möglichkeiten der Bundesdatenschutzbeauftragten noch weiter beschneiden. Außerdem sollen öffentliche Stellen, vor allem Sicherheitsstellen, bei Datenschutzverstößen in Zukunft einerseits straffrei sein und sich andererseits selbst kontrollieren: Behörden haben sich an ihren internen Datenschutzbeauftragten zu wenden, sodass Angelegenheiten intern geklärt werden können und nicht mehr nach außen dringen.

Was tun?

Wie lässt sich ein Geheimdienst [illegible] Öffentlichkeit, weil diese nicht [illegible] die existierenden Kontrollgremien [illegible] Arbeit leisten wollen, sind sie in [illegible] und personell unterbesetzt. Die einzige Möglichkeit, das Agieren eines Geheimdienstes zu kontrollieren, ist, ihn mit weniger Geld auszustatten und damit seine Ressourcen und so wiederum seine Möglichkeiten – insbesondere so massenhaft zu überwachen – einzuschränken. Tatsächlich ist aber eine kontinuierliche Aufstockung der Etats zu beobachten. Der Bundeshaushalt hat den Etat für das Bundesamt für Verfassungsschutz (BfV) um 90 Millionen Euro auf 350 Millionen Euro aufgestockt. Für den BND gab es 110 Millionen Euro mehr, womit er bei 830 Millionen steht. Diese nicht unwesentlichen Aufstockungen zeigen recht gut, wohin die Entwicklung geht. Der Wille, Geheimdienste zu beschränken, ist offensichtlich nicht da. Man will ihnen stattdessen die Möglichkeit geben, immer mehr zu tun und immer mehr Daten zu sammeln. Der BND will laut *Süddeutsche Zeitung* einen Teil des Geldes einsetzen, um Verbindungen von Satellitentelefonen abzugreifen, aber auch um Messenger wie *Signal* oder *WhatsApp* zu knacken, die er mit seinen momentanen Ressourcen nicht auswerten kann, weil deren Codes in zu kurzen Abständen aktualisiert werden.

Der NSA-Untersuchungsausschuss hat einige Antworten ans Licht gebracht, viel mehr liegt aber noch im Dunkeln. Das liegt [illegible] r Verfügung stehenden Zeit, an-[illegible] Hindernissen der Aufklärung. Der [illegible] so lange arbeiten, wie die Legisla-[illegible] müssten die Untersuchungen auch [illegible] denn es gibt noch einen großen Aufklärungsbedarf. Dieser lässt sich jedoch nur von der neuen Regierung einfordern, wenn klar weiterhin ein öffentliches Interesse dafür erkennbar ist, wenn es uns allen also nicht egal ist, wir uns empören und uns mit dem BND beschäftigen. Wir müssen verhindern, dass sich die von Snowden aufgedeckten Vorkommnisse wiederholen, alle Erkenntnisse des Ausschusses vergessen werden und wir uns immer wieder neu überraschen lassen. Um die gewonnenen Erkenntnisse und Geschehnisse der NSAUA zu dokumentieren, wurde die Website *werkontrolliert-wen.de* ins Leben gerufen. Dokumente, Hinweise und Fragen sind dort willkommen.

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

FIfF-Konferenz 2016

Transparenz zwischen normativem Anspruch und kultivierter Unsichtbarkeit

Zusammenfassung des Vortrags von Leon Hempel

Beobachtung erfolgt in sozialen Situationen. Sie verlangt Kooperation zwischen den Akteur.innen: der beobachtenden Instanz und den Beobachteten – und dies in Kontexten von erzwungener Überwachung und Kontrolle. Wird die Lebenswelt zunehmend in eine Art Laborsituation verwandelt, in der jede soziale Situation ihrer Analysierbarkeit unterworfen ist, so verflüchtigt sich die Tatsache, dass permanent ins Unbewusste kooperiert wird. An drei unterschiedlichen Praktiken alltäglicher Techniknutzung wird das Problem der Transparenz in diesem Raum kooperativen Zwangs diskutiert.

Transparenz als politischer Begriff

Im Fokus stehen soll im Folgenden die Transparenz, wobei Transparenz hier als politischer Begriff auf die Verteilung von Sichtbarkeit und Unsichtbarkeit hinweist. Mit dem französischen Philosophen Jacques Rancière gesprochen, ist das die ästhetische Dimension von Politik: Es geht um die sinnliche Aufteilung des sozialen Raumes. Dabei agieren politische Institutionen als „Polizei“ und nehmen eine Aufteilung vor, wer sichtbar ist und wer eben auch nicht.

Üblicherweise machen gesellschaftliche Umwälzungen vormals Unsichtbares sichtbar; erst dann kann eigentlich von Politik gesprochen werden. Üblicherweise werden im politischen Prozess die Ränder der Gesellschaft invisibilisiert. Egal ob links oder rechts, die Extreme werden ausgeblendet. Aktuell sehen wir jedoch, wie die Mitte invisibilisiert wird. Dabei werden die Ränder

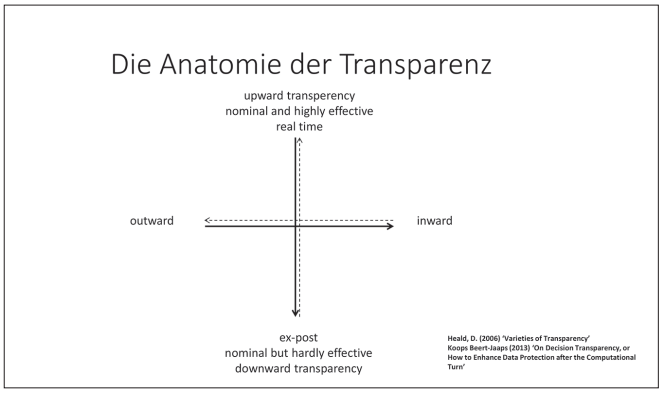
Leon Hempel

übermäßig sichtbar und geben in der vorliegenden Situtation sogar vor, das Ganze zu repräsentieren. Diese Pars-pro-toto-Argumentation ist natürlich ungerecht, denn wer spricht hier legitimerweise für wen?

Transparenz ist also die Frage nach der Verteilung von Sichtbarkeit. Diese Problemstellung hat es insbesondere bei technischen Infrastrukturen immer schon gegeben, aber sie gilt auch insgesamt für die Gesellschaft. David Heald fragt beispielsweise unabhängig von Technik danach, wie der Begriff der Transparenz – oder auch des Sichtbarkeitsregimes – in einer Gesellschaft verstanden werden kann.

Anatomie der Transparenz

Grundsätzlich beschreibt Heald dabei zwei Dimensionen: einerseits die Beziehung zwischen oben und unten, wobei *oben* die mächtigen Akteure wie Staaten, Behörden, große Organisationen wie größere Firmen/Konzerne oder internationale NGOs bezeichnet und *unten* im Gegensatz dazu die schwachen Akteure wie Individuen, kleine Gruppen oder kleine Organisationen beziehungsweise kleinere Firmen. Die horizontale Ebene bildet den Umgang der Akteure mit ihrer Umwelt ab. Innerhalb dieser Anatomie können nun verschiedene Blickrichtungen betrachtet werden.



Anatomie der Transparenz

Zum einen lässt sich so die Aufwärtstransparenz (*upward transparency*) analysieren, also inwiefern die Akteure unten in der Hierarchie nach oben hin sichtbar sind und somit von oben aus beobachtet werden können. Diese Sichtweise ist hochrelevant für den Datenschutz. Dem gegenüber steht die Abwärtstransparenz (*downward transparency*), also inwieweit Akteure oben in der Hierarchie nach unten hin sichtbar sind und daher von unten aus beobachtet werden können. Diese Richtung ist wiederum hochrelevant für die Informationsfreiheit.

Aus soziologischer Sicht ist jedoch eher die horizontale Ebene interessant. Dabei geht es um inwärts oder nach innen gerichtete Transparenz (*inward transparency*) und auswärts oder nach außen gerichtete Transparenz (*outward transparency*). Dabei bedeutet nach innen gerichtete Transparenz, inwiefern das *Außen* für die Organisation selbst sichtbar wird und daher beobachtet werden kann. Diese Richtung deutet an, auf welche Weise Sachverhalte außerhalb der organisationalen Grenzen innerhalb der Organisation „wahrgenommen" und verarbeitet werden können. Dieser Aspekt ist gerade in Bezug auf die Fähigkeiten von Geheimdiensten wie der National Security Agency der USA (NSA) hochinteressant.

Die zweite Richtung der horizontalen Differenzierung ist die nach außen gerichtete Transparenz. Dieser Begriff umfasst, auf welche Weise die Organisation für einen außerorganisationalen Akteur sichtbar und damit beobachtbar ist. Darum geht es immer, wenn Geheimdienste „kontrolliert" werden sollen, denn die Frage lautet ja: Wie gespenstisch ist es denn dort drinnen? Genau das wollen wir wissen. Aus dem Blick methodischer Ethnologie heraus geht man, soweit möglich, auf die fragliche Organisation zu, überschreitet die Grenzen und guckt sie sich dann – wenn möglich – von innen an. Die Kernfrage einer solchen Expedition lautet: Was ist transparent zu machen?

Diese Analyse der Verteilung von Sichtbarkeiten ist nicht nur auf explizit geheime Strukturen anwendbar, sondern lässt sich auch in anderen Bereichen der Gesellschaft sehen. Ein Beispiel ist die sogenannte *Infrastructural Inversion*, also das (Wieder-)Sichtbarmachen einer sonst unsichtbaren Infrastruktur. Bildlich und auch konkret auf eine Stadt bezogen könnte man sagen, die unsichtbare Stadt sorgt dafür, dass die sichtbare Stadt funktioniert. Dort „unten" (Bruno Latour) gibt es eben auch Berufe, Menschen und Orte, die überhaupt erst das gesellschaftliche Leben „oben" ermöglichen und aufrechterhalten, die aber in der Regel unsichtbar sind.

Laut Heald gibt es jedoch noch weitere Ausprägungen von Transparenz, beispielsweise Input/Output-Transparenz, also kann Ein- und Ausgehendes beobachtet werden. Aber auch eine Transparenz des gesamten Prozesses ist denkbar, insofern zusätzlich alle Zwischen- und Verarbeitungsschritte sichtbar sind. Weiterhin kann man Echtzeittransparenz und retrospektive Transparenz unterscheiden, wobei ersteres sich immer auf den aktuellen Status bezieht und letzteres nur auf vergangene Ereignisse. Zuletzt lässt sich zudem die gewünschte, nominelle Forderung nach Transparenz von der effektiven, tatsächlich vorhandenen Transparenz unterscheiden.

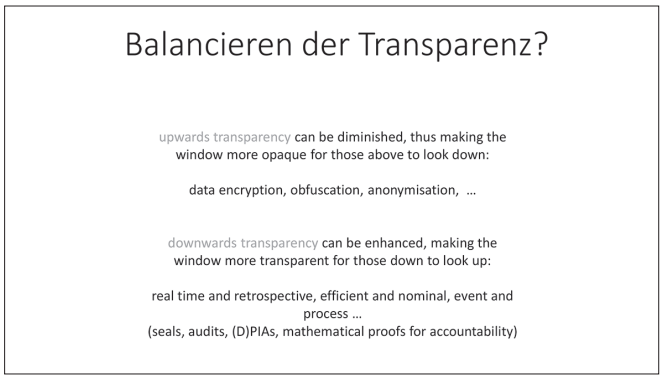
Massenhafte (In-)Transparenz und der Datenschutz

Von E. J. Koops (Universität Tilburg) werden diese Konzepte aktuell auf den Datenschutz oder genauer: auf dessen Verstöße angewendet, gerade in ihrer Ausprägung als Massenüberwachung. Mit dem obigen Theoriegebäude lässt sich die Situation wie folgt beschreiben: Bei staatlicher Massenüberwachung ist die *upward transparency* nominell und sehr effektiv, sie hat nicht nur das Einzelereignis, sondern den ganzen Prozess im Blick. Sie erfolgt in Echtzeit und ist auch retrospektiv wirksam. Möglich ist damit sowohl Strafverfolgung im Speziellen als auch Internetbeobachtung im Allgemeinen. Diese Art von Aufwärtstransparenz ist quasi *Full-Spectrum*.

Bei der entsprechenden *downward transparency* hingegen, also der Sichtbarkeit staatlichen Handelns für beispielsweise das Individuum, muss festgestellt werden, dass die Transparenz vollständig retrospektiv und größtenteils eher nominell, aber nicht effektiv abläuft.

Balance der Transparenz?

Aus dieser Analyse ergibt sich, dass eine Balance der Transparenzen nötig ist. Einer der Lösungswege dafür wäre die Stärkung – oder Modernisierung – des Datenschutzes. Um die Fähigkeiten anzugleichen, müssten gleichermaßen eine Hemmung von *upward transparency* und eine Förderung von *downward transparency* in Angriff genommen werden. Ersteres kann durch breitflächige Nutzung von Verschlüsselung oder engeren Datenschutzregelungen bewerkstelligt werden. Letztere Aufgabe kann durch Informationsfreiheitsrechte, externe Audits, glaubwürdige Siegel oder andersartige „Beweise" angegangen werden. Ziel sollten auch für die *downward transparency* letztendlich die Eigenschaften echtzeitlich, retrospektiv, nominal, effizient, event- und prozessfähig sein.



Balance der Transparenz

Natürlich haben die verschiedenen Akteure ungleiche Mittel im Kampf um die Sichtbarkeit zur Verfügung; ist ein Ausgleich also überhaupt denkbar? Am Beispiel des Attributionsproblems lässt sich diese Ungleichheit gut verdeutlichen: Das Attributionsproblem meint hier die Nichtidentifizierbarkeit derer, die sich im Netz bewegen und durch das Netz agieren. Das ist insbesondere bei *Cyberwar* und *Cybercrime* wichtig. Der US-Terror-Experte und ehemalige Sonderberater für Cybersecurity, Informationssicherheit und Cyberwar Richard Clarke sagte im Jahre 2010: „Das Attributionsproblem ist grundsätzlich gelöst." Wenn der Ursprung auch nicht sofort gefunden werde, so könne danach die Forensik bemüht werden und zur Not und bei Bedarf könne die NSA auch alles hacken. „*The NSA can do it*", das behauptet sie auch selbst und damit steht sie potent da, denn als Geheimdienst muss sie nichts groß begründen.

Andererseits erwiderte der IT-Sicherheitsexperte und bekannte Befürworter der Anonymisierungssoftware *Tor*[1], dass die vorwiegenden staatlichen Ziele sicherlich die Nichtidentifizierbarkeit staatlichen Handelns und die Totalüberwachung der Bevölkerung seien, aber so einfach umsetzen lässt sich das eben nicht, ja vielleicht niemals – siehe *Tor* und ähnliche Software, die ja auch von Polizeien und dem Bundesnachrichtendienst (BND) selbst benutzt werden, weil sie so gut funktionieren. Gibt es also vielleicht doch eine Art Gleichstand?

Der NSA-Untersuchungsausschuss des Bundestages ist ja längst zu einem NSA- und BND-Untersuchungsausschuss geworden (siehe Vortrag von Anna Biselli in diesem Heft), wodurch wir so einiges über die internen Vorgänge und Ängste erfuhren. Wir wissen jetzt, dass die drakonischen Strafen in Bezug auf „unerwünschte Computernutzung", von CFAA (Computer Fraud and Abuse Act, USA) bis StGB 202c (sogenannter *Hackerparagraph*, Deutschland) aus dieser Furcht heraus geboren sind. Diese Überreaktion hat dann sogar den US-amerikanischen Wissensfreiheitsaktivisten Aaron Schwartz[2] in den Tod getrieben.

Ungleiche Mittel

Diese vehemente Kriminalisierung unerwünschten Verhaltens findet statt, auch wenn wir – mit Jacob Appelbaums Worten – nach wie vor „experimentell im Netz unterwegs sind". Diese Schieflagen verdeutlichen die tatsächliche Sichtbarkeitsverteilung.

Transparenzparadoxon bei Infrastrukturen

Kommen wir nun zu einer gänzlich anderen Sichtweise auf den Transparenzbegriff. Betrachten wir dazu einmal das Transparenzparadoxon bei Infrastrukturen, denn die vorherige Sicht ist vielleicht zu einfach gedacht. Bestimmte Dinge wollen wir ja auch unsichtbar werden lassen, damit sichtbar wird, was dahinter liegt. Es werden also Objekte, Prozesse und Organisationen invisibilisiert, um etwas anderes sichtbar zu machen, das vorher verdeckt war. Dieses Verständnis gehört demnach in die normative Kategorie.

Setzen wir also gegen den politischen Transparenzbegriff eine zweite normative Ebene: die praktische Transparenz. Susan Leigh Star nannte dies eine *Transparenz des Nutzens*, nachzulesen in ihrem Aufsatz *Ethnography of infrastructure*. So gemeint, wird ein Wasserhahn transparent genutzt, denn er wird während seines Gebrauchs nicht verstanden oder reflektiert. Verwendete Technik wird eben dann zu Infrastruktur, wenn sie bei ihrer Verwendung nicht immer wieder neu zusammengesetzt oder durchdrungen werden muss, sondern transparent und damit unsichtbar wird. Das hat auch mit Routine zu tun, derartige Technik nennen wir *invisibly support tasks*. Nur im Fehlerfall wird Infrastruktur als solche sichtbar, aber auch der Fehlerbegriff basiert auf Zuschreibungen. In der Regel will und soll sie jedoch unsichtbar sein.

Bekannt ist diese Problematik hierzulande auch durch die Diskussion um die Sichtbarkeit von Windkraftanlagen und oberirdischen Stromleitungen. Schnell geht es dann um die „Verschandelung" von Landschaften. Unabhängig von der inhaltlichen Diskussion um diese Themen führt diese Art von Widerständen zu „kultivierter Unsichtbarkeit". In diesem Beispiel hieße das, die „Landschaft bleibt schön", z. B. durch Erdkabel. Kultivierte Unsichtbarkeit bedeutet an anderer Stelle jedoch auch, dass Unter-

nehmen sich bei Fehlern nicht rechtfertigen müssen, wenn die Probleme in unbeobachtbaren Bereichen auftreten.

Gerade die Informationstechnik ist ein Paradebeispiel für die Kultivierung der Unsichtbarkeit: Alles ist verborgen und in der Regel nur streng kontrolliert durch das *human-computer-interface* nutz- und erfahrbar. Diese Eigenschaft offenbart sich erst dann, wenn nicht alles wie erwartet funktioniert. Sehr schön kann das bei der „*mother of all demos*" (1968) nachvollzogen werden: Douglas Engelbart präsentiert darin eine der überhaupt ersten graphischen Benutzeroberflächen inklusive Computermaus, und plötzlich gibt es Fehler im Programm und es reagiert anders als erwartet. Engelbart ist absolut hilflos und fragt hilfesuchend nach einem Programmierer. Mit einem „*I haven't warmed up yet*", in etwa „ich bin noch nicht in Übung", macht er sich letztendlich zum prototypischen sich selbst für die Fehler der Maschine anklagenden User. Es braucht offensichtlich Übung, bis derartige Technik transparent nutzbar ist, so zumindest die Fehlerrationalisierung.

Verschwundene Technik

Doch die Transparenz der Technik reicht noch viel weiter. Nehmen wir das Beispiel *Google Glass*, bei dessen Funktionsdemonstrationen der Blick stets auf „schöne" Objekte gerichtet war, z. B. auf ein Baby. Der eigene Blick soll ganz natürlich sein, die Technik als Technik soll nicht mehr in den Blick kommen. Auch in der Werbung sieht man das *Glass*-Gerät niemals. Wir sprechen also von Technisierung, aber meinen eigentlich, die Visibilität der Technik herauszunehmen.

Favorit bei der Kultivierung der Unsichtbarkeit ist sicherlich Mark Weiser, der um die 1990er-Jahre am Forschungszentrum Xerox PARC forschte. Er reaktivierte den bürgerlich-romantischen Traum der „Waldwelt" für eine erstrebenswerte Mensch-Maschine-Interaktion. Dabei sollten sich die Maschinen dem Menschen anpassen, nicht andersherum. Dies vorausgesetzt, sei die Computernutzung nach Weiser stets so erfrischend wie ein Waldspaziergang. Wenn man so will, ist Weiser ein Propagandist des Erdkabels der Computerisierung. Er wünscht sich folglich, die Sichtbarkeit von Technik komplett aufzuheben – es ist dies der Wunsch nach Ganzheitlichkeit diesseits aller dinglichen Entfremdung durch Technik, nach einer selig-träumerischen unbewussten Techniknutzung.

Beobachtung im technisch Unbewussten

Kommen wir genau vor diesem Hintergrund wieder zurück zur Beobachtung. Eine wesentliche Folge des Versteckens technischer Mechanismen ist die Entstehung des technisch Unbewussten. Dieser Begriff kann gut durch ein Gegenbild erklärt werden: Jede Person kennt Kontrollen am Flughafen. In diesen Situationen ist explizit Kooperation für Kontrolle und Beobachtung nötig; es wird erwartet und vorausgesetzt, dass alle Reisenden mitmachen und sich beispielsweise für eine Abtastung richtig hinstellen oder stillhalten.

Ganz anders verhält es sich bei eher transparenter Beobachtung wie der Videoüberwachung mit Gesichtserkennung. Je transparenter Beobachtung wird, umso mehr bedarf es der Kontrolle des Raumes selbst. Es braucht „Mausefallen", damit Menschen unbewusst kooperieren. Bei Videoüberwachung wären das beispielsweise Rolltreppen, durch die Kooperation „erzwungen" wird, denn fahrend innerhalb eines definierten Bereichs kann das Gesicht sehr gut erfasst werden.

Um diese Art von Beobachtung weiterzutreiben, ist eine „*McDonaldisierung*" des Raumes nötig. Er muss vorhersehbar, berechenbar, standardisiert und kontrollierbar sein. Auch vielfältige Kontexte müssen beachtet werden, um die Nutzenden ohne ihre bewusste Mitarbeit beobachtbar zu machen. Dabei werden die Möglichkeiten der Raumbeeinflussung immer weitreichender, vom taktilen Internet bis zu cyber-physischen Systemen. In dieser kontrollierten Umgebung kann nun auch der Sicherheitsabstand zwischen Mensch und Maschine aufgehoben werden.

Steering asleep

Es lässt sich also recht treffend behaupten, wir bewegten uns schlafend oder schlafwandelnd durch die informationstechnische Infrastruktur. Doch diese Unwissenheit wird aufgrund des dadurch bedingen Kontrollverlustes der User als größte Schwachstelle dargestellt. Das technische Design wird in Folge ein paranoides, angstgetriebenes. Systeme dieser Art werden, wo es möglich ist, abgeschlossen und dann auch geschlossen gehalten. Frederick P. Brooks formulierte das in positiver Weise als „*konzeptionelle Integrität* angesichts der *Wilderness* der praktischen Welt". Im Softwaredesign sollten demnach Entwurfsentscheidungen immer konsequent umgesetzt werden, auch wenn das möglicherweise unzulässige Vereinfachungen und Verzerrungen nach sich zieht. Im Zweifel sollte also lieber einfache, aber nutzbare Software entstehen.

Diesem Ansatz entgegen steht die Sichtweise des *Maintenance and Repair*: Oberflächen werden absichtlich durchbrochen, denn das Hineinschlagen in die und das Öffnen der Technik ist nötig, um sie letztendlich besser zu machen. Dieser eher emanzipative Ansatz findet seine Ausprägung wesentlich in der Hacker- und Maker-Kultur.

Leon Hempel

Leon Hempel leitet den Forschungsbereich *Sicherheit – Risiko – Privatheit* am Zentrum für Technik und Gesellschaft (ZTG) der Technischen Universität Berlin. Er beschäftigt sich u. a. mit Beobachtungstechnologien und ihrer Geschichte, mit der Relation von Sichtbarkeit und Unsichtbarkeit im Kontext vergleichender Infrastrukturforschung sowie mit dem Thema Sicherheit und Zeit(-Bindung). Er hat zudem eine Gastprofessur für interdisziplinäre Lehre an der Technischen Universität Darmstadt inne.

Transparenz und Verantwortungsverlust

Eine weitere Anwendung des Transparenzbegriffs wurde von Barbara van Schewick entwickelt. Sie betrachtet die Transparenzebenen bezüglich des End-to-End-Prinzips des Internets. Vereinfacht gesprochen: Um Anwendungen über Netzverbindungen miteinander kommunizieren zu lassen und die Infrastruktur z. B. nur mit dem Transport zu betrauen, sind die technischen Netzwerkfunktionen des Internets in Schichten aufgeteilt. Allgemeine Funktionen wie Signalaushandlung oder Routing sind in den unteren Schichten des OSI-Netzwerk-Modells angesiedelt. Spezielle Anwendungsfunktionen sind wiederum in den oberen Schichten verortet. Van Schewick weist in ihren Arbeiten nach, dass dieses im Kern arbeitsteilige Prinzip zu dynamischer Innovation führt. Oder – um mit Bernard Stiegler zu sprechen – diese Struktur produziert eine Architektur der permanenten Innovation.

Arbeitsteilung bedeutet aber auch kognitive Unterscheidung zwischen den Agierenden des Internets. Egal auf welcher Schicht sie aktiv sind, die Verantwortlichkeiten sind – gleichlaufend zur Arbeitsteilung – ebenso verteilt. Das Resultat ist Verantwortungsdiffusion bis hin zu ihrem Verlust. Auch um diesem zu begegnen, forderte Barbara van Schewick, dass die tieferen Schichten in staatliche/öffentliche Hand gehören. Arbeitsteiligkeit ist im Grunde ein ökonomisches Prinzip.

Wir betrachteten bislang die politische Normativität des Transparenzbegriffs, die praktische Normativität des Transparenzbegriffs und zuletzt auch die ökonomische Normativität des Transparenzbegriffs. Mittlerweile ist die Beschreibung des Netzes auch nicht mehr ausschließlich in Begriffen der Technik möglich, sondern erfolgt besser primär in ökonomischen Organisationseinheiten.

Abschluss

Für alle angesprochenen Problemfelder kann hier freilich keine Lösung angeboten werden. Vielleicht aber sollte ein ganz neues Internet erdacht werden, das im Vorhinein auf bestimmte Eigenschaften überprüft wird. Sicherlich sind die nötigen theoretischen, technischen und praktischen Grundlagen dafür noch nicht hinreichend gelegt, denn man kann nur Systeme verifizieren, von denen man genau weiß, was sie tun sollen. An diese braucht es also zunächst klare Anforderungen, und auch die können wiederum Fehler enthalten. Eine ausreichend genaue Analyse ist schon bei ganz simplen SCADA-Systemen schwierig, ganz zu schweigen von komplexeren Anforderungen wie beim E-Voting. Dennoch müssen wir das angehen. Diese Überlegungen sollten jedenfalls nicht erst im Vollbetrieb angestellt werden, weil es dann für grundlegende Änderungen zu spät ist. Als nichttechnische Person kann ich daher vielleicht nur eine Bitte an die Technikerinnen und Techniker richten: Baut bitte ein neues Netz!

Zumindest muss aber die technische Featuritis zurückgefahren werden, um überschaubarere und damit nutzbarere Systeme zu schaffen.

Anmerkungen

1 *https://www.torproject.org*

2 *https://www.theguardian.com/commentisfree/2015/feb/07/aaron-swartz-suicide-internets-own-boy*

FIfF-Konferenz 2016

Sozial gerechte Algorithmen? Problematiken, theoretische Konzepte und Perspektiven der Geschlechterforschung

Zusammenfassung des Vortrags von Corinna Bath

Dass Algorithmen häufig als neutral gelten, setzt voraus, sie zunächst von ihren jeweiligen sozialen Kontexten der Entstehung und Wirkung abzutrennen. Im Vortrag möchte ich – aus der Tradition der Geschlechterforschung heraus – Unsichtbares sichtbarer machen und damit Problematiken dieses Neutralisierungstricks verdeutlichen. Im Fokus stehen Verzerrungen, die als sexistisch, rassistisch oder anderweitig ungerecht bezeichnet werden können. Zugleich geht es mir darum, ein performatives Verständnis von Algorithmen vorzustellen, welches diese Kontextualisierungen theoretisch zu fassen sucht. Ziel ist es, damit Möglichkeiten der Analyse ungerechter und der Gestaltung sozial gerechterer Algorithmen zu eröffnen.

Immer wieder wird Corinna Bath von Studierenden gefragt, warum sich die Informatik mit *Gender Studies* befasst, weil man in der Informatik doch lediglich formale Spezifikationen abarbeitet. Bath hält das jedoch für ein sehr unzutreffendes Berufsverständnis – bereits 1993 hatte sie mit Dirk Siefkes in einer Arbeitsgruppe intensiv diese Fragen diskutiert und ist zu dem Schluss gekommen: „Man kann die Informatik nicht als etwas Abgeschlossenes verstehen, das nur im technischen Raum und ohne die sozialen Kontexte steht." Nicht nur für Studierende der Informatik scheint diese Sichtweise jedoch als unnötig zu gelten – auch Professor.innen sprechen bei Forschungsprojekten noch immer von „neutraler Technik", die von ihren sozialen Kontexten losgelöst sei.

Als Bath über sexistische Algorithmen schrieb, bekam sie im Februar 2016 in der öffentlichen Debatte starken Gegenwind: Hadmut Danisch wollte ihr diesen Ansatz prinzipiell ausreden und veröffentlichte im *Focus* einen Artikel, mit dem er die „Neutralität der Algorithmen" zu retten versuchte: