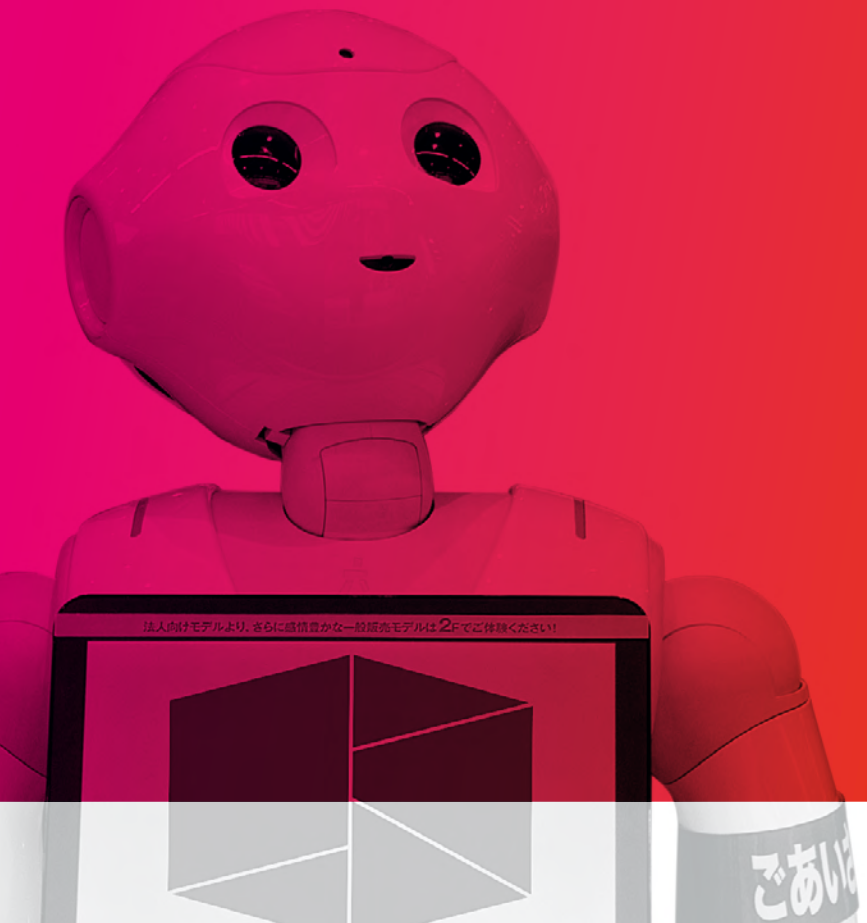
smarte worte

// DAS KRITISCHE LEXIKON
DER DIGITALISIERUNG



ROSA LUXEMBURG STIFTUNG

// UNBOXING SMARTE WORTE

Im Zeitalter von Web 2.0 ist das Erstellen von Produktrezensionen durch Laien und semiprofessionelle Rezensierende ein boomendes Genre geworden. Auf Videoplattformen wie YouTube stellen diese Videos eine äußerst beliebte Rubrik dar, sogenannte Unboxing-, also Auspack-Videos, in denen sich Menschen dabei filmen, wie sie neue Produkte auspacken und in Augenschein nehmen. Vermutlich 2006 wurde das erste dieser Videos erstellt. Wollte man sich alle Unboxing-Videos anschauen, dann wäre man mehrere Jahre damit beschäftigt. Gleichzeitig werden viele dieser Videos millionenfach angesehen, vor allem wenn es um die aktuellen Technikneuheiten geht, aber auch Spielzeug und Kosmetik sind beliebt. (Über die Grenzen des Genres und abgegrenzte Subgenres wird unter ExpertInnen gestritten.)
Unboxing ist ein Massenphänomen, und der anhaltende Boom dieser Videos ist nicht zuletzt darauf zurückzuführen, dass sich mit ihnen auch Geld verdienen lässt. Das geschieht meist über eingeblendete Werbung oder Sponsoring. Die Zuschauenden versprechen sich von den Videos, im Gegensatz zur offiziellen Produktwerbung, vor allem eine unabhängige Meinung zu dem jeweiligen Produkt. Auf einige scheint aber auch der Moment des stellvertretenden Auspackens, vom ersten Rascheln des Kartons, bis zum letzten Knistern der Folie, an sich einen besonderen Reiz auszuüben. Technisch und ästhetisch sind die meisten Videos sehr reduziert und gleichförmig.

Für eine Konferenz der Rosa-Luxemburg-Stiftung im Dezember 2016 haben wir den Begriff des «Unboxing» entwendet und als kritischen Gegenbegriff zu aktuellen Entwicklungen der Digitalisierung und ihren demokratischen Defiziten eingeführt. Denn immer weitere Bereiche unseres Alltags und unseres öffentlichen Lebens werden von intransparenten und nicht mehr nachvollziehbaren technischen Systemen beeinflusst oder gar gesteuert. Der US-amerikanische Juraprofessor Frank Pasquale spricht in diesem Zusammenhang von einer Black-Box-Gesellschaft. Angesichts der zu befürchtenden und schon jetzt zu beobachtenden Entdemokratisierungstendenzen ist es unserer Ansicht nach dringend an der Zeit für ein kritisches Auspacken dieser algorithmischen Systeme und der dahinterstehenden Geschäftsmodelle des Überwachungskapitalismus.
Hierbei sollten wir auch die Begriffe hinterfragen, die wir verwenden: Die Debatten zu Themen der Digitalisierung operieren vielfach mit Wörtern, deren Herkunft und Bedeutung vielen unklar sind. Zahreiche Begriffe sind der Marketingsprache entnommen oder haben sich mit zunehmender Kommerzialisierung des Internets in ihrer Bedeutung gewandelt, gesellschaftspolitische Dimensionen werden oft ausgeblendet. Um diese «smarten Worte» aus ihrem verschlossenen Kasten zu holen, haben sich die Rosa-Luxemburg-Stiftung und die Tageszeitung *neues deutschland,* gemeinsam mit einem Kreis von weiteren AutorInnen darangemacht, den Deckel ein erstes Stück zu öffnen. Mithilfe des vorliegenden Lexikons wollen wir fragen: Wofür stehen einige der zentralen Begriffe, woher kommen sie, wo verstellen sie unseren Blick, und sollten wir die Sachverhalte, die sie beschreiben, nicht anders benennen, nicht zuletzt um sie emanzipativer angehen zu können?

Das vollständige Lexikon gibt es natürlich auch online unter:
http://dasnd.de/smarteworte, dort mit einem Vorwort von Susanne Lang.

Wir bedanken uns ganz herzlich für die Mitwirkung an diesem Lexikon bei:
Anne Roth, Chris Piallat, Christian Meyer, Constanze Kurz, Dagmar Fink, Felix Knoke, Felix Stalder, Halina Wawzyniak, Jörg Braun, Katalin Gennburg, Marie Kochsiek, Markus Euskirchen, Norbert Schepers, Richard Heigl, Sebastian Strube, Simon Schaupp, Simon Weiß, Stefan Enke, Susanne Lang, Timo Daum.

Die HerausgeberInnen:
Martha Dörfler, Sabine Nuss, Patrick Stary (Rosa-Luxemburg-Stiftung)
Tom Strohschneider (neues deutschland)

// INHALT

// ALGORITHMEN
// AUTOMATISIERUNG DER ARBEIT

// ALGORITHMEN

Man hat sie die «neue Weltsprache» genannt und als einen der Rohstoffe des vierten Maschinenzeitalters bezeichnet: Algorithmen. In einem engeren Sinne versteht man darunter Berechnungsverfahren, mit denen mathematische Fragen gelöst werden können. Breiter gefasst ist ein Algorithmus eine «systematische, logische Regel oder Vorgehensweise, die zur Lösung eines vorliegenden Problems führt» (Werner Stangl). Dabei geht es nicht darum, einmalig eine Lösung zu finden, sondern eine für immer. Ein Navigationsgerät soll in jeder Stadt den besten Weg von A nach B finden – das Prinzip soll in jedem Einzelfall funktionieren.

Die politische und ökonomische Bedeutung von Algorithmen ist heute enorm: Sie steuern Fabriken, kaufen an der Börse oder entscheiden, welche Nachrichten einem bei Google oder in den sozialen Medien angezeigt werden und welche eben nicht. Fast überall werden große Datenmengen in staatlicher oder privatkapitalistischer Regie per Algorithmen ausgewertet und so etwa zum Predictive Policing, zur Massenüberwachung, zur Produktionsplanung oder zur Organisation des öffentlichen Nahverkehrs eingesetzt.

Damit können Algorithmen beziehungsweise ihre Macher auch Kontrolle über Menschen und eine unpersönliche Herrschaft ausüben, den privaten Einkauf oder die Wahlentscheidung beeinflussen. Algorithmen können – zum Beispiel in den USA – urheberrechtlich geschützt werden. Als entscheidende Betriebsgeheimnisse stellen sie Produktionsmittel dar, über die eigentumsrechtlich zu verfügen einen Faktor von Macht bilden kann.

Algorithmische Entscheidungen sind häufig für diejenigen, die von ihnen betroffen sind, nicht nachvollziehbar, der Code nicht einsehbar. Dies müsse aber nicht so sein, sagt zum Beispiel

die Gruppe «Algorithm Watch». Demokratische Gesellschaften hätten die Pflicht eine Nachvollziehbarkeit herzustellen, dies solle durch eine Kombination aus Technologien, Regulierung und geeigneten Aufsichtsinstitutionen passieren.

Eine häufig diskutierte Frage ist, wie Algorithmen in ethisch schwierigen Situationen entscheiden sollen. Was soll das selbstfahrende Auto in einer unausweichlichen Unfallsituation machen: Soll es seine Insassen, eine Menschengruppe auf dem Zebrastreifen oder ein Kind am Straßenrand gefährden? Und wer trägt in einem solchen Fall die Verantwortung – die Firma, die einen Algorithmus einsetzt, die Personen, die ihn nutzen, oder die ProgrammiererInnen?

Algorithmen werden auch beim maschinellen Lernen, bekannt unter den Begriffen künstliche Intelligenz oder neuronale Netze, eingesetzt. Hier werden Strukturen erkannt und Rückschlüsse aus vorherigen Ergebnissen gezogen. Lösungen werden bewertet und durch weiteres Probieren verbessert, der Algorithmus trainiert sich selbst. Das kann praktisch sein, wenn es darum geht, Katzenbilder oder gar Krebssymptome zu finden, aber problematisch, wenn es um die Bewertung von Menschen geht. Deutet die Stimmlage des neuen Bewerbers auf eine psychische Erkrankung hin, die Wortwahl auf terroristische Aktivitäten?

Algorithmen sind nicht neutral. Sie werden von Menschen geschrieben, sollen einem von Menschen bestimmten Zweck dienen und verwenden Daten, die in ihrer Struktur von Menschen ausgewählt wurden. Heute sind es vor allem junge, weiße Männer, die Programme schreiben, sie sehen Aufgaben entsprechend aus ihrer Perspektive und lösen sie im Sinne ihres Auftraggebers. Wird der Algorithmus mit Daten gefüttert, die beispielsweise rassistische Strukturen abbilden, kann er nicht anders, als diese Strukturen zu reproduzieren.

Algorithmen sind Ausdruck der Verfassung einer Gesellschaft, die sie einsetzt. Algorithmen können auch sehr hilfreich sein, zum Beispiel die Verfügbarkeit disponibler Zeit erhöhen, weil Maschinen Dinge erledigen, die bisher Menschen gemacht haben. Es ist nicht der Algorithmus das Problem, sondern jene sind es, die ihn auf bestimmte Weise interessegeleitet zum Einsatz bringen.

(Martha Dörfler, Tom Strohschneider)

// ZUM WEITERLESEN

[1] Gierow, Hauke: IBM will Flüchtlinge von Terroristen unterscheiden können, golem.de, 23.2.2016, unter: https://is.gd/Qg7aa4.

[2] AlgorithmWatch arbeitet zum Thema Algorithmic Decision Making, unter: http://algorithmwatch.org/.

[3] Ceuter, Jürgen: Brauchen wir einen Leinenzwang für Algorithmen?, Wired.de, 11.6.2015, unter: https://is.gd/T5CXBw.

// AUTOMATISIERUNG DER ARBEIT

Historisch wurde unter dem Begriff Automatisierung der Arbeit insbesondere auf Fabrikarbeit abgezielt. Unter dem Schlagwort Industrie 4.0 spielt diese nach wie vor eine große Rolle, doch auch komplexe Tätigkeiten und kognitive Fähigkeiten werden an Software übertragen. Algorithmen schreiben Zeitungsartikel, errechnen Muster zur Verbrechensbekämpfung oder fahren Auto. Im Griechischen bedeutet das Wort *automatos* in etwa, von selbst bewegend oder aus eigenem Willen machend. Auch Kaffeevollautomaten oder Bankautomaten sind letztendlich Ausdruck der Automatisierung von Arbeit, zeigen aber, dass es längst nicht nur um Fabrikarbeit geht. Der technisch-wissenschaftliche Fortschritt, verstanden als Produktivkraftentwicklung, trieb schon Marx und Engels um, die die moderne Fabrik als «automatisches System der Maschinerie» beschrieben.

Für die Automatisierung der Arbeit (oder «Automation») gibt es ein ökonomisches und ein herrschaftstheoretisches Motiv. Ersteres besteht darin, den Preis der Arbeit zu senken, Letzteres darin, möglichen Widerstand der ArbeiterInnen zu erschweren. Durch Automation gehen die Fähigkeiten auf die Maschinen über und liegen dann weniger bei den sie bedienenden ArbeiterInnen. Dies motivierte im frühen 19. Jahrhundert die Ludditen, die sogenannten Maschinenstürmer, Fabriken und Anlagen anzugreifen, als deren Arbeitsplätze durch den Einsatz von automatischen Webstühlen bedroht waren. Technologische Arbeitslosigkeit treibt auch heute viele Lohnabhängige um, beispielsweise in der Diskussion zu Industrie 4.0.

Man darf sich aber nicht nur auf die destruktive Seite konzentrieren, um das Phänomen und seinen Siegeszug zu verstehen. Dass es auch anders gehen kann, zeigen Beispiele, wie durch mehr Automation auch mehr Autonomie der Arbeit entsteht. Denn menschliche Arbeit wird paradoxerweise wichtiger, je weniger sie eingesetzt wird. Fehlerbehebung, Kreativität und situatives Wissen sind nach wie vor schwer an Maschinen zu delegieren. Automation kann so, zumindest für einzelne, höhere Qualifikation nach sich ziehen. Daraus ergeben sich mitunter Forderungen nach mehr Kontrolle über den Produktionsprozess und weitgehende Mitsprache über Unternehmensziele. Wenn aber die Möglichkeiten gegeben sind, dass die ArbeiterInnen über die Produktion und die Wirtschaft selbst bestimmen, geraten sie in Konflikt mit kapitalistischen Strukturen. Hier zeigt sich der Widerspruch von Automation unter kapitalistischen Verhältnissen: Einerseits fällt immer weniger Arbeit an, gleichzeitig aber kann nur die ausgebeutete lebendige Arbeit Profit garantieren. Automatisierung ist somit Mittel der Profitsteigerung, aber gleichzeitig Bedingung der Überwindung der Profitlogik, denn Emanzipation setzt ein gewisses Niveau der Produktivkräfte voraus. Durch Automatisierung gibt es potenziell mehr (arbeits-)freie Zeit, Muße und die Möglichkeit zur Selbstbestimmung.

Automation auf Technisches zu reduzieren unterschlägt, dass Technik generell immer Element der gesellschaftlichen

Verhältnisse ist und die betriebliche und gesellschaftliche Entwicklung sowie deren staatliche Regulation mitzubedenken sind. Denn fest steht, dass vollständige Automatisierung sich nicht einfach durchsetzt, nur weil sie machbar ist, sonst gäbe es hierzulande vollautomatisierte Textilfabriken. Studien, die vor millionenfachem Arbeitsplatzverlust durch Roboter warnen, blenden dies zumeist aus. Auch Crowdsourcing und Clickworking-Plattformen sind Beispiele dafür, wie Prozesse weiterhin von Menschen erledigt werden, anstatt sie zu automatisieren. Viele dieser Arbeiten bestehen allerdings nur aus noch nicht automatisierbaren Restaufgaben.

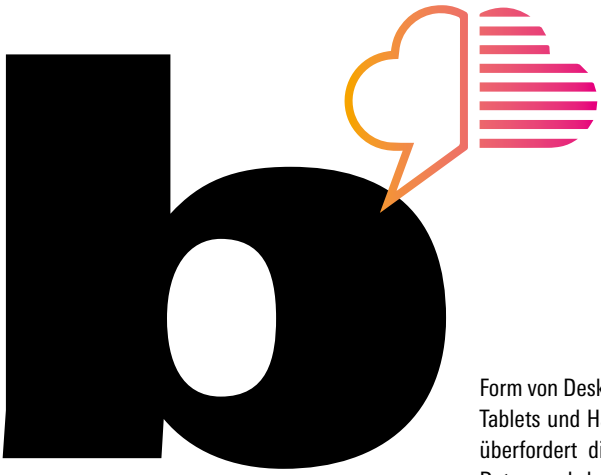
Technikentwicklung ist dennoch zentral. Die fortschreitende Automatisierung der Arbeit ist, neben anderen Gründen, aufgrund ihrer Universalität als Bruch mit vorangegangenen Prozessen zu verstehen. Leittechnologie für die aktuelle Dynamik sind frei programmierbare Computer, die hoch spezialisierte Werkzeugmaschinen steuerten. Das ändert sich aktuell, und relativ breit einsetzbare Roboter, beispielsweise in der Lagerlogistik, können inzwischen auch komplexe Tätigkeiten erledigen. Obwohl angesichts Künstlicher Intelligenz auch höher qualifizierte Arbeit nicht zwangsläufig exklusive Domäne der Menschen bleibt, gelten hoch qualifizierte und gut bezahlte Arbeitsplätze weiterhin als wenig bedroht. Automatisierung wird also *ceteris paribus* Klassenspaltungen eher vertiefen und nicht aus sich selbst heraus in ein Reich der Freiheit führen. (Christian Meyer)

// ZUM WEITERLESEN

[1] Marx, Karl: Grundrisse der Politischen Ökonomie. Das sogenannte «Maschinenfragment», 1858, in: Marx, Karl/Engels, Friedrich: Werke (MEW), Bd. 42, Berlin 1983, S. 590–605.

[2] Brynjolfsson, Erik/McAffee, Andrew: The Second Machine Age. Wie die nächste digitale Revolution unser aller Leben verändern wird, Kulmbach 2014.

[3] Projektgruppe Automation und Qualifikation: Widersprüche der Automationsarbeit. Ein Handbuch, Berlin 1987.



// BIG DATA

Der Begriff Big Data umfasst zwei schillernde Worte mit einigen wenig konkreten Bedeutungen. Zunächst ist er nur eine Art Größenangabe: Mit ihm werden Datenmengen bezeichnet, die zu groß oder komplex sind, als dass sie mit herkömmlichen Mitteln der Datenverarbeitung verarbeitet werden könnten. Das kann am Umfang der **Daten** liegen (sehr große Datensätze), an der Vielfalt der Daten (viele Datenquellen) oder an der Geschwindigkeit, mit der sie anfallen oder analysiert werden müssen (Echtzeitdaten). Mehr noch aber steht Big Data für einen vermeintlich neuen Umgang mit den im Rahmen der Digitalisierung anfallenden Daten und dem Datenbedarf einer digitalen Gesellschaft: Obwohl Rechenkraft in Form von Desktop-Computern, Laptops, Tablets und Handys allgegenwärtig ist, überfordert die schiere Menge neuer Daten und deren Analysebedarf deren Möglichkeiten. Immer neue Messpunkte (zum Beispiel Sensordaten oder auch das Nutzerverhalten im Internet) führen seit einigen Jahren zu einem rasch anschwellenden Datenvolumen. Einer Schätzung von IBM zufolge werden täglich 2,5 Trillionen Bytes an neuen Daten geschaffen, Tendenz stark steigend. Big Data beschreibt damit auch die (meist zentrale) Organisation und Aufbereitung der Daten mithilfe spezieller Computer und **Algorithmen** zum Beispiel in Rechenzentren. Letztlich umfasst der Begriff auch die Darstellung der aufbereiteten Daten, deren Speicherung und Verbreitung und sogar selbstverschriebene oder staatlich vorgegebene Richtlinien zu ihrem Umgang, wie zum Beispiel Datenschutzverordnungen.

Dass Big Data in den letzten Jahren zu einem wichtigen Schlagwort wurde, liegt allerdings an einem technologisch-ökonomischem Versprechen der Digitalisierung: Ein Datum ist nur die Infor-

mation, die es selbst darstellt. Mehrere Daten zusammengefasst ergeben aber neue Informationen: Je mehr Daten vorliegen, desto bessere, tiefere Schlüsse kann man aus ihnen ziehen, wenn man die geeigneten statistischen Methoden, ausreichend Rechenkraft und die Infrastruktur der Datenverwaltung besitzt. Die Daten sind in diesem Bild ein Rohstoff, der mithilfe von Maschinen und Algorithmen zu neuem Wissen veredelt werden kann. Dieses Wissen bedeutet Vorhersagekraft über zukünftige Entwicklungen, Aufdecken tiefer liegender Strukturen und Zusammenhänge im Datenrauschen und Optimierung von Abläufen. Eine zentrale statistische Technik ist dabei die Mustererkennung. In einem Datenstrom werden Regelmäßigkeiten identifiziert und mit anderen Regelmäßigkeiten oder auch nur Einzelereignissen korreliert: Wenn X passiert, dann passiert auch Y. Dadurch erhalten Daten einen Wert: Ihre Anhäufung, Monopolisierung und Rekonfiguration schafft erst einen Datenmarkt, einen neuartigen Daten-Kapitalismus. Da mit Big Data der Erkenntnisgewinn automatisiert werden soll, folgt der bloßen Verwaltung übermäßig großer Datenmengen in den letzten Jahren nun die Datensammlung: Weil Speicherplatz billig ist und nur die Verarbeitung von Daten teuer, versuchen Firmen und Staaten nun Daten erst zu horten, um sie später auszuwerten.

Durch Big Data ergeben sich so ganz neue Autonomieprobleme: Für sich genommen unverfängliche Daten entfalten möglicherweise durch Anreicherung mit anderen Daten ein Machtpotenzial, zum Beispiel wenn es um die Vorhersage oder das Verständnis des individuellen Verhaltens geht. Andererseits ist das Thema noch so neu und voller Ungewissheiten, dass es noch keine Ansatzpunkte für eine staatliche Regulierung gibt. Ab wann können Daten Macht entfalten? Wer darf Daten schöpfen und besitzen? Wie verhalten sich Daten und Individuum zueinander? Welche Analysemethoden sollen erlaubt sein? Die größte Herausforderung für Big Data ist damit keine technische oder technologische: Vielmehr muss es darum gehen, ein neues Verständnis von Daten und ihrer etwaigen Macht zu erhalten.

(Felix Knoke)

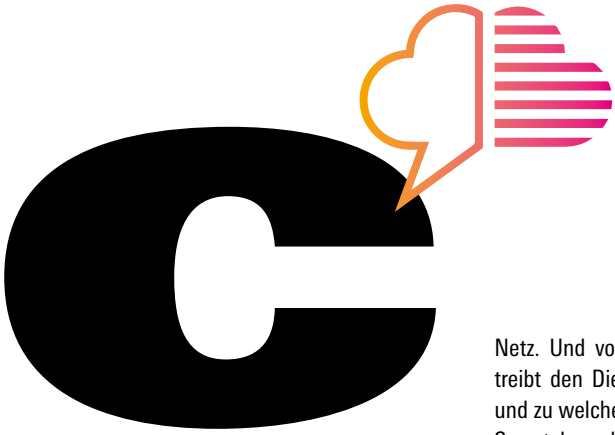
// ZUM WEITERLESEN

[1] Aronova, Elena/Oertzen, Christine von/Sepkoski, David: Die Geschichte von Big Data, Max-Planck-Institut für Wissenschaftsgeschichte, unter: www.mpiwg-berlin.mpg.de/de/node/7455.

[2] Morozov, Evgeny: Digital Technologies and the Future of Data Capitalism, Social Europe, 23.6.2015, unter: https://is.gd/TAUqRt.

[3] Sitte, Petra: Big Data und Big Government erfordern einen Paradigmenwechsel, Digitale Linke, 13.6.2014, unter: https://is.gd/nHtMdb.

// CLOUD // CYBERWAR
// CYBORG



// CLOUD

Cloud ist ein Wort aus dem Englischen und heißt Wolke. Es wird oft im Zusammenhang mit dem Internet gebraucht: «Ich hab mein Backup in der Cloud.» Oder: «Die Datei ist zu groß für E-Mail, ich pack sie dir in die Cloud.» Auch gern: «Mein Routenplaner läuft in der Cloud.» Allein diese drei Beispiele bezeichnen drei sehr unterschiedliche Dinge: die individuelle Nutzung von Speicherplatz im Netz, Online-Kommunikation und -Datenaustausch und die Auslagerung von kompletten Programmen, die nicht mehr auf dem eigenen Gerät, sondern auf dem Server der BetreiberIn installiert sind.

Das Schlagwort Cloud verschleiert also zunächst eher, als dass es erklärt, was genau passiert und wo, in welchem Netz. Und vor allen Dingen: Wer betreibt den Dienst, zu welchem Zweck und zu welchen Konditionen?

So stehen hinter unterschiedlichen Diensten mit vergleichbarem Angebot mitunter unterschiedlichste Motive: Die beiden Karten- und Navigationsdienste Google Maps und OpenStreetMap bieten in den Grundfunktionen ähnliche Möglichkeiten und verlangen kein Geld für ihre Dienstleistungen, die auf zentralen Servern – also in der «Cloud» – errechnet werden. Google Maps sammelt aber **Daten** und **Metadaten** und vervollständigt das Wissen des Konzerns um die Geolokalisationsinformationen seiner BenutzerInnen. Auf der Basis dieses Wissens bastelt der Konzern verkäufliche Produkte: zum Beispiel nutzerspezifische Werbeschaltungen, die mich auf Konsummöglichkeiten verweisen, die zufälligerweise gerade um die nächste Ecke liegen. Auch die Manipulation von Suchergebnissen erfolgt unter Einbezug von Geodaten. Darüber hinaus lassen sich staatliche Überwacher mit diesen Daten versorgen, und Dritte können sie kaufen. Was *genau* hinter den Ober-

flächen von Plattformkapitalisten wie Google und Co. passiert, bleibt jedoch Betriebsgeheimnis.

Der community-basierte Kartendienst OpenStreetMap hingegen ist nicht an einen Konzern angeschlossen. Dort werden die anfallenden Daten lediglich so genutzt, wie es für eine Kartenansicht oder die Berechnung einer Route nötig ist. OpenStreetMap basiert auf Freier Software (Free and Open Source Software, FOSS), das heißt, es gibt kein Betriebsgeheimnis bei diesem Kartendienst, jede und jeder kann sich anschauen, wie die Software funktioniert und was mit den bei der Nutzung anfallenden Daten passiert, weil der menschenlesbare Programmcode vorliegt.

Kartenmaterial am Rechner zu nutzen und die zugrunde liegenden riesigen Datenmengen und aufwendigen Berechnungen auf zentralisierte leistungsstarke Server auszulagern, ergibt durchaus Sinn. Ob ich mich und meine Daten im Zuge dieser Auslagerung einem kapitalistischen Konzern ausliefere oder einem den Prinzipien von Selbstverwaltung verpflichteten FOSS-Projekt anvertraue: Diese Wahl besteht und noch steht sie uns frei.

Die Rede von «der Cloud» jedoch macht alle Anbieter eines bestimmten Gebrauchswerts (in diesem Beispiel: Kartendienst) gleich. Sie «entnennt» die Unterschiede hinsichtlich Organisationsweise, Eigentumsform und Interessen verschiedener Anbieter und verstärkt Schwarmdummheit: Viele NutzerInnen kommen gar nicht auf die Idee, dass es etwas zu wählen gäbe. Das Bezeichnete ist so wolkig, dass es meines Erachtens auch keinen «besseren» Ersatzbegriff gibt. Stattdessen sollten wir, geht es um «die Cloud» – und gerade wenn eine technikaffine Person spricht –, nachfragen, was genau gemeint ist. Liegt uns selbst das Wort auf der Zunge, dann sollten wir es schlucken und einen Satz mehr als geplant verwenden: Über welche Art von Internetdienst sprechen wir? Wie sehen Eigentümerschaft und Interessen des Anbieters aus?

Zum Programm digitaler Selbstverteidigung gehört auch derart differenzierteres Sprechen: Wir drücken uns dabei nicht nur klarer aus, sondern erinnern uns gleichzeitig auch an Handlungsmöglichkeiten jenseits von Konkurrenz und Massenüberwachung im Rahmen von Staat und Kapital.

(Markus Euskirchen)

// ZUM WEITERLESEN

[1] Stallman, Richard: Wem dient dieser Server wirklich?, Gnu.org, 30.7.2015, unter: https://is.gd/j4Ovo1.
[2] Liste von Software und Dienstanbietern zur Unterscheidung von Konzernprodukten und Communityprojekten, unter: http://stop-prism.org.
[3] Kartendienste vergleichen bei Geofabrik Map Compare, unter: http://tools.geofabrik.de/mc/.

// CYBERWAR

Unter Cyberwar versteht man kriegerische Aktionen, die über die Informationstechnik ausgeführt werden. Mit Cyberwar-Attacken können Infrastrukturen dauerhaft zerstört und große Massen an Menschen getötet werden. Besonders gefährlich ist dabei das gezielte Eindringen in Netze, der Aufbau von Bot-Netzen (eine Sammlung kompromittierter PCs, die ein Angreifer aus der Ferne kontrollieren kann) und das Auslegen «logischer Bomben», die beim Eintreten bestimmter Bedingungen aktiviert werden. Diese Attacken manipulieren und beschädigen gezielt Steuerungssoftware, um die damit betriebene Hardware oder auch ganze Versorgungssysteme zu zerstören. Bedroht sind hier vor allem die Energie- und Trinkwasserversorgung, das Gesundheits- und Rettungswesen, Banken und Versicherungen, Verwaltungen, Chemie- und Atomanlagen sowie Telekommunikationssysteme.

Die Gefahren eines Cyberwars werden vielfach unterschätzt, weil der Begriff auch für vergleichsweise harmlose Angriffe verwendet wird: Spionage, Denial-of-Service-Attacken («Dienstblockade»), Hacking und Manipulation digitaler Inhalte.

Cyberwar ist damit auch Thema terroristischer Gruppen. Die größte Bedrohung geht aber von der herrschenden Logik in Wirtschaft und Politik aus. Denn der Cyberwar wird vor allem durch den digitalen Hightech-Kapitalismus möglich. Wettbewerbsdruck zwingt Unternehmen, Staaten und private Haushalte zur Steuerung und Kontrolle zentraler Prozesse durch Software und zum Aufbau einer (Netz-)Infrastruktur, um zum Beispiel durch die Automatisierung der Arbeit (siehe auch Stichwort Industrie 4.0) effizienter produzieren zu können. Technologische Monokulturen und der Aufbau des Internets der Dinge (die zunehmende Vernetzung aller Gegenstände; siehe «smart everything») potenzieren die Angriffspunkte.

Cyberwar-Angriffe auf vernetzte Steuerungssoftware sind für Regierungen und Militärs aus vier Gründen interessant: 1. Mit verdeckten Aktionen lassen sich Ziele ohne Beteiligung der Öffentlichkeit, der Einbindung von Parlamenten und ohne eigene Verluste erreichen. 2. Zerstörungen lassen sich aus dem Internet heraus an den bestehenden militärischen Verteidigungsstrukturen vorbei organisieren. 3. Man kann in kürzester Zeit weltweit Ziele angreifen, ohne dass der Angreifer eindeutig festgestellt werden kann. 4. Der Ressourceneinsatz für den Aufbau digitaler Angriffswaffen ist im Vergleich zu ABC-Waffen verschwindend gering, wobei Cyberattacken durch die Zerstörung ganzer Energieversorgungsnetze ähnliche Dimensionen erreichen könnten.

Kritiker wie der ehemalige Vizepräsident des Europäischen Parlaments, Gerhard Schmid (SPD), weisen darauf hin, dass aber die Strategie der Abschreckung im Netzkrieg nicht funktioniere, da sich versteckte logische Bomben nicht gegeneinander aufrechnen ließen. Ebenso gebe es für Cyberattacken keine Vorwarnzeit. Dies lade zum Erstschlag ein. Zudem seien, so Schmid, die Auswirkungen eines echten Netzkrieges völlig unvorhersehbar.

Diese zunehmende Unsicherheit löst eine Rüstungsspirale aus, bei der alle

Industriestaaten ihre Angriffe vorbereiten und bereits durchführen. Durch die digitale Aufrüstung und heimlich Cyberattacken, wie der Stuxnet-Angriff auf Atomanlagen im Iran, verschwimmen die Grenzen zwischen Krieg und Frieden. Die Spannungen erhöhen sich. Der Aufbau einer wirkungsvollen IT-Sicherheitsinfrastruktur ist ein politisches, technologisches und ökonomisches Großprojekt, bei dem sich rivalisierende Akteure auf gemeinsame Standards und Verfahren einigen müssten. Dabei lässt sich die Sicherheit im Netz nur mit aktiver Einbindung des zivilen Sektors herstellen. Dort wird man im Gegenzug fordern, die Politik der Kontrolle und Massenüberwachung privater Nutzer aufzugeben. (Richard Heigl)

// ZUM WEITERLESEN

[1] Gaycken, Sandro: Cyberwar. Das Internet als Kriegsschauplatz, München 2010.

// CYBORG

Cyborg leitet sich von «cybernetic organism» ab und bezeichnet Hybridwesen aus Organismus und Maschine. Der Begriff entstand im Kontext des «Wettlaufs ins All». So richtig populär wurden Cyborgs allerdings erst durch das Kino und die Literatur, beispielsweise als «Six-Million-Dollar-Man», «Bionic Woman», «Borg-Kollektiv» etc. Wesentlich ausformuliert und erweitert wurde das Konzept Cyborg dagegen in der feministischen Theorie und in der Science-Fiction.

Der Biokybernetiker Manfred Clynes und der Psychiater Nathan Kline verwendeten den Begriff erstmals 1960 in einem Aufsatz, in dem sie Raumfahrt weniger als technische, sondern vor allem als geistige Herausforderung charakterisierten. Zukünftige Astronauten (wohlgemerkt die männliche Form) sollten den Bedingungen des Weltraums angepasst werden, und zwar nicht durch Schutzanzüge, sondern durch biochemische, physiologische und elektronische Modifikationen an ihnen selbst. Der Raumfahrer als «sich selbst steuerndes Tier-Maschine-System» sei befreit von allen körperlichen Begrenzungen und könne so ungehindert entdecken, schaffen, denken und fühlen. Weder einem Gott noch der Evolution sei das Schicksal der Menschheit länger unterworfen.

Geschichten über Automaten und Roboter reichen historisch weiter zurück. Cyborgs waren jedoch erst durch die Kybernetik, die Lehre von der Kommunikation, Steuerung und Regelung von Maschinen, lebenden Organismen und sozialen Organisationen, möglich

geworden. Denn die auf militärische Forschung zurückgehende Kybernetik entwirft Lebewesen und Maschinen als «im Grunde gleich», als lebende *und* technische Systeme. Information als körperlose Entität hat nichts mehr mit Inhalt oder Bedeutung zu tun. Infolgedessen lässt sich die gesamte Welt als eine Frage der Kodierung darstellen. Planeten, Pflanzen, Menschen, Tiere, Maschinen – alle werden gleichermaßen als Kommunikationssystem beschrieben und können entsprechend zerlegt und neu kombiniert werden, sie alle unterliegen einer Logik der Investition und des Tauschs.

Das Mainstream-Kino wurde durch diese Ideen zu Robocops und Replikanten angeregt. Der US-amerikanischen Wissenschaftsforscherin* Donna Haraway hingegen diente das Bild der Cyborgs als komprimierte Karte einer (be)streitbaren Welt und als Figur für emanzipatorische, nicht-identitätslogische Politiken und (Selbst-)Praktiken zugleich. In ihrem 1985 verfassten «Manifest für Cyborgs» verglich sie die gesellschaftlichen Entwicklungen im Gefolge der Informations- und Kommunikationstechnologien mit den Umbrüchen der industriellen Revolution. Das weiße kapitalistische Patriarchat in seiner zeitgenössischen Form bezeichnete sie entsprechend als «Informatik der Herrschaft». In den 1980er Jahren ist die Informatik der Herrschaft geprägt durch Reagans «Krieg der Sterne» (SDI – Strategic Defense Initiative), durch die weltweite Herausbildung einer neuen Arbeiter*innenklasse, in der Frauen* die meiste Arbeit verrichten und Arbeit «feminisiert» wird, internationale Arbeitsteilung, Informatisierung sowie die Verquickung von Bio- und Informationstechnologien. Sollen die veränderten Lebensverhältnisse nicht nur erlitten, sondern auch mitgestaltet werden, müssen feministische Analysen den neuen Herrschaftsverhältnissen Rechnung tragen.

Darüber hinaus fragt Haraway, wenn Planeten, Menschen, Tiere, Pflanzen, Maschinen – wenn alle als Kommunikationssystem betrachtet werden, welche Gemeinsamkeiten tun sich dann auf, was ist das Verbindende zwischen Menschen und Maschinen, Menschen und Pflanzen, Maschinen und Pflanzen etc.? Die Frage nach den Gemeinsamkeiten ermöglicht es, Dualismen wie Natur/Technik, männlich/weiblich, schwarz/weiß etc. aufzubrechen – Dualismen, die sich in einer Zeit, in der viele Menschen Technik wie Smartphones und andere Gadgets als Erweiterung ihrer selbst verwenden, ohnehin nicht halten lassen. Das Aufbrechen der Dualismen ist Haraway wichtig, weil sie diese als «systematischen Bestandteil der Logiken und Praktiken der Herrschaft [...] über all jene, die als «Andere» konstituiert werden», betrachtet. Hier verbindet sie also zwei Argumentationen, die nie zusammengedacht worden waren: eine kritische Analyse der Technowissenschaften einerseits und postkoloniale Bestrebungen, ein politisches Kollektiv aus dem Nicht-Identischen zu entwerfen, andererseits.

Schreiben ist bei Haraway eine der bedeutendsten Cyborg-Technologien. Schreiben ermöglicht, gegen die Übersetzung vielfältiger Bedeutungen in den einen eindeutigen Code zu kämpfen. Schreiben ermöglicht darüber hin-

aus, zentrale Geschichten neu oder anders zu erzählen und dabei Hierarchien und naturalisierte Identitäten zu verrücken. Beispiele hierfür findet Haraway in lesbischen und Chicana-Literaturen. Gerade in der feministischen Science Fiction jedoch werden Geschichten erzählt, die Dualismen, wie weiblich/männlich, Mensch/Maschine, primitiv/zivilisiert etc. infrage stellen. Aktuell sind es die Cyborgs in postkolonialen queer-feministischen Science-Fictions, die auf höchst spannende Weise nicht nur dominante okzidentale Erzählungen, sondern auch unsere Vorstellungen von Technologien herausfordern. (Dagmar Fink)

// ZUM WEITERLESEN

[1] Haraway, Donna: Ein Manifest für Cyborgs. Feminismus im Streit mit den Technowissenschaften, in: Hammer, Carmen u.a. (Hrsg.): Die Neuerfindung der Natur. Primaten, Cyborgs und Frauen, Frankfurt a.M. 1995, S. 33–72.
[2] Fink, Dagmar: Lese ich Cyborg, lese ich queer?, in: Babka, Anna/Hochreiter, Susanne (Hrsg.): Queer Reading in den Philologien. Modelle und Anwendungen, Göttingen 2008, S. 157–170.
[3] Hopkinson, Nalo: Midnight Robber, New York 2000.
[4] Filme: «Ghost in the Shell», R: Mamoru Oshii, J 1995; «Dandy Dust», R: A. Hans Scheirl, A/GB 1998; «The Last Angel of History», R: John Akomfrah, GB 1996.

// DATEN: EIGENTUM

// DIGITALE SELBSTVERMESSUNG & DIGITALISIERTE GESUNDHEIT

// DIGITALE SELBSTVERTEIDIGUNG

// DIGITALE SPALTUNG

// DROHNENKRIEG

// DATEN: EIGENTUM

Die Bundeszentrale für politische Bildung hat jüngst eine Broschüre herausgegeben mit dem Titel «Meine Daten gehören mir!». Der Leitfaden soll der Jugend zeigen, «wie du deine Daten schützen kannst». Gemeint sind persönliche Informationen, die Menschen im Internet oder auf mobilen Datenträgern (Scheckkarten, Gesundheitschip etc.) hinterlassen: Auf welchen Websites tummeln sie sich wie lange, für welche Produkte interessieren sie sich oder welche Krankheiten hatten sie schon.

Datenschutz ist nicht nur aktives Handeln derer, die Daten preisgeben oder für sich behalten. Er ist in Deutschland auch ein Grundrecht. In Form der «informationellen Selbstbestimmung» soll grundsätzlich jede und jeder bestimmen können, welche persönlichen Informationen bekannt werden. Zum Grundrecht erhoben wurde dieses Prinzip 1983 als Reaktion gegen die (analoge) Volkszählung durch die Bundesregierung.

KritikerInnen sagen, dieses Prinzip funktioniere heute nicht mehr. Dank Big Data ist es seit Kurzem interessant geworden, personenbezogene Daten systematisch zu erheben, daraus Profile abzuleiten und diese (kommerziell) zu verwerten. Die massenweise Nutzung von Social Media zeigt darüber hinaus: Das Mitteilungs- und Kommunikationsbedürfnis der Menschen ist offenbar so groß, dass sich die wenigsten an die von Datenschützern propagierte Datensparsamkeit halten. Dabei werden oft persönliche Daten anderer Menschen preisgegeben, ohne dass diese dies zuvor explizit erlaubt haben.

Eine Reaktion auf diese Entwicklung ist, dass JuristInnen und PolitikerInnen diskutieren, ob es nicht analog zum Urheberrecht ein geistiges Eigentum an den «eigenen» Daten geben sollte. Auch einzelne Start-up-Unternehmen versuchen bereits, Daten generierende

«UserInnen» an der Verwertung «ihrer» Daten finanziell zu beteiligen («Sell Your Data»).

An einzelnen Daten kann bislang kein «geistiges Eigentum» begründet werden, denn dieses gilt bisher nur für kreative Schöpfungen (Zeitungsartikel, Musikstücke, Fotos etc.) und systematisch oder methodisch angeordnete Daten.

Wenn einzelne Daten im Rechtssinne Eigentum werden sollten, müsste die Definition des geistigen Eigentums entsprechend gesetzlich geändert werden. Geistiges Eigentum steht aber schon bisher im Widerspruch dazu, dass Informationen (wie wissenschaftliche Artikel oder politische Diskussionen) erst durch ihre Verbreitung und Bearbeitung an ideellem Wert für die Gemeinschaft gewinnen. Dies könnte auch für persönliche Daten gelten. Anonymisierte Gesundheitsdaten könnten gesellschaftlich gewollten Fortschritt in der Medizin ermöglichen, Verkehrsdaten könnten Straßenbahntaktungen in Echtzeit optimieren.

Ein Eigentum an Informationen würde vielleicht deren Verwertung vereinfachen, aber es würde potenziell auch die Verbreitung und den Austausch von Information einschränken. Das mag mit Blick auf die Privatsphäre der DatenproduzentInnen von Vorteil sein. Dateneigentum könnte aber auch dazu führen, dass die, die ihr sprichwörtlich letztes Hemd geben müssen, künftig dem ökonomischen Zwang unterliegen, «ihre» Daten verkaufen zu müssen.

Auf das Missverhältnis zwischen der Idee der informationellen Selbstbestimmung und der digitalen Realität der permanenten Datenverknüpfung macht die Post-Privacy-Bewegung aufmerksam. Sie geht davon aus, dass die Menschen durch die Digitalisierung einen «Kontrollverlust» bezogen auf die persönlichen Daten erlitten haben, der nicht mehr umkehrbar ist. Einige der Post-Privacy-VertreterInnen sehen dies durchaus positiv, weil sie hoffen, durch diese Transparenz Ungleichheiten in der Gesellschaft aufdecken und aufheben zu können.

(Jörg Braun, Sabine Nuss)

// ZUM WEITERLESEN

[1] Stichwort «Selbstbestimmung», Wikipedia, Stand: 30.8.2016, unter: https://de.wikipedia.org/wiki/Informationelle_Selbstbestimmung.

[2] Seemann, Michael: Das neue Spiel. Strategien für die Welt nach dem digitalen Kontrollverlust, Freiburg 2014.

[3] Heller, Christian: Post-Privacy. Prima leben ohne Privatsphäre, München 2011.

[4] Kurz, Constanze/Rieger, Frank: Die Datenfresser. Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen, Frankfurt a.M. 2012.

// DIGITALE SELBSTVERMESSUNG & DIGITALISIERTE GESUNDHEIT

Das Grundprinzip der digitalen Selbstvermessung besteht darin, Daten über den eigenen Körper zu erheben, um sie auszuwerten und schließlich für die Selbstoptimierung zu nutzen. Dabei können einzelne Körper- und Gesundheitsdaten mithilfe einer Smartphone-App oder mittels anderer digitaler Geräte (wie z. B. Fitness-Armband, Smart-Watch etc.) gemessen werden (siehe smart everything).

Zu den beliebtesten Möglichkeiten des Self-tracking, also der Selbstüberwachung und Selbstvermessung, gehört das Schritte zählen. Es funktioniert meist über Geräte, die am Körper getragen werden und mit Sensoren ausgestattet Erschütterungen messen können. Diese werden dann mithilfe von bestimmten Algorithmen als Schritte interpretiert, und entsprechende Apps werten die Informationen aus. UserInnen werden dabei motiviert, sich nicht nur selbst zu vermessen, sondern sich auch an bestimmten Zielen oder an Leistungen anderer UserInnen messen zu lassen. Wöchentliche oder tägliche Herausforderungen sollen Anreize liefern, ein bestimmtes Leistungsniveau zu halten oder zu steigern.

Self-tracking ist in diesem Ausmaß zweifelsfrei durch die technische Entwicklung möglich geworden. In einem soziokulturellen Kontext jedoch, in dem das Individuum die Hauptverantwortung für das eigene Leben zu tragen hat, wird Selbstkontrolle und Selbstüberwachung zur logischen Schlussfolgerung. Self-tracking steht für die Vorstellung, dass jeder Mensch allein durch Eigeninitiative imstande ist, sein Leben zu verbessern, gesund, schön und erfolgreich zu sein. Was Nina Degele den Autonomieimperativ nennt, verweist auf das mit der Individualität verbundene Ausrufezeichen, was nicht nur befähigt Dinge selbst in die Hand zu nehmen, sondern Autonomie geradezu einfordert.

Wissen über den eigenen Körper und Gesundheit beruht bei der digitalen Selbstvermessung allein auf den aus Daten generierten Informationen und wird in quantitativ genormte Messkategorien gegossen. Dabei wird ein stark eindimensionales Bild von Körper und Gesundheit als quantifizierbare Objekte gezeichnet. Soziokulturelle Einflüsse auf Gesundheit oder rechtliche und politische Rahmenbedingungen spielen keine Rolle mehr. Obwohl Self-tracking also individualisierte Gesundheit propagiert, funktioniert die Datenauswertung bei vielen Apps mittels normierender Algorithmen und vergleicht individuelle Gesundheitswerte mit Werten aus aggregierten Datenmengen.

Auch das öffentliche Gesundheitssystem versprechen digitale Technologien langfristig verbessern und effizienter gestalten zu können. Vor allem die Vernetzung von digitalisierten Patientendaten soll die Gesundheitsversorgung profitabler machen, da Informationen für medizinisches Personal überall und ständig verfügbar werden. Dazu machen Selbstüberwachung und die Vermessung eigener Körperdaten UserInnen quasi zu ihren eigenen PatientInnen, bei denen die eigene Gesundheit zu einem neoliberalen Projekt mit

unternehmerischem Charakter wird. So gewinnt das Teilen der hoch sensiblen Gesundheitsdaten an Zuspruch, sowohl auf öffentlicher als auch auf privater Ebene.
Bislang werden die Self-tracking-Apps und -Messgeräte durch unabhängige Stellen in der Regel weder geprüft noch zertifiziert. Dies führt dazu, dass sich die Geräte in Messgenauigkeit und Interpretation der Daten erheblich unterscheiden können. Der meist intransparente oder mangelnde Datenschutz der erhobenen Gesundheitsdaten verweist auf weitere Problematiken bei der digitalen Selbstvermessung und dem Teilen von Gesundheitsdaten. (Marie Kochsiek)

// ZUM WEITERLESEN

[1] Degele, Nina: Normale Exklusivitäten. Schönheitshandeln, Schmerznormalisieren, Körper inszenieren, in: Villa, Paula-Irene (Hrsg.): Schön normal. Manipulationen am Körper als Technologien des Selbst, Bielefeld 2008, S. 67–84.
[2] Lupton, Deborah: The commodification of patient opinion: the digital patient experience economy in the age of big data, in: Sociology of Health & Illness 36(2014)6, S. 856–869.
[3] Lupton, Deborah: Self-tracking Modes: Reflexive Self-Monitoring and Data Practices. Paper for the workshop «Imminent Citizenships: Personhood and Identity Politics in the Informatic Age», University of Canberra, Canberra 2014.

// DIGITALE SELBSTVERTEIDIGUNG

Der Begriff Selbstverteidigung ruft bei vielen Menschen Bilder von Bruce Lee oder anderen Kampfsportlern hervor. Obwohl wir durch Medien und Filme vor allem die Stars der Kampfkunstschulen im Blick haben, war fast allen ein kollektiver Gedanken ursprünglich: Arme, Bauern, Frauen oder Kolonialisierte übten gemeinsam eine bestimmte Selbstverteidigungstechnik ein, um sich gegen ihre übermächtigen GegnerInnen zur Wehr zu setzen.
Auf diesen Begriff der Selbstverteidigung bezieht sich auch die digitale Selbstverteidigung. Aufgetaucht ist der Begriff bereits Ende der 1990er Jahre, als die ersten digitalen, für EndverbraucherInnen zugänglichen, Verschlüsselungstechniken ein Absichern von Kommunikation möglich machten – und die ersten Überwachungsskandale die Notwendigkeit von konkreter Selbstabsicherung unterstrich.
Digitale Selbstverteidigung ist in erster Linie eine Aufforderung zum gemeinsamen Handeln, zur gemeinsamen Organisierung gegen Massenüberwachung und zum Aneignen des Internets durch VerbraucherInnen und BürgerInnen. Die einzige wirksame Strategie gegen Massenüberwachung ist Verschlüsselung und darum ist auch das Verschlüsseln einer der Kernpunkte jeder Initiative zur digitalen Selbstverteidigung. Dazu gehört meistens, die E-Mail mit dem Verschlüsselungsprogramm Pretty Good Privacy zu verschlüsseln und die Festplatte des Computers zu verschlüsseln, sodass sie im Fall von Entwendung nicht ausgelesen werden kann.

Auch die verschlüsselte Kommunikation beim Browsen im Web, wie auch das verschlüsselte Kommunizieren mit Mobiltelefon-Messengern wird mit zu Maßnahmen der digitalen Selbstverteidigung gezählt. Die konkreten Ideen, wie man sich gemeinsam mit FreundInnen und Familie, KollegInnen und GenossInnen gegen den allgegenwärtigen digitalen Zugriff von Unternehmen und Staat durch Tracking, Verhaltensanalyse und Überwachung zur Wehr setzt, können aber viel weitreichender und vielfältiger sein.

Gründe für die digitale Selbstverteidigung gibt es viele. Spätestens seit den Veröffentlichungen des Ex-Geheimdienstmitarbeiters Edward Snowden ist die Totalüberwachung der BürgerInnen durch Geheimdienste und Unternehmen öffentlich. Die Regierungen sind nicht in der Lage, dem etwas entgegenzusetzen und die Rechte der BürgerInnen zu wahren. Stattdessen werden unter dem Deckmantel der Terrorbekämpfung neue Verschärfungen eingeführt, die wiederum Grundrechte weiter beschneiden. Aktuell wird sogar von Regierungs- und Geheimdienstseite ein Verbot von Verschlüsselung gefordert beziehungsweise eine Pflicht für Softwarehersteller, Hintertüren einbauen zu müssen. Diese Initiativen werden lautstark vorgetragen, obwohl Verschlüsselung die einzige Möglichkeit in der digitalen Welt ist, das Bürgerrecht auf informationelle Selbstbestimmung wahrzunehmen.

Hindernisse für eine breit angelegte digitale Selbstverteidigung gibt es leider auch viele: Das Absichern von Systemen ist – ähnlich wie verschiedene Sicherheitsschlösser an der Wohnungstür – erst einmal aufwendig und nicht intuitiv. Die Praxis ist zwar schnell eingeübt, aber die Hürden, die VerbraucherInnen auf dem Weg zur Verschlüsselung an ihrem persönlichen Schweinehund vorbei zu überwinden haben, sind für viele mühsam. Das geschieht am einfachsten zusammen mit Freunden oder Familie. Unterstützung existiert dafür in vielfältiger Form: neben vielen Online-Hilfestellungen und Schritt-für-Schritt-Anleitungen gibt es auch Workshops, Seminare oder Selbsthilfe-Treffen, wie beispielsweise Cryptoparties, die es inzwischen in jeder größeren deutschen Stadt gibt. Dort wird gemeinsam, ohne dass Vorkenntnisse mitgebracht werden müssen, in angenehmer Atmosphäre über digitale Selbstverteidigung geredet und danach auch ganz praktisch miteinander geübt.

(Susanne Lang)

// ZUM WEITERLESEN

[1] Portal für Selbstdatenschutz und digitale Selbstverteidiung, www.selbstdatenschutz.info.

[2] Lang, Susanne: Offenes Geheimnis – Mythen und Fakten zu Überwachung und digitaler Selbstverteidigung, argumente 10, hrsg. von der Rosa-Luxemburg-Stiftung, Berlin 2016, unter: www.rosalux.de/publication/42538.

[3] Stichwort «Digitale Selbstverteidigung», Netz für Alle, netzpolitischer Blog der Rosa-Luxemburg-Stiftung, unter: http://netzfueralle.blog.rosalux.de/.

[4] Was ist digitale Selbstverteidigung?, Einführungsvortag auf der CryptoCon16 in Leipzig, Mai 2016, unter: https://is.gd/dBXzkp.

// DIGITALE SPALTUNG

Das Internet vernetzt, vermittelt Wissen und demokratisiert, so die allgemeine Argumentation. Jede und jeder könne sich unabhängig von der realen Person im Cyberspace aus einem unermesslichen Wissensschatz bedienen. Was diese Überlegungen außer Acht lassen, ist, dass es in Zeiten der Wissensgesellschaft durchaus Menschen gibt, die keinen Zugang zu Informationstechnologie haben, vor allem keine Möglichkeit, das Internet zu nutzen. Hier spricht man von einer digitalen Spaltung oder Kluft zwischen denen, die online, und denen, die offline sind – im englischen häufig auch als «digital divide» und «digital inequality» bezeichnet.

Theorien zur Digitalen Spaltung stehen in der Tradition der Wissenskluft-hypothese. Diese geht davon aus, dass Wissensunterschiede zwischen Bevölkerungsgruppen – Trennlinien können regional, ökonomisch, aufgrund des Geschlechts, des Alters oder der Bildung verlaufen – durch massenmediale Informationsmöglichkeiten und deren spezifische Nutzung verstärkt werden, sodass Chancenungleichheiten weiter ausgebaut werden.

Ein Ausbau der Netzinfrastruktur hat dazu geführt, dass es in vielen westlichen Ländern seit einigen Jahren immer weniger Menschen ohne Internetanschluss gibt. Fast 80 Prozent der Deutschen ab 14 Jahren waren laut ARD-ZDF-Onlinestudie im Jahr 2015 regelmäßig online. Begünstigt wird dies durch gesunkene Kosten für die Internetnutzung und einfachere Bedienung. Natürlich ist das nicht überall so. Laut Bericht der Breitbandkommission der Vereinten Nationen hatten in Mali im Jahr 2015 nur 6,7 Prozent aller Haushalte einen Internetanschluss, in Afghanistan nur 2,7 Prozent. Diese Trennung zwischen Personen, die Zugang zum Internet haben, und solchen ohne, sieht die Wissenschaft als eine erste Ebene. Eine zweite hingegen verläuft zwischen den Personen, die das verfügbare Wissen für sich nutzbar machen können, also Fähigkeiten im Umgang mit dem Internet haben oder nicht. Unterschiede bestehen aber auch hinsichtlich der Geschwindigkeit mit der Daten übertragen werden, bei den Preisen, die dafür verlangt werden und bei möglichen Schranken, die das Internet kontrollieren und die Freiheit einschränken.

In den Bereich des Infrastrukturausbaus in armen Regionen drängen seit einigen Jahren privatwirtschaftlich organisierte Unternehmen mit ihren Interessen, zum Beispiel die Initiativen «loon for all» von Google oder «Free Basics» von Facebook. Mittels solarbetriebener Drohnen oder Gasballons wollen sie (ihr) Internet dort hinbringen, wo es bisher nicht ist. Ihre Argumente: Internet bringe Bildung, könne die Gesundheitsvorsorge verbessern, Teilhabe am globalen Markt ermöglichen oder Wetterdaten zur produktiveren Landwirtschaft in abgelegene Regionen liefern. Tatsächlich beinhalten viele dieser Projekte aber nur ein «Schmalspurinternet»: Einige von den Anbietern ausgewählte Websites können kostenlos genutzt werden, für Dienste außerhalb dieses Bereichs werden jedoch Gebühren erhoben, oder die Geschwindigkeit der Datenübertragung

wird eingeschränkt. Insofern bleibt diese privatwirtschaftliche Initiative ein zweischneidiges Schwert. Grundsätzlich – so wird häufig gesagt – sei der «digital divide» nicht das vorrangige Problem in extrem armen Regionen, gemessen an existenziellen Krisen wie Bürgerkriege, Hungersnöte, Aids etc., doch kann der Zugang zum Internet ein Mittel sein, Informationen zu erhalten und zu verbreiten. Die Chance auf Teilhabe und Sichtbarkeit sowohl im lokalen als auch im globalen Maßstab sinkt daher noch mehr, wenn die digitale Kluft nicht kleiner wird.
(Martha Dörfler)

// ZUM WEITERLESEN

[1] Bericht der Breitbandkommission der Vereinten Nationen 2015, unter: https://is.gd/pL17Ko.
[2] Zillen, Nicole: Ungleichheit der Internetnutzung, Vortrag, unter: https://youtu.be/-G2cU5Y8mek.
[3] Rennie, Ellie u.a.: Internet on the Outstation. The Digital Divide and Remote Aboriginal Communities, Amsterdam 2016, unter: https://is.gd/NHAvyX.

// DROHNENKRIEG

Drohnen sind unbemannte und ferngesteuerte Luftfahrzeuge, seltener sind auch Wasser- und Landfahrzeuge gemeint. In den letzten drei Jahrzehnten hat der militärische Gebrauch von Drohnen zugenommen, zunächst zur Aufklärung und Überwachung, seit den Anschlägen vom 11. September 2001 werden Drohnen auch für Luftschläge gegen Terrorverdächtige eingesetzt.
Spätestens seit dem Ersten Weltkrieg werden Drohnen militärisch genutzt, aber erst ab den 1990er Jahren verlor die Drohnentechnologie ihr Nischendasein, seit sowohl Steuerung als auch Datennutzung nahezu in Echtzeit möglich sind. Der «globale Krieg gegen den Terrorismus» nach 9/11 brachte den politischen Impuls für den Einsatz einer Reihe von automatisierten und ferngesteuerten Technologien. Das Scheitern der Weltmächte in den asymmetrischen Konflikten in Vietnam in den 1970er und in Afghanistan in den 1980er Jahren hatte für die Bereitstellung von erheblichen Budgets für Forschung und Entwicklung gesorgt. Neben vielen taktischen Vorteilen bei den Drohneneinsätzen ist insbesondere der fehlende menschliche Faktor das Erfolgskriterium: Hier besteht kein Risiko für die eigenen Soldaten, was eine der zentralen Taktiken insbesondere von dschihadistischen Aufständischen konterkariert.
Die Bezeichnung Drohnenkrieg wurde in den letzten fünf Jahren zu einem populären Schlagwort und fasst eine Reihe von politischen und militärischen Entwicklungen zusammen. Bekannt wurden insbesondere Einsätze US-amerikanischer ferngesteuerter Kampfdroh-

nen der Typen Predator und Reaper, welche vor allem mit Hellfire-Raketen Bodenziele beschießen. Diese Einsätze (insbesondere in Afghanistan, Pakistan, Jemen, Somalia) dienen der gezielten Tötung von vermuteten Mitgliedern terroristischer Gruppen. Doch diese Form der «Jagd auf TerroristInnen» ist alles andere als präzise und sauber, denn immer wieder sterben Unbeteiligte beziehungsweise ZivilistInnen, zum Beispiel durch den Beschuss von Wohngebäuden, PKWs oder anderen zivilen Zielen. Die «Signature Strikes» sind eine Art Rasterfahndung mit Drohnen und Vor-Ort-Exekution, zum Beispiel in den Stammesgebieten in Nordwest-Pakistan. Die Identität der Zielpersonen muss dabei nicht einmal bekannt sein: Es reichen bereits sehr allgemeine Verhaltensmuster und Gruppenmerkmale («all military-age males in a strike zone») als Verdachtsgrund.

Zur Zielbestimmung für Drohnenschläge werden auch anlasslos gesammelte Metadaten aus den globalen Überwachungsprogrammen der Geheimdienste genutzt. Diese ermöglichen eine nahezu beliebige Identifikation, Lokalisierung und Liquidierung ausgewählter Personen. Die Frage nach dem Sinn weltweiter Massenüberwachung ist mit Blick auf solche Tötungsprogramme neu gestellt.

Die rechtlichen und politischen Probleme dieser Form der verdeckten Kriegsführung sind schwerwiegend und vielfältig, schließlich handelt es sich um eine Form außergerichtlicher, staatlicher Hinrichtung auf Verdachtsgrundlage. Gefahren liegen in der rasanten Eskalationsdynamik, welche die Drohnenkriege mit sich bringen: Die Welt steht am Beginn eines neuen Wettrüstens mit automatisierten Waffensystemen. Das Gesicht moderner Kriegsführung wandelt sich grundlegend, weitgehend autonom handelnde Killerroboter sind bereits in der Entwicklung.

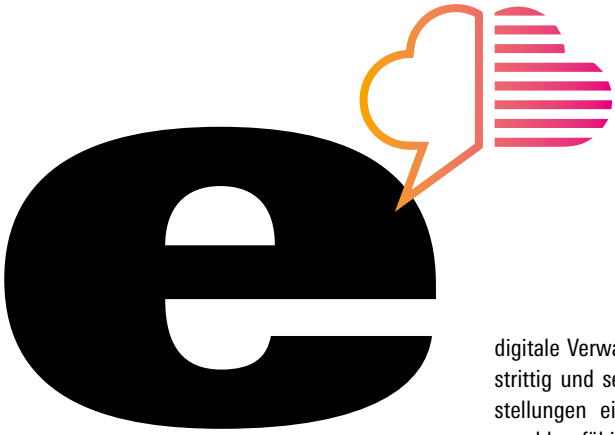
Die weltweite «Antiterrorkriegführung» der letzten Jahre hat in mehrfacher Hinsicht eine Relativierung der Menschenrechte gebracht. Die extralegale Hinrichtung von Verdächtigen mithilfe von Drohnen untergräbt jegliche Unschuldsvermutung und Rechtsstaatlichkeit. Automatisierte Kriegsführung treibt die Erosion internationaler Normen und Institutionen weiter voran. Sobald Killerroboter selbstständig Tötungsentscheidungen treffen können, werden weitere zentrale Grundsätze der Rechtsstaatlichkeit außer Kraft gesetzt: Es gibt keine abrechenbare Verantwortlichkeit mehr. Der technologische und waffentechnische Fortschritt gebietet, sowohl für unbemannte und ferngesteuerte Systeme als auch für automatisierte Roboterwaffen neue Regulierungsrahmen auf internationaler Ebene zu schaffen. (Norbert Schepers)

// ZUM WEITERLESEN

[1] Scahill, Jeremy: The Assassination Complex. Inside the Government's Secret Drone Warfare Program, New York 2016, unter: http://interc.pt/1Lvu1R3.

[2] Schepers, Norbert: Drohnenkriege. Warum Big Data tödlich sein kann, in: LuXemburg 3/2014, S. 78–83, unter: www.zeitschrift-luxemburg.de/drohnenkriege/.

[3] Woods, Chris: Sudden Justice. America's Secret Drone Wars, Oxford 2015.



// E-GOVERNMENT/ E-DEMOCRACY

Unter den Schlagwörtern E-Government und E-Democracy werden Ansätze zusammengefasst, demokratische beziehungsweise staatliche Prozesse zu digitalisieren, also mithilfe von Computertechnik und Internet abzubilden und zu erweitern.

Im engsten Sinne wird mit E-Government die Digitalisierung der staatlichen Verwaltung selbst bezeichnet, das heißt elektronische Abwicklung sowohl interner Abläufe als auch der Behördenkommunikation von Privatpersonen und Unternehmen. Mit durchgängig elektronischen Verfahren wird die Erwartung verbunden, beträchtliche Effizienzgewinne zu erzielen. Als politisches Vorhaben ist die digitale Verwaltung daher weithin unstrittig und selbst für neoliberale Vorstellungen eines «schlanken Staats» anschlussfähig. Hindernisse sind vor allem Komplexität und Selbstbeharrungskräfte der Institutionen, weshalb E-Government speziell in Deutschland noch unterentwickelt ist.

Im weiteren Sinne erfasst der Begriff auch neue staatliche Informationsangebote wie die Bereitstellung von öffentlichen oder behördlichen Daten im Sinne von Open Data und öffentliche Infrastrukturen.

Der Begriff E-Democracy deckt ebenfalls ein weites Feld ab, von der unmittelbaren Digitalisierung formaler demokratischer Prozesse bis zu Strukturwandel im gesamten öffentlichen Diskurs. Im engsten Sinne fällt darunter die elektronische Stimmabgabe bei Wahlen oder Abstimmungen (E-Voting).

Im weiteren Sinne umfasst E-Democracy verschiedene Instrumente zur Beteiligung an demokratischen Prozessen, die sich nach Formalisierung, Verbindlichkeit und Interaktivität unterscheiden. Zumeist handelt es sich um Angebote, die existierende Prozesse wie

etwa die parlamentarische Beratung von Gesetzen oder die Öffentlichkeitsbeteiligung im Rahmen der Bauleitplanung nicht ersetzen, sondern ergänzen sollen. Neben staatlich organisierten Angeboten treten solche, die aus der Zivilgesellschaft heraus aufgebaut werden (z. B. Abgeordnetenwatch, «Frag den Staat» oder diverse private Petitionsplattformen) und in verschiedener Weise und verschiedenem Maße an existierende politische Strukturen – oft, aber nicht ausschließlich, Parlamente – andocken. In einigen Fällen werden solche Angebote von weitaus mehr Menschen genutzt, als dies bei staatlichen E-Democracy-Angeboten üblich ist.

Im weitesten Sinne umfasst E-Democracy alle Einflüsse der Digitalisierung auf die öffentliche Meinungsbildung. Optimistische Vorhersagen, dass bereits die einfachen und nicht hierarchischen Kommunikationsmittel, die das Internet eröffnet, eine besser informierte und politisch aktivere Öffentlichkeit schaffen würden, sind einer gewissen Resignation gewichen: Die Erfahrung zeigt, dass politische Diskurse online nicht unbedingt sachlicher oder tief gehender geführt werden als offline. Das Internet hat aber unstrittig neue Rahmenbedingungen und Möglichkeiten für politische Kommunikation und politischen Aktivismus geschaffen.

E-Voting als einfacher Ersatz für die klassische Urnenwahl ist aufgrund des Wahlcomputerdilemmas sehr kritisch zu sehen: Eine Abstimmung bei einer Wahl muss gleichzeitig nachvollziehbar und geheim sein. Bei der «analogen» Urnenwahl ist das nahezu problemlos möglich, hier geht eine Zuordnung zwischen Stimme und stimmabgebender Person in dem Moment verloren, wo der anonyme Stimmzettel in die abgeschlossene Urne geworfen wird. Da kann jede und jeder nachvollziehen, wie die Wahl geheim und anonym durchgeführt wird. Auch die Auszählung lässt sich beobachten und damit nachvollziehen. Eine elektronische Abstimmung kann das nicht gewährleisten, weil in jedem nicht perfekt nachvollziehbaren Schritt «hinter den Kulissen» im Prinzip alles passieren könnte.

Bei Prozessen, die keine geheime Stimmabgabe erfordern, besteht aber ein noch weitgehend ungenutztes Potenzial durch Wegfall logistischer Hürden, da Verfahren verwendet werden können, die in der manuellen Durchführung sehr aufwendig wären (ein Versuch in diese Richtung ist die Software LiquidFeedback, die Konzepte von Liquid Democracy und der Social-Choice-Theorie anwendet).

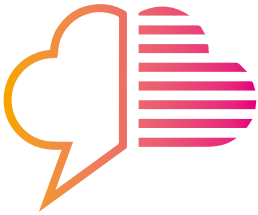
Eine allgemeinere Kritik an E-Democracy verweist darauf, dass sie verstärkt von Gruppen benutzt wird, die in der Politik bereits überrepräsentiert sind (männlich, weiß, höherer formeller Bildungsgrad), und auch die sogenannte **Digitale Spaltung** zwischen Bevölkerungsgruppen muss bedacht werden. Dies ist kein einzigartiges Problem im Vergleich zu anderen Partizipationsmöglichkeiten, zeigt aber die Notwendigkeit, die Frage des Zugangs umfassender mitzudenken.

Insgesamt steht digitale Demokratie noch am Anfang, jedenfalls was die tatsächliche Einbettung elektronischer Verfahren in Entscheidungsstrukturen angeht. An weniger formellen Partizipationsmöglichkeiten besteht ein grö-

ßeres Spektrum, wobei sich zeigt, dass diese vor allem dann erfolgreich sein können, wenn die Auswirkungen von Beteiligung von vornherein klar definiert sind.
(Simon Weiß)

// ZUM WEITERLESEN

[1] Fromm, Jens u. a.: E-Government in Deutschland. Vom Abstieg zum Aufstieg, Berlin 2015, unter: https://is.gd/aAWCAm.
[2] Lindner, Ralf/Aichholzer, Georg/Hennen, Leonhard (Hrsg.): Electronic Democracy in Europe: Prospects and Challenges of E-Publics, E-Participation and E-Voting, New York u. a. 2016.
[3] Behrens, Jan: The Principles of LiquidFeedback, Berlin 2014.



// INDUSTRIE 4.0

Industrie 4.0 ist ein vor allem in Deutschland gebräuchlicher Begriff, der die digitale Vernetzung von Maschinen, Produkten, Fertigungsprozessen und Logistik in der Industrie beschreibt. In der englischsprachigen Debatte ist vor allem der Begriff «industrial internet» gebräuchlich. Eine allgemein akzeptierte Begriffsdefinition existiert bislang nicht. Es handelt sich aber nicht bloß um einen Marketingbegriff, sondern er ist darüber hinaus eng verknüpft mit einem Zukunftsprojekt der deutschen Bundesregierung zum Umbau der deutschen Industrie und zur Erschließung weiterer Wertschöpfungspotenziale.

Es geht bei Industrie 4.0 um eine weitere Vernetzung der physischen mit der digitalen Welt, die über vorherige Ansätze der Digitalisierung der Produktion hinausgeht. Grundlage hierfür ist das sogenannte Internet der Dinge, also die Verknüpfung von sogenannten intelligenten Objekten (Smart Objects, siehe smart everything) beziehungsweise Cyber-Physischen-Systemen (CPS), die durch den Einsatz von Sensorik laufend Informationen über ihren Ort, ihren Zustand und ihre Umgebung liefern und damit die Steuerung von betrieblichen Prozessen in Echtzeit und sogar über verschiedene miteinander vernetzte Unternehmen hinweg ermöglichen. Diese können sich entsprechend der Anforderungen selbstständig steuern und kontinuierlich selbst optimieren. Es handelt sich im Kern um eine neue Form der Steuerung und Organisierung von Produktionsabläufen.

Die Erwartungen an Industrie 4.0 sind hoch: Sie vereint die Großproduktion mit den jeweiligen Wünschen ganz unterschiedlicher Kunden und ist dabei kostengünstig wie die Massenproduktion bei gleichzeitig hoher Qualität und Spitzenwerten bei den Produktions-

und Rüstzeiten. Reagiert wird damit auf sich rascher wandelnde Absatzmärkte und die immer kürzer werdenden Produktzyklen. Der Umbau der Produktion zur intelligenten Fabrik (Smart Factory) soll die hiesige Wirtschaft insgesamt wettbewerbsfähiger machen und so Zugang zu neuen Märkten eröffnen, neue Geschäftsmodelle ermöglichen und damit insgesamt für bessere Perspektiven von Kapital und Arbeit sorgen. Der Produktionsprozess soll energie- und ressourceneffizient sein. Durch neue Assistenzsysteme soll die Belastung und Beanspruchung bei der Arbeit reduziert und diese «demografiesensibel» auch noch in hohem Alter ermöglicht werden und damit eine wichtige Antwort auf den Fachkräftemangel in der deutschen Industrie sein.

Bisher sind Industrie-4.0-Konzepte in der Realität jedoch allenfalls in Ansätzen verwirklicht und kaum in einem umfassenden Sinne umgesetzt, dennoch werden bereits lautstark ihre Chancen verkündet, die es – so die Bedrohungskulisse – nicht zu verpassen gelte. Die Debatte bleibt dabei vor allem auf die technologischen Aspekte fokussiert, die arbeitsmarkt- und gesellschaftspolitischen Folgen bleiben unscharf. Droht ein massiver Arbeitsplatzverlust, eine neue technologische Arbeitslosigkeit oder werden sich nur Tätigkeitsprofile verschieben? Wird dies zu mehr Arbeitszeitsouveränität im Sinne einer «Wahlarbeitszeit» führen, oder wird es vielmehr zu einem weiteren Unterlaufen arbeitsrechtlicher Standards, in Gestalt von mehr Deregulierung, Flexibilisierung und Dequalifizierung kommen?

Im Zentrum der Debatte steht vor allem die Frage der Anpassung des Menschen an Technologie und Märkte. Nur wenn wir diese Fragestellung umdrehen und zusätzlich die Folgen für die global vernetzte Weltwirtschaft und die tatsächlichen ökologischen Kosten, jenseits der Behauptungen der Werbebroschüren, in den Blick nehmen, bieten sich Chancen für eine demokratischere Arbeitswelt und gesellschaftlichen Fortschritt.

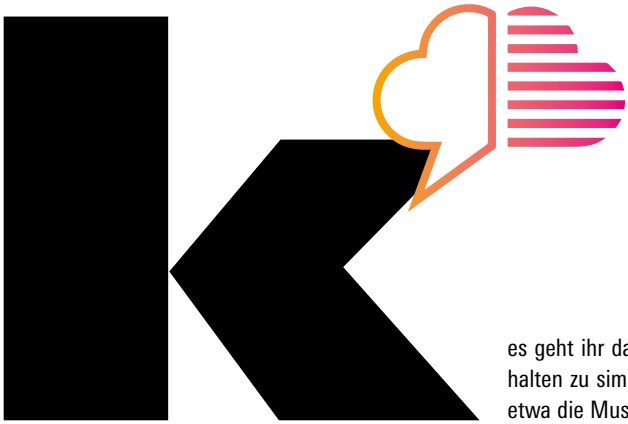
(Patrick Stary)

// ZUM WEITERLESEN

[1] Pfeiffer, Sabine: Industrie 4.0 und die Digitalisierung der Produktion. Hype oder Megatrend?, in: Aus Politik und Zeitgeschichte 31–32/2015, unter: https://is.gd/BKv0td.

[2] Matuschek, Ingo: Industrie 4.0, Arbeit 4.0 – Gesellschaft 4.0? Eine Literaturstudie, Studien 2/2016, hrsg. von der Rosa-Luxemburg-Stiftung, Berlin 2016, unter: www.rosalux.de/publication/42201.

[3] Butollo, Florian/Engel, Thomas: Industrie 4.0 – arbeits- und gesellschaftspolitische Perspektiven, in: Z. Zeitschrift marxistische Erneuerung 103/2015, unter: https://is.gd/ri6ASu.



// KÜNSTLICHE INTELLIGENZ

Es gibt nicht viele Begriffe, mit denen sich große Fortschrittshoffnungen, Weltuntergangsprophetie und allerlei Missverständnis gleichermaßen verbinden – Künstliche Intelligenz (KI) gehört dazu. Unter KI wird in der Regel ein Teilgebiet der Informatik verstanden, in dem es darum geht, eine menschenähnliche Intelligenz per Computer nachzubauen, um so Maschinen in die Lage zu versetzen, eigenständig Probleme zu bearbeiten. Unterschieden wird zwischen starker KI und schwacher KI, wobei die starke KI eine «Intelligenz» anstrebt, in der das vollständige menschliche Denken nachempfunden ist.

Die schwache KI dagegen befasst sich mit einzelnen Anwendungsproblemen, es geht ihr darum, «intelligentes» Verhalten zu simulieren. Teilbereiche sind etwa die Mustererkennung bei Bildern und Sprache oder wissensbasierte Systeme, die aus formalisierter Fachkenntnis logische Schlüsse ziehen und Antworten geben können. In der Robotik geht es um manipulative Intelligenz, also die Fähigkeit, bestimmte Tätigkeiten selbstständig auszuüben.

Zentrale Anforderungen an Künstliche Intelligenz sind Lernfähigkeit, die Kompetenz, mit Unsicherheit umzugehen und Wahrscheinlichkeitsaussagen zu treffen. Vor allem auf dem Gebiet des maschinellen Lernens sind zuletzt große Fortschritte gemacht worden, künstliche Systeme können immer besser aus Beispielen lernen, Muster in Daten finden und die so gewonnenen «Erkenntnisse» verallgemeinern.

Mit der Künstlichen Intelligenz sind eine Reihe von definitorischen Problemen verbunden – zum Beispiel die Frage: Was ist Intelligenz? Erfüllt die Maschine, der «intelligentes» Tun nachgesagt wird, nicht bloß eine Funktion, die vom Menschen zuvor implementiert werden musste? (Ad Aertsen)

Die Forschung zur starken KI «krankt» zudem daran, dass es an hinreichenden Abgrenzungen etwa von Konzepten wie «Bewusstsein» mangelt – zugleich steht sie aber in einer bis zur Aufklärung zurückreichenden Tradition der Idee des «Menschen als Maschine». Hier dockte der bisher erfolglose Ansatz an, per Reverse Engineering das menschliche Gehirn quasi «nachzubauen».

Begonnen hat alles übrigens Mitte der 1950er Jahre – mit einem Antrag, der die Finanzierung eines Forschungsseminars am Dartmouth College in Hanover im US-Bundesstaat New Hampshire sicherstellen sollte. Formuliert von John McCarthy war darin zugleich der Begriff Künstliche Intelligenz erstmals umrissen worden: «Es soll versucht werden herauszufinden, wie Maschinen dazu gebracht werden können, Sprache zu benutzen, Abstraktionen vorzunehmen und Konzepte zu entwickeln, Probleme von der Art, die zurzeit dem Menschen vorbehalten sind, zu lösen und sich selbst weiter zu verbessern.» Beteiligt an dem Projekt waren viele Pioniere der Computerentwicklung und Informatik, darunter Marvin Minsky, Nathaniel Rochester und Claude Shannon. Damalige Vorstellungen über die Geschwindigkeit, mit der Antworten gefunden werden könnten, erwiesen sich als viel zu optimistisch.

Die Forschung zur und die Debatte über Künstliche Intelligenz hat in den vergangenen Jahren spürbar angezogen, was mit besseren technischen Möglichkeiten beim auch wirtschaftlichen Umgang mit sehr großen Mengen von Daten zu tun hat. Autonome Autos, sprechende Smartphones, Computer, die Texte lesen, schreiben oder Sprachen übersetzen, sind so alltäglich wie der Einsatz humanoider Roboter schnell voranschreitet.

Visionäre und dystopische Vorstellungen stehen sich in der Debatte über Künstliche Intelligenz gegenüber. Auf der einen Seite etwa die Idee eines für die gesamte Menschheit segensreichen Fortschritts, der soziale, medizinische, ökologische und ökonomische Probleme löst – bis hin zur Überwindung des natürlichen Todes. Wie eine solche Zukunft aussehen mag, ist aber gerade auch wegen der sich entwickelnden Künstlichen Intelligenz unklar. Die Idee der technologischen Singularität beschreibt einen Zeitpunkt, über den «wir Menschen» nicht prognostizierend hinausblicken können, weil dann «die Maschinen» per Künstlicher Intelligenz einen Entwicklungsstand erreicht haben, der sich den derzeit bekannten Vorstellungen entzieht. Mit dieser Vorstellung korrespondiert das Untergangsszenario, demzufolge eine Computerintelligenz den Menschen irgendwann als Störfaktor ansehen und sogar vernichten könnte, wie es in dem 2016 erschienenen Buch «Evolution ohne uns: Wird Künstliche Intelligenz uns töten?» ausgemalt wird. In einem Ausschuss des Europaparlaments war 2016 davon die Rede, dass wir «an der Schwelle einer Ära» stehen, in der «immer ausgeklügeltere Roboter, Bots, Androiden und sonstige Manifestationen Künstlicher Intelligenz anscheinend nur darauf warten, eine neue industrielle Revolution zu entfesseln, die wahrscheinlich keine Gesellschaftsschicht unberührt lassen wird». Auch Wissenschaftler wie Stephen

Hawking oder Unternehmer wie Elon Musk haben sich warnend geäußert. In einem 2015 veröffentlichten «Digitalen Manifest» riefen ExpertInnen unterschiedlichster Fachbereiche «zur Sicherung von Freiheit und Demokratie» auf, weil eine «Automatisierung der Gesellschaft mit totalitären Zügen» wahrscheinlich sei – »im schlimmsten Fall droht eine zentrale Künstliche Intelligenz zu steuern, was wir wissen, denken und wie wir handeln». Der Publizist Thomas Wagner hat vor einiger Zeit vor dem Aufziehen einer «Robokratie» gewarnt.

Dem stehen Betrachtungen gegenüber, wonach die Künstliche Intelligenz heute «zwar besser als natürliche Dummheit» sei, aber: «Die menschliche Intelligenz ist doch bei weitem überlegen» (Wolfgang Wahlster). Ohnehin käme es unter dem Strich vor allem darauf an, unter welchen gesellschaftlichen Bedingungen (Produktionsverhältnissen) intelligente Maschinen eingesetzt und gesteuert werden. Eine Welt voller Künstlicher Intelligenz, in der etwa die Verteilung des gesellschaftlich produzierten Reichtums nach denselben Regeln funktioniert wie heute, wäre eine gar nicht so verschiedene Welt. Und ob KI-Systeme zu mehr Umweltschutz oder zu mehr Überwachung beitragen, ist auch eine politisch entscheidbare Frage. Oder um es mit Neil Jacobstein von der Stanford University zu sagen: Man muss wegen Künstlicher Intelligenz nicht nachts vor Angst wach liegen, wovor man sich fürchten muss, ist die menschliche Dummheit.

(Tom Strohschneider)

// ZUM WEITERLESEN

[1] Stiftung für Effektiven Altruismus: Künstliche Intelligenz – Chancen und Risiken, Diskussionspapier, 2015, unter: https://ea-stiftung.org/kuenstliche-intelligenz/.

[2] Künstliche Intelligenz: Ist das schon Denken?, Chaosradio Podcast, 1.4.2016, unter: https://chaosradio.ccc.de/cr221.html.

[3] Schlieter, Kai: Die Herrschaftsformel. Wie Künstliche Intelligenz uns berechnet, steuert und unser Leben verändert, Frankfurt a.M. 2015.

// KYBERNETISCHER KAPITALISMUS

Die Kybernetik wurde während des Zweiten Weltkriegs von Norbert Wiener als «Wissenschaft von Kommunikation und Kontrolle» begründet. Ziel war es, auf Grundlage massiver Datenerhebung selbstregulierende Systeme zu schaffen – von einer sich selbst ausrichtenden Flugabwehrkanone bis zur vollautomatischen Fabrik. Im Zuge der Entwicklung der Informationstechnologien wurde die Kybernetik zu einem wichtigen Bezugspunkt für die Organisation von Produktion und Kontrolle. Der Begriff des kybernetischen Kapitalismus umfasst dabei drei Ebenen: Ideologie, Kapitalakkumulation und soziale Kontrolle.

Auf der ideologischen Ebene kann von einer Verschmelzung von Kybernetik und Neoliberalismus zur zentralen Ideologie des Informationszeitalters gesprochen werden. So prophezeite Bill Gates, dass im Zuge der allgemeinen Verfügbarkeit von Internetzugängen endlich Adam Smiths These der vollständig informierten MarktteilnehmerInnen Realität werden würde. Dadurch entstehe ein weltweites, auf der Basis von Preisinformationen selbstreguliertes Marktsystem, das er als «reibungslosen Kapitalismus» bezeichnet. Mit der Entwicklung der Big-Data-Analyseverfahren geht diese Ideologie über in einen Glauben an algorithmenbasierte Selbstregulierung, die imstande ist, Entscheidungen zu fällen, die sich dem menschlichen Verständnis entziehen, weil sie sich auf eine riesige Datenbasis stützen.

Auf der Ebene der Kapitalakkumulation verweist der Begriff des kybernetischen Kapitalismus darauf, dass Produktion, Kommunikation und Kontrolle immer öfter in einen einzigen Prozess zusammenfallen und sogar von derselben technischen Infrastruktur ermöglicht werden: Produktionsprozesse (zum Beispiel in der Industrie 4.0) werden mittels Sensortechnik überwacht, um Angestellte zu kontrollieren und Abläufe zu rationalisieren – und die Daten können schlussendlich als zusätzliche Ware neben dem materiellen Produkt verkauft werden. In physischen und virtuellen Verkaufsräumen wird das Kundenverhalten überwacht und analysiert, um so gleichzeitig Diebstähle verhindern, den Verkauf optimieren und personalisierte Werbung anbieten zu können.

Die soziale Kontrolle nach dem kybernetischen Modell wurde im deutschsprachigen Raum erstmals von BKA-Chef Horst Herold popularisiert. Im Kampf gegen die Rote Armee Fraktion (RAF) wollte Herold seiner Polizei den entscheidenden Vorteil durch den Einsatz von Computertechnologie verschaffen, wodurch eine «kybernetische Präventionspolizei» entstehen sollte, die Verbrechensrisiken vorausberechnen könne. Dieses Modell wurde auf der Grundlage von Big-Data-Analyseverfahren zum sogenannten Predictive Policing weiterentwickelt, bei dem Algorithmen dafür sorgen sollen, dass die Polizei vor den TäterInnen am Tatort ist. Ähnliche Modelle kommen in der präventiven Epidemiologie oder im sogenannten *riot forecasting* zum Einsatz. Kybernetische Kontrolle besteht jedoch nicht nur aus dem Auswerten, sondern auch aus dem gezielten steuern von Informationen. So setzen Poli-

zeien immer stärker auf soziale Medien wie Twitter und Facebook, nicht nur um ihre Inhalte ohne journalistische Kontrolle direkt verbreiten zu können, sondern auch um direkt auf brisante Situationen wie Demonstrationen oder Aufstände einwirken zu können, weil davon ausgegangen werden kann, dass viele der Beteiligten die Botschaften live auf ihren Smartphones empfangen. Der kybernetische Kapitalismus zeichnet sich also nicht nur durch die Inwertsetzung von Daten, sondern vor allem durch eine datenbasierte Steuerung nach dem Modell der undurchschaubaren Blackbox aus. Jede Abweichung soll so zum Feedback werden, das zur Stabilisierung des Gesamtsystems beiträgt. (Simon Schaupp)

// ZUM WEITERLESEN

[1] Witheford, Nick Dyer: Cyber-Proletariat. Global Labour in the Digital Vortex, Toronto 2015.
[2] Tiqqun: Kybernetik und Revolte, Zürich 2007.
[3] Wiener, Norbert: Mensch und Menschmaschine, Frankfurt a.M. 1952.

// LINKE UND TECHNIK

Das Verhältnis von Linken zur Technik schwankt seit 150 Jahren zwischen zwei Polen: Auf der einen Seite steht ein technologisch grundierter Fortschrittsoptimismus, der in Lenins Parole vom Kommunismus seinen Ausdruck findet, der »Sowjetmacht plus Elektrifizierung« sei. Den anderen Pol illustriert eine Anekdote aus der Geschichte des Kommunistischen Bundes, in dem anfangs ausdrücklich vor dem Aufkommen von Computern gewarnt wurde – die entsprechenden Flugblätter wurden wahrscheinlich auf mechanischen Schreibmaschinen getippt.

Im Technikoptimismus der frühen Arbeiterbewegung und des realsozialistischen Lagers findet eine Utopie der produktivistischen Modernisierung ihren Niederschlag, in der Technik, Wissenschaft und Innovation vor allem als Mittel zur Steigerung der Produktivität betrachtet wurden, die Früchte hervorbringt, deren gerechte Verteilung zum Wohle aller nur im Sozialismus möglich sei. Von diesem Denken befördert, erhielten technische Innovationen den Charakter von Fortschrittsmotoren – von der chemischen Industrie über die Atomkraft und den Kybernetik-Hype Mitte des 20. Jahrhunderts bis zur elektronischen Datenverarbeitung und zur Raumfahrt.

Einerseits wurde Technik hier als «neutrale» Angelegenheit betrachtet, die in der unmittelbaren Auseinandersetzung mit der Natur ihre Anwendung findet und auf ihren Charakter als Produktivkraft reduziert wurde – es andererseits aber in dieser Perspektive darauf ankam, unter welchen Produktionsverhältnissen die Technik zum Einsatz kommt. Eine zugespitzte Form dieses Denkens war die Behauptung westdeutscher Parteikommunisten, die Atomkraft sei nur im Realsozialismus eine gute und sichere Angelegenheit. Nach dem Reaktorunglück von Tschernobyl 1986 sagte das aber auch in der DKP niemand mehr.

Längst hatte sich zu diesem Zeitpunkt eine vor allem ökologisch inspirierte Technikkritik ausgebreitet. Vor allem gegen die Gefahren der Atomkraft, der Gentechnologie und generell die Folgen kapitalistischer Reichtumsproduktion für Umwelt und Mensch organisierten sich immer mehr Menschen in Bewegungen. Intellektuell begleitet wurde diese zweite Phase des Verhältnisses von Linken und Technik von einer Kritik, die kulturpessimistische, risikowissenschaftliche und philosophische Momente verband, etwa in der Zurückweisung eines Wissenschafts- und Technikbegriffes, der beides auf eine Rolle als Produktivkraft reduziert und von einem Denken der Sachgesetzlichkeit und instrumentellen Vernunft geprägt war.

Die Kritik rückte immanente Eigenschaften von Technik und den Herrschaftscharakter von Technologie ins Blickfeld schlug aber nicht selten in ein technikdeterministisches Weltbild um, das zu apokalyptischen Prognosen einlud und die Befreiungspotenziale von Technik komplett unterschlug.

Ob es solche überhaupt gibt, wurde in der linken Debatte schon früher grundlegend von Raniero Panzieri infrage gestellt. Der operaistische PCI-Politiker hatte sich 1961 «Über die kapitalistische Anwendung der Maschinerie im Spätkapitalismus» Gedanken gemacht und die damals in der realsozialistischen und parteikommunistischen Bewegung dominante Tradition der an sich guten, in Bezug auf die Klassenverhältnisse neutralen Technologieentwicklung zurückgewiesen. Technologische Rationalität, untersucht am Maschineneinsatz in Fabriken, wurde bei Panzieri als Form kapitalistischer Herrschaft – unauflöslich mit der Profitrationalität des Kapitals verknüpft – angesehen und der Technikeinsatz als unmittelbares Instrument der Klassenherrschaft kritisiert.

Karl Marx hatte in den «Grundrissen» die Maschinerie als «die adäquateste Form des Kapitals überhaupt» bezeichnet und in der Dynamik ihres Einsatzes zugleich etwas gesehen, das den Kapitalismus unterwandert, nach dem Motto: «Je fortschrittlicher der Kapitalismus wird, umso weniger wird er kapitalistisch» (Christian Lotz). Theodor W. Adorno hatte den dahinterstehenden Technikbegriff von Marx als unklar kritisiert, er sei «von Saint-Simon übernommen, ohne dass dieser seine Stellung zu den Produktionsverhältnissen durchdacht hätte».

Spätestens seit den 1990er Jahren kann von einer dritten Phase des Verhältnisses von Linken und Technik gesprochen werden. Sie ist abermals von Ambivalenz gekennzeichnet. Während große Hoffnungen in die demokratischen, organisatorischen und kritischen Potenziale zum Beispiel des Internets gesetzt wurden, wurde zugleich der herrschaftskonforme Charakter kritisiert und vor allem vor den Möglichkeiten umfassender Kontrolle gewarnt. In die Figur des Hackers wurden einerseits ethische Aspekte von Technik projiziert – der anonyme Kämpfer für das Gute –, die Figur des Internetunternehmers drückte hingegen die janusköpfige Erschaffung der Welt per Technik aus – wenn man so will die Ablösung von Heideggers «Ingenieur», in dem der Mensch zum Ebenbild Gottes als wahrer «Schöpfer» wird.

Linke Kritik begreift Technik und Technologien heute nicht nur als einen Gegenstand von Risikofolgenabschätzung, sondern unterstreicht ihre sozialen und gesellschaftspolitischen Folgen sowie den ihnen innewohnenden Herrschaftscharakter. Sie ist verknüpft mit der Kritik am Wachstumsparadigma des Kapitalismus und richtet ihren Blick auf die globale Ungleichheit der Möglichkeiten, Technik zum Wohle des Menschen einzusetzen, etwa im Gesundheitsbereich. Flankiert wird dies von einer Kritik, welche die Auswirkungen von technologischer Entwicklung durch Automatisierung und Digitalisierung auf Arbeitswelt, soziale Beziehungen und Persönlichkeit betont. Auch der kommodifizierende Charakter von «neuen Tec≤hnologien» steht im Blickfeld linker Technikkritik.

Der linke Technikoptimismus ist deshalb aber nicht verschwunden. Zugespitzt wird das etwa im Akzelerationismus. Dieser geht davon aus, dass der Kapitalismus mit seinen eigenen Mitteln schneller zu schlagen ist, wenn die Entwicklung von Technik beschleunigt wird. Neben dieser «Mischung aus Techno, Terminator und Marx» finden sich auch emanzipatorisch aufgeladene Cyborg-Theorien oder Versuche, zu einer Synthese aus Sozialismus und Transhumanismus zu finden, im Lager des linken Technikoptimismus.

(Tom Strohschneider)

// ZUM WEITERLESEN

[1] Marx, Karl: Grundrisse der Kritik der politischen Ökonomie, Berlin 1983 (= Marx-Engels-Werke, Bd. 42).

[2] Panzieri, Raniero: Über die kapitalistische Anwendung der Maschinerie im Spätkapitalismus, in: Quaderni Rossi 1/1961.

[3] Linke und Technikkritik im 21. Jahrhundert, in: Gen-ethisches Netzwerk 193 (2009).

[4] Haraway, Donna: Ein Manifest für Cyborgs. Feminismus im Streit mit den Technowissenschaften, in: Hammer, Carmen u. a. (Hrsg.): Die Neuerfindung der Natur. Primaten, Cyborgs und Frauen, Frankfurt a.M. 1995, S. 33–72.

[5] Srnicek, Nick/Williams, Alex: Beschleunigungsmanifest für eine akzelerationistische Politik, unter: http://akzelerationismus.de/beschleunigungsmanifest.pdf.

// MASSENÜBERWACHUNG
// METADATEN

// MASSENÜBERWACHUNG

Seit den Enthüllungen von Edward Snowden ist allgemein bekannt, was vorher nur einige ahnten: Unsere digitale Kommunikation wird von Geheimdiensten überwacht. Nicht zielgerichtet einzelne, vielleicht viele Terrorverdächtige, sondern alles, was die Datenspeicher fassen können.

Es ist nicht neu, dass Sicherheitsbehörden so viele Daten haben wollen, wie sie kriegen können.

In Westdeutschland wurde die Rasterfahndung Ende der 1970er Jahre erstmals eingesetzt. Bei dieser Methode werden alle Personen erfasst, auf die bestimmte Merkmale zutreffen, die auch bestimmte Verdächtige haben. 2006 erklärte das Bundesverfassungsgericht die Rasterfahndung für verfassungswidrig und legte fest, dass sie nur erlaubt ist, wenn konkrete Gefahren «etwa für die Vorbereitung oder Durchführung terroristischer Anschläge» vorliegen.

2007 beschloss der Bundestag die Vorratsspeicherung, also die sechsmonatige Speicherung der Verkehrsdaten (auch Metadaten genannt) von Telefonaten und Internetnutzung. 2010 kassierte das Verfassungsgericht auch dieses Gesetz und legte fest, dass die Nutzung zwar nicht grundsätzlich verboten sei, aber sehr viel klarere Grenzen bräuchte.

Während sich die Bundesregierung am nächsten Entwurf probierte, wurden im Juni 2013 die ersten Artikel veröffentlicht, die auf den Snowden-Dokumenten basierten.

Der *Spiegel* veröffentlichte Zahlen zur Überwachung der NSA in Deutschland: Im Dezember 2012 hatte die NSA beispielsweise jeden Tag die Metadaten von 15 Millionen Telefonaten und 10 Millionen Internetverbindungen gespeichert.

Der britische Geheimdienst GCHQ zapfte laut BBC 200 internationale Glas-

faserkabel an und speicherte bis zu 600 Millionen Verbindungen pro Tag, jeweils 30 Tage lang. In den USA wurden sämtliche KundInnen des Providers Verizon überwacht, außerdem die Daten aller NutzerInnen der großen Internetfirmen, darunter Microsoft, Google, Apple und Facebook. Und das war erst der Anfang.

2014 beschloss der Bundestag den NSA-Untersuchungsausschuss, der feststellen soll, ob die von Snowden enthüllte Massenüberwachung in Deutschland stattfindet und was die deutschen Dienste damit zu tun haben.

Ergebnis bisher: reichlich Rechtsbrüche der deutschen Geheimdienste bei ihrer Kooperation mit ausländischen Nachrichtendiensten und ein handfester Skandal um Selektoren (Suchbegriffe), mit denen der BND erfasste Daten durchforstet.

Trotzdem hören wir immer wieder aus der Großen Koalition, dass es in Deutschland keine anlasslose Massenüberwachung gebe. Ein interessanter rhetorischer Schachzug, denn unter «anlassloser Massenüberwachung» wird verstanden, was landläufig als Vorratsdatenspeicherung bezeichnet wird: die vollständige Speicherung aller Kommunikationsdaten. Der BND speichert nach bisherigen Erkenntnissen tatsächlich nicht alle Daten, die er kriegen kann, sondern nur die, die er für die Erfüllung seiner – recht weit – gefassten Aufgaben braucht. Dazu gehört beispielsweise die Überwachung von Terrorismus, Schleuserei oder der weltweiten Konfliktregionen. Da fallen schon einige Daten an. Aber, so das Argument, über den Vorwurf der Massenüberwachung sei er jedenfalls erhaben. Massenhaft bedeutet jedoch nicht, dass alle Daten gespeichert werden, sondern sehr viele, und darunter sicherlich die Daten von sehr vielen Menschen, die gänzlich unverdächtig sind.

Alle Fakten ignorierend hat die Große Koalition nun das neue BND-Gesetz beschlossen und damit sogar eine Ausweitung der Überwachung. Warum das ein Problem ist, wusste schon Richelieu vor über 400 Jahren: «Man gebe mir sechs Zeilen, geschrieben von dem redlichsten Menschen, und ich werde darin etwas finden, um ihn aufhängen zu lassen.» Es gibt keine harmlosen Daten.

(Anne Roth)

// ZUM WEITERLESEN

[1] Humanistische Union: Geheimdienste vor Gericht, vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik 3/2016 (Themenheft 215), unter: https://is.gd/MqhNss.

[2] «Citizenfour», R: Laura Poitras, USA 2014.

[3] Wer kontrolliert wen?, Online-Archiv zum NSA-Untersuchungsausschuss, unter: https://werkontrolliertwen.de/.

// METADATEN

Metainformationsdaten, kurz Metadaten sind Informationen über Daten. Wer schon einmal in einer Bibliothek ein Buch ausgeliehen hat, hat bereits mit Metadaten gearbeitet. Auf der Suche nach einem Buch in einem Bibliothekskatalog durchstöbert man die Metadaten von katalogisierten Büchern, wie beispielsweise Autoren, Titel, Verlag oder Erscheinungsjahr.

In der Internet- und Telefonkommunikation werden Metadaten manchmal auch Verkehrsdaten genannt. Hierzu gehören unter anderem Verbindungs-, Kunden- und Geodaten. Während die eigentlichen Inhalte eines Telefonats oder einer E-Mail als Inhaltsdaten bezeichnet werden, beziehen sich Metadaten zum Beispiel auf die Teilnehmenden an einem Gespräch, Ort, Zeit und Dauer des Gesprächs, die genutzte Hard- und Software, die IP-Adressen oder Telefonnummern und dazugehörige Telefon- oder Internetverträge sowie eventuelle Bewegungen während, vor und nach dem Gespräch.

Metadaten geben ziemlich viel Auskunft über uns, sind leicht zu erfassen und leicht auszuwerten. Sie entstehen überall dort, wo mithilfe von technischen Geräten kommuniziert wird oder Daten transferiert werden. Als die Bundesregierung im Jahr 2007 zum ersten Mal ein Gesetz zur Vorratsdatenspeicherung beschlossen hatte, wurde darin beispielsweise festgelegt, dass solche Metadaten sechs Monate lang von den jeweiligen Internetdienstleistern aufbewahrt werden müssen, für den Fall, dass sie noch einmal von Strafverfolgungsbehörden gebraucht werden. Nach Protesten von gesellschaftlichen Gruppen und mehreren Bundestagsabgeordneten und einer damit einhergehenden Verfassungsbeschwerde wurde das Gesetz im Jahr 2010 für verfassungswidrig erklärt und vorerst zurückgenommen.

Am 16. Oktober 2015 hat die Große Koalition eine neue Variante, das Gesetz zur «Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten», im Schnellverfahren beschlossen, seit Dezember 2015 ist es in Kraft. Es legt für alle Anbieter von Internet- und Telekommunikationsdienstleistungen fest, dass sie Standortdaten der TeilnehmerInnen aller Mobiltelefonate, Rufnummern, Zeit und Dauer aller Telefonate, aller SMS-Nachrichten sowie die IP-Adressen aller InternetnutzerInnen und Zeit und Dauer der Internetnutzung bis zu zehn Wochen lang speichern müssen. Es bedarf keiner richterlichen Anordnung zur Herausgabe der Daten an Stellen der Strafverfolgung oder Gefahrenabwehr. Das bedeutet für die Praxis: Die Überwachung des E-Mail- und Telefonverkehrs wird zu einem Standardinstrument in der Strafverfolgung, von dem ohne weitere gesetzliche oder richterliche Genehmigungen Gebrauch gemacht werden kann.

Das Entscheidende an Metadaten ist, dass sie nicht verschlüsselt werden können. Ich kann beispielsweise den Inhalt meiner E-Mail verschlüsseln, aber an wen ich von welchem Computer und E-Mail-Programm und welcher IP-Adresse aus die E-Mail geschickt habe, lässt sich nicht verschlüsseln. Deshalb benötigen Metadaten einen besonderen rechtlichen Schutz. Mit dem neuen Gesetz zur Vorratsdaten-

speicherung hat die Bundesregierung jedoch genau das Gegenteil getan.
Eine Variante der **digitalen Selbstverteidigung** ist es, mithilfe von Verschleierungstechniken Anonymität und Privatsphäre zumindest teilweise wieder herzustellen. Nach diesem Prinzip funktioniert beispielsweise der Tor-Browser, der die Herkunft des Web-Surfenden durch eine Vielzahl von Weiterleitungen derart verschleiert, dass darüber die Anonymität des Nutzers oder der Nutzerin faktisch wiederhergestellt werden kann.
(Susanne Lang)

// ZUM WEITERLESEN

[1] Visualisierung eines Handy-Bewegungsprofils des Bundestagsabgeordneten von Bündnis 90/Die Grünen Malte Spitz, unter: https://is.gd/A2PHIT.
[2] Verein zum Betreiben von Tor-Servern in Deutschland, unter: www.zwiebelfreunde.de.
[3] Englischsprachige Website des Tor-Projekts, das die Tor-Software entwickelt, die auch auf der Website heruntergeladen werden kann, unter: www.torproject.org.

// NETZINFRASTRUKTUR
// NETZNEUTRALITÄT
// NUDGE/VERHALTENSÖKONOMIK

// NETZINFRASTRUKTUR

Struktur und Weiterentwicklung der technischen Voraussetzungen und Standards des Internets kommen weitgehend ohne den Staat zustande. Dieser begleitet die Entwicklung lediglich und greift nur im Falle von Fehlentwicklungen ein. Dies beruht auf der Regelung in Art. 87f. GG, nach der zwar der Staat dafür Sorge zu tragen hat, dass «angemessene und ausreichende Dienstleistungen» bei der Telekommunikationsinfrastruktur gewährleistet werden, die Dienstleistungen selber jedoch durch private Anbieter oder aber durch die aus dem Sondervermögen der Deutschen Bundespost hervorgegangenen Unternehmen zu erbringen sind. Um der Gewährleistungsverantwortung für die telekommunikative Grundversorgung (Art. 87 Abs. 1 GG) gerecht zu werden, sollte ein Breitband-Universaldienst mit einer zur Verfügung zu stellenden Bandbreite implementiert werden, die der Mehrheit der NutzerInnen zur Verfügung steht.

Zentrale Bedeutung im Rahmen der Nutzung des Internets kommt einer flächendeckenden Verfügbarkeit einer Breitbandgrundversorgung zu. Diese ist neben der Netzneutralität eine Grundvoraussetzung für Innovation und Sicherung eines freien Internets. Nur mit einer flächendeckenden Breitbandgrundversorgung können gleichwertige Lebensverhältnisse gesichert und kann eine digitale Spaltung der Gesellschaft verhindert werden. Neben der Übertragungsrate ist auch die Latenzzeit von großer Bedeutung. Darunter ist die Zeit zwischen dem Absenden eines Datenpakets und der Antwort des angesprochenen Servers zu verstehen.

Die Sicherstellung von flächendeckender Breitbandversorgung kann über verschiedene Wege geschehen. Im Rahmen von FTTC (Fiber-to-the-Curb) werden Glasfaserkabel bis zu den Kabelverzweigern verlegt und wird für die

letzte Meile die vorhandene Kupferkabelinfrastruktur genutzt. Die mobile Variante LTE wird vor allem in entlegenen und dünn besiedelten Regionen genutzt. Notwendig ist aber der Ausbau von FTTH (Fiber-to-the-Home) Glasfaserleitungen, auch wenn dies einen hohen Investitionsbedarf mit sich bringt. Denn es ist zu berücksichtigen, dass der mobile Internetzugang eine geteilte Ressource (ein sogenanntes «shared medium») ist. Je mehr NutzerInnen innerhalb einer Funkzelle, desto weniger verfügbare Bandbreite und desto länger die Latenzzeit. Schließlich kommt hinzu, dass im Regelfall die maximal erreichbaren Bandbreiten abhängig vom gewählten Tarif nur für ein begrenztes monatliches Datenvolumen zur Verfügung stehen.
Der Staat ist gefragt, die Sicherstellung mit Glasfaserbreitbandinternet aktiv zu unterstützen. Dies kann zum Beispiel über die Förderung von Kooperationen oder Investitionszuschüsse ebenso geschehen wie über staatliche Förderprogramme. Eine Möglichkeit wäre, Leerrohre bei Tiefbauarbeiten verpflichtend zu verlegen und Synergieeffekte zwischen kommunalen Versorgungsunternehmen und Telekommunikationsanbietern zu nutzen.
(Halina Wawzyniak)

// ZUM WEITERLESEN

[1] Deutscher Bundestag: Neunter Zwischenbericht der Enquete-Kommission «Internet und digitale Gesellschaft», Bundestags-Drucksache 17/12541, 19.3.2013, unter: https://is.gd/97lOg8.
[2] Initiative gegen digitale Spaltung, unter: www.geteilt.de.

// NETZNEUTRALITÄT

Unter Netzneutralität werden die Gleichbehandlung von Daten bei der Übertragung im Internet und der diskriminierungsfreie Zugang bei der Nutzung von Datennetzen verstanden. Bestandteil der Netzneutralität ist mithin die Gleichbehandlung aller Datenpakete unabhängig von Sender und Empfänger, dem Inhalt der Datenpakete und der Anwendung, welche diese Pakete generieren.
Internetdiensteanbieter (Provider oder auch Anbieter von Diensten, Inhalten oder technischen Leistungen, die für die Nutzung oder den Betrieb von Inhalten und Diensten im Internet erforderlich sind) behandeln nach dem Prinzip der Netzneutralität alle Datenpakete bei der Übertragung gleich. Dies nennt sich Best-Effort-Prinzip.
Netzneutralität ist eine Grundbedingung für ein freies und offenes Internet. Sie ist zudem auch ein Motor für Innovationen. Die Netzneutralität trägt zur Sicherung von Meinungsvielfalt und Pluralismus bei, dadurch wird kommunikative Chancengleichheit sichergestellt.
Netzneutralität verlangt ausreichend Übertragungskapazitäten. Netzbetreiber behaupten immer wieder, es gäbe Kapazitätsengpässe, ohne dies nachgewiesen zu haben. Unabhängig davon ist der Ausbau der Netzinfrastruktur dringend notwendig. Denn auch er wäre ein Gegenargument, im Hinblick auf die Bestrebungen eines nicht unerheblichen Teils der Betreiber von Telekommunikationsnetzen Qualitätsklassen einzuführen. Nur innerhalb dieser Kategorien soll dann die Netzneutralität

noch Geltung beanspruchen. Moderne IP-Netze bieten nämlich den Netzbetreibern die Möglichkeit für Netzwerkmanagement.

Es gab und gibt deshalb immer wieder Versuche, die Netzneutralität gesetzlich festzuschreiben. Mittlerweile ist allerdings die EU-Verordnung zum Telekommunikationsbinnenmarkt gebilligt und beschlossen worden. Diese Verordnung erlaubt Telekommunikationsunternehmen bestimmte Angebote vom Prinzip der Netzneutralität auszunehmen und sie als priorisierte Dienste zu behandeln und auf Überholspuren auszulagern. Die Telekommunikationsanbieter sehen hier die Möglichkeit zweiseitige Märkte und Zero-Rating-Angebote zu etablieren. Bei zweiseitigen Märkten müssten Anbieter von Inhalten nicht nur für den Anschluss an das Netz, sondern auch für die Nutzung zahlen. Zero-Rating meint, dass spezifische Dienste vom monatlichen Datenvolumen ausgeklammert werden. Da allerdings nach der EU-Verordnung angemessene Maßnahmen des Verkehrsmanagements und damit eine Durchbrechung des Prinzips der Netzneutralität nicht auf kommerziellen Erwägungen beruhen dürften und nur im Fall der Erforderlichkeit eines spezifischen Qualitätsniveaus erlaubt sind, dürften die Telekommunikationsanbieter falsch liegen. Derzeit laufen die Verhandlungen der Europäischen Regulierungsbehörden, wie die Verordnung konkret umgesetzt werden soll. (Halina Wawzyniak)

// ZUM WEITERLESEN

[1] La Quadrature du Net verteidigt die Rechte und Freiheiten von BürgerInnen im Internet, www.laquadrature.net/en/Net_neutrality.

[2] Berners-Lee, Tim: Long Live the Web: A Call for Continued Open Standards and Netneutrality, Scientific American, 1.12.2010, unter: https://is.gd/31xCbq.

[3] Netzneutralität im Rahmen der Vorgaben der EU-Verordnung gesetzlich absichern, Antrag, unter: https://is.gd/NEuVVZ.

[4] Deutscher Bundestag: Vierter Zwischenbericht der Enquete-Kommission «Internet und digitale Gesellschaft», Bundestags-Drucksache 17/8536, 2.2.2012, unter: https://is.gd/DICwKt.

// NUDGE/VERHALTENS-ÖKONOMIK

Behavioural Economy (dt.: Verhaltensökonomik) ist der Versuch, menschliches Verhalten in wirtschaftlichen Situationen zu erklären. Dafür wird das Verhalten des Menschen als rational, also stets gewollt und begründet angenommen. Dieser Rational-Choice-Theorie zufolge versuchen Individuen in sozialen Situationen ihren Nutzen im Rahmen ihrer Möglichkeiten zu optimieren, also bei einem möglichst geringen Einsatz einen möglichst hohen Gewinn zu erzielen. Weil dieses statische Modell unrealistisch ist, sprechen neuere Theorien den Menschen die Fähigkeit zu, ihre Situation zu verändern, um so bessere, zu ihren Vorstellungen passendere Ergebnisse zu erzielen. Sie versuchen also, ihren Handlungsrahmen zu verändern, und spekulieren dabei auf eine bessere Zukunft. Die aus der Summe dieser individuellen Spiele hervorgehende Gesellschaft muss aber nicht rational sein, sondern kann aus vielfältigen Gründen abträgliche Folgen für alle Beteiligten haben.

Der Begriff Nudging beschreibt nun den Versuch, gemäß solchen Theorien eine staatliche oder betriebliche Handhabe für die Gestaltung von Gesellschaften und Gemeinschaften zu entwickeln. Individuen sollen durch kleine «Stupse» (engl.: nudge) zur erwünschten Handlung mit größerem Nutzen für das Gemeinwohl gebracht werden. Der Rechtswissenschaftler Cass Sunstein und der Wirtschaftswissenschaftler Richard Thaler haben den Begriff in ihrem Buch «Nudge: Wie man kluge Entscheidungen anstößt» (2008) geprägt. Ihnen zufolge können zum Beispiel staatliche Institutionen den Rahmen verändern, in dem Individuen Entscheidungen treffen, und zwar nicht durch ökonomische Anreize, Zwang oder Verbote, sondern durch subtile Eingriffe. Das erwünschte Verhalten wird erleichtert, nahegelegt oder das unerwünschte Verhalten erschwert. Weil dabei auch immer das unerwünschte Verhalten möglich bleibt, sprechen die Autoren von einem libertären Paternalismus: Man muss nicht, man soll. Ein Beispiel für so einen Nudge sind Organspende-Regelungen, bei denen das erwünschte Verhalten «Organe spenden» vorausgesetzt wird und das unerwünschte Verhalten einen extra Handlungsschritt bedarf: «Ich will kein Organspender sein!» Beide Handlungsalternativen bleiben, theoretisch, offen. Laut Thaler sei dies ein dritter Weg zwischen völliger, unregulierter Freiheit und staatlicher Planwirtschaft. Besondere Möglichkeiten ergeben sich durch Verhaltensökonomik und Nudging in der digitalen Gesellschaft. Hier sind soziale Kontexte und Verhaltensrahmen oft besonders gut beeinflussbar – und überwachbar. Allein durch die Gestaltung von Benutzeroberflächen kann so ein erwünschtes Verhalten unterstützt werden. Wird dies gegen die Interessen der Nutzer versucht, spricht man von Dark Patterns: Ein Design, das schädliches Verhalten unterstützt, indem zum Beispiel Alternativen verschleiert werden oder gewohnte Handlungsmuster in einem anderen Kontext präsentiert werden, wo sie etwa zum Abschluss eines Abonnements führen. Die Identifikation von besonders wirksamen Nudges

kann wiederum durch die Auswertung massiv erfasster Verhaltensdaten verbessert werden. Der Staat, die Organisation, versucht ein möglichst passendes Modell individuellen Verhaltens zu erstellen, um es dann zu verändern. Je weiter die Digitalisierung des Alltags voranschreitet, desto mehr Möglichkeiten zur noch subtileren Gestaltung der Handlungsrahmen durch Nudges ergeben sich. Weil Nudges auch einen Verlust von Autonomie bedeuten können, wenn sie nicht transparent sind oder keine wirklichen Alternativen offen lassen, werden sie kontrovers diskutiert, zumal wenn sie in vielen Lebensbereichen angewendet werden. Aus dem Nicht-müssen-aber-Sollen, also aus individuellen Entscheidungen moralischen Charakters kann so ein neuer Zwang entstehen. Oft genug in die richtige Richtung gestupst, verschließen sich andere, richtige, frei gewählte Richtungen.
(Felix Knoke)

// ZUM WEITERLESEN

[1] Cameron, David: The Next Age of Government, TEDTalks, unter: https://youtu.be/3ELnyoso6vI.
[2] Friebe, Holm/Pankow, Mads: Nudge! Nudge! – Was Design von Verhaltenspsychologie lernen kann, Vortrag auf der re:publica 2015, 6.5.2015, unter: https://youtu.be/XD937-w-43E.
[3] Leonard, Thomas/Thaler, Richard/Sunstein, Cass: Nudge. Improving Decisions about Health, Wealth, and Happiness, New Haven 2008, unter: https://is.gd/fGTl0s.

// OPEN DATA

Das Konzept Open Data (Offene Daten) ist beseelt von der Idee, dass Offenheit gut für eine lebendige Demokratie und gesellschaftliche Innovationen ist. Open Data bedeutet, dass Daten, insbesondere jene, die bei öffentlichen Institutionen anfallen, frei verfügbar und weiter nutzbar sein sollen. Der Bund, Kommunen, öffentliche Einrichtungen wie Ministerien, Behörden oder Verwaltungen produzieren eine Unmenge von Daten, die sich bisher kaum produktiv wenden lassen.

Die Daten sind dabei sehr unterschiedlicher Natur. Es kann sich dabei um Rohdaten handeln wie Klimadaten oder Daten von Wetterstationen, Geodaten von Landschaftsvermessungen, Verkehrsdaten des öffentlichen Personennahverkehrs oder bearbeitete Daten in Form von Gesetzen, Urteilen oder Gutachten. Angesichts dieses ungehobenen Datenschatzes verfallen nicht nur Wissenschaft und Forschung, sondern auch zahlreiche (junge) Unternehmen in Goldgräberstimmung. Sie wittern neue Geschäftsmodelle und Big-Data-Anwendungen, wie beispielsweise Apps (Software-Anwendungen) für die Parkplatzsuche, für die spontane Wahl des Verkehrsmittels oder für die Vorhersage von Pollenbelastungen. Kritische Stimmen sehen darin eine weitere ökonomische Inwertsetzung eines öffentlichen Gutes.

Ob vorranging datengetriebene Unternehmen von der Öffnung der Daten profitieren oder auch zivilgesellschaftliche Akteure gemeinwohl-, sozial- oder ökologisch orientierte Modelle entwickeln können, hängt maßgeblich davon ab, unter welcher (Urheberrechts-)Lizenz Daten freigegeben werden. Open Data rüttelt damit auch an einer gesellschaftspolitischen Grundfrage der Wissensgesellschaft. Sollte die Nutzung von öffentlich produzierten Daten von der Gnade der Verwaltung abhängen

oder sollten Daten als Gemeingüter (Commons) verstanden werden, sollte Daten-Eigentum erhoben werden?

Die Bundesregierung hat ein Portal für einige staatliche Daten aufgesetzt. Allerdings wurde für dieses «GovData» genannte Internetportal eine eigene Lizenz entwickelt, die nur bedingt kompatibel zu offenen Modellen wie Creative Commons ist. Open Data ist ein Puzzleteil der Openess-Bewegung (Open Source, Open Access, Open Government etc.). Nicht nur offene Lizenzen sind nötig, sondern auch offene Schnittstellen (API), damit auf die Daten zugegriffen werden kann, oder offene Standards, damit Daten interoperabel über Plattformen hinweg genutzt werden können. Die Enquete-Kommission «Internet und digitale Gesellschaft» des Deutschen Bundestages hat in ihren Handlungsempfehlungen an die Bundesregierung Kriterien formuliert, damit Open Data zur vollen Entfaltung kommt. Den BürgerInnen müssen von öffentlichen Stellen Daten nutzerfreundlich, vollständig, primär, zeitnah, kosten- und barrierefrei, maschinenlesbar, nicht diskriminierend, interoperabel, nicht proprietär und lizenzfrei zugänglich gemacht werden.

Open Data entstammt also einerseits der Openess-Bewegung. Andererseits wurde die Idee auch stark von der Debatte um «Transparenz» beeinflusst. Für eine vitale Demokratie ist es essentiell, dass der Staat transparent agiert. Denn nur informierte BürgerInnen können mündig über die gesellschaftliche Zukunft mitbestimmen. Open Data ist also auch eng mit E-Democracy verwoben.

Aus dieser Idee heraus wurden Informationsfreiheitsgesetze (IFG) verabschiedet. Diese gestehen den BürgerInnen ein Recht auf Zugang zu Informationen gegenüber Behörden zu. Ein großer Schritt, aber noch kein Paradigmenwechsel. Denn Behörden sitzen wie zu Zeiten des preußischen Obrigkeitsstaates auf Daten und geben sie nur auf einzelne Nachfragen frei, oder auch nicht. Neben den erwähnten Urheberrechten wird immer wieder das Feigenblatt der Betriebs- und Geschäftsgeheimnisse zur Ablehnung angeführt, da diese einen höheren verfassungsrechtlichen Stellenwert genießen. Daten per IFG-Anfrage zu befreien ist ein teilweise kostspieliges und zeitaufwendiges Unterfangen. Nur wenige Akteure der engagierten Zivilgesellschaft verfügen über das technische und rechtliche Wissen, um beispielsweise Gutachten des Wissenschaftlichen Dienstes des Bundestages öffentlich zugänglich zu machen (u. a. Open Knowledge Foundation). Trotz der Hürden nehmen die IFG-Anfragen jährlich drastisch zu.

Open Data wiederum verlangt eine echte Umkehr eines Verwaltungsprinzips und einen Kulturwandel. Behörden müssen selber proaktiv sämtliche Daten freigeben. Nur in begründeten Einzelfällen, wenn beispielsweise die Wahrung von Grundrechten wie Persönlichkeits- oder Datenschutz dagegen sprechen, dürfen einzelne Informationen zurückgehalten werden – getreu der alten Ethik des Chaos Computer Clubs «Öffentliche Daten nützen, private Daten schützen».

Und doch, zahlreiche Studien der EU-Kommission, des Normenkontrollrats und der Open Knowledge Foundation konstatieren, dass Deutschland zu den Schlusslichtern beim Zugang zu öf-

fentlichen Datenbeständen gehört. Und das, obwohl es die letzten Jahre wahrlich nicht an (Lippen-)Bekenntnissen gefehlt hat. Alle Fraktionen im Bundestag haben in zahlreichen Anhörungen und Plenardebatten den Wert von Open Data gepriesen, die G8 hat eine Open Data Charta verabschiedet, die Bundesregierung ist nach Jahren des Zauderns der Open Government Partnership beigetreten und hat einen nationalen Aktionsplan ausgerufen. Nur geschehen ist in den vergangenen Jahren sehr wenig. Immerhin hat die Bundesregierung angekündigt, auf den letzten Metern der Legislaturperiode ein Open-Data-Gesetz zu liefern, das Behörden zur Öffnung der Daten verpflichtet. Der Zwang zur Freiheit kommt also vielleicht doch noch.
(Chris Piallat)

// ZUM WEITERLESEN

[1] Website der Open Knowledge Foundation Deutschland, unter: https://okfn.de/.
[2] Das Open Data Handbuch der Open Knowledge Foundation, unter: http://opendatahandbook.org/.
[3] Bundeszentrale für Politische Bildung: Dossier Open Data, unter: www.bpb.de/gesellschaft/medien/opendata/.
[4] Deutscher Bundestag: Siebter Zwischenbericht der Enquete-Kommission «Internet und digitale Gesellschaft», Bundestags-Drucksache 17/12290, 6.2.2013, unter: https://is.gd/2mQW2s.
[5] The Open Data Research Portal, Online-Portal des Instituts «Fraunhofer FOKUS», unter: http://open-data.fokus.fraunhofer.de.

// PLATTFORMKAPITALISMUS
// PLATTFORMNEUTRALITÄT
// PREDICTIVE POLICING

// PLATTFORMKAPITALISMUS

Plattformen sind proprietäre Anwendungen oder Online-Angebote, die meist kostenlos eine Dienstleistung anbieten. Die Plattformen stellen eine virtuelle Infrastruktur zur Verfügung, auf der zwischen Dritten vermittelt wird. Der englische Begriff «platform» kommt aus der Software-Entwicklung und bezeichnet dort eine Basistechnologie, auf der dann bestimmte Dienste aufbauen.

Das weltweit größte Taxiunternehmen besitzt keine Taxis (Uber), der weltweit größte Vermittler von Übernachtungen besitzt keinerlei Immobilien (Airbnb) und die das Internet dominierenden Medienkonzerne (Google, Facebook) stellen selbst keine Medien ins Netz. Allen diesen Unternehmen ist gemeinsam, dass sie lediglich die Plattform zur Verfügung stellen, auf der die UserInnen kommunizieren, Geschäfte abschließen, etwa Taxifahrten oder Übernachtungen buchen. Die Unternehmen selbst sind nicht für die Inhalte verantwortlich, beherrschen aber die Form.

Oft wirken sie sich disruptiv auf bestehende Branchen aus, weil sie schnell und günstig einen privaten, viel weiter gefassten Markt bedienen oder diesen erst kreieren. Sie stoßen nicht selten in unbekanntes und nicht reguliertes Terrain vor, setzen damit eigene Standards oder umgehen bestehende gesetzliche Regelungen. Diese werden ersetzt durch ein System gegenseitiger Bewertungen aller Beteiligten und ein disziplinierender Feedback-Loop entsteht.

Alle Plattformen behalten sich vor, jederzeit die Spielregeln zu verändern, wie Bezahlmodelle oder Änderungen der Privatsphäre-Einstellungen. Ihnen gegenüber stehen die einzelnen NutzerInnen, die keinerlei Einfluss auf das Gesamtsystem haben. Dadurch entsteht Plattformkapitalismus in Reinform.

Durch den Netzwerkeffekt, bei dem der Nutzen eines Gutes mit steigender

Zahl der NutzerInnen zunimmt, erzielen sie rasch eine Monopolstellung. Solche Effekte treten insbesondere bei Internetplattformen auf, zum Beispiel bei Social-Media-Plattformen oder Auktionshäusern. Der Netzwerkeffekt, der zur Herausbildung von Monopolen führt, ist auch ökonomisch spürbar. So entfallen etwa 70 Prozent des Umsatzes von 300 Milliarden Dollar, den alle börsennotierten US-Internetfirmen zuletzt gemacht haben, auf gerade einmal fünf Firmen. 57 Prozent der Erlöse flossen allein in die Kassen von Amazon und Alphabet (Google).

Das Paradebeispiel für eine Plattform ist Google: Die Websuchmaschine Google stellt selbst keine Inhalte ins Netz, sie vermittelt lediglich zwischen Website-Betreibern und deren BesucherInnen. Diese Kernfunktion führt ein Algorithmus aus, keine Beschäftigten. Nicht nur skaliert der Algorithmus besser, er ist auch viel billiger als menschliche Arbeitskraft. Die eigentliche Arbeit machen in Googles Modell nicht Angestellte der Firma, sondern das Publikum, die KundInnen und NutzerInnen selbst – die dafür keinerlei Bezahlung erhalten.

Jaron Lanier nennt diese Plattformen – angelehnt an Homers Odyssee – «Sirenen-Server». Sie locken NutzerInnen mit kostenlosen Services an, lassen sie dann aber nie mehr aus der Umklammerung los. Die Sirenen waren erfolgreich, sobald ein Wechsel nicht mehr möglich ist, sei es aus Mangel an Alternativen, weil zu kostspielig, oder weil schlicht alle beim Anbieter gelandet sind: Microsoft, Google, Facebook.

Der Plattformkapitalismus kommt für die Inhalte, die von ihm angeboten werden, weitgehend ohne ArbeiterInnen aus: Bei Facebook, Pinterest, Google gibt es niemanden, der Beiträge erstellt, Fotos hochlädt oder Suchanfragen bearbeitet. Alle Aktionen und Inhalte, von denen sich diese Plattformen nähren, entstehen einzig und allein durch das Verhalten der NutzerInnen.

(Timo Daum)

// ZUM WEITERLESEN

[1] Lanier, Jaron: Wem gehört die Zukunft?, Hamburg 2013.

[2] Choudary, Sangeet Paul/Van Alstyne, Marshall W./Parker, Geoffrey G.: Platform Revolution: How Networked Markets Are Transforming the Economy, New York 2016.

[3] Lobo, Sascha: S.P.O.N. – Die Mensch-Maschine: Auf dem Weg in die Dumpinghölle, Spiegel Online, 3.9.2014, unter: http://spon.de/aejBc.

// PLATTFORMNEUTRALITÄT

Im Kern geht es bei der Plattformneutralität um einen diskriminierungsfreien Zugang zu den Infrastrukturen (Plattformen), die einen gesellschaftlichen Austausch ermöglichen. Damit greift der Begriff der Plattformneutralität die Debatte auf, nach der zukünftig der Zugang zu Ressourcen weniger über Eigentum stattfinden wird. Vielmehr komme es auf eine diskriminierungsfreie Zugangsmöglichkeit zu Ressourcen an.

Auf der einen Seite verlangt demnach Plattformneutralität, dass ein Programm auf verschiedenen Plattformen ausgeführt werden kann. Auf der anderen Seite – und häufiger im Zentrum von Debatten – verbindet sich mit dem Konzept der Plattformneutralität der Gedanke, dass Webplattformen (z. B. YouTube, Spotify und der Apple Store) ihre Position nicht zum Nachteil anderer Stakeholder (Interessierte und Betroffene eines Prozesses) missbrauchen dürfen. Im Rahmen von Kommunikation und Wissen soll durch Plattformneutralität eine Selektion der Kommunikation von Dritten verhindert werden. Eine genaue und allgemein anerkannte Definition von Plattformneutralität existiert bisher wohl aber nicht. Frühere VertreterInnen der Theorie von der Plattformneutralität stellen diese teilweise heute wieder infrage.

Bei der Debatte um Plattformneutralität geht es am Ende aber auch um die Frage, wie eine Monopolbildung verhindert werden kann, da diese die Freiheit des Internets einschränkt und einen diskriminierungsfreien Zugang zu den entsprechenden Angeboten nicht sicherstellen kann. Mit welchen Mitteln die Regulierung von Plattformen und die Verhinderung von Monopolen stattfinden soll, ist heftig umstritten. Auf der einen Seite wird in Richtung staatlicher Regelungen gedacht, auf der anderen Seite wird auf den Wettbewerb oder Selbstorganisation gesetzt.

Das Konzept der Plattformneutralität, soweit es sich auf den diskriminierungsfreien Zugang bezieht, lässt sich auf viele gesellschaftliche Bereiche ausweiten und lässt sich vielleicht am besten mit dem Begriff Teilhabegerechtigkeit umschreiben.

(Halina Wawzyniak)

// ZUM WEITERLESEN

[1] Seemann, Michael: Netzinnenpolitik. Grundzüge einer Politik der Plattformgesellschaft, Vortrag auf der re:publica 2016, unter: https://voicerepublic.com/talks/4570.

[2] Sohn, Gunnar: Plattformen als regulierender Leviathan – Kann das funktionieren?, 11.5.2016, unter: https://is.gd/bAQfcy.

[3] Monopolkommission, Wettbewerbspolitik: Herausforderung digitale Märkte, Sondergutachten 68, unter: https://is.gd/GPzK6X

// PREDICTIVE POLICING

Mit dem Begriff Predictive Policing (dt.: vorhersagende Polizeiarbeit) ist allgemein ein Vorgehen in der Kriminalitätsbekämpfung gemeint, das auf zukünftiges Verhalten von Menschen schließt, um so präventiv kriminelle Taten zu unterbinden oder einzudämmen. Spezieller spricht man heute von Predictive Policing, wenn mittels Software und großen Datenmengen (**Big Data**) mögliche Tatorte und -zeiträume vorhergesagt werden. Dabei deutet sich eine Entwicklung an, dass zukünftig auch Tatverdächtige vor ihrer Tat ermittelt werden. In Deutschland gibt es seit 2013 einige Modellversuche vor allem mit der vom Institut für musterbasierte Prognosetechnik entwickelten Software «Precobs». In anderen Ländern, insbesondere den USA, werden vergleichbare Programme bereits in der Praxis umfangreich eingesetzt. Einige Systeme suchen dabei bereits gezielt nach Menschen und Gruppen, die aus Sicht der Software in nächster Zeit zum Beispiel an einem Gewaltverbrechen beteiligt sein könnten.

In herkömmlicher Polizeiarbeit werden Erfahrungen mit Kriminalität dazu genutzt, zeitliche und räumliche Schwerpunkte krimineller Aktivitäten zu identifizieren. Hierzu werden bereits seit Langem statistische Methoden eingesetzt. Es entstehen so Wahrscheinlichkeitsaussagen über das Auftreten bestimmter Taten in örtlichen und zeitlichen Räumen. Die Grundlage bilden kriminologische und soziologische Modellüberlegungen zu Mustern im Verhalten von Kriminellen. Diese sind aber in der Regel nur bedingt aussagekräftig und lassen sich meist nur auf bestimmte Deliktfelder anwenden.

Predictive Policing im eigentlichen Sinne erweitert diese Analysemethoden durch Digitalisierung. Größere Datenmengen und komplexere **Algorithmen** ermöglichen der Software eine wachsende Präzision in der Erkennung von Mustern und der Vorhersage der nächsten Entwicklungen. Neben den üblichen kriminologischen **Daten** können dabei auch fachfremde Daten, zum Beispiel Bevölkerungsstatistiken, Daten der Wirtschafts- und Sozialgeografie sowie ähnliche bereits erhobene Daten herangezogen werden. Überlegungen zielen darauf ab, diese Datenbasis weiter auszubauen und ihre Analyse zu verstetigen. So könnten zukünftig **Metadaten** aus digitaler Kommunikation, Daten aus **sozialen Netzwerken**, kameragestützten Erkennungsverfahren und ähnlichen Quellen in eine solche Analyse in Echtzeit einfließen.

Die Herkunft des Predictive Policing aus der herkömmlichen Polizeiarbeit macht sich auch bei der Bestimmung ihrer Problemen und Gefahren bemerkbar. So inkorporieren die genutzten Programme zum Teil problematische Praktiken der Polizeiarbeit. Je nach Datengrundlage und Gestaltung der Software reproduzieren die Algorithmen diskriminierende Sichtweisen und geben ihnen den Anschein objektiver Kriterien. Während bestehende Brennpunkte oder Personengruppen so weiter stigmatisiert werden, kann sich ein blinder Fleck bei Straftaten ergeben, die nicht den herkömmlichen Mustern entsprechen. Die ohnehin illegale Kriminalisierung von Menschen durch die Polizei allein auf-

grund äußerer und sozialer Merkmale wie beim Racial Profiling könnte so zum alltäglichen Vorgehen werden. Auch kann Predictive Policing als eine Form der Rasterfahndung angesehen werden, da mit ihr anlasslos und automatisiert beliebige Daten durchsucht werden, um aus typisierten Mustern vermeintliche TäterInnen zu identifizieren.

Wie jeder andere Algorithmus kann auch eine bei Predictive Policing verwendete Software durch Beobachtung in ihrer Arbeitsweise nachverfolgt werden. So kann von Kriminellen mit einer gewissen Wahrscheinlichkeit vorausbestimmt werden, welche Ergebnisse die Software ausgibt und wie die Polizei daraufhin ihre Arbeit gestaltet. Damit ist es möglich, Polizeiarbeit gezielt zu umgehen, da sie vorhersagbar wird (Predictible Policing).

(Stefan Enke)

// ZUM WEITERLESEN

[1] Gluba, Alexander (LKA Niedersachsen): Predictive Policing – eine Bestandsaufnahme. Historie, theoretische Grundlagen, Anwendungsgebiete und Wirkung, Hannover 2014, unter: https://is.gd/fBevJt.

[2] Jones, Chris: Predictive policing: mapping the future of policing?, opendemocracy.net, 10.6.2014, unter: https://is.gd/IAfkx2.

[3] Brühl, Jannis: Polizei-Software soll Verbrechen voraussagen, in: Süddeutsche Zeitung, 10.9.2014, unter: https://is.gd/0kPxR3.

[4] Biermann, Kai: Noch hat niemand bewiesen, dass Data Mining der Polizei hilft, Zeit Online, 29.3.2015, unter: https://is.gd/AygKqz.

// ROBOTIK/ROBOTER

Robotik befasst sich mit der Entwicklung von Robotern. Roboter sind Maschinen, bei denen bewegungsgebende Elemente («Aktoren») zusammenwirken mit Sensoren, die Umweltreize aufnehmen können, und der Steuerung der Maschine durch Software. Heute liegt der Schwerpunkt der Steuerung bei Algorithmen und Künstlicher Intelligenz. Roboter reichen vom Mars-Rover in der Raumfahrt über teilautonome Fertigungsroboter in der Industrie, Pflegeroboter als künftiges Wohl oder Wehe im Gesundheitsbereich hin zu Staubsauger-, Rasenmäher- und Spielzeugrobotern oder Robotern für die Rettung von Erdbebenopfern. Drohnen genannte Flugroboter reichen vom massentauglichen Spielzeugflieger bis zum tödlichen Kriegsroboter.

Auch Rollstühle mit Autopilotfunktion, selbstfahrende Autos oder intelligente Gabelstapler fallen unter die Definition. Hier werden Motoren, Räder, Lenkachsen oder Hubsysteme gekoppelt mit 3-D-Kameras, positionsbestimmenden Sensoren und Software, die es dem Gerät erlaubt, selbstständig Waren im Lager zu verrücken, ältere Menschen vom Supermarkt nach Hause zu geleiten oder im fahrerlosen öffentlichen Personennahverkehr eingesetzt zu werden.

Smartphones erfüllen dank ihrer Sensoren und immer intelligenteren Steuerung mindestens zu zwei Dritteln die Definition eines Roboters. Wenn Menschen sich anhand einer Karten-App durch die Stadt bewegen, mutieren sie dann in Symbiose mit dem Gerät zum menschenähnlichen, aber fremdbestimmten Androiden oder zum Cyborg, der kraftvollen postmodernen Kombination aus Mensch und Maschine?

Roboter erweitern oder ersetzen Aktionsradius und Blickfeld der Menschen. Dieses Ersetzen menschlichen Agierens macht den Hauptteil der Debatte um das Für und Wider der Robotik aus.

Wie viel (Lohn-)Arbeit Roboter künftig ersetzen und ob das die endgültige Unterdrückung der Arbeiterklasse oder endlich den Beginn der freien Menschheit darstellt, darüber streiten sich nicht nur Linke von Beginn der Robotik an (siehe Automatisierung der Arbeit). Ein Vorschlag, wie auf das Ersetzen menschlicher Arbeit durch Roboter reagiert werden könnte, ist die Automatisierungsdividende. Der mithilfe von Robotern erwirtschaftete Profit soll durch eine besondere Abgabe anteilig vergesellschaftet werden.

Doch Roboter fordern uns nicht nur hinsichtlich Lohnarbeit und Warenproduktion heraus, sondern allgemein bezüglich ihres Interagierens in der Welt. Selbstfahrende Autos zum Beispiel bewegen sich auf realen Straßen, erkennen autonom Verkehrszeichen, Verkehrslage und mehr. Dazu kommunizieren sie in Echtzeit mit Datenbanken im Internet. Dies wiederum kann (wie beim Mitführen eines Smartphones) der lückenlosen Überwachung der NutzerInnen dienen.

Die 1942 von Isaac Asimov formulierten Robotergesetze laufen darauf hinaus, dass Roboter den Menschen hilfreich und nicht schädlich sein sollen. Aber wer bezahlt die Entwicklung neuer Roboter? Rüstungskonzerne, Spielzeughersteller oder der Staat über Förderprogramme, etwa für den Katastrophenschutz oder die Zukunft der Altenpflege? Und wer haftet, wenn Roboter Unfälle verursachen? Die Systeme werden derzeit künstlich dümmer gehalten als nötig, damit die Verantwortung für ihr Tun und damit auch die Haftung bei den NutzerInnen liegt.

Wie autonom könnten Autos sein, wenn die Industrie die Haftung für die Technik übernehmen würde? Oder gar die Roboter selbst? Die EU-Kommission denkt darüber nach, im Rechtswesen neben natürlichen und juristischen Personen auch eine elektronische Person mit auf sie zugeschnittenen Rechten und Pflichten einzuführen.

(Jörg Braun)

// ZUM WEITERLESEN

[1] Nourbakhsh, Illah: Robot Futures. Cambridge 2013, begleitendes Blog, unter: http://robotfutures.org.

[2] Dath, Dietmar: Maschinenwinter, Frankfurt a.M. 2008.

[3] Rieger, Frank: Roboter müssen unsere Rente sichern, in: Frankfurter Allgemeine Zeitung, 18.5.2012, unter: http://www.faz.net/-gqz-6zy1g.

[4] Hegmann, Gerhard: EU will Roboter per Gesetz bändigen, welt.de, 23.6.2016, unter: https://is.gd/vXVT6G.

// SCHWARMINTELLIGENZ/SCHWARMDUMMHEIT
// SHARING ECONOMY // SILICON VALLEY // SMART CITY
// SMART EVERYTHING // SOZIALE MEDIEN/WEB 2.0
// STAATSTROJANER

// SCHWARMINTELLIGENZ/ SCHWARMDUMMHEIT

Der Begriff Schwarmintelligenz (auch Weisheit der Massen oder Kollektive Intelligenz) wird immer dann herangezogen, wenn man das Verhalten eines Kollektivs beschreiben will, das komplexer ist als das der einzelnen Individuen. Der Begriff Schwarmdummheit beschreibt dasselbe Phänomen, nur mit einem unerwünschten, also *dummen* komplexen Verhalten als Konsequenz. Oft wird der Begriff aber auch vereinfacht als Quelle für ein kollektiv erarbeitetes Wissen verwendet, zum Beispiel bei Wikipedia oder spontanen sozialen Bewegungen und Trends in sozialen Medien. Etwas allgemeiner ausgedrückt, beschreibt der Begriff also die Alltagserfahrung, dass Kollektive ein Eigenleben zu führen scheinen. Dabei kann das ganz unterschiedlich sein: Bei Wikipedia wird aus genügend Halbwissen ein ganzes Wissen, spontane Smart Mobs können dank technischer Unterstützung wie ein Vogelschwarm um Hindernisse fließen und bestimmte Themen schälen sich im Internet aus dem Alltagsrauschen heraus und nehmen, ohne dass eine einzelne Person das beschlossen hat, feste Formen an. Der Duden beschreibt das hübsch als «Fähigkeit eines Kollektivs zu sinnvoll erscheinendem Verhalten».
Das immer wieder vorgebrachte Beispiel ist der Ameisenstaat, indem eine Vielzahl kommunikativ miteinander verbundener Ameisen einen komplexen Superorganismus bildet. Dessen Fähigkeiten gehen weit über die der einzelnen Ameisen hinaus. Aus dem Zusammenspiel der einzelnen Elemente entsteht ein komplexes System mit neuen Eigenschaften, die nicht mehr direkt aus den einzelnen Eigenschaften der Elemente erklärt werden können. Dieses Phänomen nennt man Emergenz.
Weil Emergenz eine Funktion der zunehmenden Komplexität eines Systems ist und Komplexität mit der

Anzahl der möglichen Kombinationen der miteinander verschalteten Individuen wächst, erlebt dieser Begriff im Internet eine Renaissance: Hier sollen technisch vermittelt neue, globale und trotzdem eng verknüpfte Kollektive entstehen. Weil sich solche Gebilde nicht langwierig herausbilden müssen, sondern relativ spontan entstehen können, spricht man auch von Smart Mobs: spontane, intelligent und effizient handelnde Kollektive. So sollten zum Beispiel soziale Bewegungen durch technische Vernetzung neues Handlungspotenzial gewinnen. Howard Rheingold prägte diesen Gedanken in seinem Buch «Smart Mobs: The Next Social Revolution» (2007): «Bringt man diese verschiedenen technischen, ökonomischen und sozialen Komponenten zusammen, entsteht eine Infrastruktur, die ein bestimmtes, menschliches Handeln ermöglicht, das zuvor nie möglich war. Die ‹Killer-Apps› der zukünftigen mobilen Infocom-Branche werden nicht Hardware oder Software sein, sondern soziale Praktiken.»

Oft berücksichtigen solche Theorien aber nicht die Anfälligkeit der technischen Unterstruktur für Manipulation und Überwachung. In dem Maße, in dem sich soziale Bewegungen technisch organisieren, machen sie sich abhängig von deren Integrität – die kaum überprüfbar und gewährleistbar ist. Zumal «Effizienz» und «intelligentes Handeln» eben kein zwangsläufiges Ergebnis von Schwarmorganisationen ist – sie können genauso gut schädliches oder dummes Verhalten hervorbringen und stabilisieren.

Das wohl interessanteste Potenzial des Begriffs Schwarmintelligenz ist seine Nützlichkeit als Analyse-Brille, um vernetzte Strukturen zu kritisieren, wie sie auch im kybernetischen Staat oder in Smart Citys forciert werden. In einer ausreichend komplexen Struktur treten unvorhergesehene, emergente Phänomene auf, die konkrete Auswirkungen für alle Personen in und außerhalb dieser Struktur haben. Ob diese Phänomene erwünscht sind oder nicht, ist eine politische Entscheidung. Wie sie verstärkt oder abgeschwächt werden können, bedarf aber idealiter ein Wissen über das gesamte Netzwerk und darüber hinaus. Wer in so einer vernetzten Situation das größte Wissen über die Struktur besitzt, hat das größte Potenzial sie gezielt zu beeinflussen. Den anderen bleibt vor allem eine Sabotage der Infrastruktur oder ein Verweigerungshandeln, um Netzwerkanalysen zu erschweren oder einfacher zu handhabende Strukturen zu erzwingen. Denn ein Schwarm kann ein interessantes Eigenleben entwickeln, aber er ist auch als Ganzes empfänglich für äußere Einflüsse, auch wenn es die einzelnen Mitglieder nicht wollen oder besser wissen. Und wer ist eigentlich verantwortlich für ein emergentes Phänomen – der Schwarm? (Felix Knoke)

// ZUM WEITERLESEN

[1] Grotelüschen, Frank: Weniger dumm im Kollektiv, Deutschlandfunk, 26.12.2013, unter: https://is.gd/B9eZqe.
[2] Reuter, Matthias: Schwarmintelligenz, Video, unter: https://youtu.be/eNeLXnuWi2M.
[3] Rheingold, Howard: Smart Mobs. The Next Social Revolution, Cambridge 2007.

// SHARING ECONOMY

«Sharing is caring» (dt.: wer teilt, der hilft), so lautet ein englisches Sprichwort, das von den VertreterInnen der Sharing Economy gern und oft angeführt wird. Das Sprichwort impliziert, dass Teilen etwas ist, das man nicht tut, um daraus einen Vorteil oder einen Gewinn zu erlangen, sondern schlicht, um zu helfen. Als ein Akt, der keine Gegenleistung einfordert, scheint das Prinzip des Teilens der ökonomischen Logik also grundlegend entgegenzustehen.

Dieser Vorstellung vom Teilen widerspricht die Sharing Economy schon in ihrem Namen grundsätzlich, ein Begriff, der Mitte der 2000er Jahre in den USA entstand und keinem spezifischen Autor zugeschrieben werden kann. Ursprünglich diente der Begriff dazu, ein Gegenmodell zu einer auf Eigentum basierenden Ökonomie zu beschreiben. Die gemeinsame Nutzung geteilter Güter steht im Vordergrund. Der Grundgedanke war, dass viele Güter von einem einzigen Eigentümer nicht effizient ausgelastet werden. Würden sich mehrere Personen Güter teilen, müsste es insgesamt weniger Güter geben, eine Verschwendung von Ressourcen würde verhindert. So könnten sich zwei oder mehr benachbarte Familien ein Auto teilen, wenn sie es nicht täglich benötigen. Zusammengefasst wird dieser Gedanke in dem Slogan: «Unused Value is wasted value.»

Dieser Grundgedanke steckt immer noch in vielen Unternehmen der Sharing Economy. Die Geschäftsidee von Uber ist die, dass Privatpersonen ihren selten voll ausgenutzten PKW dazu nutzen, andere Personen zu transportieren, die sich dann kein eigenes Auto kaufen müssen. Der Grundgedanke von Airbnb ist, dass man leer stehenden privaten Wohnraum an andere vergibt, sodass kein Wohnraum verschwendet wird. Crowdfunding **Plattformen**, auf denen online von verschiedensten Projekten um Spenden geworben wird, sollen wiederum unproduktives privates Kapital freisetzen und bei Crowdworking-Geschäftsmodellen, wie «Amazon Mechanical Turk», bei denen online Heimarbeit nach Bedarf abgerufen wird, behauptet man immer noch, dass Privatpersonen unproduktiv «verschwendete Zeit» dazu einsetzen könnten, um schnell, quasi nebenher, ein wenig zu arbeiten.

Der Unterschied zum ursprünglichen Gedanken besteht darin, dass ein großer Teil des Werts, der aus diesen neu erschlossenen privaten Ressourcen erwirtschaftet wird, an globale Konzerne wie Uber abfließt. Die Effizienzgewinne, die die Sharing Economy ermöglicht, dienen also nicht mehr der Ressourcenschonung, sondern werden in Form von Gewinnen an Unternehmen und ihre Risikokapitalgeber beziehungsweise Shareholder abgeführt. Zudem werden die Güter oder die Arbeit nicht mehr in einer Community von Gleichen geteilt, sondern verstärkt in einer anonymisierten Crowd. Dort ersetzt oft eine zentralisierte Kontrollinstanz das gegenseitige Vertrauen, das bei den früheren Formen, wie etwa «couchsurfing» wesentlich für die Sharing Economy war.

Es sind vor allem drei Prinzipien, die die Sharing Economy dabei so erfolgreich machen. Erstens: Vereinfachung. Uber hat sowohl die Vermittlung von Taxifahrten als auch das Taxifahren selbst

mithilfe seiner App und GPS-Navigation so vereinfacht, dass theoretisch tatsächlich jeder und jede mit seinem/ihrem Auto sofort als TaxifahrerIn arbeiten kann. Airbnb hat die zeitweilige Vermietung von Wohnungen so vereinfacht, das jede/r ohne Probleme seine/ihre Wohnung kurzzeitig vermieten kann. Zweitens: Zugang zu Arbeit. Uber und andere Sharing-Unternehmen versprechen gerade denjenigen einfachen Zugang zu Arbeit und Einkommen, die auf dem regulären Arbeitsmarkt eher zu den Benachteiligten gehören, wie etwa MigrantInnen. Hinzu kommt, dass versprochen wird, dass diese Arbeit nicht nur angemessen bezahlt sei, sondern auch ein höheres Maß an Eigenständigkeit und Unabhängigkeit erlaube, als reguläre Erwerbstätigkeit – Versprechen, die selten eingelöst werden und oft in prekäre Scheinselbstständigkeit münden. Drittens: Kontrolle. Die Apps, Websites und **Algorithmen** der Sharing-Unternehmen dienen nicht nur dazu, zwischen KundInnen und AnbieterInnen zu vermitteln, Preise festzulegen oder Zahlungen abzuwickeln. Sie werden auf vielfältige Weise genutzt, um die ArbeiterInnen in der Sharing Economy zu überwachen und zu steuern. Am Ende unterliegen diese ArbeiterInnen trotz der informellen Strukturen der Sharing Economy teilweise einer strengeren Kontrolle als klassische ArbeitnehmerInnen. Der gesellschaftliche Nutzen einer Sharing Economy wird sich künftig daran entscheiden, ob ihre potenziellen Vorteile weiterhin dem Profitinteresse vor allem großer, nach Monopolen strebenden Unternehmen geopfert werden.
(Sebastian Strube)

// ZUM WEITERLESEN

[1] Slee, Tom: Das «Problem of trust» in der Sharing Economy, 29.9.2013 unter: https://is.gd/uI3EFX.
[2] Katz, Vanessa: Regulating the sharing economy, in: Berkeley Technology Law Journal 30(2015)4, unter: https://is.gd/SL71IB.
[3] Lage, Nutzung sowie Umsätze von Airbnb-Wohnungen in großen Städten weltweit, unter: http://insideairbnb.com/.

// SILICON VALLEY

Das «Silizium-Tal» ist streng genommen gar kein Tal, eher eine leicht ansteigende Hügelkette in Nordkalifornien, östlich von San Francisco, die etwa die fünffache Fläche Berlins einnimmt. Viele der weltgrößten Hightech-Firmen, wie Apple, Cisco, Hewlett-Packard oder Intel, sind hier angesiedelt. Hinzu kommen die ebenso bedeutsamen Stars der Internetökonomie: Google, Ebay, Yahoo, Facebook und PayPal. Die dortige Konzentration an Start-ups aus dem Technologiesektor ist weltweit einzigartig. Ein Drittel des weltweiten Risikokapitals akkumuliert sich hier. Die herrschende Klasse des digitalen Kapitalismus hat in Kalifornien ihre wichtigsten Bastionen, von hier aus werden neue digitale Innovationen, Produkte und Geschäftsmodelle in die ganze Welt exportiert. Das Silicon Valley mit seiner verdichteten Hightech-Industrie und ihren innovativen Gründern wird zunehmend nachgeahmt, zumindest marketingtechnisch: Die Silicon Allee in Berlin oder das indische Silicon Valley in Bangalore sind nur zwei Beispiele für solche Versuche.
1955 gründete William Shockley, der Erfinder des Transistors, seine erste Firma in Mountain View. Mit der Verbreitung der Computertechnik seit den 1960er Jahren konzentrierten sich immer mehr Hardware-Unternehmen in dieser Region, so auch Intel, der weltweit bedeutendste Hersteller für Computerchips. Ab den 1970er Jahren siedelten sich auch immer mehr Software-Firmen hier an. Die Elite-Hochschule Stanford liegt in unmittelbarer Nähe zum Silicon Valley und gilt als entscheidender Wachstumsfaktor der Region. Viele Akteure (die männliche Form ist hier gewollt) des Silicon Valley haben dort studiert. Die Verbindungen zwischen der Universität, der Finanzwirtschaft und der Gründerszene sind eng.
1951 wurde der Stanford Industrial Park gegründet, eine Art an die Uni angeschlossenes Gewerbegebiet. Stanford rühmt sich, damit den weltweit ersten Technologiepark installiert zu haben und damit entscheidend am Erfolg des Silicon Valleys beteiligt zu sein. Das Konzept, Start-ups mit Uni-Geldern zu fördern, ist also schon wesentlich älter als die digitale Ökonomie. Die Universität hat viele Gründer von bekannten IT-Unternehmen hervorgebracht. Auch die beiden Google-Gründer Larry Page und Sergey Brin sind Absolventen der Stanford University und haben dort einst das Konzept ihrer Suchmaschine entwickelt.
Die Blüte der Halbleiterindustrie des Silicon Valley liegt maßgeblich in Aufträgen aus dem Verteidigungsministerium begründet: dem Pentagon als wichtigsten Kunden der entstehenden Hightech-Industrie. Bis heute ist das Department of Defense der einflussreichste Unterstützer der technologischen Entwicklungen im Valley und verantwortlich für den Aufkauf von innovativen Produkten zu Höchstpreisen. Thomas Heinrich zufolge haben großzügige Finanzierung von Forschung und Entwicklung durch das Militär den Grundstein gelegt für eine neue Generation von Firmen, die den ökonomischen Wiederaufstieg in den 1990er Jahren mit hervorgebracht haben.
Angedichtete Mythen sind typisch für das Silizium-Tal, wie etwa die unschein-

baren Garagen der Apple- und Hewlett-Packard-Tüftler oder die Pioniere, aus deren Anfängen später Weltfirmen wurden, oder der Mythos, allein geniale Ideen würden wie von selbst zum ökonomischen Erfolg führen. Andrew Keren etwa beschreibt die Fähigkeit des Silicon Valley, die Realität zu verzerren, Phantasmen aufzubauen, Banales unwiderstehlich wirken zu lassen als «reality distortion field».
Das Silicon Valley hat aus einem Amalgam aus Einflüssen der kalifornischen Gegenkultur der 1960er Jahre, gekoppelt mit ausgeprägtem Wirtschaftsliberalismus und dem Glauben an die Lösbarkeit aller Menschheitsprobleme, durch den Einsatz von Informationstechnologien seine eigene Vorstellungswelt entwickelt: das, was wir heute als die kalifornische Ideologie bezeichnen. (Timo Daum)

// ZUM WEITERLESEN

[1] Keen, Andrew: The Internet Is Not the Answer, New York 2015.
[2] Keese, Christoph: Silicon Valley, München 2014.
[3] Silicon Valley, TV-Serie, Mike Judge, USA, seit 2014.

// SMART CITY

Das Paradigma der Smart City hat in den letzten Jahren an Bedeutung gewonnen. Mit der Idee einer intelligenten, einer selbst denkenden Stadt geht das Versprechen eines ganzheitlichen und innovativen Entwicklungskonzepts einher. Es suggeriert, mit dem klugen Einsatz neuer Informations- und Kommunikationstechnologien könnten Städte nicht nur effizienter, moderner und inklusiver werden, sondern auch noch das dringlichste Problem unserer Zeit, den Klimawandel, in den Griff bekommen. Die Sorgen um die Klimapolitik und die Trends der erneuerbaren Energien befördern so neue technische Lösungsangebote für das persönliche Umfeld der Menschen: Smart Homes von StadtbewohnerInnen in Smart Citys weltweit.
Gegenwärtig bestimmen so vor allem technizistische Ansätze sowie einseitige ökonomische Interessen die Debatte, bei der die soziale Frage völlig außen vor bleibt. Debatten um intelligente Rauchmelder, intelligente Stromzähler, intelligente Staubsauger und selbstfahrende Elektroautos vernebeln die Wahrnehmung davon, was seitens linker Stadt- und Raumtheorie seit 30 Jahren als Common Sense gilt: Gesellschaftliche Probleme lassen sich nicht technisch, sondern nur durch soziale Antworten lösen. In der Perspektive geht es um Teilhabe und Selbstbestimmung derjenigen, die den Stadtraum alltäglich neu produzieren und Stadtentwicklung sprichwörtlich «selber machen».
So ist es umstritten, wie eine linke Antwort auf Smart City aussehen kann und

wie mit dem Begriff selbst umzugehen ist. Sollte man ihn von links besetzen oder ist das angesichts des Charakters dieser neuen neoliberalen Landnahmestrategie aussichtslos?

Unabhängig von der Frage der Begriffsverwendung müssen die ihm zugrunde liegenden technischen Neuerungen von links aufgegriffen und mit einem linken, fortschrittlichen und emanzipativen Gesellschaftsentwurf verwoben werden. Eine Smart City von links einzufordern kann deshalb nur heißen: Digitalisierung städtischer Infrastrukturen plus Vergesellschaftung aller Infrastrukturen in den Städten und Dörfern; also: Orte für jene, die in ihnen leben! Das neoliberale Zeitalter hat zur Privatisierung von Wohnungen, Stadtwerken, Energieversorgung, Boden und städtischem Grün geführt. Die Digitalisierung öffentlicher Infrastrukturen würde deshalb zuerst eine Rekommunalisierung bedingen und anschließend an die Digitalisierung städtischer Infrastrukturen, die als öffentliche Aufgabe verstanden wird, einen Zukunftsort auf der Grundlage von Gemeingütern ermöglichen.

Einer Privatisierung der **Daten** müssen Ansätze des **OpenData** entgegengesetzt und aktiv durch die Politik unterstützt werden. So wäre gewährleistet, dass die in der Stadt produzierten Daten nicht von privatem Gewinnstreben abgeschöpft oder zur Grundlage neuer Ebenen der **Massenüberwachung** würden. Die Möglichkeiten und Gefahren solcher Entwicklungen, etwa das **Predictive Policing**, sind schon längst keine originellen TV-Serien mehr, sondern Realität.

Bleiben die Daten öffentliches Gut, könnte über ihre Erhebung und Verwaltung einerseits öffentlich und demokratisch entschieden werden. Eine anti-neoliberale Smart City würde die demokratische Teilhabe ihrer BewohnerInnen erweitern und wäre mit Instrumenten der **eDemoracy** verbunden: Warum nicht selbstorganisierte Kiez-Räte, die sich auch digital vernetzen und über ein eigenes **Social-Media**-Netz AnwohnerInnen zu Abstimmungsprozessen einladen?

Eine anti-neoliberale Smart City? Diese Forderung nach einer intelligenten Stadt für alle muss mit einer Repolitisierung und Wiederaneignung von städtischen Themen, Entwicklungen und Technologien verbunden sein.

(Katalin Gennburg)

// ZUM WEITERLESEN

[1] Diesselhorst, Jonathan/Gennburg, Katalin: Wie smart kann die Stadt für alle sein?, Standpunkte 11/2016, hrsg. von der Rosa-Luxemburg-Stiftung, Berlin 2016, unter: www.rosalux.de/publication/42414.

[2] Forum Umwelt und Entwicklung: Gute Stadt – Böse Stadt: Landromantik vs. Stadt für alle, Rundbrief 4/2015, S. 6ff., unter: https://is.gd/jFCJve.

[3] SmartCity Wiki: Urban Commons/Partizipation und Teilhabe, Stand: 31.10.2016, unter: https://is.gd/X30iK2

[4] Stollmann, Jörg u. a.: Beware of Smart People! Re-defining the Smart City Paradigm towards Inclusive Urbanism. Berlin i.E.

// SMART EVERYTHING

Mit sanfter Musik beginnt das smarte Radio seine Besitzerin am Ende einer Tiefschlafphase zu wecken. Langsam fährt es die Beleuchtung hoch, aktiviert die Kaffeemaschine und die Heizung im Bad und schaltet dann auf die 7-Uhr-Nachrichten um. 20 Minuten später gibt der intelligente Kühlschrank passend zur Auswertung des Fitness-Armbands eine leckere Frühstücksempfehlung, informiert über die Aufgaben des Tages und erinnert dann rechtzeitig daran zur Car-sharing-Gruppe aufzubrechen, natürlich nicht ohne den Hinweis, einen Regenschirm mitzunehmen, später ist Regen vorhergesagt. Die Haustür verriegelt sich, und ab jetzt würde das Smart Home seiner Bewohnerin augenblicklich eine Nachricht schicken, sollte sich etwas in der Wohnung bewegen oder die Luftfeuchtigkeit steigen, die eigene, regennasse Katze ausgenommen.

«Home smart home», «smart-up your life» oder «make everything smart» lauten die Slogans diverser Anbieter, die eine komfortable, vernetzte Welt versprechen. Vom smarten Strom-Wasser-Gas-Zähler, zur Smart City mit smarter Verwaltung (siehe E-Government) bis zur smarten Waffe (siehe Drohnenkrieg) gibt es alles. Quasi alle Gegenstände können mit Sensoren ausgestattet, untereinander vernetzt und an das Internet angeschlossen werden. Das «Internet der Dinge» soll Prozesse effektiver machen, umweltfreundlicher, inklusiver und leichter bedienbar. Die Kommunikation zwischen BürgerInnen und der Stadt oder Dienstleistern soll transparenter und partizipativer werden. Dafür sammeln Kameras, ausgestattet mit Bilderkennungssoftware, und viele unterschiedliche Sensoren Daten, die häufig in der Cloud gespeichert und (später) kombiniert werden. Diese Sensoren, zum Beisppiel sogenannte RFID-Transponder, sind mittlerweile so klein und hauchdünn, dass sie in den Personalausweis und in Textilien eingearbeitet oder Haustieren implantiert werden können und eine berührungslose Identifikation ermöglichen.

Besonders viele Daten liefern Smartphones. Mit ihren Bewegungsmustern kann man einen Verkehrsstau erkennen oder Konsumentenverhalten im Einkaufszentrum analysieren. Auch im Gesundheitsbereich sind viele Innovationen greifbar. DiabetikerInnen könnten sich entscheiden, den Komfort einer smarten Insulinpumpe zu nutzen und damit auch die Forschung zu unterstützen, sofern sichergestellt ist, dass die Daten anonymisiert sind und vor Diebstahl oder Weitergabe geschützt. In Zukunft ist es aber auch denkbar, Tarife für Krankenkassen, Dienstleistungen oder Strom zu haben, die für jene KundInnen günstiger sind, die einer Aufzeichnung und Auswertung ihres Verhaltens zustimmen. Wer wenig finanzielle Ressourcen hat, wird dann die Datenschutzvariante nicht mehr bezahlen können.

Von smarten Geräten gesammelte Daten müssen jedoch nicht zwangsläufig als Problem betrachtet werden. Insgesamt wird sich die Gesellschaft der Herausforderung stellen müssen, eine neue Souveränität von KonsumentInnen und BürgerInnen zu entwickeln. Jede und jeder sollte die Wahl haben, unter fai-

ren Bedingungen selbst zu entscheiden, ob und wenn ja, welche Daten sie wem zu welchem Zweck zur Verfügung stellen. Dabei darf keine Zweiklassengesellschaft entstehen, in der sich nur die Einkommensstärkeren Datenschutz leisten können. Transparenz ist in jedem Fall entscheidend, denn wer würde im analogen Leben einen Fremden mit Notizblock in seine Wohnung lassen, damit dieser jeden Atemzug, jede Handlung, jede Regung notiert? (Martha Dörfler)

// ZUM WEITERLESEN

[1] Pasquale, Frank/Sadowski, Jathan: Smart City. Überwachung und Kontrolle in der «intelligenten» Stadt, Analyse 23, hrsg. von der Rosa-Luxemburg-Stiftung, Berlin 2016 unter: www.rosalux.de/publication/41847.
[2] Smart home, dumb people?, Breitband topic, 5.12.2015, unter: https://is.gd/IJBuUZ .
[3] Greenberg, Andy: Now You Can Hide Your Smart Home on the Darknet, wired.com 7.2.2016, unter: https://is.gd/FiCCji.

// SOZIALE MEDIEN/WEB 2.0

Mit dem Begriff soziale Medien (engl.: Social Media) werden neuartige Kommunikationsformen beschrieben, die erst durch das Internet ermöglicht oder zumindest bis zur Nutzbarkeit erleichtert werden: Statt dass Informationen wie herkömmlich von Medienorganisationen einseitig verbreitet werden, fließen Informationen entlang der Verbindungslinien in sozialen Netzwerken, wie sie das Internet abbildet. Die traditionelle Rollenteilung von AnbieterInnen und KonsumentInnen von Inhalten wird so aufgeweicht («Jede/r kann ein Sender sein»).

Informationen verschiedener Quelle können miteinander verbunden, verändert und zu neuen Informationsangeboten gebündelt werden. Der «Wert» einer Nachricht oder die Information wird so von der sozialen Position ihrer Quelle getrennt und kann sich je nach Relevanz mehr oder weniger erfolgreich im sozialen Netz verbreiten. Besonders in der Anfangszeit der sozialen Medien erhoffte man sich von ihnen eine befreite(re) Kommunikation, weil sie traditionelle Machtgefälle ausgleichen, Gegenöffentlichkeiten bestärken und Hierarchien beseitigen sollten.

Bis vor wenigen Jahren meinte man mit sozialen Medien vor allem Weblogs, Wiki-Seiten wie von Wikipedia und offene Nachrichtenplattformen. Im Vordergrund stand damals, dass im frühen Internet potenziell jede/r mit einem Internetzugang und etwas Speicherplatz im Netz ihre/seine eigenen Bilder, Texte und Töne veröffentlichen konnte und dass potenziell jede/r mit einem Internetzugang diese Informa-

tionen auch einsehen und – zum Beispiel bei den Wikis – sogar verändern konnte. Außerdem konnten diese Informationen mit anderen Informationen und **Plattformen** querverbunden oder zu ganz neuen Informationsplattformen zusammengebracht werden. Das trennte die sozialen Medien von den klassischen Massenmedien. Dort bereitete eine kleine Personengruppe Informationen für eine große Gruppe von EmpfängerInnen auf. Zwischen den Medien und zwischen AbsenderIn und EmpfängerIn konnte kaum wechselseitig Einfluss ausgewirkt werden. All diese neuen Möglichkeiten plus eine (damals) neue, verbesserte Nutzbarkeit von Internetangeboten fasst der Begriff Web 2.0 zusammen, der 2004 auf einer Internetkonferenz geprägt wurde. Heute sind die Begriffe soziale Medien und Web 2.0 als Kategorien beinahe überflüssig geworden – zumindest umfassen sie heute von **sozialen Netzwerken** bis Instant Messengers, Online-Spielen und Intranets, Bewertungsplattformen und Videodiensten eine sehr große Bandbreite von Kommunikationsfällen im Internet: Im Grunde alle Orte, an denen InternetnutzerInnen eigene Inhalte zugänglich machen können. Viele derzeitige Medienangebote vermischen außerdem Elemente der Social Media mit klassischen Darreichungsformen, zum Beispiel als Kommentarbereich unter Nachrichtenartikeln und der Möglichkeit, Artikel, Bilder und Töne mit anderen zu teilen. Sie suggerieren damit, «auf Augenhöhe» mit ihren KundInnen zu kommunizieren und deren Rückmeldungen in die Berichterstattung einfließen zu lassen.

Technisch ist den beiden Begriffen soziale Medien und Web 2.0 ohnehin kaum mehr beizukommen. Mehr als für eine technische Struktur, über die Kommunikation übertragen wird, stehen sie für eine veränderte Erwartungshaltung an die Verbreitung und den Konsum von Informationen: Jede/r kann mitmachen, jede Information und Quelle hat zunächst gleich viel Gewicht. Weil diese Erwartung aber entweder nicht erfüllt wurde oder sich viel komplexer ausgestaltet, geriet das Konzeptbündel soziale Medien ins Abseits.

Neue Relevanz hat es allerdings jüngst durch den Erfolg der sozialen Netzwerke wie Facebook und der neuen Kommunikationsplattformen wie WhatsApp bekommen: Hier entstehen nun aus der Verschmelzung von privater Kommunikation und Öffentlichkeit eine Vielzahl neuer Teilöffentlichkeiten in allen möglichen Arrangements. Weil diese wiederum von einigen wenigen Firmen gesteuert, erlaubt und verboten, ausgebeutet und gefördert werden können, droht dadurch ein Verlust des an sich emanzipativen Potenzials einer weniger hierarchisch strukturierten Öffentlichkeit. In einer technisch vermittelten Öffentlichkeit beherrscht derjenige die Kommunikation, der das zugrunde liegende Medium kontrolliert. Dieses Problem wird dadurch verschärft, dass soziale Medien als Internetsystem auch maschinell auswertbar und beeinflussbar sind. Das heißt, die über das Internet verbreiteten Informationen werden auch von **Algorithmen** mitgelesen, die Informationen einordnen und Inhalte und deren Verbreitung beeinflussen können. Die ohnehin zersplitterte Online-Öffentlichkeit wird

damit zu einem heiß umkämpften Feld von Partikularinteressen: das egalitäre Prinzip des Netzes zum Wettbewerbsvorteil der besser ausgerüsteten, schnelleren Seite.
(Felix Knoke)

// ZUM WEITERLESEN

[1] Tippelt, Florian/ Kupferschmitt, Thomas: Social Web: Ausdifferenzierung der Nutzung – Potenziale für Medienanbieter, Media Perspektiven 10/2015, unter: https://is.gd/a9BRu7.
[2] Landesanstalt für Medien Nordrhein-Westfalen: Vernetzte Öffentlichkeit, Erklärvideo, 15.4.2014, unter: https://youtu.be/55Rhi7ss1vs.
[3] Finger, Lutz: Do Evil – The Business of Social Media Bots, forbes.com, 17.2.2015, unter: https://is.gd/RY5V7Q.

// STAATSTROJANER

Im Beamtendeutsch wird der seit Jahren umstrittene Staatstrojaner auch mit dem sperrigen Begriff «Remote Forensic Software» bezeichnet. Das klingt nach sauberer Arbeit und so gar nicht nach Lauschangriff und behördlichem Hacken von Computern mithilfe kommerzieller Anbieter. Gemeint ist mit dem Staatstrojaner aber eigentlich genau das: eine mehr oder minder professionelle Spionagesoftware, ein Trojaner, der hinter dem Rücken von Betroffenen nach Dateien mit bestimmten Begriffen oder nach Passwörtern suchen soll oder mit dem Gerät geführte Kommunikation mithorcht.
Zweimal schon hat sich das Bundesverfassungsgericht mit dem Staatstrojaner befassen müssen, um zu prüfen, ob deren Einsatz verfassungskonform ist. Vonseiten der Polizei, der Politik und der Geheimdienste wurde vor dem hohen Gericht behauptet, das staatliche Hacken sei unverzichtbar. Man müsse beispielsweise in der Lage sein, nutzerseitige Verschlüsselung mit dem Trojaner zu umgehen oder konkrete verschlüsselte Gespräche direkt auf dem Gerät abzugreifen. Dennoch liegen auch nach Jahren des Streits noch immer keine faktenbasierten Zahlen dazu vor, in welchen Fällen heimliches behördliches Hacken wirklich ein geeignetes, geschweige denn notwendiges oder gar unverzichtbares Mittel wäre.
Im Herbst 2011 enttarnte der Chaos Computer Club (CCC) einen der Staatstrojaner und zeigte, dass die Spionagesoftware technischen und juristischen Standards nicht genügte und zudem

ausgesprochen schlampig programmiert war. Der Trojaner konnte mehr, als er rechtlich durfte. Mit der staatlichen Spionage auf Festplatten war für drei Jahre Schluss, nachdem der CCC die Verfehlungen öffentlich nachweisen konnte. 2014 entschloss man sich aber, neue Trojaner zu kaufen.

Es scheint im Nachhinein überraschend dreist, dass Staatstrojaner jahrelang im praktischen Einsatz waren, ohne dass die staatlichen Stellen den Quellcode der von einer kommerziellen Firma gekauften Software jemals geprüft oder auch nur gesehen hätten. Die genaue Funktionsweise der Spionagesoftware konnten die Behörden nur ahnen, man ließ den Trojaner dennoch auf die Betroffenen und ihre Computer los.

Das ist deshalb von Bedeutung, weil an eine solche Software rechtliche Bedingungen geknüpft sind, die technisch umzusetzen gewesen wären. Außerdem muss im Falle des Einsatzes des Trojaners im Rahmen einer Strafverfolgung auch gewährleistet sein, dass protokolliert wird, wie genau der Rechner gehackt wurde. Denn vor Gericht müssen die Ermittlungsbehörden zeigen, dass die so erlangten Daten auch wirklich von dem infiltrierten Computer stammen und nicht etwa manipuliert sind oder darauf erst plaziert wurden.

Wichtiger aber ist der rechtliche Schutz vor dem zu weiten Eindringen in den intimsten Bereich eines Menschen. Denn der kann durchaus geöffnet sein angesichts der Tatsache, dass wir uns zuweilen unseren Geräten in einer höchstpersönlichen Weise anvertrauen. Diese Tatsache hat das Bundesverfassungsgericht in seiner ersten Entscheidung zum Staatstrojaner mit einem neuen Grundrecht gewürdigt, das die Integrität und Vertraulichkeit von informationstechnischen Systemen gewährleisten soll, gerade weil wir ihnen nicht nur unsere Kommunikation, unser digitales Gedächtnis, sondern auch Höchstpersönliches überlassen. Diese Sphäre eines Menschen ist durch die Menschenwürdegarantie des Grundgesetzes besonders geschützt. Auch wenn es technisch möglich wäre, darf man nicht in sie eindringen.

(Constanze Kurz)

// ZUM WEITERLESEN

[1] Neumann, Linus/Pritlove, Tim/Kurz, Constanze: Logbuch Netzpolitik Podcast 179 Flensburg für Verfassungssünder, unter: https://is.gd/Xjh1Vh.

[2] Chaos Computer Club: Stellungnahme an das Bundesverfassungsgericht zum BKA-Gesetz und zum Einsatz von Staatstrojanern, 2015, unter: https://is.gd/rCC52u.

[3] Rehak, Rainer: Angezapft. Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung, Münster 2013.

// WISSENSGESELLSCHAFT

Wissensgesellschaft ist ein ambitionierter, aber höchst unscharfer Großbegriff, der besonders im deutschen Sprachraum oft anstelle des etwas zurückhaltenderen Begriffs Informationsgesellschaft verwendet wird. Der Begriff stammt aus den US-amerikanischen Wirtschaftswissenschaften, die damit die Auswirkungen der wachsenden Komplexität von Verwaltung und Wirtschaft der Nachkriegsjahre zu fassen versuchten. 1957 sprach der Managementtheoretiker Peter Drucker erstmals vom Wissensarbeiter («knowledge worker»), um damit eine wachsende Klasse von Angestellten in privaten wie öffentlichen Verwaltungs-, Entwicklungs- und Forschungsabteilungen zu bezeichnen, deren Aufgabe es war, komplexe, wissenschaftlich gestützte Tätigkeiten auszuüben. 1962 veröffentlichte der Makroökonom Fritz Machlup die empirische Studie «The Production and Distribution of Knowledge in the United States» in der er resümierte, dass bereits mehr als 40 Prozent aller Beschäftigten in der «Wissensökonomie» («knowledge economy») tätig seien. Die empirische Orientierung auf die US-Wirtschaft hatte zur Folge, dass stillschweigend vorausgesetzt wurde, dass die Wissensgesellschaft eine kapitalistische sei und Wissen als Eigentum zu behandeln sei. Daran hat sich bis heute wenig geändert.

Bereits in den frühen Studien lassen sich darüber hinaus gehende begrifflich-politische Probleme erkennen, die bis heute nicht gelöst sind. Mehr noch als der Begriff Information gilt Wissen als ein positiver Begriff, der sich nahtlos in ein Narrativ von Aufklärung und Rationalität einfügt. Damit wird er nicht nur analytisch-deskriptiv, sondern auch politisch-proskriptiv. Das heißt, Analysen der Wissensgesellschaft beschreiben zumeist nicht nur einen tatsächlichen Wandel von

Wirtschaft und Gesellschaft, sondern liefern auch politische Handlungsanleitungen mit, denn diese «wissensbasierten» Tätigkeiten werden zumeist auch als «höherwertig» beschrieben. Entsprechend wird es als Aufgabe der Politik dargestellt, diesen Wandel zu fördern.

Eines der fundamentalen Probleme des Begriffs ist allerdings, dass es keine handhabbare Definition von Wissen gibt. Am nächsten kam einer solchen der Soziologe Daniel Bell, der Anfang der 1970er Jahre in seinem Buch «Die Post-Industrielle Gesellschaft» darunter formal-wissenschaftliche Expertise verstand und konsequenterweise die Entstehung einer postideologischen, technokratisch verwalteten Gesellschaft voraussah beziehungsweise forderte. Damit einher ging nicht nur die Abwertung von manuell-produktiven Tätigkeiten, die zunehmend in Billiglohnländer ausgelagert werden sollten, sondern auch jene Tätigkeiten, die kommunikationsintensiv sind, aber nicht wissenschaftlich formalisiert werden konnten, etwa im Sozial-, Pflege- oder Bildungsbereich. Zusätzlich übersah der Fokus auf «höherwertige» Tätigkeiten im Dienstleistungssektor, dass gerade in diesem Bereich eine Dequalifizierung stattfand, welche auch dort die Entstehung eines neuen Niedriglohnsektors begünstigte.

Heute könnte sich der Fokus auf formalisierte Aspekte von Wissen und deren politische Privilegierung im informationellen Kapitalismus als eines der größten Probleme dieser Konzeptualisierung entpuppen. Denn genau jene Berufsfelder, die stark formalisiertes Wissen bearbeiten, sind heute besonders von der Automatisierung der kognitiven Arbeit, angetrieben durch Algorithmen, intelligente Software und Big Data, bedroht. Der so konzipierten Wissensgesellschaft drohen die Subjekte auszugehen, während immer mehr Menschen überflüssig erscheinen.

Stattdessen täte es not, den Begriff Wissen breiter zu fassen und auch alle Tätigkeiten einzuschließen, in denen implizit-situiertes Wissen eine wichtige Rolle spielt, etwa im Kultur-, Sozial- oder Gesundheitsbereich. Eine solchermaßen veränderte Perspektive würde einerseits den Gemeingut-Aspekt von Wissen besser sichtbar machen und anderseits zeigen, dass auch außerhalb der kapitalistischen Ökonomie sehr viel Wissensarbeit geleistet wird, etwa in unbezahlter oder freiwilliger Arbeit. (Felix Stalder)

// ZUM WEITERLESEN

[1] Bittlingmayer, Uwe H.: «Spätkapitalismus» oder «Wissensgesellschaft»?, in: Aus Politik und Zeitgeschichte 36/2001, S. 15–23, unter: www.bpb.de/files/Z32LKV.pdf.

[2] Engelhardt, Anina/Kajetzke, Laura (Hrsg.): Handbuch Wissensgesellschaft. Theorien, Themen und Probleme, Bielefeld 2010.

[3] Gorz, André: Welches Wissen? Welche Gesellschaft?, Beitrag zum Kongress «Gut zu Wissen» der Heinrich-Böll-Stiftung, Mai 2001, unter: https://is.gd/cHCrsW.

// AKTUELLE PUBLIKATIONEN

Bestellung aller Publikationen unter **bestellung@rosalux.de** oder unter **Tel. 030 44310-123**

Susanne Lang

OFFENES GEHEIMNIS

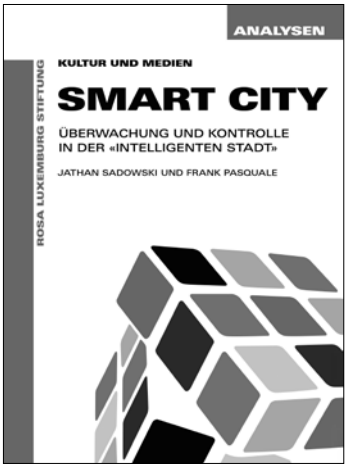
MYTHEN UND FAKTEN ZU ÜBERWACHUNG UND DIGITALER SELBSTVERTEIDIGUNG

luxemburg argumente Nr. 10, August 2016

Die ersten Enthüllungen durch den ehemaligen NSA-Systemadministrator Edward Snowden im Juni 2013 liegen nun eine Weile zurück. Seither ist deutlich geworden, wie tief auch die deutschen Behörden, angefangen mit dem Bundesnachrichtendienst (BND) bis hin zum Bundeskanzleramt, in die Affäre verstrickt sind. Die totale Massenüberwachung, Sabotage und gezielte Industriespionage sind amtlich.

Anstatt dem entgegenzusteuern, weitete die Bundesregierung die Möglichkeiten der Überwachung aus: Die Geheimdienste wurden aufgerüstet und mit mehr Befugnissen ausgestattet, etwa durch die Verfassungsschutzreform und das IT-Sicherheitsgesetz. Und um auch den Strafverfolgungsbehörden Überwachung zu erleichtern, wurde in einem Schnellverfahren die Vorratsdatenspeicherung neu aufgelegt und um einen Paragrafen erweitert, der das Arbeiten mit geleaktem Material unter Strafe stellt – ein Anti-Whistleblower-Paragraf.

Download unter:
www.rosalux.de/publication/42538



Jathan Sadowski und Frank Pasquale

SMART CITY

ÜBERWACHUNG UND KONTROLLE IN DER «INTELLIGENTEN STADT».

Analysen Nr. 23, Januar 2016

Die Vorstellung von Städten als Orten, in denen wir uns zugleich daheim und fremd fühlen können, hat einen gewissen Reiz. Man kennt die Straßen und Geschäfte, die Alleen und Gassen, kann aber dennoch ganze Tage dort verbringen, ohne erkannt zu werden. Städte werden jedoch zunehmend von den Eliten mit «intelligenten» oder «smarten» Technologien versehen und damit zu Plattformen für das «Internet der Dinge» gemacht: für in physische Objekte eingebettete Sensoren und Rechner, die sich über das Internet miteinander verbinden, kommunizieren und Informationen übertragen.

Download unter:
www.rosalux.de/publication/41847

Patrick Stary (Hrsg.)

DIGITALISIERUNG DER ARBEIT

ARBEIT 4.0, SHARING ECONOMY UND PLATTFORM-KOOPERATIVISMUS

Manuskripte Neue Folge Nr. 18, Juli 2016

Die Debatte um die Digitalisierung der Arbeitswelt ist in den deutschsprachigen Feuilletons und Wirtschaftsredaktionen angekommen. In ihrem Zentrum stehen vor allem die Begriffe Industrie 4.0 und, daran anschließend, Arbeit 4.0.

Download unter:
www.rosalux.de/publication/42470

IMPRESSUM

Herausgegeben von der Rosa-Luxemburg-Stiftung
V. i. S. d. P.: Stefan Thimmel
Franz-Mehring-Platz 1 · 10243 Berlin · www.rosalux.de
ISSN 2199-7713 · Redaktionsschluss: November 2016

Redaktion: Martha Dörfler
Grafiken: Michael Heidinger · www.michael-heidinger.com
Layout/Herstellung: MediaService GmbH Druck und Kommunikation
Gedruckt auf: Circleoffset Premium White, 100 % Recycling

Smarte Worte

auch bei uns im Blog

www.neues-deutschland.de/rubrik/smarteworte/

Arbeit Automatisierung Big Data Computer Cloud
Datenerfassung Datenschutz Datensicherheit
Digitalisierung Eigentum Fortschritt Industrie
Internet Kapitalismus Kapitalismuskritik Kritik
linke Bewegung Neoliberalismus Netzneutralität
Netzwerk Technik Technologie Überwachung

Dies und viele andere aktuelle Blogs und News lesen Sie täglich unter www.neues-deutschland.de

neues deutschland
SOZIALISTISCHE TAGESZEITUNG
nd

WWW.ROSALUX.DE