hinweis: Wir bitten alle Mitglieder und Abonnenten, Adressänderungen dem FIfF-Büro möglichst umgehend mitzuteilen.

Aktuelle Ankündigungen

(mehr Termine unter *www.fiff.de*)

33. FIfF-Konferenz (#FIfFKon17)
20. bis 22. Oktober, Universität Jena (siehe auch Seiten 63–65)

FIfF-Mitgliederversammlung
22. Oktober, Universität Jena, 12:30 bis 14:00 Uhr

FIfF-Kommunikation

4/2017 „Informatik und Gesellschaft – Gesellschaft und Informatik"
Stefan Hügel u.a.
Redaktionsschluss: 3. November 2017

1/2018 „TRUST – Wem kann ich trauen im Netz und warum?"
Stefanie Jäckel, Eberhard Zehendner u. a.
Redaktionsschluss: 2. Februar 2018

2/2018 „Staats-Hacking – Die ‚Gerätchenfrage'"
Rainer Rehak u.a.
Redaktionsschluss: 4. Mai 2018

W&F – Wissenschaft & Frieden

1/17 Facetten des Pazifismus (mit Dossier 84: Gender, Frauen und Friedensengagement)
2/17 Flucht & Migration
3/17 Ressourcen des Friedens

vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik

#216 Rechtspopulismus/Rechtsextremismus
#217 Der Islam als Herausforderung für das deutsche Religionsverfassungsrecht
#218 Rückkehr zum gerechten Krieg?
#219 Soziale Menschenrechte

DANA – Datenschutz-Nachrichten

4/16 – Tracking, Profiling, Werbung, Marketing
1/17 – Verbraucherschutz
2/17 – BDSG-Nachfolgegesetz (alternativ: Geheimdienste)
3/17 – 40 Jahre DVD

Das FIfF-Büro

Geschäftsstelle FIfF e. V.
Ingrid Schlagheck (Geschäftsführung)
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

Schluss FIfF

FREIHEIT 2.0

eine soziale partizipative Kunstinstallation von Florian Mehnert

ein Zugang zu einem besseren Hintergrundverständnis über Big Data

ab Seite 12

Geeignete Texte für den SchlussFIfF bitte mit Quellenangabe an *redaktion@fiff.de* senden.