Software wirkt immer als Verstärker, von Besonderheiten in Organisationen, hinsichtlich eventueller Bias, Einbindungen oder Auslassungen. Sie vergrößert alle Effekte, die aus den sozialen Zusammenhängen gezogen werden, sie bestätigt und zementiert nicht nur Verhältnisse, sondern reifiziert und vertieft gesellschaftliche Ungleichgewichte. Dies noch unvergleichlich mehr, wenn die Datenprodukte in iterierte und rekursive Prozeduren gefüttert werden, wie dies beispielsweise für Big Data der Fall ist. Zudem werden sie durch die Virtualisierung oft unsichtbar und verfestigen sich. Dringender denn je ist deshalb zu fragen, wieweit es zuträglich ist, unsere Arbeits- und Lebenswelt weiter zu automatisieren. Es ist ein Fehler zu glauben, mit KI, Big Data, Handlungsplänen und Optimierungsverfahren die Welt steuern zu können. Der Menschen zugängliche Umgang mit dem Unerwarteten wird mit der Automatisierung darauf beschränkt, das Mögliche als aufzählbar zu betrac
auf die De- oder Induktion aus Ve

Wir sind es, die wir Daten an s
dort Profile erstellen, bestimmte
etc. verstärken, während wir gleichzeitig Internetdienste umsonst nutzen (wollen); wir, die wir als Informatik-Profession eine ahistorische und angeblich neutrale, vermeintlich objektive Haltung einnehmen. Die Verantwortung bleibt jedoch immer bei uns, auch wenn wir gern die Schuld an andere oder etwas anderes abschieben. Erweitert man aber den Algorithmusbegriff auf jegliche Automatisierung, so weist man individuelle und kollektive Verantwortung als Objektives und Unveränderliches ab.

Ich danke Cecile Crutzen für Anregungen und Verbesserungen an diesem Text, und Jörg Pflüger und Wolfgang Coy für klärende Gespräche darüber.

Anmerkungen

1 *Crutzen CKM (2013) Masks between the Visible and the Invisible. In: Ernst W, Horwath I (eds) Gender in Science and Technology. Interdisciplinary Approaches. Transcript, Bielefeld, pp 79–110*

2 *Im Bereich der Gender Studies wurde später der „ego-approach" von Madeline Akrich in The De-Scription of Technical Objects (1992) Bijker W, Law J (eds) Shaping Technology / Building Society. MIT Press, Cambridge, pp 205–224 als sogenannte „I-methodology" neu entdeckt und wird heute so bezeichnet. Dort betrifft sie allerdings vorzugsweise die Benutzung, die sich Entwickelnde gemäß ihren eigenen Bedürfnissen vorstellen.*

3 *Suchman, L (1987) Plans and Situated Action. The Problem of Human-Machine Communication. Cambridge University Press, Cambridge*

4 *http://www.zeit.de/digital/internet/2015-07/neuronale-netzwerke-google-inception*

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Differenzierung nicht nach der Haut-
ch der Kopfform, oder aber auch gar
Unterscheidungen.

Online Ad Delivery. CACM 56(5): 44–54

mation and Privacy in the Information Society. Springer, Berlin

8 *http://www.washington.edu/news/2015/04/09/whos-a-ceo-google-image-results-can-shift-gender-biases/*

9 *Freie dezentrale verteilte soziale Netzwerke wie Diaspora oder firendica finanzieren sich durch Spenden, ebenso freie Suchmaschinen, wie DuckDuckGo, Wegtam, DeuSu, MetaGer, Unbubble oder ixquick.eu, die jeweils auch Datenschutzaspekte berücksichtigen*

10 *http://www.spektrum.de/kolumne/die-macht-der-algorithmen/1429137, https://www.theguardian.com/politics/2017/feb/26/robert-mercer-breitbart-war-on-media-steve-bannon-donald-trump-nigel-farage*

11 *http://www.theverge.com/2015/7/1/8880363/google-apologizes-photos-app-tags-two-black-people-gorillas*

12 *https://qz.com/653084/microsofts-disastrous-tay-experiment-shows-the-hidden-dangers-of-ai/*

Rainer Rehak und Jens Wernicke

Die Manipulation von Denken und Handeln ist zur treibenden Kraft der IT-Entwicklung geworden

Jens Wernicke interviewt Rainer Rehak, erstveröffentlicht auf dem Nachrichtenportal *nachdenkseiten.de*

In unserer technologisierten Gesellschaft untergraben unsichtbare Systeme zunehmend die individuelle Selbst- und demokratische Mitbestimmung. Das ist kein Zufall, sondern explizit so gewollt: Die Wirtschaft „erzieht" sich ihre Kunden, der Staat sich seine Bürger. So ist die Manipulation von Denken und Handeln längst zur treibenden Kraft der IT-Entwicklung geworden und verkommt die Technik, die uns das Leben erleichtern sollte, mehr und mehr zur Instanz der totalen Kontrolle über uns. Eine Entwicklung, die die Informatikerinnen und Informatiker für Frieden und gesellschaftliche Verantwortung nicht hinnehmen wollen. „Versteckte Informationstechnik ist nicht diskutierbar", kritisiert Rainer Rehak*, einer der Organisatoren der diesbezüglichen Jahreskonferenz[1], im Interview mit* Jens Wernicke*.*

Jens Wernicke (JW): *Herr Rehak, Sie sind im Vorstand des FIfF, dem Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, und dieses Jahr Mit-Organisator der 32. FIfF-Konferenz, die vom 25. bis 27.11. in Berlin stattfindet und die Gefahren sogenannter „unsichtbarer Systeme" behandeln wird. Als Informatiker und Informatikerinnen, die sich für Frieden engagieren, postulieren Sie im FIfF: „Die Manipulation von Denken und Handeln ist zur treibenden Kraft der IT-Entwicklung geworden." Was bitte sind „unsichtbare Systeme"? Und wer bemüht sich um Kontrolle unseres Denkens und Handelns?*

Rainer Rehak (RR): Das lässt sich am besten anhand eines technischen Beispiels erklären: Früher bestand ein Auto aus Motor, Fahrgestell, Getriebe, Reifen usw. Die komplexesten Dinge waren viel-

leicht der Motor und das Getriebe, aber die waren von der Funktion her eher auch noch verständlich. Der Motor dreht eine Antriebswelle und das Getriebe bringt diese Drehung über die Räder auf die Straße – das Auto fährt. Heutzutage bestehen Autos aus Hunderten von Minicomputern, die den Motor steuern und überwachen, Abgase messen oder die Reifenlage kontrollieren, den Airbag checken und so weiter. Das sind alles hochkomplexe Systeme geworden. Ab 2018 ist es sogar gesetzlich vorgeschrieben, dass neue Autos ein Mobilfunkmodul eingebaut haben müssen.[2]

Tatsächlich sind Autos also fahrende Computer geworden – und das merkt man kaum, was Vor- wie Nachteile hat. Aber damit ist auch erklärbar, wie VW den Diesel-Abgasbetrug durchführen konnte: Die Autosoftware war einfach so „schlau" gebaut, dass sie selbst analysieren konnte, wann das Auto im staatlichen Labor getestet wurde. Dann, und nur dann, hat sie das Auto auf „gesetzeskonform" geschaltet. Damit ist aber der VW kein Einzelfall – solche Entwicklungen betreffen immer mehr Geräte, vom „smarten" Fernseher,[3] der kontinuierlich die Umgebungsgeräusche mitschneidet oder die Sehgewohnheiten aufzeichnet und diese per Internet an seinen Hersteller sendet, über elektronische Fahrkarten, die unsere Wege festhalten[4] bis hin zu raffinierten Methoden programmierter „Selbstzerstörung"[5], die nach einiger Zeit die Nutzer und Nutzerinnen zum Kauf eines neuen Gerätes zwingen. Wir wissen einfach nicht mehr, was diese Dinge wirklich – meist im Hintergrund – tun und für wen sie arbeiten. Darum nennen wir sie „unsichtbare Systeme".

JW: *Das ist durchaus beunruhigend, aber wie beeinflusst das unser Denken und Handeln?*

RR: Deutlich wird der Einfluss dieser „unsichtbaren Systeme", wenn man sich aktuelle Entwicklungen im Internet einmal genauer ansieht. Da bekommt man auf Webseiten etwa individuelle Preise[6] serviert, je nachdem, welche Eigenschaften die Big-Data-Analysen[7] über einen errechnet haben, zum Beispiel ob man aus einer reichen oder armen Gegend die Shop-Seite ansurft oder was ähnliche Konsumenten auch gekauft haben. In der Konsequenz wird einem dann bei Einkäufen beispielsweise immer das nächstteurere Produkt so weit heruntergesetzt, dass man es sich gerade noch leisten kann. Beim Kauf wird dann also jeweils mehr Geld ausgegeben als ursprünglich gewollt. Das heißt, hier ermöglichen es diese Systeme, dass jahrelange Forschung aus Betriebswirtschaft, Informatik und Psychologie direkt auf den nichtsahnenden Kunden angewendet wird. Das funktioniert ziemlich gut, weswegen sich inzwischen auch die Verbraucherzentrale Bundesverband e. V. mit solchen Mechanismen intensiv beschäftigen[8] muss.

Richtig problematisch wird es dann, wenn Menschen Angebote bekommen, die exakt auf sie zugeschnitten sind – sie also nicht nur Informationen enthalten, die beim Empfänger auf Zustimmung stoßen, sondern explizit auch andere Informationen nicht enthalten, die die Person abschrecken würde. Oder sie eben auch ganz explizit für bestimmte Produkte keine Kaufvorschläge bekommen.

JW: *Das verstehe ich nicht. Wieso ist das besonders problematisch?*

RR: Nun, genauso wie man auf diese Art sehr individuell für ein Produkt werben kann, kann man natürlich auch für politische Kandidatinnen und Kandidaten werben. Das Stichwort hier ist „Microtargeting",[9] also das Unterteilen der wahlfähigen Bevölkerung in sehr kleine, teilweise individualisierte Zielgruppen. So kann man einerseits schon gefestigte Personen einfach ignorieren, andererseits sich aber auch speziell auf unentschiedene Wähler stürzen und diese ganz individualisiert ansprechen, beispielsweise explizit jene Positionen eines Kandidaten herausheben, die auch im Interessensbereich des Wählers liegen, oder gezielt Positionen nicht erwähnen, die er kritisch finden würde. Und das bedeutet dann eine gewollt einseitige Informationsweitergabe, abgestimmt auf die individualisierten Datensätze der wählenden Person.

Im Wahlkampf von Obama im Jahre 2008 beruhte die Wahlstrategie unter anderem auf diesem Microtargeting: Es wurden millionenfach Wählerdaten gekauft oder erhoben und auf deren Basis dann individuelle Kontaktstrategien erstellt. Jemand, der also seinem Datensatz nach grün denkt, aber gegen eine allgemeine Krankenversicherung ist und lieber telefoniert als E-Mail zu lesen, bekam daher telefonisch Werbung für Obama, in der wiederum dezidiert von erneuerbaren Energien die Rede war, aber tunlichst nicht von Obamas Versicherungsreformen. Meiner Ansicht nach ist das Manipulation, wenn es wie in diesem Beispiel systematisch betrieben wird. Und wenn es darüber hinaus in solch großem Maßstab erfolgt, finde ich das auch aus demokratischer Sicht hochproblematisch. Man kann an diesem Fall wunderbar sehen, dass diese Technologien bestehende Machtverhältnisse weiter festigen. Unabhängige Kandidaten können sich das nämlich nicht unbedingt leisten.

Gleiches gilt übrigens auch ganz allgemein für Suchergebnisse im Internet. Aktuell wird viel über Facebook und Co. diskutiert, also welche Artikel und Posts wie dargestellt werden, aber der eigentliche Megaplayer Google wird selten erwähnt, dabei erstellt er buchstäblich unsere Sicht auf das Internet. Webseiten, die Google nicht findet, gibt es für uns nicht – so wie wir ein Buch im Regal einer Bibliothek nicht finden, wenn es nicht im Bibliothekskatalog geführt wird. Seiten, die Google besser bewertet und als erste anzeigt, werden nicht nur maßgeblich öfter angeklickt, sondern schon ab Seite 2 sind die Suchergebnisse im Grunde irrelevant. Dahinter steckt eine große unsichtbare Macht.

Das ist auch überhaupt nicht hypothetisch, denn wenn bestimmte Webseiten und Informationen aus dem Google-Index verschwinden sollen, kann man sich mit seiner Begründung einfach direkt an die Suchmaschinenbetreiber wenden.[10] Diese Möglichkeit zu haben ist sicherlich eine gute Idee, denn so lassen sich die vielzitierten bildgewordenen Jugendsünden im Nachhinein unauffindbar machen. Doch damit trifft Google aktuell eine Entscheidung, die eine Abwägung zwischen dem Recht auf Privatheit und dem Interesse der Öffentlichkeit an umfassender Information voraussetzen sollte. Eine Firma fällt demzufolge mitunter rechtsrelevante Entscheidungen nach internen, geheimen Kriterien.

Und selbst wenn alle Informationen im Google-Index zu finden wären, ist die Anzeigereihenfolge immer noch ganz bedeutend. US-amerikanische Wissenschaftler haben – in der Tat! – herausgefunden, dass wir weiter oben stehenden Suchergebnissen unbewusst mehr Wahrheitsgehalt zuschreiben. Das ist sogar dann noch wirksam, wenn zuvor deutlich darauf hingewiesen worden ist.[11]

Drastisch formuliert: Google und Co. bestimmen also maßgeblich, was wir für wichtig und relevant, für glaubwürdig und un-

glaubwürdig halten. Dabei wird sehr deutlich, welche Macht diejenigen haben, die Informationen – vermeintlich in unserem Sinne – vorstrukturieren. Es ist meiner Ansicht nach auch eher zweitrangig, ob sie die Macht aktuell bewusst einsetzen oder nicht – von Softwarefehlern dabei ganz zu schweigen. Allein die Möglichkeit einer solchen Einflussnahme ist Gift für eine Demokratie.

Übrigens sind das auch gar keine abstrakten Gedankenspiele. Suchen Sie mal mit derselben Suchmaschine nach demselben Begriff auf zwei verschiedenen Computern – und Sie werden überrascht sein, wie unterschiedlich die Ergebnisse sind.

JW: *Es ist doch aber, ganz pragmatisch gedacht, andererseits zugleich notwendig, dass die unüberschaubar vielen Informationen auf irgendeine Art und Weise vorsortiert werden, weil sie uns völlig unaufbereitet heillos überfordern würden.*

RR: Natürlich ist das grundsätzlich nützlich und daher auch wünschenswert. Aber es kommt eben darauf an, *wie* solche Prozesse erfolgen und wer sie steuert, mit welchem Ziel und wie nachvollziehbar das geschieht. Diejenigen, die das heute für uns übernehmen, sind ja mächtige internationale Konzerne, die damit ganz eigene Interessen verfolgen – und diese wiederum stehen unseren teilweise durchaus diametral entgegen.

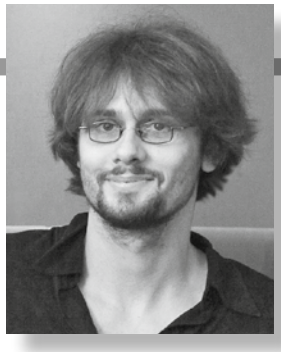
Da sich die NachDenkSeiten viel mit Medienkritik beschäftigen, nehme ich hier mal ein Beispiel aus diesem Bereich: Google und Facebook haben jeweils Funktionen, die den Nutzern und Nutzerinnen zum Beispiel Nachrichten präsentieren. Natürlich müssen diese ausgewählt werden, egal ob von Menschen oder von Algorithmen. Die tatsächlichen Mechanismen, die hier dahinterstehen, sind uns zunächst einmal unbekannt, aber sie sorgen dafür, welche Artikel und Informationen sichtbar oder unsichtbar, weiterverteilt oder vergessen werden. Weder Menschen noch Algorithmen sind dabei übrigens neutral, zweitere tragen ja auch immer die Werte und Wertungen ihrer Software-Entwickler in sich. Dabei kann es sich um eher greifbare Wertungen handeln, wieviel nackte Haut auf Fotos zu sehen sein „darf" zum Beispiel, aber auch um sehr komplexe Einschätzungen, etwa welche politischen Ansichten als „zu extrem" gelten. Und bestimmt werden die Parameter, die diesen Wertungen zu Grunde liegen, letztlich von genau den Medien, deren Nachrichtenauswahl wir lesen.

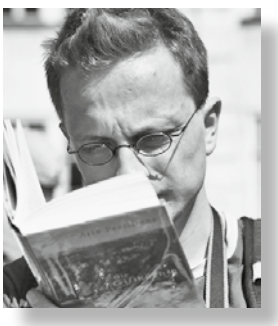
Über die traditionellen Medien wissen wir mittlerweile genug, um in Machtkonzentrationen, wie sie ja Google und Facebook wiederum im digitalen Gefüge verkörpern, immer auch eine Gefahr zu erkennen, weil diese leicht in interessengesteuerte Berichte münden können[12] und leider auch genug dazu geführt haben, dass etwa Kriege erst durch die mediale Steuerung die Akzeptanz der Bevölkerung erhalten haben und so überhaupt nur möglich wurden[13]. Diese Grundprobleme müssen wir gerade bei den Medienakteuren im Internet dringend angehen, denn unregulierte und intransparente Informationstechnik begünstigt noch einmal in ganz anderem Ausmaß das Recht des Stärkeren, seien das „die Märkte" oder politische Kräfte mit „alternativlosen" Lösungen. Aktuell lässt sich sogar eine „Refeudalisierung" des vormals sehr bunten und vielfältigen Internets feststellen. Wenn man sich die weltweiten Nutzungsstatistiken anschaut, besteht das Internet für sehr viele Menschen der westlichen Welt mittlerweile nur noch aus Facebook, Google und YouTube, also hochgradig monopolistischen und vermachteten Webseiten.

JW: *Müsste die folgerichtige Konsequenz also sein, keine Computer mehr für wichtige und persönliche Aktivitäten zu nutzen, besonders als Nachrichtenfilter?*

RR: Natürlich nicht, das wäre ja auch eine merkwürdige Position für einen Informatiker. Aber, Scherz beiseite, die Frage ist doch schon lange nicht mehr, ob wir diese Technik überhaupt nutzen wollen. Es geht darum, wie wir diese Technik gestalten, was sie versteckt oder sogar aktiv verhindert und was sie wiederum offenlegt. Die Frage ist, wie wir dafür sorgen können, dass sie im Dienste der Demokratie und Pluralität wirkt. Für ein besseres Verständnis dieser bisher angesprochenen Probleme und die Entwicklung möglicher Lösungsansätze müssen wir den Blick wieder etwas erweitern.

Rainer Rehak und Jens Wernicke





Rainer Rehak beschäftigt sich seit rund zehn Jahren mit dem Themenfeld *Informatik und Gesellschaft*. Er studierte Informatik und Philosophie in Berlin, Hong Kong und Peking. Während des Studiums arbeitete er am Lehrstuhl für *Informatik in Bildung und Gesellschaft* von Wolfgang Coy. Aktuell lehrt er an der HTW Berlin in den Bereichen *Datenschutz und Datensicherheit, Informatik und Gesellschaft sowie Netzwerke*. In der Wirtschaft ist er als IT-Sicherheits- und Datenschutzberater sowie Unix-Server-Administrator tätig.

Jens Wernicke, Jahrgang 1977, arbeitete lange als Gewerkschaftssekretär und in der Politik. Inzwischen ist er freier Journalist und Geschäftsführer der *Initiative zur Demokratisierung der Meinungsbildung gGmbH*, der Trägergesellschaft des *Rubikon – Magazin für die kritische Masse*. Zuletzt erschien von ihm *Netzwerk der Macht – Bertelsmann. Der medialpolitische Komplex aus Gütersloh* im BdWi-Verlag. In 2017 erscheinen von ihm *Lügen die Medien? Propaganda, Rudeljournalismus und der Kampf um die öffentliche Meinung* im *Westend-Verlag* sowie *Fassadendemokratie und Tiefer Staat* als Mitherausgeber im *Promedia-Verlag*.

Ganz allgemein gesprochen haben wir Menschen ja aus dem Grunde technische Geräte konstruiert, dass wir nicht mehr alles selbst machen und im Detail verstehen müssen. Ich wüsste auch nicht auf Anhieb, wie ich einen Fernseher bauen sollte. Ich möchte einfach, dass er den ersten Sender zeigt, wenn ich die „1" auf der Fernbedienung drücke. Dafür muss ich nichts von Schwingkreisen und Kondensatoren verstehen. Allerdings möchte ich auch nicht, dass die Gerätehersteller ohne mein Wissen Funktionen einbauen, die nur ihnen selbst nutzen, ja, die mir vielleicht sogar schaden, weil sie mich ausspionieren oder meine Handlungsmöglichkeiten unbemerkt einschränken.[14]

Die Snowden-Dokumente haben wunderbar belegt, wie die Geheimdienste der USA technische Geräte präpariert haben, um an Kompromat, also für Erpressungen verwendbares Material über bestimmte wichtige Personen, zu gelangen.[15] Man weiß nie, wann so ein Wissen einmal nützlich sein kann. Das hat ja sogar Angela Merkel selbst zu spüren bekommen, als sie bemerkte, dass sie abgehört wurde.

All diese Dinge haben gemeinsam, dass wir solche hochkomplexen Geräte immer näher in unser persönliches, wirtschaftliches und gesellschaftliches Leben einbinden. Das ist aus meiner Sicht gut so, weil es viele Arbeiten erleichtert. Diese Entwicklung muss aber kritisch begleitet werden, sowohl von Fachleuten in etwa der IT-Branche oder von den Rechtswissenschaften, aber auch von der Gesellschaft als solcher, also auch jedem Einzelnen, damit nicht nur Firmen oder Geheimdienste diese „digitale Welt" gestalten. Daher ist der Untertitel unserer Konferenz auch „Versteckte Informationstechnik ist nicht diskutierbar", denn das ist nicht akzeptabel, wir müssen sie dringend diskutieren.

JW: *Nun geht es bei den Vorträgen auf Ihrer Konferenz unter anderem auch um das Thema „Der Staat als Krimineller" – eine Vorstellung, die vielen sicher abgeht, dass die Obrigkeit demnach aktiv gegen statt für uns arbeitet. Was genau dürfen wir uns unter einem „kriminellen Staat" vorstellen?*

RR: Sie spielen auf unseren Eröffnungsvortrag von Erich Möchel an. Darin wird es um staatliches Hacking gehen, also darum, dass sich Staaten wie selbstverständlich technischer Methoden bedienen, die eigentlich ins Instrumentarium von Kriminellen gehören. Konkret reden wir hier beispielsweise von der Infiltration fremder Computersysteme zum Zwecke der Sabotage von Industrieanlagen, von Energienetzen oder anderen Infrastrukturen. Rechtlich sind diese Aktivitäten auch noch nicht eindeutig interpretiert, denn auf so etwas war das Völkerrecht natürlich nicht direkt vorbereitet; die NATO wiederum hat dazu ebenfalls eine ganz eigene Position, aber das würde hier den Rahmen sprengen.

Jedenfalls haben wir inzwischen mehr oder weniger detaillierte Beschreibungen, was hinter den Kulissen der Staatsmächte passiert, zum Beispiel aus den diversen Dokumenten, die Edward Snowden und andere Whistleblower „befreit" haben. Staaten setzen demzufolge diese hochentwickelte Schadsoftware gegeneinander ein und überbieten sich jeweils mit ihren aggressiven Offensivfähigkeiten. Ein bekanntes Beispiel war das Stuxnet-Virus vor einigen Jahren. Und dabei mischen auch alle großen Staaten gemäß ihren Fähigkeiten mit, egal ob Deutschland, Russland, Israel, die USA oder China.

Es geht also um einen neuartigen, fatalen IT-Rüstungswettlauf, der außer Kontrolle geraten ist und der unsere Geräte im Endeffekt unsicherer macht statt sicherer. Wir alle werden dadurch verwundbarer, durch diesen Machtkampf einiger weniger Akteure. Solche Methoden müssen natürlich dringend gesellschaftlich diskutiert werden, denn sie haben auch schwerwiegende gesellschaftliche Folgen, und genau zu dieser Debatte wollen wir etwas beitragen. Für die Details dazu würde ich Sie allerdings zu Erich Möchels Vortrag einladen, denn auf diesem Gebiet ist er der Experte. Es wird von den Vorträgen übrigens auch einen Live-Stream und danach die Videoaufzeichnung geben.

JW: *Da Sie von Kompromat sprachen … Ich frage mich schon lange, ob der sogenannte „Staatstrojaner", dessen Einsatz sich jedweder demokratischen Kontrolle entzieht, nicht auch dazu genutzt werden kann, Rechner überhaupt erst durch seinen Einsatz so zu manipulieren, dass man dem Besitzer nachfolgend eine Straftat vorwerfen und ihn dafür belangen kann. Was meinen Sie? Ich denke dabei an Folgendes: Wir leben in Zeiten, wo immer klarer wird, dass der NSU offenbar von Dutzenden V-Leuten über Jahre beschützt und abgeschirmt wurde; und in Zeiten, in denen Menschen wie etwa Gustl Mollath, die wichtigen Banken gefährlich werden könnten, mal eben ihrer Bürgerrechte beraubt und psychiatrisiert werden können …*

RR: Grundsätzlich ist der Staatstrojaner im informatischen Sinne erstmal ein normaler Trojaner, der von Behörden eingesetzt werden soll, um Informationen zu sammeln. Ein Trojaner ist eine Software, die beispielsweise über Sicherheitslücken in ein System gelangt und dann dort einprogrammierte Aktivitäten ausführt. Das kann, wie eben erwähnt, eine Informationssuche sein oder aber auch ganz andere Funktionen umfassen. Ich habe vor einiger Zeit selbst zu der grundsätzlichen Beschränkbarkeit solcher Software geforscht und bin zu dem Ergebnis gekommen, dass das, also ihre Beschränkung, effektiv gar nicht möglich ist.[16] Dementsprechend ist gut vorstellbar, dass eine Software wie diese auch bestimmte neue Dateien auf Systemen hinterlegt – dabei ist es auch erst einmal egal, ob das absichtlich, durch Fehler oder aber Dritte erfolgt, die ihre ganz eigenen Interessen verfolgen.

Es gab ja auch schon Viren, die genau das getan haben: beispielsweise Videos von Kindesmisshandlungen auf die Computer von ahnungslosen Personen aufzuspielen,[17] leider sehr folgenreich, wie man sich denken kann. Deswegen ist es so wichtig, dass Computersysteme gut gesichert sind, und zwar gegenüber allen Angreifern.

Aus den USA wissen wir von noch tiefergreifenden Aktivitäten, da erfahren wir von IT-gestützter Spionage der politischen Opposition oder von NSA-Programmen zur Zerstörung der Reputation von prominenten Gegnern der jeweils herrschenden Meinung.[18] Von anderen Ländern wie Russland oder China ist dazu noch wenig bekannt, aber warum sollte es dort anders sein?

Und man muss natürlich auch sehen, dass staatliche Stellen wie die jeweilige Polizei mitunter sicherlich auch gerechtfertigt bestimmte Informationen erlangen sollten, zum Beispiel zur klassischen Verbrechensbekämpfung. Auch darum ist das ein sehr schwieriges Thema, denn ganz ohne polizeiliche Rechtsdurchsetzung geht es ja vielleicht auch nicht in einem Rechtsstaat. Wichtig bleibt dabei, dass die rechtlichen Hürden für solche Methoden

sehr, sehr hoch und klar definiert sein müssen, schließlich haben wir in Deutschland seit dem Urteil des Bundesverfassungsgerichts im Jahre 2008 zur heimlichen Online-Durchsuchung explizit ein „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme". Das interessiert ausländische Geheimdienste natürlich genauso wenig wie sich der BND bei seinen Aktivitäten um die Gesetze anderer Länder schert. Ein Zustand, der schnellstmöglich behoben werden muss.

Aber um auf Ihre Frage zurückzukommen: Natürlich wäre es technisch möglich, inkriminierende Daten auf den Computern von unliebsamen Personen zu platzieren. Ich sehe allerdings ein ganz anderes Problem im Vordergrund. Ich postuliere mal ganz frei, dass jeder Mensch direkt oder indirekt in Aktivitäten verstrickt ist, die – wenn auch nicht unbedingt strafbewehrt – doch mindestens in Teilen der Gesellschaft verpönt oder geächtet sind. Das können kreative Steuermodelle, unübliche Bekanntschaften oder seltene Sexualvorlieben sein. Wenn die staatlichen Stellen und ihre Trojaner nun gut arbeiten, bekommen Sie diese Art von Informationen über alle relevanten Personen heraus und können sich dann bequem aussuchen, wen Sie wie loswerden wollen. Das Perfide daran ist, dass die Dinge, die man dann bei Bedarf an die Öffentlichkeit „gelangen" lässt, alle vollkommen richtig sind und die betroffene Person keine Chance auf Verteidigung hat. Wissen ist Macht!

Und wie bei den zuvor diskutierten Sachverhalten ist auch das keine abstrakte Möglichkeit, sondern bereits heute belegbare Realität. So sammelte[19] die NSA etwa die Erotikvorlieben US-amerikanischer Muslime, natürlich nur für alle Fälle, ohne jede böse Ansicht und so, Sie verstehen schon …

JW: *Gibt es etwas, das Sie „normalen Verbrauchern" wie mir, die wenig IT-Kenntnisse haben, raten? Etwas, womit wir die eigene Manipulierbarkeit ggf. reduzieren können?*

RR: Ein paar Dinge kann man schon tun. Einerseits kann man Software und Internetservices ein wenig so behandeln wie Lebensmittel, die man für sich kaufen würde. Damit meine ich, nicht einfach nur nach der bunten Verpackung einzukaufen, sondern ab und zu einen Blick auf die „Inhaltsstoffe" und „Produktionsbedingungen" zu werfen. Auf die IT-Welt übertragen bedeutet das, nicht nur die Anbieterwerbung zu lesen, sondern auch mal Hintergrundinformationen zur Firma zu recherchieren und mehr über deren Reputation zu erfahren. Wenn das Ergebnis nicht zufriedenstellend ist, kann man nach Alternativen suchen – oder weiß zumindest, woran man eigentlich ist. Und es gibt durchaus Anbieter, die eine kritische Haltung haben, sich fair und transparent ihren Anwendern gegenüber verhalten und offen kommunizieren, wie ihr Geschäftsmodell wirklich funktioniert. Posteo.de für E-Mails oder Uberspace.de für Hosting sind zwei Beispiele dafür. Als Einstieg in die Thematik empfehle ich die Erklärfilme[20] von Alexander Lehmann und das Buch „Die Datenfresser"[21] von Constanze Kurz und Frank Rieger.

Grundsätzlich geht es – wie auch im Medienbereich – vor allem darum, eine kritische Sicht auf IT-Systeme und Internetservices zu entwickeln, diese zu diskutieren und letztlich auf politische Lösungen im Daten- und Verbraucherschutz oder bei der Geheimdienstkontrolle hinzuwirken, damit die digitale Revolution nicht unsere Grundrechte und -freiheiten zerstört, sondern diese sichert.

JW: *Noch ein letztes Wort?*

RR: Wissen Sie, wer kürzlich in einer wesentlichen Datenschutzfrage das mächtige Facebook in die Knie gezwungen hat und damit einen lange bestehenden Vertrag zur Datenweitergabe zwischen Europa und den USA gesprengt hat? Ein österreichischer Jurastudent!

Max Schrems hat letztes Jahr in einer Klage unter Bezugnahme auf die Enthüllungen Edward Snowdens quasi im Alleingang das EU-US-Safe-Harbour-Abkommen zu Fall gebracht, weil er dem Europäischen Gerichtshof schlüssig darlegen konnte, dass die NSA stets und ständig ganz bewusst europäische Datenschutzgesetze missachtet.

Was ich damit sagen will? Wir sind den oben beschriebenen Problemen nicht machtlos ausgeliefert, ganz im Gegenteil. Wir müssen unsere Hausaufgaben machen, dann können wir wirksame öffentliche Diskurse starten, denn die unsichtbaren Systeme können ihre Macht nur entfalten, solange sie unsichtbar bleiben.

JW: *Ich bedanke mich für das Gespräch.*

Vielen Dank auch an Juliane Krüger für ein schlaues Lektorat mit klarem Blick und spitzem Stift.

Links/Verweise

1 *https://www.youtube.com/embed/zDqxA1P4HXg*
2 *http://www.zeit.de/mobilitaet/2015-04/auto-notruf-ecall-verkehrsunfall*
3 *http://www.planet-wissen.de/video-smarte-spione---wie-uns-fernseher-und-co-ueberwachen-100.html*
4 *http://www.golem.de/news/vbb-fahrcard-busse-speichern-seit-mindestens-april-2015-bewegungspunkte-1601-118269.html*
5 *http://www.nachdenkseiten.de/?p=27578*
6 *http://www.tagesspiegel.de/medien/digitale-welt/verbraucherschutz-ein-individueller-preis-fuer-jeden/8353500.html*
7 *https://de.wikipedia.org/wiki/Big_Data*
8 *http://www.vzbv.de/meldung/individuelle-preise-transparent-machen*
9 *https://de.wikipedia.org/wiki/Mikrotargeting*
10 *https://www.verbraucherzentrale.de/recht-auf-vergessen*
11 *https://aeon.co/essays/how-the-internet-flips-elections-and-alters-our-thoughts*
12 *http://www.nachdenkseiten.de/?p=35780*
13 *http://www.nachdenkseiten.de/?p=33071*
14 *https://www.youtube.com/watch?v=OFgQUGTf8BQ*
15 *http://worldnewsdailyreport.com/edward-snowden-the-nsa-steals-and-produces-sex-tapes-to-use-them-for-blackmail/*
16 *https://netzpolitik.org/2012/angezapft-warum-staatstrojaner-mit-gesetzen-nicht-kontrollierbar-und-damit-grundsatzlich-abzulehnen-sind/*
17 *http://www.cbsnews.com/news/viruses-frame-pc-owners-for-child-porn/*
18 *https://theintercept.com/2014/02/24/jtrig-manipulation/*
19 *https://motherboard.vice.com/blog/the-nsa-tracked-porn-habits-to-embarrass-religious-radicals*
20 *https://www.youtube.com/playlist?list=PLQqYRGYVdbVmi3m0kFdLKnHtBwLFEh01N*
21 http://www.fischerverlage.de/buch/die_datenfresser/9783596190331