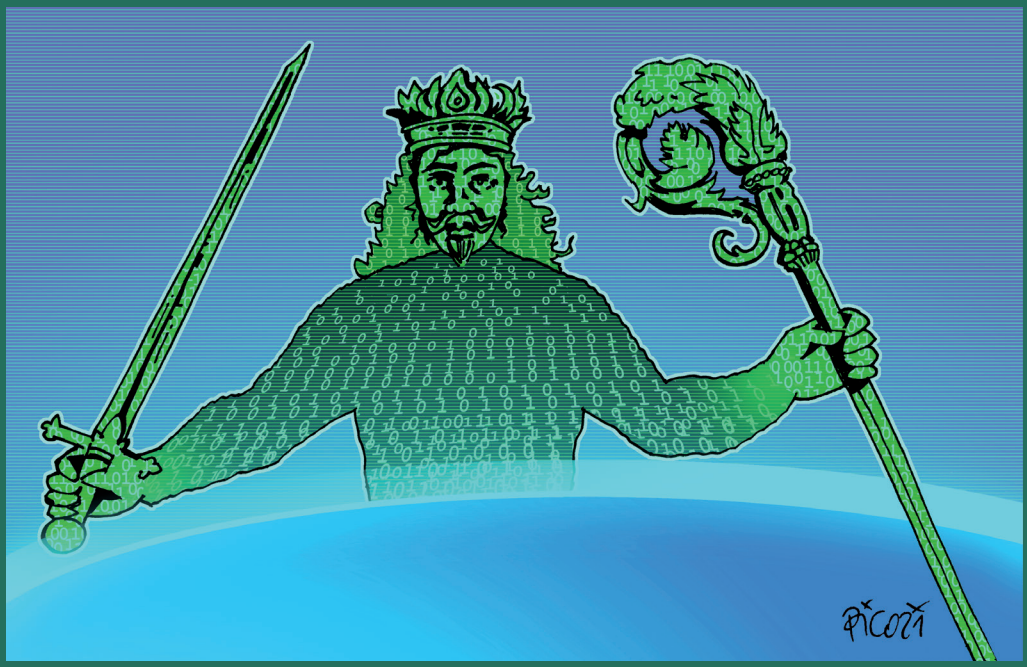
EDITED VOLUMES

Martina Bachor, Theo Hug, Günther Pallaver (Hg.)

DataPolitics

Zum Umgang mit Daten im digitalen Zeitalter



innsbruck university press

EDITED VOLUME SERIES

innsbruck university press

universität
innsbruck

Martina Bachor, Theo Hug, Günther Pallaver (Hg.)

DataPolitics

Zum Umgang mit Daten im digitalen Zeitalter

Martina Bachor
Institut für Medien, Gesellschaft und Kommunikation, Universität Innsbruck

Theo Hug
Leiter des Instituts für Medien, Gesellschaft und Kommunikation, Universität Innsbruck
Sprecher des interfakultären Forums *Innsbruck Media Studies* an der Universität Innsbruck

Günther Pallaver
Institut für Politikwissenschaft und Institut für Medien, Gesellschaft und Kommunikation, Universität Innsbruck
Institut für vergleichende Föderalismusforschung/Eurac Research, Bozen

Gedruckt mit finanzieller Unterstützung der Moser Holding AG, der Austria Presse Agentur (APA), des Interfakultären Forums Innsbruck Media Studies sowie des Vizerektorats für Forschung der Universität Innsbruck.

Universität Innsbruck
1. Auflage

Umschlagbild: © Christoph Pirker
www.uibk.ac.at/iup
ISBN 978-3-99106-046-8

Inhaltsverzeichnis

Editorial

Chancen und Gefahren der politischen Nutzung von Daten

Martina Bachor, Theo Hug, Günther Pallaver

Der Umgang mit digitalen Daten steht seit Jahren im öffentlichen Diskurs und hat im Zusammenhang mit COVID-19 zusätzliche Aufmerksamkeit erfahren. Dabei wurde in den vergangenen fünfundzwanzig Jahren eine zunehmende Erfassung, Speicherung und Verbreitung digitaler Daten beobachtet. (Selwyn 2015, S. 64) Das wirft die Frage auf, welche Funktion digitale Daten in der modernen Gesellschaft haben oder haben sollten, welche Auswirkungen sie auf Grundrechte ausüben und inwiefern sie die gesellschaftliche Ungleichheit fortschreiben, vergrößern oder den entgegengesetzten Weg der gesellschaftlichen Gleichheit fördern.

Auf der einen Seite des Diskurses werden hauptsächlich die Vorteile gesehen, welche die Digitalisierung und die damit einhergehende Datenerfassung hat. Dabei liegt der Fokus insbesondere auf kompetitiven Vorteilen im ökonomischen Sektor (Raguseo et al. 2021, S. 9) Auf der anderen Seite herrschen oft dystopische Zukunftsvorstellungen, in denen die Digitalisierung zur absoluten Kontrolle der BürgerInnen führt, welche dadurch in ihren Freiheiten massiv eingeschränkt werden. Fälle von Datenmissbrauch, wie beispielsweise im US Wahlkampf 2016 durch Cambridge Analytica, stützen diese Ansicht. (Isaak, Hanna 2018, S. 57)

Die umfangreiche Nutzung von Daten wird besonders von Wirtschaft und Politik eingesetzt, um Einfluss auf KonsumentInnen und WählerInnen zu nehmen. Dabei kann zum Beispiel eine Analyse der hinterlassenen Datenspuren als Hinweis dienen, um einen spezifischen Content an den/die UserIn weiterzugeben. Dadurch entsteht der Eindruck, dass diese eine Seite des Diskurses die einzig valide ist. Anstatt kritischen Stimmen den Vorzug zu geben, werden Algorithmen so programmiert, um immer weiter ähnliche Beiträge zu pushen. Dadurch können allzu leicht sogenannte Filterblasen entstehen. (Bozdag & Van den Hoven 2015, S. 250)

Wenngleich auf der einen Seite digitale Datenerfassung zu einer enormen Verbesserung der individuellen Empfehlungen für die NutzerInnen des Internets sowie eine exaktere Prognose im gesellschaftlichen Rahmen führt, birgt sie zugleich die Gefahr des Missbrauchs im ökonomischen sowie politischen Wettbewerb. Besondere deutlich wird dies am Beispiel des Social Credit Systems in China. Dabei wird das individuelle Fehlverhalten systematisch erfasst und hat dadurch reale Konsequenzen für die Einzelnen. (Creemers 2018, S. 3) Durch die digitale Überwachung und die immer effizienter werdenden Auswertungsmethoden entsteht eine Welt, die mitunter sehr an Orwells 1984 erinnert. Dieses

Gefühl der andauernden Beobachtung beeinflusst nachgewiesen das Verhalten der Individuen sowohl in der physisch-realen als auch in der digitalen Welt. (Goggin 2013, S. 13)

Durch die immensen Vorteile, die sich durch die Daten-Analyse ergeben, stellt sich die Frage, wie demokratische Systeme Lösungen entwickeln können, um die Daten vor Missbrauch von außen sowie von innen zu schützen, ohne vollständig auf diese zu verzichten. Daten können ideologisiert und instrumentalisiert, aber auch zu einer besseren und konkreteren Adressierung der Bedürfnisse der BürgerInnen genutzt werden.

Dabei gibt es verschiedene Ebenen der Verantwortung – eine makropolitische, die durch die globale Nutzung des Internets als eine weltweite begriffen werden kann, eine mesopolitische Verantwortung auf der Ebene von Institutionen und individuelle Verantwortungsbereiche. In den Beiträgen in diesem Band werden die verschiedenen Ebenen analysiert, wobei der Schwerpunkt primär auf den globalen Auswirkungen liegt. Gerade mit Blick auf die Entwicklungen im Gesundheitswesen des vergangenen Jahres ist es umso wichtiger geworden zu diskutieren, wie der Schutz der Gesundheit auf der einen Seite möglich wird, ohne ein System zu schaffen, das zum Missbrauch und zur staatlichen oder globalen Überwachung einlädt.

Vielfältig wie kontrovers ist somit die Suche nach Lösungen aus diesem Dilemma zwischen Gebrauch und Missbrauch von Daten. Innerhalb dieses Diskurses setzen sich die Beiträge in diesem Sammelband mit einer Reihe von relevanten Fragen auseinander und zeigen Ansätze für Lösungen auf. Solche Fragen, die um diese Themen kreisen, hätten beim für 2020 geplanten Medientags diskutiert werden sollen und waren Gegenstand der gekoppelten Ringvorlesung mit Übung. Aufgrund der im November 2020 eingeführten Maßnahmen rund um COVID-19 wurde der Medientag auf das Folgejahr 2021 verschoben und beschlossen, den Themenkomplex auch im kommenden Wintersemester 2021/22 im Rahmen der Ringvorlesung zu behandeln. Unverändert bleibt die Zielrichtung, sich von verschiedenen Perspektiven dem Thema anzunähern, um zu einem möglichst umfassenden Bild der Situation zu gelangen. Der Medientag sowie die damit verbundene Ringvorlesung mit Übung wurden und werden durch das interfakultäre Forum „Innsbruck Media Studies“ in Kooperation mit der Moser Holding AG sowie der Austria Presse Agentur an der Universität Innsbruck veranstaltet. Die Grußworte von Tilmann Märk, Rektor der Leopold-Franzens-Universität Innsbruck, Hermann Petz, CEO der Moser Holding, und Clemens Pig, CEO der APA, leiten zu den Beiträgen in diesem Band über.

Oliver Leistert leitet den Band mit seinem Text *Das Phänomen Trump als Effekt von Microtargeting und Psychometrie* ein, in dem er kritisch und meinungsstark die Entwicklung des Internets und die damit einhergehende Datennutzung analysiert. Dabei legt er die Überwachungs- und Trackingtechnologien bloß und erläutert das Dispositiv des Datenextraktivismus als primäres Geschäftsmodell heutiger Datenökonomien. Die Präsidentschaft von Donald Trump und die mit ihm verbundene, inzwischen aufgelöste Firma Cambridge Analytica, die unter anderem ihn sowie dem Brexit zum Erfolg geführt haben, können als

Zäsur der politischen Kommunikation angesehen werden. Diese zielt erfolgreich auf die Zersetzung demokratischer Regeln und Prozesse ab und greift dazu auf Mittel der Des- und Falschinformation zurück.

Die Autoren Marian Adolf und Nico Stehr erörtern in ihrem Beitrag *Information, Wissen und die Wiederkehr der Sozialen Physik* auf Basis eines genuin soziologischen Wissensbegriffs Möglichkeiten und Gefahren einer Rückkehr des mechanistischen Gesellschafts- und Menschenbildes im Sinne der „physique sociale“ im digitalen Zeitalter. Dabei gehen sie unter anderem darauf ein, wie schnell dadurch ideologische Kontrolle ermöglicht wird.

Der Beitrag *Vom Machiavellismus zur Hospitalisierung – Expertokratie oder Mündigkeit im Zeitalter der Digitalisierung* von Hans-Martin Schönherr-Mann setzt sich mit der Hospitalisierung der Gesellschaft in Folge der Corona-Pandemie auseinander und geht insbesondere auf die damit einhergehenden Freiheitsbeschränkungen ein, die durch digitale Überwachungstechniken entstehen, sowie auf die verlorengehende Mündigkeit der BürgerInnen. Dabei kritisiert er die mangelnde Möglichkeit, sich zur Wehr setzen zu können, weil es an seriöser kritischer Information mangelt.

Im Beitrag *Das digitale Panopticon – Wie die NSA-Überwachung unser Verhalten verändert* überträgt die Autorin Elsa-Margareta Venzmer das Konzept des Panopticons von Jeremy Bentham auf die heutige digitale Welt. Dabei geht sie insbesondere auf die entstehenden Effekte der Selbstzensur ein, welche durch das Bekanntwerden der Datenaufzeichnungen durch die NSA nachweisbar sind.

Datenpolitiken ‚von unten‘ zwischen Aktivismus und Politischer Medienbildung ist Gegenstand der Ausführungen von Valentin Dander. Dabei setzt er sich mit den reaktiven und proaktiven Praktiken und Taktiken der auf den verschiedenen Ebenen agierenden Figuren und deren Fähigkeiten auseinander, insbesondere in Bezug auf Data Literacy.

Anna-Maria Neuschäfer stellt im Beitrag *Datenaktivismus und Digital Citizenship* das Konzept der gesellschaftlichen Teilhabe über digitale Medien vor. Dabei geht sie insbesondere auf die Themen Clicktivismus, Hacktivismus ein und beschreibt Handlungsräume, welche im Datenaktivismus relevant sind.

Die fortschreitende Digitalisierung im Bereich des Lehrens und Lernens ist zentraler Gegenstand im Beitrag *Learning Analytics – Datenschutzrechtliche Bestimmungen als Ausgangspunkt einer verantwortungsvollen Nutzung von Bildungsdaten* von Silvia Lipp. Die Autorin differenziert zwischen den Chancen, die durch die Nutzung von Bildungssoftware, und den Gefahren, die durch Vernachlässigung der Rechte der involvierten Personen in Bezug auf den Schutz ihrer Daten entstehen.

Auf das Handlungsfeld Forschungsdatenmanagment richtet die Autorin Michaela Rizzolli im Text *Umgang mit (digitalen) Forschungsdaten: Rahmungen, Effekte und Herausforderungen* ihren Blick. Sie bezieht sich dabei auf Daten, welche im universitären Kontext

durch Studien erhoben werden und inwiefern diese zugänglich gemacht werden können und sollen.

Funktionsweisen von Verschwörungserzählungen auf Social Media und der parallel aufkeimende Antisemitismus ist der Titel des Beitrags von Andre Wolf, dessen Aktualität durch fast tägliche Medienberichte zu diesem Thema unterstrichen wird. Dabei geht es um Narrative in Krisenzeiten, Feindbilder und Radikalisierung, die eine Gefahr für die Demokratie darstellen.

Tobias Stadler schreibt in *Ölstandsanzeiger: Über die Unsichtbarmachung und Naturalisierung der Produktion personenbezogener Daten* über die Debatte, in der Datengewinnung mit Ölgewinnung verglichen wird. Dabei hebt er hervor, dass diese Metapher eine ideologische Funktion einnimmt und dazu dient zu verschleiern, dass auch eine Alternative zur Datengewinnung existiert.

Im Text *Digitale Mündigkeit im Spannungsfeld zwischen ich und wir – Ein Ratgeber in zehn konkreten Schritten* von Leena Simon legt die Autorin dar, wie man mit wenigen Schritten Mündigkeit trainieren und die digitale Identität schützen kann.

Abschließend möchten wir darauf hinweisen, dass die Beiträge in diesem Band verschiedene Modi des Genderns verwenden und insgesamt als geschlechtsneutral zu verstehen sind.

Sowohl die Veranstaltungsorganisation als auch die Herausgabe des Sammelbands waren ein gemeinschaftliches Unternehmen, für das wir in mehrfacher Hinsicht zu danken haben. Unser besonderer Dank gilt unseren beiden Veranstaltungspartnern für ihre Unterstützung, der Moser Holding AG mit Herrn Mag. Hermann Petz und der Austria Presse Agentur mit Herrn Dr. Clemens Pig. Wir danken Frau Mag. Lisa Berger-Rudisch, Frau Barbara Rauchwarter und Herrn Mag. (FH) Norbert Adlassnigg für die gute Zusammenarbeit. Die Publikation wäre ohne die finanzielle Unterstützung des Vizerektorats für Forschung der Universität Innsbruck sowie der beiden Veranstaltungspartner nicht möglich gewesen. Zu danken haben wir außerdem Dr. Birgit Holzner und Carmen Drolshagen von *innsbruck university press* für die verlegerische Betreuung.

Innsbruck, im Juni 2021 Martina Bachor, Theo Hug & Günther Pallaver

Literatur

Bozdag, Engin & van den Hoven, Jeroen (2015): Breaking the filter bubble: democracy and design. *Ethics Inf Technol* 17, S. 249–265. Abgerufen unter: https://doi.org/10.1007/s10676-015-9380-y

Creemers, Rogier (2018): *China's Social Credit System: An Evolving Practice of Control, University of Leiden,* Abgerufen unter: http://dx.doi.org/10.2139/ssrn.3175792

Goggin, Gerard (2013): Democratic affordances: Politics, media, and digital technology after WikiLeaks, Ethical Space. *The International Journal of Communication Ethics*, Vol 10, No 2/3, S. 6–14.

Isaak Jim & Hanna Mina J. (2018): User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, Vol. 51, No. 8, S. 56-59, doi: 10.1109/MC.2018.3191268

Raguseo, Lisabetta; Pigni Federico & Vitari Claudio (2021): Streams of digital data and competitive advantage: The mediation effects of process efficiency and product effectiveness. *Information & Management*, Vol. 58. Abgerufen unter: https://doi.org/10.1016/j.im.2021.103451.

Selwyn, Neil (2015): Data entry: towards the critical study of digital data and education, Learning. *Media and Technology*, 40:1, S. 64-82, DOI: 10.1080/17439884.2014.921628

Grußworte zum Medientag 2021

Tilmann Märk, Rektor der Universität Innsbruck

Sehr geehrte Damen und Herren, liebe Kolleginnen und Kollegen,

der Medientag und die parallel dazu organisierte Ringvorlesung der „Innsbruck Media Studies“ ist mittlerweile zu einem fixen Bestandteil im Jahreskalender der Universität Innsbruck geworden. Auch in diesem Jahr wird unter dem Titel „DataPolitics – Umgang mit Daten im digitalen Zeitalter“ ein hochaktuelles Thema von ausgewiesenen Expertinnen und Experten aus Forschung und Praxis diskutiert.

Daten prägen unser Leben in zunehmendem Ausmaß. Es ist nachgerade zur Normalität geworden, dass die von uns erzeugten Daten in weiterer Folge, beispielsweise unsere soziale Interaktion, unseren beruflichen Alltag oder zahlreiche Konsumentscheidungen maßgeblich beeinflussen. Jeden Tag produzieren wir auf die unterschiedlichste Art und Weise, ganz bewusst und offensichtlich oder aber im Verborgenen ohne unser Wissen, eine Flut an Daten, und diese stellen in verschiedenen Kontexten einen enormen Wert dar. Die Art und Weise, wie Daten gesammelt und gespeichert werden, wie und von wem auf sie zugegriffen wird und welcher Verwendung sie schlussendlich zugeführt werden, verändert sich in den modernen Gesellschaften zum Teil in rasanter Geschwindigkeit. Ob Daten angemessen be- und verarbeitet und in weiterer Folge auch verwendet werden, wird dabei nicht zuletzt auch maßgeblich von politischen Systemen und Kontexten beeinflusst.

So sehr also eine gezielte und sorgsame Analyse und Aufbereitung von Daten potentiell zur Verbesserung der Lebenssituation des Individuums beitragen kann, so gefährlich kann die massenhafte und intrasparente Datenerfassung und -auswertung sein, die in letzter Konsequenz mitunter auch zu einer asymmetrischen Machtdynamik zwischen Staat und Bürgerinnen und Bürgern führt. Gerade einer Volluniversität wie der Universität Innsbruck steht es gut zu Gesicht, der vielfach grundsätzlich positiven Wahrnehmung einer kontinuierlichen technischen Weiterentwicklung – und der damit unweigerlich verbundenen Datenaggregation – eine kritische Reflexion dieser Situation und dieser Entwicklungen entgegenzusetzen. In gleichem Ausmaß, wie wir uns als Universität mit unserem Know-how in die Weiterentwicklung von datenproduzierenden, -speichernden und -auswertenden Systemen und Prozessen einbringen, sollten wir ein wachsames Auge auf die individuellen, politischen und gesellschaftlichen Auswirkungen haben. Wie und wofür also Daten eingesetzt und gegebenenfalls auch instrumentalisiert werden und wie sich eine funktionierende Demokratie zum Wohle ihrer Bürgerinnen und Bürger auch gegen missbräuchliche Verwendungen schützen kann, muss ein mindestens ebenso

wichtiges Forschungsthema bleiben wie die technische Weiterentwicklung der datenhaltenden Systeme.

Die vielgestaltigen Beiträge in diesem Band zeigen, dass sich mittlerweile zahlreiche Expertinnen und Experten mit diesen wichtigen Forschungsthemen beschäftigen. Es ist von großer Bedeutung, auf Basis von gesicherten wissenschaftlichen Erkenntnissen ein wachsames und kritisches Auge auf so manche Entwicklung zu haben. Den Veranstalterinnen und Veranstaltern, den „Innsbruck Media Studies“ und dessen Sprecher, Herrn Kollegen Theo Hug, allen Kooperationspartnerinnen und -partnern, Vortragenden und Mitdiskutierenden möchte ich auf diesem Wege für ihre Beiträge und ihren Einsatz danken.

Grußworte zur Eröffnung des Medientags 2021

Hermann Petz, Vorstandsvorsitzender Moser Holding AG

Sehr geehrte Damen und Herren,

das Sammeln und Nutzen von Daten hat in einem Zeitalter der globalen Vernetzung einen enorm hohen Stellenwert eingenommen, Daten werden immer wieder als das Gold des 21. Jahrhunderts bezeichnet. Daten sind untrennbar mit unserem Leben und dem Ausbau moderner Gesellschaften verknüpft, mit unserer Mobilität, Gesundheit, Arbeit und nicht zuletzt der Kommunikation. Das Vergleichen, Aufbereiten und Vernetzen von Daten ist elementar, um Entwicklungen zu erklären und um Forschung und Technologie voranzutreiben. Letztlich können Daten aber auch missbräuchlich verwendet werden, um zu steuern, um zu manipulieren und auf Kosten der Allgemeinheit gigantischen Profit zu schlagen. Das passiert täglich in unterschiedlichen Ausprägungen und jeder Einzelne von uns kann betroffen sein.

Welch hohen Preis der neue globale Datenmarkt fordert, war den meisten Menschen nicht bewusst, als sie sich Anfang dieses Jahrtausends euphorisch bei Social Media Kanälen angemeldet, ihre Rabatt-Kundenkarte registriert oder ihre Vorlieben auf einer Partnerbörse geteilt haben. Im Vordergrund standen die unglaublichen Erleichterungen für Beruf und Alltag. Und anfänglich sogar die vage Hoffnung, dass die zunehmende Vernetzung schließlich auch zu einer weltweiten Demokratisierung im Sinne von Vielfalt und Gleichberechtigung beitragen könnte.

Längst macht sich Ernüchterung breit und das Wissen darum, dass wir den digitalen Fortschritt mit dem Preis unserer Daten bezahlen, ist Allgemeingut. Die Konsequenzen aus diesem Prozess werden unterschiedlich spürbar. In autoritären Staaten haben Datentechnologien die Möglichkeiten der Totalüberwachung der Bevölkerung befeuert. In China beobachten wir beispielsweise eine zunehmende Verschränkung von steigendem materiellen Wohlstand mit dem wachsenden Einfluss des Staates über Individuen. In Demokratien sind es eine Handvoll internationale Konzerne, die mit global gesammelten und vernetzten Daten eine weltweite Monopolstellung erreichen konnten.

Für Medien und Demokratien ist die Nutzung von Daten und Social Media mitunter widersprüchlich: Soziale Medien bedeuten einerseits einen niederschwelligen Zugang zu Informationen für alle, auch für jene, die früher von redaktionellen Berichten weitgehend ausgeschlossen blieben. Sie ermöglichen es Redaktionen, so unmittelbar wie noch nie mit ihren Rezipientinnen in Kontakt zu treten, auch im Sinne der laufenden Qualitätssicherung.

Andererseits kennen wir die alarmierenden Entwicklungen im Bereich Sozialer Netzwerke, wie beispielsweise die missbräuchliche Verwendung von Daten, die nachweislich schon zur Manipulation von Wahlen geführt haben. Wir kennen die Logik von Fake News und Skandalisierungen, welche die Aufgeregtheitsspirale noch schneller drehen und automatisch öfter gesehen werden. Nicht nur in Corona Zeiten laden soziale Netzwerke ein, in Meinungsblasen von Verschwörungstheoretikern zu verharren, anstatt den Blick für das große Ganze zu öffnen.

Tatsächlich ist Datenpolitik heute eine Gratwanderung zwischen Fortschritt und Wachstum einerseits und dem verantwortungsvollen Umgang mit Daten auf der anderen Seite. Mehr denn je wird deshalb die enorme Bedeutung von DataPolitics bewusst, einem Politikbereich, der in den letzten Jahren an Bedeutung gewonnen hat. Um künftig Fortschritt und Sicherheit verbinden zu können, braucht es eine entschlossene Politik auf nationaler und EU-Ebene und sogar darüber hinaus. Diese muss auf Augenhöhe mit den globalen Akteuren aktiv sein, um Fairness, aber auch Handlungsfähigkeit von demokratischen Staaten und Individuen nachhaltig zu gewährleisten. Gleichermaßen müssen wir gemeinsam an einer breiten Bewusstseinsbildung arbeiten, im Bereich Medienkompetenz für Menschen allen Alters, aber auch in Wissenschaft und Forschung. Einen Beitrag dazu soll der Medientag 2021 leisten, auf den ich mich schon sehr freue.

Datenpolitik zwischen Wert und Wandel – Geleitwort für den Medientag Innsbruck 2021

Clemens Pig, geschäftsführender Vorstand der APA – Austria Presse Agentur

Sehr geehrter Herr Rektor,
sehr geehrte Professoren und Professorinnen,
verehrte Veranstaltungsteilnehmerinnen und -teilnehmer,

Daten sind in einer digitalisierten Welt ein zentraler Roh- und Treibstoff. Der Handel damit ist lukrativ. Wirtschaft, Politik und Wissenschaft haben längst erkannt: Wer den Menschen und sein Verhalten kennt, kann daraus Schlüsse wie auch Vorteile ziehen. So ist es kein Zufall, dass die großen Tech-Giganten Baustein um Baustein des digitalen Raumes gestalten und einnehmen. Immer geht es darum, Userinnen und User zur pausenlosen Nutzung und zum Hinterlassen möglichst vieler Spuren und Daten zu bewegen – und diese schließlich mit Milliardenprofiten zu verkaufen. Ihre rapid steigende Marktdominanz ist das Resultat.

Die Datenschutzgrundverordnung der EU als Versuch, diesem Ungleichgewicht entgegenzutreten, ist vom Grundgedanken her richtig, hat aber das Problem nicht gelöst. Dass wir im Always-on-Modus täglich „Cookies akzeptieren" und AGBs zustimmen, die wir oft keines Blickes gewürdigt haben, kann weder Teil einer politisch-systematischen Antwort noch ein befriedigender persönlicher Umgang damit sein.

Datenanalyse funktioniert nur in der Skalierung. Deshalb zielt das Motiv weit häufiger auf das kollektive Verhalten ab, das möglichst exakt vorausgesagt und in unlauteren Fällen auch manipuliert werden kann. Cambridge Analytica, Trump oder Brexit bilden in diesem Zusammenhang nur die großen Headlines ab. Daten sind in sehr vielen Bereichen ein begehrtes Steuerungselement für wirtschaftliche oder politische Partikularinteressen. Die Entwicklung einer Gesellschaft darf jedoch nicht davon abhängen, in wessen Händen ihre Daten liegen. Praktikable, sinnvolle und effiziente Datenschutz-Initiativen sind in einer demokratischen Wertegemeinschaft auch unter diesem Gesichtspunkt notwendig.

Europa positioniert sich in Sachen Datenschutz zwischen zwei Extremen: Die für die kommerzielle Nutzung in Datenangelegenheiten weitgehend unregulierte USA auf der einen und das chinesische Modell mit autoritärem Zugang und staatlicher Überwachung (Stichwort Social Scoring) auf der anderen Seite. Die große politische Aufgabe wird es sein, den vermeintlichen Widerspruch zwischen der Einhaltung europäischer Werte und dem Anschluss an einen globalen digitalen Datenstrom zu überwinden – digitale Unabhängigkeit zu erlangen und zu behalten, ohne dabei in die digitale Isolation zu geraten.

Europa wird nicht nur auf politischer Ebene alle Anstrengung unternehmen müssen, um diese Balance zu finden.

Mir ist Balance wichtig, nicht nur als Bürger, der sich eines verantwortungsvollen und sensiblen Umgangs mit seinen Daten sicher sein möchte, sondern auch als Geschäftsführer eines österreichischen Medienunternehmens. Denn auch hier ist das Datenthema ein zentrales, das uns zusehends mehr beschäftigt. Datenjournalismus ist als professionelle Disziplin in Medienhäusern ohnehin nicht mehr wegzudenken. Hinzu kommen allerdings neue journalistische Formate, die sich zum Teil oder zur Gänze auf Daten stützen. Automatisierte Berichterstattung etwa, die auf Unmengen an oft unstrukturierten Zahlen und Tabellen basiert, die dann von Algorithmen in publikationsfertige Texte gegossen werden. Wir schaffen damit Storys, die es zuvor nicht gab, weil wir nicht die Ressourcen hatten, sie zu erzählen. Daten dienen hier also als wichtige Grundlage für faktenbasierten Agenturjournalismus. Was wir brauchen und aufbauen, ist spezifische Expertise – in rechtlichen, inhaltlichen und technologischen Fragen.

Ich möchte damit betonen, dass ein effizientes Datenmanagement – von der Aufbereitung bis zur Nutzung und Analyse – eine derart wichtige Rolle spielt, dass wir diese Kompetenz keinesfalls den großen Tech-Firmen überlassen dürfen. Neben den gesetzlichen und politischen Rahmenbedingungen und Initiativen macht es Sinn, sich auch auf unternehmerischer und wissenschaftlicher Ebene zusammenzuschließen, unser Know-how zu vernetzen und Lösungen zu entwickeln, um den Bereich Data- und Digital-Competence zu stärken und damit gemeinsam faire Wettbewerbsbedingungen zu schaffen. Dazu möchte ich Sie herzlich einladen.

Das Phänomen Trump als Effekt von Microtargeting und Psychometrie

Oliver Leistert

Zusammenfassung

Der Alptraum Präsident Trump mag vorerst vorbei sein, zu befürchten ist aber, dass er einen Politikstil salonfähig gemacht hat, der auf die Zersetzung demokratischer Regeln und Prozesse abzielt und dafür zu Mitteln der Des- und Falschinformation greift. Dieser Text diskutiert das Phänomen Trump in zugespitzter Weise als einen Effekt von Internettechnologien, die insbesondere im letzten Jahrzehnt alltäglich und allgegenwärtig geworden sind. Ausgehend von einer unvollständigen Nacherzählung der Geschichte des Internets als Geschichte der Entwicklung von Überwachungs- und Trackingtechnologien, über das Aufstellen des Dispositivs des Datenextraktivismus als primäres Geschäftsmodell heutiger Datenökonomien und dessen Akteuren, widmet sich der Text der inzwischen aufgelösten Firma *Cambridge Analytica*, die gegen Bezahlung Trump, dem Brexit und einigen anderen zum Erfolg verholfen hat.

1. Die Lüge der gefälschten US Wahl als nachhaltige Bifurkation der US-Gesellschaft

Als am 8.11.2020 nach vier langen Tagen der Stimmenauszählungen auch CNN als letzter seriöser TV-Sender Joe Biden zum 46. Präsidenten der USA ausrief, war allen BeobachterInnen längst klar, dass in den USA eine Bifurkation stattgefunden hat, die ein historisches Ausmaß angenommen hat und wohl für länger bestehen bleiben sollte: die überwältigende Mehrheit der Trump-WählerInnen waren überzeugt, dass die Wahl gefälscht, bzw. „gestohlen" war. Eine aufwendige, auch von vielen KleinstspenderInnen mitfinanzierte Kampagne, die von praktisch allen PolitikerInnen der Republikaner mitgetragen und in Fernsehinterviews gebetsmühlenartig wiederholt wurde, führte zum Glauben an diese Lüge. Damit hatte Trump sichergestellt, dass Wahlergebnisse in den USA von weiten Teilen der Bevölkerung fortan nicht mehr akzeptiert werden würden, oder, zumindest wenn ihr Kandidat unterlag, als „gestohlen" angesehen würden. Vielleicht ist dies rückblickend der größte Erfolg Trumps, denn wenn einmal das Vertrauen in faire und freie Wahlen zerstört ist und der tatsächliche, mit deutlicher Mehrheit gewählte Präsident somit in den Augen vieler kein rechtmäßiger Präsident ist, hat Trump eine zutiefst loyale und weitestgehend emotional steuerbare AnhängerInnenschaft hinter sich vereint, die noch zu weitaus radikaleren Mitteln zu greifen gewillt ist.

Die geplante und erfolgreiche Erstürmung des Kapitols am 6.1.2021 ist der bisher gewalttätigste und beängstigendste Ausdruck einer absichtlich in die Irre geleiteten

Menschenmenge in den USA in diesem Jahrhundert. Nur mit viel Glück kam es nicht zu noch mehr Toten, Verletzen und zu Geiselnahmen verhasster demokratischer VertreterInnen durch die rechten TerroristInnen. Diese, zu allem bereiten Gruppierungen, waren sicher nicht die einzigen, die an diesem Tag ins Kapitol eingedrungen sind, jedoch stellten sie auch keine politische Ausnahme innerhalb des wütenden Mobs dar, der sich wiederholt gewalttätig, rassistisch, homophob und antisemitisch zu erkennen gab.

Wer den Ereignissen vor dem Fernseher folgte und nichts von den zur Vorbereitung der Erstürmung sowie den zur Koordination genutzten Kanäle auf Parler, Telegram, Discord, Snapshot, Twitch usw. wusste, sowie keine der zahlreichen Kampagnenseiten auf Facebook, Instagram, YouTube, Pinterest, Reddit oder im altbekannten WWW kannte, die die Lüge von der gestohlenen Wahl permanent verbreiteten und noch lange mit stets neuen Zweifeln garnierten, konnte sich das Verhalten tausender US-AmerikanerInnen wohl kaum erklären. Denn ohne die sehr schlaue, effektive und intensive Nutzung einer Vielzahl von Online-Kanälen (und einiger weniger TV-Sender und Radios) hätte es diesen Aufstand der Totalmanipulierten niemals geben können. Die Erstürmung des Kapitols geht in die Geschichte ein als der Moment, an dem das Internet eine Art Apokalypse der Verwirrten und des Hasses auswarf.[1]

Als Trump und sein Team sowie seine organisierten AnhängerInnen noch am selben Tag oder nur wenige Tage später auf praktisch allen Plattformen im Netz, denen es technisch möglich war, gesperrt wurde, schlossen sich scheinbar die Tore wieder, aus denen all die Trolle und Hater zuvor gepurzelt waren. Diese einhellige und bisher nie dagewesene Reaktion der praktisch gesamten US-Internetindustrie zeigt in drastischer Deutlichkeit, dass Plattformen nur dann reagieren, wenn es opportun für sie ist. Hatten sie alle bis zum 6.1. noch gut am Datenverkehr verdient, war nun der Zeitpunkt gekommen, sich als Beschützer der Demokratie zu inszenieren. Vielleicht sollte uns dies sogar mehr Sorge bereiten, als der rechte Mob und sein Führer Trump. Mit den stark zentralisierten Internet-Plattformen hat sich eine Machtkonzentration hinter dem Pogrom-artigen Geschehen offenbart, deren demokratische Kontrolle scheinbar kein Staat mehr ernsthaft anstrebt, so sehr haben sich diese Konzerne in die Kapillaren des Alltagslebens eingenistet.

Ein bescheidener Beitrag zu ihrer Genese und wofür sie genutzt werden, sollen die folgenden Passagen leisten, die in groben Schritten den schnellen Weg der Plattformen zu ihrer heutigen

1 Es war keine uniforme, homogene, paramilitärische Kampfeinheit, die das Kapitol erstürmte. Es ist wichtig zu sehen, dass der Mob aus TrumpistInnen mit durchaus unterschiedlichen Ansichten bestand. Auch ist davon auszugehen, dass nicht alle Anwesenden den im Vorfeld kursierenden Aufruf zur Erstürmung kannten oder ernst nahmen. Fest steht aber, dass alle Anwesenden, die zum Zeitpunkt der Erstürmung die Gegend um das Kapitol nicht verließen, wussten, was sie taten. Das Kaleidoskop der Verwirrten um Trump ist recht vielfältig. Am bekanntesten sind AnhängerInnen der Q-Anon-Verschwörungsmythen, eine Art popkulturell erneuerter Mythos alter, antisemitischer Verschwörungsmotive, der nicht nur in den USA an Zuspruch gewinnt.

Machtfülle skizzieren und die Frage verfolgen, welche technischen und organisatorischen Schritte es waren, die uns in die heutige Lage brachten.[2]

2. Die Entwicklung des Internets zu einem Tracking- und Capture-Apparat in groben Zügen

Im Dezember 1995 hatten 16 Millionen Menschen Zugang zum Internet[3], für Januar 2019 wird die Zahl von 4,4 Milliarden „active internet users" angegeben.[4] Doch an welches Internet sich diese Menschen in den jeweiligen Jahren verbanden, geht aus solchen Zahlen nicht hervor. Die das Internet begleitenden technologischen Schübe und Erneuerungen sind schnell und an ihnen hängen u.a. Hardware-Industrien, weshalb hier ein sehr komplexes Zusammenspiel verschiedener Akteure zu radikal schnellen Erneuerungszyklen beiträgt.

Eigentlich lässt sich sagen, dass 1995 ein anderes Netz als heutzutage im Betrieb war. Nicht nur ist wohl wahrscheinlich kein einziges Hardware-Element von damals mehr in Betrieb, sondern es gab auch softwareseitig eine kaum überschaubare Schar von Updates, Upgrades, und vollständigen Neuheiten.[5] In diesem technischen Wandel ist eine Perspektive versteckt, die die These des Textes tragen soll: dass Phänomene wie Trump auch und insbesondere durch technische Entwicklungen des Internets möglich wurden. Dabei ist es nicht einfach eine Entwicklung im emphatischen, naiv-modernen Sinne, die gemeint ist, sondern die allmähliche Perfektionierung des Internets zu einem kommerziellen Überwachungsapparat, der bis heute weitgehend unverstanden ist, obwohl er drastisch das Geschehen in der Welt beeinflusst.

Die Geschichte des Internets in diesem Sinne, und um die es hier nur kursorisch gehen kann, lässt sich wie folgt darstellen: mit der Einführung von JavaScript durch Netscape und Sun und damit von dynamisch-erzeugten Inhalten um 1996 erschien zum ersten Mal die Möglichkeit

2 Stellvertretend für die kritische Forschungsliteratur zu den Praktiken rechter Gruppierungen im Netz und deren Dynamiken, auch mit Bezug zu ihren realen Opfern, sei hier das hervorragende Buch von Veronika Kracher (2020) zu Incels genannt. Ferner hat Simon Strick einen konzisen Überblick zur rechten Unkultur im Netz vorgelegt (Strick 2021).

3 Quelle: https://www.internetworldstats.com.

4 Quelle: https://dailywireless.org/internet/usage-statistics/. Diese Zahlen sind gewiss ungenau und es wird zunehmend schwieriger, genaue Zahlen zu liefern, da das Phänomen immer globaler geworden ist und die Zahl derer, die per Mobiltelefon ins Netz gehen, rapide angestiegen ist, insbesondere in ärmeren Ländern. Ein Zugang zum Netz kann sich sehr unterscheiden; nicht nur hinsichtlich des Endgeräts, der Kosten, des Budgets und der verfügbaren Datenraten, sondern auch bezüglich der erreichbaren Webseiten, denn Internetzensur nimmt weltweit rapide zu. Die Rede von „dem Internet" ist eigentlich hinfällig.

5 Siehe den Sammelband *Signal traffic: critical studies of media infrastructures* (Parks & Starosielski 2015) für eine Übersicht.

für Webapplikationen, etwas über die Clients, denen sie Daten ausliefern, protokollieren und speichern zu können und somit die ersten Meta-Informationen über Nutzungen zu sammeln.[6]

Lange Zeit in seiner Geschichte blieb die Frage, wie mit dem Internet Geld verdient werden könne, offen. Die Werbeindustrie hatte sich eine technische Krücke gebaut, um überhaupt ein Feedback zu erhalten, wie „wirksam" ihre Werbung im Netz ist: die Page-Impressions, die bis heute eine Rolle spielen, sollen den Erfolg einer Kampagne messen. Hierbei wird ein einzelnes Pixel von einem dezidierten Server bei jedem Abruf einer Website geladen und dieser Ladevorgang wird vom Server protokolliert. Das Laden des Pixels wird gleichgesetzt mit dem Ansehen einer Website: ein offensichtlich etwas grobes Verfahren, das auch leicht manipulierbar ist.

Die Einführung von HTTP-Cookies war der nächste wichtige Schritt der Überwachung im Netz. Das zugehörige RFC[7] 2109 datiert vom Februar 1997.[8] Hier wird zum ersten Mal beschrieben, wie zwischen Client und Server ein State Management Mechanism implementiert wird, der Sessions zwischen beiden ermöglicht. Damit wird zwischen einem Client und einem Server ein identischer Zustand festgehalten, der u.a. den einzelnen Browser für den Server wiedererkennbar macht. Dies passiert mittels einer kleinen Datei, Cookie genannt, die insbesondere eine eindeutige Session ID enthält, z.B: 31d4d96e407aad42. Laut Spezifikation soll ein Browser mindestens 3000 Cookies speichern und verwalten können.

Cookies sind für eine Vielzahl von Anwendungen sinnvoll, einige werden durch sie erst möglich. Leider werden sie aber überwiegend von der Werbeindustrie zum Tracken eines Browsers über mehrere Seiten hinweg eingesetzt. Es sind Cookies, die es ermöglichen, dass über mehrere, heterogene Webseiten hinweg stets eine Produktart beworben werden kann, für die zu Beginn der Session ein passendes Cookie gesetzt wurde. Das Setzen, Verfolgen und Auslesen von Cookies ist heute zur tragenden Säule des kommerziellen Internets geworden und durch die stark vorangeschrittene Zentralisierung von Auslieferungsdiensten ist es trivial geworden, einen Browser und dessen Aktivitäten mehr oder weniger vollständig bis zur Löschung der Cookies zu verfolgen.[9]

Das Internet ist dezentral konzipiert, d.h. die Datenpakete können unterschiedliche Routen nehmen, und die Knoten, die sie verteilten, sind – sehr vereinfacht gesagt – auf gleicher

6 Siehe https://de.wikipedia.org/wiki/JavaScript#Geschichte.

7 RFC steht für Request for Comments. Dies sind die natürlich-sprachlich verfassten Beschreibungen der technischen Elemente des Internets durch die Internet Engineering Task Force (IETF), ein loser, nicht-kommerzieller Verbund von TechnikerInnen, die ganz wesentlich das Internet entwickelt. Die RFCs sind öffentliches Archiv dieser Entwicklungen.

8 Siehe https://datatracker.ietf.org/doc/html/rfc2109. Interessanter sind jedoch die Überarbeitungen 2965 vom Oktober 2000, in der das Setzen und Auslesen der Cookies weiterentwickelt wurde, sowie 6265 aus dem April 2011.

9 Fingerprinting von Browsern ist eine weitere Trackingtechnologie. Um einen Überblick zu gewinnen, siehe die sehr guten Seiten der Electronic Frontier Foundation EFF zum Thema: https://www.eff.org/issues/online-behavioral-tracking

Augenhöhe untereinander. Am Ende sorgen technische Protokolle dafür, dass alles in der richtigen Reihenfolge wieder zusammengesetzt wird und z.B. als Website erscheint. Insbesondere mit dem enormen Wachstum des Cloud Computings seit ca. 2006 und der Marktmacht darin durch nur wenige Anbieter[10] muss heute das Narrativ eines dezentralen Internets entschieden zurückgewiesen werden. Im Gegenteil: noch nie hatten so wenige Firmen direkte Verfügungsgewalt über derart viele, auch extrem sensible und wertvolle Daten, die sie durchaus auch analysieren, was z.T. notwendig ist, um den Betrieb der Data Center zu gewährleisten. Amazons Erfolg beruht weniger auf dem Verkauf von Alltagsgegenständen, sondern auf dem Hosten von Daten, Applikationen und Services auf ihren Cloudservern – zumindest war dies vor der Pandemie der Fall.

Ähnlich gelagert ist der Fall derjenigen Plattformen, die, wie Facebook seit 2004, so richtig an Fahrt gewinnen konnten. Auch hier findet eine Zentralisierung von Datenflüssen unter einer Firma statt (Helmond 2015). Jedoch sind die Veränderungen, die mit dem Aufstieg insbesondere der Social Media Plattformen auftreten, noch tiefgreifender. Dies betrifft zunächst die Einhegung: wer auf diesen Plattformen aktiv ist, befindet sich sozusagen auf Privatgelände und muss die Regeln der Betreiber befolgen. Dies mag harmlos klingen, aber was in den Terms of Services (ToS) insbesondere geregelt ist, sind die Besitzverhältnisse an den Daten und die Rechte der Betreiber, Daten zu sammeln, zu aggregieren, zu korrelieren und zu verkaufen, aber auch auf der Grundlage der Ergebnisse dieser Datenauswertungen Daten zurückzuspielen, insbesondere Werbung, wovon Facebook (und Google) leben. Es ist ein perfekter Kreislauf, der einerseits von den BenutzerInnen alle nur denkbaren Informationen einzieht und darauf basierend Werbung zurückspielt.

In der Geschichte der Werbung ist es nun zum ersten Mal möglich geworden, passgenau und automatisiert Werbung zu schalten: anhand von hunderten von Attributen, die die BenutzerInnen z.T. selbst eingegeben haben, z.B. auf ihren Profilseiten, und solcher, die Facebook nach der Zustimmung zu den ToS legal durch permanente Totalüberwachung des Browserverhaltens speichern darf,[11] soll eine „passende“ Mischung von Inhalten zurückgespielt werden, die z.T. nur schwer als Werbung oder gekaufter Inhalt erkennbar ist. Die Algorithmen, die bestimmen, was im Feed erscheint, schmiegen ihre Ergebnisse dem psychometrischen Modell, das sich Facebook vom Menschen am Gerät gemacht hat, an (Stark 2018). Das Ziel dabei ist „demand generation“, wie es Sheryl Sandberg, seit 2008 Chief Operating Officer bei Facebook, einmal unverhohlen ausdrückte: BenutzerInnen sollen durch Facebook den Wunsch entwickeln, etwas zu kaufen, etwas zu klicken, an etwas zu glauben, ohne zu merken, dass es Facebook war, das diesen Wunsch weckte. Nach Google, mit der Google-Suche, hat Facebook entdeckt, wie mit dem Internet Geld verdient werden kann, ohne

10 Amazon Web Services, Microsoft Azure, Google Cloud, IBM Cloud und Alibaba Cloud teilen sich den Kuchen im Wesentlichen untereinander auf. Dies macht auch die Arbeit von Geheimdiensten wie der NSA viel einfacher.

11 Dies geht soweit, dass Facebook weiß, ob Sie müde sind, da sich dann Ihre Scrollgeschwindigkeit regelmäßig verlangsamt, und sich dazu über die Zeit ein Muster bildet, das eine eigene Struktur aufweist.

dass die BenutzerInnen selbst Geld bezahlen: sie bezahlen mit dem Geld-Ersatz persönlicher Daten, Aufmerksamkeit, Lebenszeit usw. durch Totalüberwachung. Facebook hat die Werbeindustrie in vielerlei Hinsicht revolutioniert und nebenbei mitgewirkt, das Internet vom dezentralen, Webseiten- bzw. Blog-basierten Netz zu einem zusehends zentralisierten Plattform-basierten Netz umzubauen. Im Kern funktionieren alle sogenannten Plattformen ähnlich (Sadowski 2020, Dijck et al. 2018, Langley & Leyshon 2017, Srnicek 2017).[12]

Als 2007 Apple das iPhone präsentierte, das bis heute über zwei Milliarden verkaufte Exemplare zählt, und Google 2008 mit dem ersten Android-Phone die größte Expansion von Googles Trackingtechnik jenseits der Google-Suche auf den Weg brachte und heute damit 85% des Marktanteils von sogenannten Smartphones damit besitzt, wurde die Capture-Zone erneut ausgeweitet.

Mit dem mobilen Datentransfer rückte nun die International Telephone Union (ITU) in die Mitte derer, die die Technik des Netzes fortan mitbestimmen. Die ITU ist im Unterschied zu den wichtigen Internetorganisationen über staatliche Mitglieder definiert, vertreten durch ihre jeweiligen Industrien. Die Standardisierungsinteressen und Technologieentwicklungen des mobilen Internets sind durch diese Struktur der ITU wesentlich stärker kapitalgetrieben als in der verhältnismäßig akademischen Internet Engineering Task Force (IETF). Die gesamte Vorgehensweise der ITU ist hierarchischer, verschlossener und intransparenter, als die der IETF oder auch noch des World Wide Web Consortiums (W3C), das für z.B. den HTML-Standard zuständig ist.[13] Das ist auch für Trackingtechnologien hilfreich, sowie für die Schwächung der Netzneutralität (damit z.B. ruckelfrei und „live“ EM-Fußball auf Millionen Smartphones läuft), oder auch für die Verschränkung von bezahlpflichtigen Diensten mit dem Netz. Seit 2016 haben mobile Browser Desktop-Browser überholt.[14]

Da das Smartphone nicht nur eine IMEI und eine IMSI mitliefert,[15] sondern notwendigerweise immer auch die Cell-ID des Sendemasten mitteilen kann, in den es eingeloggt ist, ist mit ihm auf sehr basale Weise die Grundlage flächendeckender automatisierte Überwachung gegeben, die z.B. Google für seine Location Based Services braucht. Das automatisierte und stets aktuelle Wissen über die Aufenthalte an Orten zu bestimmten Zeiten von BenutzerInnen,

12 Und die NSA freut sich ein weiteres Mal.

13 Das W3C führt insbesondere einen utopischen Kampf um ein standardisiertes HyperText Markup Language (HTML) und Cascading Style Sheets (CSS), um zu vermeiden, dass einzelne Browser eigene Wege gehen. Dies geht aber nur solange gut, wie kein Browser zu mächtig wird. Mit Googles Chrome ist dieser Punkt jedoch schon eine Weile überschritten. Er hat einen Anteil von über 60%.

14 Es ist aber immer eine Frage, wie gemessen und gerechnet wird. Siehe: https://en.wikipedia.org/wiki/Usage_share_of_web_browsers#Differences_in_measurement.

15 Die International Mobile Equipment Identity (IMEI) ist eine einmalige Gerätenummer und die International Mobile Subscriber Identity (IMSI) ist eine einmalige vom Provider durch die SIM-Karte für das Gerät vergebene Nummer. Beides sind technische Bedingung zum Betrieb eines Mobiltelefons und damit herausragende Möglichkeit zur Überwachung desselben. Auch dies erfreut die NSA und ähnliche staatliche Überwachungsstellen.

ergänzt durch das Global Positioning System (GPS) und oft auch lokale WiFi-Netze, ist dabei in vielerlei Hinsicht verwertbar. Die Aggregation solcher Daten lassen Verkehrsflüsse visualisieren, Mob-Bildungen früh erkennen oder natürlich auch einzelne Geräte tracken. Allein der Verkauf dieser Sorte Daten, ergänzt mit den Kontakten der Smartphones, die über etliche Apps unbemerkt extrahiert werden, hat einen eigenen Industriezweig gebildet, der im Abschnitt zum Datenextraktivismus genauer behandelt wird.

Facebook hat insbesondere in ärmeren Ländern, in denen es praktisch nur mobilen Internetzugang gibt, mit den Telekommunikationsprovidern, wie z.B. Orange in einige afrikanischen Ländern, Verträge geschlossen, die es erlauben, dass die BenutzerInnen kostenfrei ins Netz dürfen. Frecher Weise heißt dieses Geschäft *internet.org*. Allerdings besteht das Netz dann nur aus Facebook und Facebook eigenen Diensten. Dieser brillante Schritt erweckt bei Millionen Menschen die Vorstellung, dass Facebook das Internet ist.[16] Es ist aber genau in diesen ärmeren Ländern oft auch mit den demokratischen Prozessen nicht so einfach, weshalb eine unabhängige Medienlandschaft umso wichtiger wird. Diese ist aber mit Facebook wiederum nicht zu haben. Im Gegenteil: mit Facebook lassen sich sehr effektiv WählerInnen beeinflussen und dazu bringen, gegen ihre eigenen Interessen abzustimmen, wie es Cambridge Analytica vielfach bewiesen hat. Doch bevor es um diese dritte Sorte von Geschäft mit Daten geht, werden nun nach den Plattformen erst einmal die ganz großen Player des Datenhandels skizziert.

3. Der Datenextraktivismus und die Data Analytics nach 9/11

Nach den Anschlägen auf die USA am 11.9.2001 begann für die Datenverarbeitung weltweit ein neues Zeitalter. Das Versagen der hochgepäppelten Sicherheitsdienste ließ in Washington und insbesondere im Pentagon, das für die National Security Agency (NSA) zuständig ist, alle Alarmglocken klingeln. Die Verwundbarkeit der USA zuhause durch islamistische Terroristen sollte einen Wandel der Politiken und staatlichen Praktiken einleiten, der verhindern wird, dass so etwas jemals wieder passieren kann. In der Folge wurden mit teils windigen Gesetzen und Notstandsdekreten Datensammlungen und Methoden der Datenanalyse vieler Behörden zusammengelegt und intensiviert. Vor allem aber begann die Integration des privaten Sektors, indem kommerzielle Data Broker und Analysten entweder Zugang zu Daten der Behörden bekamen, oder auf anderem Wege diese bisher aus guten Gründen getrennten Datensammlungen zusammengeführt werden konnten. Die Fähigkeit zur sog. *Preemption* sollte gestärkt werden, d.h. die Vorhersage von Terroranschlägen (und anderen Katastrophen) und deren Verhinderung im Vorhinein durch neue Wege der

16 „Percent of respondents who agree with the following statement: Facebook is the Internet“: Nigeria 65%, Indonesia, 61%, India 58%, Brazil 55%. Siehe: https://qz.com/333313/milliions-of-facebook-users-have-no-idea-theyre-using-the-internet/.

Datenanalysen, -verbindungen, und Exekution von militärischen Handlungen auf deren Grundlagen. Um jedoch mögliche Zukünfte zu erkennen, müssen epistemische Probleme gelöst werden, die bis heute (wenig überraschend) ungelöst geblieben sind (de Goede et al. 2014). Nichtsdestotrotz entstand ein neuer Komplex bisher eher konkurrierender oder wenig interagierender Firmen und Behörden zur Datensammlung und -analyse in bisher unbekannten Ausmaß, wie uns die Snowden-Enthüllungen gezeigt haben (Lyon 2015, Greenwald 2014), der z.B. die Metadaten unterschiedlichster Quellen im sogenannten Kampf gegen den Terror zur Grundlage von Tötungsentscheidungen macht (Weber 2016, Amoore & de Goede 2015).

9/11 hat zur Integration heterogener Datenbestände geführt, den *function creep* zur Norm gemacht,[17] und somit eine Praxis und auch ein Geschäftsmodell etabliert, das weit in die zivile Alltagswelt diffundiert ist (West 2019). Der Kampf gegen den Terror rechtfertigte und rechtfertigt bis heute das Schleifen von Freiheitsrechten und fortgesetzte diskriminierende Praktiken in Polizei und Justiz gegenüber Minderheiten, die aufgrund ihres Aussehens oder ihrer Religionszugehörigkeit unter einen Generalverdacht gestellt werden. Trumps Projekt des Mauerbaus nach Mexiko reiht sich hier nur ein, steht es doch stark im Kontext rassistischer Zuschreibungen von Nord nach Süd und dem Schüren von Hass und Angst. Erst seit kurzer Zeit werden die rassistischen Effekte von Technologien der Überwachung und Big Data überhaupt diskutiert (Benjamin 2019a, Benjamin 2019b, Flynn & Mackay 2018, Noble 2018) und die Frage aufgeworfen, was *data justice* sein könnte (Dencik et al. 2019).

Ebenso bedeutsam ist die operative Verbindung der verschiedenen Data Analytics Konzerne im Zuge der Liberalisierung der Zusammenarbeit mit staatlichen Behörden, sowie große Investitionen in Mustererkennung und Analysen von Big Data an US-Universitäten, die gerne zu Firmenausgründungen führten, um in der Folge von Google oder Facebook gekauft zu werden. Was unter dem Label *Big Data* euphemistisch als Paradigma der Informatik behandelt wird, lässt sich treffender als *Datenextraktivismus* bezeichnen, in Anlehnung an die Praktiken des Extraktivismus, der die meist gewaltförmige Ausbeutung von Rohstoffen meint. Auch dieses Paradigma des 19. und 20. Jahrhunderts westlicher Hegemonie, insbesondere gegenüber dem afrikanischen Kontinent im Kontext des Kolonialismus, das aber bis heute mit unvermittelter Brutalität weltweit fortgeführt wird (Lessenich 2016), hat im 21. Jahrhundert sein Daten-Upgrade erhalten (Couldry & Mejias 2019). Der Datenextraktivismus, der insbesondere seit dem Boom der mobilen Endgeräte ab 2008 und der damit verbundenen ubiquitären Datennutzung sowie dem Entstehen hunderter Data Centers auf dem Planeten ebenfalls verheerende ökologische und soziale Folgen zeigte (Brodie 2020, Cubitt 2017), ist in vielerlei Hinsicht die Fortsetzung hegemonialer Politiken und bedroht zunehmend die Freiheiten von Gesellschaften, da mit ihm Modelle der Berechnung von Profitmaximierung *und* Preemption untrennbar verbunden sind.

17 Dies bezeichnet die Benutzung von Technik in einem anderen, vorher oft explizit ausgeschlossenen Kontext und ist insbesondere in der Datenverarbeitung leider alltäglich geworden.

Zwar erscheint die Welt der Daten stets immateriell, doch ist dies ein fataler Trugschluss. Ganz im Gegenteil: die Verdatung der Welt führt zu einer rapiden Zunahme an Ressourcenverbrauch, von seltenen Erden, von Edelmetallen (und damit zu neuen Kriegen) und besonders von Strom, der nach wie vor überwiegend nicht regenerativ erzeugt wird. Die Ausweitung der Überwachungs- und Beeinflussungszone feuert folglich den Klimawandel an. Extraktivismus von Rohstoffen und Datenextraktivismus liegen im Raubbau an der Welt deshalb überraschend nah beieinander. Was letzteren angeht, so kommen zu den ökologischen Folgen die eigentlichen, primären Folgen obendrauf: ein industrieller Datenraubzug, der bis in die kleinsten Kapillaren des Sozialen eindringt und insbesondere durch die Verbindung heterogener Datenbestände durch Korrelationen versucht neue „Erkenntnisse" zu gewinnen. Nicht ohne Grund wird inzwischen von einer „environmentalitären Situation" gesprochen (Hörl 2018), um der Ubiquität und Heterogenität der Daten als Grundlage von Steuerungsprozessen überhaupt semantisch noch hinterher zu kommen (vgl. Gabrys 2016).

Dabei beginnt alles im Kleinen: Wenn einmal den ToS von Facebook zugestimmt wurde, können je nach Marktlage die permanent registrierten affektiven Regungen in einen Verbund von Analysen übertragen werden, deren Existenz im Verborgenen bleibt (Langlois & Elmer 2018).[18] Laut *Propublica* benutzte Facebook 2016 über 52.000 verschiedene Attribute zur Klassifizierung seiner BenutzerInnen.[19] Bereits 2013 wurde mit hoher Treffsicherheit allein durch die sogenannten „Likes" der BenutzerInnen deren ethnischen Hintergrund, Geschlecht, sexuelle Orientierung, politische Einstellung und so weiter prognostiziert (Kosinski et al. 2013).

Was in materieller Hinsicht in Form von den 15 riesigen Data Centers, die allein Facebook betreibt, ausgerollt wurde und weiterhin ausgerollt wird, wurde aus soziologischer Perspektive treffend als algorithmische Gouvernementalität beschrieben, in der Subjekte nicht mehr nur Regeln und Verhalten internalisieren und somit eine Rationalisierung bestimmter Regierungstechniken leben, die insbesondere das Ökonomische als Dispositiv des Sozialen figuriert. Im Weiterdenken der nach Michel Foucault (2006a, 2006b) benannten

18 Ich kann nur empfehlen, die Terms of Services von Facebook einmal in Ruhe zu studieren. Dies vermittelt recht eindringlich den Grad der Unverschämtheit dieses Konzerns. Hier ein Auszug: „Werbetreibende, App-Entwickler und -Publisher können uns über die von ihnen genutzten Facebook Business-Tools, u. a. unsere sozialen Plugins (wie den „Gefällt mir"-Button), Facebook Login, unsere APIs (application programming interface*)* und SDKs (Software Development Kit) oder das Facebook-Pixel, Informationen senden. Diese Partner stellen uns Informationen über deine Aktivitäten außerhalb von Facebook bereit, u. a. Informationen über dein Gerät, von dir besuchte Websites, von dir getätigte Käufe, Werbeanzeigen, die du siehst und darüber, wie du ihre Dienste nutzt, und zwar unabhängig davon, ob du ein Facebook-Konto hast oder bei Facebook eingeloggt bist. Beispielsweise könnte ein Spieleentwickler unsere API nutzen, um uns mitzuteilen, welche Spiele du spielst, oder ein Unternehmen könnte uns von einem Kauf berichten, den du in seinem Geschäft getätigt hast. Wir erhalten außerdem Informationen über deine Online- und Offline-Handlungen und -Käufe von Dritt-Datenanbietern, die berechtigt sind, uns deine Informationen bereitzustellen" (https://www.facebook.com/about/privacy/update).

19 https://www.propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them

Gouvernementalität, hat Antoinette Rouvroy das wechselseitige Verhältnis von Subjekten zu „ihren" Datensätzen und deren statistischer Operationalität algorithmische Gouvernementalität genannt (Rouvroy et al. 2013), die einen digitalen Behaviorismus ermöglichen. Niemals jedoch kann dieser der vielfältigen Realität gerecht werden, und letztendlich wird durch ihn das Offene der Zukunft, des Kommenden, zu überschreiben versucht (Rouvroy 2013), um ein Kontinuum sicheren Regierens zu etablieren. Was die Ausweitung der Verwertungszone des Kapitalismus in den Informations- und Datenbereich hinein angeht, werden inzwischen drastische Warnungen ausgesprochen, so z.B. jüngst Joseph Vogl: „Es steht vielmehr die Produktion des Wirklichen selbst auf dem Spiel" (Vogl 2021, S.132; siehe auch Cheney-Lippold 2017).

Dabei lassen sich die großen Akteure dieses Datenhandels[20] in nur drei Kategorien einteilen:

1) die größten Online Plattformen: Facebook (1,9 Milliarden Profile aus Facebook, 1,2 Milliarden aus Whatsapp und 600 Millionen aus Instagram), Google (2 Milliarden aus Android und über eine Milliarde aus Gmail, sowie über eine Milliarde aus YouTube) und Apple (eine Milliarde aus iOS/iPhone OS).
2) die Credit Reporting Agencies: Experian (Credit Data zu 918 Millionen Menschen, Marketing Data zu 700 Millionen und sogenannte „insights" zu 2,3 Milliarden), Equifax (Daten über 820 Millionen Menschen und eine Milliarde Geräte), sowie TransUnion (Daten zu einer Milliarde Menschen).
3) die Konsumdatenhändler: Acxiom (Daten zu 700 Millionen Menschen und 3,7 Milliarden Konsumentenprofile ihrer Kunden im Management) und Oracle (mit 1 Milliarde Datensätzen über mobile EndgerätebenutzerInnen, sowie Daten zu 1,9 Milliarden Webseiten-BesucherInnen. Ferner besitzt Oracle 5 Milliarden „unique" consumer IDs, die das Unternehmen Dritten bereitstellt).

Schon diese summarische, inzwischen veraltete und unvollständige Aufzählung lässt erkennen, dass sich nicht nur viel Geld mit den Daten, die Menschen generieren, verdienen lässt, sondern dass damit auch eine enorme Machtkonzentration einhergeht. Diese Konzerne können Modelle generieren, die bis ins kleinste Detail eine Person abbilden können sollen. Allerdings kann die Person sich nicht dagegen wehren oder das Modell überprüfen, denn sie weiß in der Regel nichts davon. Ist die Diskrepanz zwischen Modell und Realität zu groß, führt dies zu falschen Bewertungen von KundInnen, denen dann Zugang zu Diensten und Produkten verwehrt wird (von Versicherungen bis zum Autokauf), ohne dies erklären zu können. Das algorithmische *Data Double* wirkt sich performativ aus, und entwickelt hinter dem Rücken der Subjekte eine Wirkmächtigkeit, die die Handlungsoptionen des Subjekts auf der Basis von Daten-Relationen vorstrukturieren. Dies ist Preemption im Alltag. Von Manipulation zu reden reicht insofern nicht mehr aus. Es gibt keine demokratische Kontrolle

20 Ich folge hier der Einfachheit halber den Forschungen von Cracked Labs aus dem Jahr 2017: https://crackedlabs.org/en/corporate-surveillance.

gegenüber den zunehmend das Soziale strukturierenden Datenoperationen der großen Datenhändler und Data Analytics Firmen.

Doch auch kleine Firmen wollen am Datenextraktivismus teilhaben. Zusätzlich zu den Giganten des Datenextraktivismus hat sich ein wachsendes Universum von Start-Ups etabliert, deren Geschäftsmodell im Extrahieren von überwiegend mobilen Daten besteht. Die Idee ist, wie so oft, simpel: es werden Apps kostenlos zum Download und Installieren über die offiziellen Kanäle von Apple und Google angeboten. Diese Apps sind mit einem Framework hergestellt, das unabhängig von der Funktionalität der Apps zahlreiche Daten von mobilen Endgeräten herunterlädt, insbesondere Geodaten und Kontakte.

Beispielhaft wird hier xmode.io kurz vorgestellt. Deren Motto lautet: „Empowering Innovation with Qualitative Location Data". Diese Firma verkauft Location Data. Doch woher kommen diese Daten? Ein Framework zur App-Entwicklung stellt sicher, dass die mit ihm entwickelten Apps zuverlässig und angeblich „privacy-conscious" eine Vielzahl von Datensorten liefern: Geschwindigkeit und andere telematische Daten, die Device-IDs samt 150 Datenpunkten pro Daily Active User, ferner werden über 60 Millionen monatliche aktiver BenutzerInnen versprochen, die durch das in über 400 Apps installierte Kit ihre Daten verlieren. Die App-Entwickler, die das Entwicklungskit benutzen sollen, erhalten als Bezahlung ein passives Einkommen, insofern die BenutzerInnen ihrer App durch xmode.io erfolgreich ausspioniert werden.[21]

4. Der Fall Cambridge Analytica

Mit dem bisher Geschilderten lässt sich nun einer der prominentesten und skandalträchtigsten Fälle in der Geschichte der kommerziellen Überwachung und Manipulation hoffentlich besser einordnen. Die errichteten Datensilos und ihre untereinander korrelierbaren Daten lassen, kurz gesagt, sehr genau Bevölkerungen in Sets einteilen und diese nach gewünschten Parametern mit Inhalten adressieren. Der Wiederholung von Botschaften sind hier keine Grenzen gesetzt. Die Kosten sind vernachlässigbar.

Cambridge Analytica (CA) war ein von den ultrakonservativen US-Milliardären Mercers und dem offen rechtsextremen Publizisten Steve Bannon, der dem Unternehmen nach eigener Aussage auch den Namen gab, 2013 gegründetes Unternehmen, das 2018 eingestellt wurde und sich selbst den Titel „global election management agency" gab. Nach eigenen Angaben übte CA Einfluss auf über 100 Wahlen aus, davon 44 in den USA (z.B. SenatorInnen-Wahlen). Die Brexit- und die Trump-Kampagne waren dabei wohl die größten Kampagnen. 2020 kam ein britischer parlamentarischer Untersuchungsausschuss zu dem Schluss, das CA keinen Einfluss auf den Brexit genommen hatte. Dies mag daran liegen, dass es sich bei CA

21 Siehe für alle Angaben die Website des Unternehmens: https://xmode.io/.

um eine Unterorganisation der SCL Group handelte, deren Selbstbeschreibung bereits nahelegt, wieso der notwendig einwandfreie Nachweis nicht erbracht werden konnte:

> „The SCL Group has been working at the forefront of behavioural change communication for 25 years. Developed in conjunction with the Behavioural Dynamics Institute, SCL has evolved into a multi-disciplined group of behavioural research and communication agencies. […] In today's global information environment SCL has the knowledge, the people and the experience to help global brands, political organisations, world leaders and militaries deliver measurable and lasting behaviour change."
> (https://web.archive.org/web/20160208184806/http://scl.cc/)

Es handelt sich bei SCL um ein im Geheimen operierendes Unternehmen, das darauf ausgelegt ist, so wenig wie möglich im Licht der Öffentlichkeit zu stehen (vgl. Shaw 2018). Der Nachweis illegaler Aktivität ist somit nur schwer zu erbringen.

Im Kern der Techniken, die CA in seinen Wahlkampagnen angewendet hat, steht die algorithmische Psychometrie: mit ihr kann automatisiert, allein durch Algorithmen, ein recht einfaches Psychoprofil einzelner Personen erzeugt werden (Stark 2018). Ziel ist dann, ganz im Sinne des Behaviorismus, aus dessen Geschichte eine Vielzahl heute digital angewandter Psychotechniken stammt, die betreffende Person zu einem bestimmten Verhalten zu bewegen, ohne dabei verstehen zu wollen, warum diese Person das Verhalten an den Tag legt. Die in diesem Psychomodell verwandten Kategorien sind recht schlicht und beschreiben anhand weniger Merkmale eine Persönlichkeit. Wenn dieses simple Modell dann mit Daten aus anderen Quellen, zB. Anschrift, sexuelle Vorlieben, Bewegungsprofile und all den Merkmalen, die z.B. Facebook sammelt und weiterverkauft, sowie den Daten von Data Brokern wie Axciom verbunden werden, kann eine Firma wie CA passende Botschaften generieren, die einem Set an BenutzerInnen, deren Wahlverhalten entscheidend sein wird, oder die vom Wählen deshalb abgehalten werden sollen, in genau kalkulierten unterschiedlichsten Situationen auf unterschiedlichen Kanälen ausgespielt werden. Dieses Microtargeting muss nicht immer „passen", aber wenn es „passt", wird eine affektive Bindung erzeugt, die die Empfänglichkeit für Botschaften, egal ob wahr oder falsch, dramatisch erhöht. Das berühmteste und berüchtigtste Beispiel ist dabei die „Crooked Hillary"-Kampagne, die CA zu verantworten hat,[22] und mit der der demokratischen Präsidentschaftskandidatin Hillary Clinton erfolgreich und nachhaltig ein schlechtes Image angehängt wurde, das möglicherweise den entscheidenden Ausschlag für Trumps Sieg gab.[23]

22 In einer BBC Channel 4-Doku von 2018 zu CA wird dessen CEO Alexander Nix heimlich aufgenommen, während er sich mit dieser Kampagne brüstet.

23 Hu (2020) gibt einen Überblick, wie die Federal Trade Commission mit dem CA Skandal umging und warum Facebook am Ende fünf Milliarden USD Strafe zahlen musste, sich in der Sache selbst aber nichts geändert hat.

5. Fazit

Die Entwicklung des Internets ist seit dem 21. Jahrhundert auf eine Bahn geraten, die zivilgesellschaftlichen und demokratischen Kräften mehr zu schaden als zu helfen scheint und autoritäre und totalitäre Strömungen begünstigt. Dabei sind im Wesentlichen zwei Linien zu beobachten, die sich gegenseitig verstärken: seit 9/11 überwachen staatliche Behörden hemmungslos und zum Teil gesetzeswidrig weite Teile des Internetverkehrs.

Dieser Trend setzt sich ungebrochen fort. Hier scheint sich ein Automatismus etabliert zu haben, durch den die Behörden immer neue Befugnisse und Technologien erhalten. In Anbetracht der hohen Zahl von Opfern rechter Gewalt in Europa und den USA scheinen die Behörden unter den Bevölkerungsgruppen nach schützenswert und weniger schützenswert zu unterscheiden. „Black Lives Matter“ ist der Slogan, der dies auf den Punkt gebracht hat.

Die zweite Linie betrifft die kommerziellen Entwicklungen des Internets, insbesondere die mobilen Endgeräte und die Plattformen, die seit ca. 2005 für viele Menschen definieren, was das Internet ist. Hier wird auf privatem Grund und nach den Regeln der GrundbesitzerInnen kommuniziert, was die Idee von Plattformen ist. BenutzerInnen sind gegenüber den GrundbesitzerInnen weitestgehend machtlos, sobald sie in die Terms of Services der Plattformen eingewilligt haben. Datenschutzgesetze mögen starke Formulierungen haben, aber ohne ihre Durchsetzung sind sie Ornament.

Indem mittels Microtargeting und automatisierten psychometrischen Techniken die kommerziellen Datensilos und Algorithmen zur Manipulation von PlattformbenutzerInnen in Bezug auf Wahlen erfolgreich eingesetzt werden, wie es Trump bewiesen hat, treffen sich nun beide Linien der Netzentwicklung an der politischen Kreuzung von autoritären Staaten und autoritären Führern. Das Ergebnis sind autoritäre, populistische Politiken, die Kritik und Widerspruch unterdrücken.

Literatur

Amoore, Louise & De Goede, Marieke (2008): Transactions after 9/11: the banal face of the preemptive strike. *Transactions of the Institute of British Geographers,* 33 (2), S. 173–185.

Benjamin, Ruha (2019a): *Race after technology: abolitionist tools for the new Jim code*. Medford, MA: Polity.

Benjamin, Ruha (Hrsg.) (2019b): *Captivating technology: race, carceral technoscience, and liberatory imagination in everyday life*. Durham: Duke University Press.

Brodie, Patrick (2020): Climate extraction and supply chains of data. *Media, Culture & Society* 42 (7–8), S. 1095–1114.

Cheney-Lippold, John (2017): *We are data: algorithms and the making of our digital selves*. New York: New York University Press.

Couldry, Nick & Mejias, Ulises (2019): Making data colonialism liveable: how might data's social order be regulated? *Internet Policy Review* 8(2), DOI: 10.14763/2019.2.1411.

Cubitt, Sean 2017. Finite media: environmental implications of digital technologies. Durham: Duke University Press.

Dencik, Lina u.a. (2019): Exploring Data Justice: Conceptions, Applications and Directions. Information, *Communication & Society* 22 (7), S. 873–881.

Dijck, José van, Poell, Thomas & Waal, Martijn de (2018): *The platform society*. New York: Oxford University Press.

Flynn, Susan & Mackay, Antonia (Hrsg.) (2018): *Surveillance, Race, Culture*. Cham: Springer International Publishing.

Foucault, Michel (2006a): *Sicherheit, Territorium, Bevölkerung. Geschichte der Gouvernementalität I: Vorlesungen am Collège de France 1977/1978*. Frankfurt am Main: Suhrkamp Verlag.

Foucault, Michel (2006b): *Die Geburt der Biopolitik. Geschichte der Gouvernementalität II: Vorlesungen am Collège de France 1978/1979*. Frankfurt am Main: Suhrkamp Verlag.

Gabrys, Jennifer (2016): *Program earth: environmental sensing technology and the making of a computational planet*. Minneapolis: University of Minnesota Press.

de Goede, Marieke, Simon, Stephanie & Hoijtink, Marijn (2014): Performing preemption. *Security Dialogue,* 45 (5), S. 411–422.

Greenwald, Glenn (2014): *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. London: Penguin Books.

Helmond, Anne (2015): The Platformization of the Web: Making Web Data Platform Ready. *Social Media+ Society* 1 (2), S. 1–11.

Hörl, Erich (2018): Die environmentalitäre Situation. *Internationales Jahrbuch für Medienphilosophie* 4 (1), S. 221–250.

Hu, Margaret (2020): Cambridge Analytica's black box. *Big Data & Society* 7 (2), July 2020.

Kosinski, Michal, Stillwell, David & Graepel, Thore (2013): Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences,* 110 (15), S. 5802–5805.

Kracher, Veronika (2020): *Incels: Geschichte, Sprache und Ideologie eines Online-Kults*. Mainz: Ventil-Verlag.

Langley, Paul & Leyshon, Andrew (2017): Platform capitalism: The intermediation and capitalization of digital economic circulation. *Finance and Society* 3 (1), S. 11–31.

Langlois, Ganaele & Elmer, Greg (2019): Impersonal subjectivation from platforms to infrastructures. *Media, Culture & Society* 41 (2), S. 236–251.

Lessenich, Stephan (2016): *Neben uns die Sintflut: die Externalisierungsgesellschaft und ihr Preis*. München: Hanser.

Lyon, David (2015): *Surveillance After Snowden*. Cambridge, Malden, MA: Polity.

Noble, Safiya Umoja (2018): *Algorithms of oppression: how search engines reinforce racism*. New York: New York University Press.

Parks, Lisa & Starosielski, Nicole (Hrsg.) (2015): *Signal traffic: critical studies of media infrastructures*. Urbana: University of Illinois Press.

Rouvroy, Antoinette (2013): The end(s) of critique: data-behaviourism vs. due-process. In: Hildebrandt, Mireille & Vries, Katja de (Hrsg.): *Privacy, due process and the computational turn: the philosophy of law meets the philosophy of technology*. London: Routledge, S. 143–168.

Rouvroy, Antoinette, Berns, Thomas & Libbrecht, Elizabeth (2013): Algorithmic governmentality and prospects of emancipation. *Reseaux,* 177 (1), S. 163–196.

Sadowski, Jathan (2020): The Internet of Landlords: Digital Platforms and New Mechanisms of Rentier Capitalism. *Antipode* 52 (2), S. 562–580.

Shaw, Tamsin (2018): The New Military-Industrial Complex of Big Data Psy-Ops. *The New York Review of Books*. https://www.nybooks.com/daily/2018/03/21/the-digital-military-industrial-complex/ [Stand 2018-03-24].

Srnicek, Nick (2017): *Platform capitalism*. Cambridge, Malden, MA: Polity.

Stark, Luke (2018): Algorithmic psychometrics and the scalable subject. *Social Studies of Science* 48 (2), S. 204–231.

Strick, Simon (2021): *Rechte Gefühle. Affekte und Strategien des digitalen Faschismus*. Bielefeld: transcript.

Vogl, Joseph (2021): *Kapital und Ressentiment: eine kurze Theorie der Gegenwart*. München: C.H. Beck.

Weber, Jutta (2016): Keep adding. On kill lists, drone warfare and the politics of databases. *Environment and Planning D: Society and Space* 34 (1), S. 107–125.

West, Sarah Myers (2019): Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society* 58 (1), S. 20–41.

Information, Wissen und die Wiederkehr der Sozialen Physik

Marian Adolf & Nico Stehr[1]

Zusammenfassung

Die Möglichkeiten der digitalen Informationsökologie (*Big Data*) lassen längst vergangen geglaubte Vorstellungen der totalen Information über individuelle und gesellschaftliche Zusammenhänge wiederauferstehen, etwa die Idee der abschließenden wissenschaftlichen Formulierung einer „Physik des Sozialen". Auf Basis eines genuin soziologischen Wissensbegriffs und einer Darstellung der differenziellen Eigenschaften von Information und Wissen diskutieren wir die Möglichkeiten und Gefahren einer Rückkehr eines mechanistischen Bildes von Mensch und Gesellschaft im digitalen Gewand und erläutern dies am Beispiel des Pioniers der „physique sociale", dem belgischen Sozialstatistiker Adolphe Quetelet. Wir argumentieren, dass dieselben Defizite, die einst Quetelets Vorhaben scheitern ließen, auch die Neuformulierung einer algorithmisch gewendeten Sozialphysik unterminieren. Die eigentliche Gefahr, so schließen wir, liegt in einem datenpolitischen Szientismus, der sich seiner eigenen normativen Blindstellen nicht bewusst ist und daher leicht zum Opfer ideologischer Übernahmeversuche werden kann.

1. Einleitung

Die Frage, wie sich die digitale Revolution unserer technischen Umwelt auf die Strukturen und Prozesse der sozialen Organisation auswirkt, wird spätestens seit der Ankunft des Internet als Massenmedium diskutiert. Anfang der 2010er Jahre nahm diese Diskussion unter dem Eindruck der massenhaften Sammlung, Vernetzung, Verknüpfung und Auswertung immenser Datenbestände eine neue Form an: die Frage nach der Re-Organisation der gesellschaftlichen Kommunikation wurde ergänzt um neue Möglichkeiten der soziotechnischen Steuerung auf Basis bis dahin unvorstellbarer Datenbestände. Der Begriff der *Data Politics* scheint angesichts der Entwicklung besonders passend, geht es doch nicht länger um die spezifische, digitaltechnisch getriebene Entwicklung einzelner Gesellschafts- oder Lebensbereiche, sondern um potenziell immer umfassendere Veränderungen im Verhältnis zwischen Individuum und Gesellschaft, Bürger*in und Staat.

---

[1] Dieser Beitrag basiert auf einem Text, der ursprünglich in *Administration & Society* (Adolf und Stehr 2018) erschienen ist. Er liegt hier in einer aktualisierten und gekürzten Form und erstmalig in deutscher Übersetzung vor. Die Autoren danken Theo Hug für kritische Fragen und hilfreiche Kommentare.

Dabei stechen insbesondere neue Differenziale hinsichtlich der Produktion von und Verfügung über Datenbestände hervor: die Angst vor dem gläsernen Bürger und dem Verlust der informationellen Selbstbestimmung richtet sich nicht länger nur gegen einen mächtigen Staat, der nun neben hoheitlichen Macht- auch mit informationellen Wissensüberschüssen ausgestattet ist; sondern vor allem auch einer neuen Kategorie von digitalen „superstar companies" (Rosen 1981) bzw. der als „big tech" bezeichneten Riege von in dieser Form bislang unbekannten Technologiekonzernen, die neben ihrem immensen ökonomischen Pouvoir auch ein Oligopol an datenbasierten Dienstleistungen innehaben und jene Informationsressourcen und Kommunikationsplattformen effektiv kontrollieren, die für unsere Gegenwart so zentral geworden sind (Facebook, Google, Twitter, Microsoft, Apple).

In einem Punkt jedoch gleichen sich die Positionen sowohl der Verfechter als auch der Gegner einer datenbasierten Soziotechnik unserer „digitalen" Gesellschaft. Beide halten die aus dem digitalen Lebensvollzug endlos entströmenden Daten für unmittelbar praktische Entitäten. Doch während die einen die Vorteile einer neuen Informationsdichte und -tiefe als Möglichkeit zur Verbesserung der wissenschaftlichen Forschung, etwa in der Ökonomie (Einav & Levon 2013) oder der Kriminologie (Lynch 2018) sowie der Praxis sozialer und politischer Systeme zum Beispiel in der Gesundheitspolitik (siehe Miller und Tucker 2017) preisen, verweisen die anderen auf die Abgründe und Gefahren einer datengetriebenen Welt.

In unserem Beitrag zur Debatte über *Data Politics* wollen wir einen Aspekt beisteuern, der allzu schnell abgehandelt, wenn nicht gleich ganz übersehen wird: Information ist nicht gleichbedeutend mit Wissen, und die Konfusion dieser beiden Phänomene führt regelmäßig in die Irre. Sie überschätzt sowohl die Möglichkeiten als auch die Risiken einer datengetriebenen Politik, deren potenzielle Gefahren wir anderswo verorten. Zur Veranschaulichung unserer Argumentation bedienen wir uns einer historischen Episode und ihrer rezenten Wiederauferstehung im Zuge der Big Data-Debatte: der Vorstellung einer Physik des Sozialen.

2. Wissen als Handlungsvermögen

Wir beginnen mit einer kurzen Diskussion über die gesellschaftliche Bedeutung von Wissen, dessen historisch gewachsene, zentrale Rolle für die moderne Gesellschaft immer noch oft dadurch konterkariert wird, dass es in vielen Sozialwissenschaften als eine Art „Blackbox" behandelt wird (vgl. Adolf & Stehr 2017). Das Defizit im Wissen über das Wissen liegt unter anderem darin begründet, dass der wissenschaftliche Diskurs ein gewisses Selbstverständnis gegenüber dem eigenen Wissen entwickelt hat. Er legt ein Selbstverständnis des von ihm produzierten Wissens an den Tag, das dazu neigt, nicht nur

die Objektivität seiner Behauptungen zu überschätzen, sondern auch die *unmittelbare* und *unvermittelte* gesellschaftliche Relevanz wissenschaftlichen Wissens, also dessen Macht.

Wissen, Ideen und Informationen (wobei ganz bewusst sehr weit gefasste und ambivalente Kategorien verwendet werden, die es in der Folge weiter zu differenzieren gilt) sind höchst eigentümliche Entitäten mit Eigenschaften, die sich von denen von Waren, Geheimnissen oder Geld unterscheiden. Wenn sie verkauft werden, gehen Wissen, Ideen oder Informationen in den Besitz anderer über und bleiben dennoch in der Domäne ihres Produzenten (*non-rival*). Wissen wird im Prozess des Konsums nicht zerstört. Wissen hat keine Nullsummeneigenschaften. Wissen ist zunehmend allgemein verfügbar. Im Gegensatz zu Geheimnissen verliert Wissen seinen Einfluss nicht, wenn es enthüllt wird. Seine scheinbar uneingeschränkte Verfügbarkeit mindert nicht seine Bedeutung, sondern macht es auf eigentümliche Weise resistent gegen Eigentum.

Für die Zwecke der folgenden Diskussion und als Grundlage für unsere Argumentation bezüglich der sozialen und politischen Rolle von Daten und Informationen in „information ecosystems" (Cortada 2018) möchten wir Wissen als eine Fähigkeit zu sozialem Handeln definieren (siehe Stehr 1994). Unsere Begriffswahl leitet sich von Francis Bacons berühmter Feststellung ab, deren Übersetzung jedoch bisweilen in die Irre führt: „Wissen ist Macht". Bacons Formulierung legt jedoch nahe, dass Wissen seinen Nutzen daraus ableitet, etwas in Bewegung zu setzen. Der Begriff *potentia* beschreibt die „Fähigkeit", die dadurch gewonnen wird, etwas zu wissen. Dabei ist es wichtig, dass Wissen als verallgemeinerte Handlungsfähigkeit nur dann eine „aktive" Rolle im Verlauf des sozialen Handelns einnehmen kann, wenn dieses Handeln nicht rein stereotypen bzw. routinehaften Mustern folgt oder auf andere Weise streng reglementiert ist.

Wissen als Handlungsfähigkeit kann nicht auf naturwissenschaftliches Wissen reduziert werden. Andere Formen des Wissens stellen ebenso „Handlungsvermögen" dar. Unabhängig von der besonderen Rolle wissenschaftlichen Wissens in der modernen Gesellschaft lässt sich seine Bedeutung nicht aus der Tatsache ableiten, dass es eine unmittelbare Handlungsfähigkeit darstellt. In dieser Hinsicht unterscheidet sich wissenschaftliches Wissen nicht von Alltagswissen oder religiösem „Wissen". Auch die Wissenschaft ist kaum in der Lage, so etwas wie kognitive Gewissheit zu bieten. Auch das von ihr produzierte Wissen bietet meist nichts anderes als mehr oder weniger plausible und oft umstrittene Annahmen, Szenarien und Wahrscheinlichkeiten, wie uns die Corona-Pandemie einmal mehr vor Augen führt. In der Auseinandersetzung mit der praktischen Rolle und dem Status wissenschaftlichen (und technischen) Wissens ist es daher von Bedeutung, sich stets daran zu erinnern, dass die Kontrolle der relevanten Handlungsbedingungen, innerhalb derer Wissen realisiert wird, sozialer Durchsetzungsfähigkeit, also der Macht bedarf.

Ein solches Verständnis verankert Wissen fest in gesellschaftlichen Beziehungen und beschäftigt sich weniger mit wissenschaftstheoretischen Fragen als mit seinen sozialen Anwendungen und Konsequenzen – eine Perspektive, die für unsere Diskussion über die

Bedeutung von Information und Datenpolitik und den ihr zugeschriebenen praktischen Nutzen wichtig ist. Bevor wir uns der Diskussion eines solchen Beispiels, der „Sozialen Physik“, zuwenden, müssen wir kurz auf eine andere relevante Frage in diesem Zusammenhang eingehen, nämlich jene, wie sich die Begriffe Wissen und Information zueinander verhalten. Diese Frage stellt sich, weil diese Begriffe häufig vermischt, wenn nicht gar gleichgesetzt werden.

3. Zum Unterschied von Information und Wissen

Deshalb stellt sich zunächst die Frage, ob es heute überhaupt noch sinnvoll ist, zwischen Information und Wissen zu unterscheiden – angesichts eines fast unbezwingbaren Konvoluts an konkurrierenden Konzeptionen von Wissen und Information, die noch dazu unterschiedlichen epistemologischen und ontologischen Perspektiven entspringen.

Eine autoritative Stimme in diesem Gewirr mag jene von Daniel Bell sein (1979, S. 168): „By information I mean data processing in the broadest sense; the storage, retrieval, and processing of data becomes the essential resource for all economic and social exchanges (in post-industrial society).“ Diese Definition gleicht jener eines technischen Kommunikationsbegriffes, bei dem Bedeutung und Vermittlung von Quelle und Empfänger unabhängig sind.

Wissen hingegen bezeichnet Bell als „organized set of statements of fact or ideas, presenting a reasoned judgment or an experimental result, which is transmitted to others through some communication medium in some systematic form“ (ibid.). Infolgedessen wird Information schnell zu „bloßer Information“, während Wissen methodisch erzeugt, eingeordnet und bewertet wird. In Bells Definition gibt es keinen Hinweis auf den kontingenten Charakter von Information und Wissen. Anscheinend können sowohl Wissen als auch Information praktisch ungehindert zirkulieren. Information ist der Handlanger des Wissens. Zudem scheint Bell von der (unbestrittenen) Autorität, Vertrauenswürdigkeit und Macht von Informationen und Wissen überzeugt zu sein. Empirisch ist dies jedoch nur selten der Fall.

Wissen, so wie wir es definiert haben, stellt Handlungsvermögen dar. Wissen befähigt Akteure – in Verbindung mit der Kontrolle über die kontingenten Umstände des Handelns – etwas in Bewegung zu setzen. Die Funktion der Information ist zugleich begrenzter als auch allgemeiner: Ersteres, weil ihr die befähigenden Eigenschaften des Wissens fehlen; letzteres, weil Information keineswegs so rar ist wie Wissen. Informationen verbreiten sich leicht und erfordern keine besonderen kognitiven Fähigkeiten. Ein Beispiel für Informationen wäre der Preis oder andere Marktinformationen, etwa über die Verfügbarkeit eines Produkts. Solche Informationen können sicherlich nützlich sein, sind dabei doch meist recht unspezifisch. Information ist, mehr noch als Wissen, ein

öffentliches Gut. Information ist autark. Sie ist jedoch nicht handlungsermöglichend in dem Sinne, dass sie einem Akteur erlauben, ein Produkt zu erzeugen. Informationen spiegeln lediglich Eigenschaften der Dinge wider, von denen sie abstrahiert sind. Kurz gesagt, Wissen bezieht sich im Gegensatz zu Informationen auf einen Prozess oder Input, während sich Informationen auf Eigenschaften eines Gegenstands oder Outputs beziehen.

Diese Unterscheidungen und Eigenschaften gilt es in Erinnerung zu behalten, wenn wir uns in der Folge einem frühen sozialwissenschaftlichen Projekt widmen: der „Sozialen Physik".

4. Die Verlockung allumfassender Information: Quetelets Sozialphysik

Vor mehr als einem Jahrhundert war Adolphe Quetelet (1796-1874), der belgische Pionier der empirischen Sozialforschung, der erste Wissenschaftler, der große Bestände an empirischen Daten sammelte und analysierte. Er mag daher heute nicht nur als Begründer der Sozialstatistik gelten, sondern war auch einer der Gründerväter der Soziologie.[2] Im Rahmen unsere Diskussion soll er als Begründer, aber weitgehend vergessener Vorgänger der heutigen „Datenwissenschaft" gelten, dessen Werk uns hilft, mehr über die Versprechen und Hoffnungen von Big Data zu erfahren.

Im frühen 19. Jahrhundert arbeitete Adolphe Quetelet an einem Plan zur Quantifizierung dessen, was er den *homme moyen* nannte: ein arithmetisches Mittel des Einzelmenschen. Die Summe aller durchschnittlichen menschlichen Eigenschaften würde zu einer quantitativen Repräsentation des Individuums führen, die für die Sozialwissenschaften die Funktion eines „Gravitationszentrums" übernehmen könnte (Beirne 1987, S. 1151). Darüber hinaus erlaubte die Messung individueller und kollektiver, sozialer und physischer Eigenschaften, die Dynamik der Gesellschaft nachzuvollziehen. Quetelet war überzeugt, wenn nur genügend Daten gesammelt werden könnten, es möglich wäre, einen Menschen zu berechnen, der die gesamte Menschheit repräsentiert, und damit den Weg für eine Wissenschaft zu ebnen, die er später *Sozialphysik* nennen sollte.

Quetelets „Sozialphysik" lässt sich als empirische Beschreibung der sukzessiven Eingrenzung der Abweichung vom Mittelwert relevanter individueller Eigenschaften des Menschen sowie kollektiver Attribute der Gesellschaft in deren Entwicklung darstellen. Beispiele sind das Ausmaß gesellschaftlicher Konflikte, die Verteilung von Vermögen und

[2] Paul Felix Lazarsfeld, Doyen der modernen Sozialforschung, benannte 1963 sogar seinen Lehrstuhl an der Columbia University nach dem Pionier „Quetelet Professor of Social Science" (Fleck und Stehr 2007). Nach heutigen Maßstäben war Quetelets Arbeit hochgradig interdisziplinär und erstreckte sich über viele Wissenschaftsbereiche, von der Astronomie bis zur Kriminologie.

Einkommen oder die Kriminalitätsstatistik. Aber die Phänomene, die Quetelet interessierten, waren keineswegs auf das beschränkt, was die moderne Sozialwissenschaft als genuin soziale Phänomene betrachtet, wie etwa Bildung oder Moralvorstellungen. Quetelets Interesse erstreckte sich auch auf physikalische Phänomene wie das Gehirn oder die Anatomie im Allgemeinen. Zu diesem Zweck bediente sich Quetelet schon vor mehr als 150 Jahren großer Datenmengen, und verwendete etwa die Körpermaße von 5.738 schottischen Soldaten. Von dort aus machte er sich an die Errechnung des „Durchschnittsmenschen".

Doch was genau beabsichtigte Quetelet mit der Anhäufung solch disperser Datenmengen zu erreichen? Im Jahr 1831 beschrieb er seine Methode und seine wissenschaftlichen Ziele wie folgt:

> Initially, by examining the physical and mental abilities of the people I wanted to discover the law by which they develop at different ages, and learn about the modifications that impact upon them according to place, time, season, sex, and all causes in general. However, in order to estimate these properties correctly and determine their relative value among different peoples and in different periods, one would have to be able to measure them, or at least show that this would be possible once science had collected sufficient observational data. I now hope to have clarified this possibility to the fullest so that no further doubt can exist in this regard. (Quetelet 1831, o.S.)

Die „Sozialphysik", wie Quetelet sie sich vorstellte, sollte mehr sein als eine vornehmlich deskriptive sozialwissenschaftliche Methode zur Erfassung der Abläufe der sozialen Wirklichkeit. Wenn sie richtig betrieben würde – d.h. durch eine vollständige Auflistung sozialer Tatsachen – würde sie die Ursachen sozialen Handelns enthüllen. Zwar betonte Quetelet (1842, S. vii) zunächst, dass "I am less desirous to explain phenomena than to establish their existence […] I have […] no other aim than to collect […] the phenomena affecting man. I confine myself to the citation of facts, such as society presents to our view"; und doch sah er in den von ihm gesammelten empirischen Daten und den daraus abgeleiteten Regelmäßigkeiten hinsichtlich der Verteilung bestimmter Eigenschaften innerhalb einer Population den Schlüssel zur Lösung einer ganzen Reihe von politischen und sozialen Problemen. Es war nicht nur möglich, so seine Überzeugung, soziale Muster zu entdecken, sondern auch die „soziale Mechanik" des gesellschaftlichen Lebens („mecanique sociale") zu enthüllen und in ihre Abläufe einzugreifen. Beispielsweise empfahl Quetelet das optimale Alter für die Einberufung junger Männer in die Armee, Strategien zur Unterdrückung von Kriminalität und abweichendem Verhalten oder zur Preisgestaltung von Getreide, die seiner Meinung nach den größten Einfluss auf die Sterblichkeits- und Reproduktionsrate hatte.

Quetelet, der zeitlebens nur mit bereits vorhandenen Daten operierte (bspw. dem Zensus), erweiterte seine „soziale Mechanik" in der Folge zur „moralischen Statistik", und

bearbeitete Daten zu Phänomenen wie Selbstmord, Heirat und Kriminalität (Letzteres machte ihn auch zu einem Mitbegründer der Kriminalistik). Er führte die Normalverteilung (auch Gauß-Verteilung) als wichtiges Mittel zur Bestimmung von Wahrscheinlichkeiten ein. Auf Basis des Wissens um die Normalverteilung vieler solcher sozialen Fakten wandte er sich zunehmend den Ursachen und Konsequenzen der Abweichungen zu.

Kurz, es ist unbestreitbar, dass Adolphe Quetelet zu jenen Pionieren der Soziologie gehört, die die grundsätzliche Möglichkeit entdeckten, sich mithilfe einer umfangreichen Sammlung sozialer Fakten der Lösung praktischer Probleme anzunähern. Paul Lazarsfeld (1961, S. 278) würdigt Quetelets Vorreiterrole „[He] expanded census activities undertaken by various government agencies. He anticipated with varying degrees of precision many basic concepts of quantification, and his writings led to sophisticated controversies which continued into the 20th century."

Mehr als ein Jahrhundert später wird nun, vor dem Hintergrund des Datenreichtums der zeitgenössischen „information ecosystems" (Cortada 2018), erneut die Möglichkeit einer Physik des Sozialen beschworen (Pentland 2014). Im Folgenden versuchen wir, die Grundannahmen dieser spezifischen Herangehensweisen an die soziale Welt herauszuarbeiten und einige der grundlegenden, unserer Meinung nach fehlerhaften Prämissen solcher Vorhaben zu erschließen. Bemerkenswert ist, dass sowohl die klassische Sozialphysik als auch ihre jüngste Wiederentdeckung auf der Grundlage von Big Data mit dem Sammeln von Daten beschäftigt sind und dabei Ideen oder theoretische Perspektiven vernachlässigen, die die Konzentration, Clusterung oder Verteilung von Attributen sozialer Phänomene erklären könnten; ganz zu schweigen davon, aus solchen Beobachtungen unmittelbar praktische Handlungsanleitungen ableiten zu können. Dem Fehlen einer theoretischen Untermauerung der bloßen Datenerhebung wollen wir besondere Aufmerksamkeit schenken. Davor müssen wir uns jedoch den materiellen und technischen Grundlagen unter den Bedingungen einer zusehends „digitalisierten" Gesellschaft widmen.

5. Die Informationalisierung des gesellschaftlichen Lebens

Was die alte Idee der Enthüllung der sozialen Realität durch die Berechnung der Summe all ihrer Teile wiederzubeleben scheint, ist die beispiellose Verfügbarkeit digitaler Daten über immer größere Bereiche des sozialen und natürlichen Lebens. Die Echtzeitüberwachung durch allgegenwärtige Sensoren und die Ausstattung von Alltagsgeräten mit Informationstechnologie machen soziale Räume zu Orten der omnipräsenten Überwachung. In dem Maße, in dem immer mehr Alltagstätigkeiten ins Internet verlagert werden, in dem webbasierte Dienste für typische Erledigungen und berufliche Tätigkeiten

genutzt werden, sammeln sich immer größere Datenmengen an. Jeder Telefonanruf, jede Online-Bestellung, jede Google-Abfrage, jeder Aufruf einer Website wird protokolliert. Die Nutzung von Social Network Sites (SNS), von Fahrtendiensten, von Rabatt- und Kreditkarten, um nur einige zu nennen, erzeugt Bewegungs- und Aktivitätsprofile, die eine immense Menge an Informationen enthalten. So wie die Metadaten von Telefongesprächen und Server-Logins letztlich mehr sensible Informationen über ein Individuum offenbaren können als der Inhalt der Kommunikation selbst, enthält die Protokollierung unserer Interaktionen und Aktivitäten innerhalb der zeitgenössischen Medien- und Informationsökologie nicht nur Informationen über unser Verhalten, sondern auch über Vorlieben und Wünsche (sog. „psychographic profiling“).

Diese Entwicklung, die bereits unter dem Begriff Big Data diskutiert wurde, steht für die zunehmende Informationalisierung des gegenwärtigen gesellschaftlichen Lebens. Der Prozess hat seine Wurzeln in der weitgehenden Datafizierung (datafication) alltäglicher Aktivitäten, die sich allgegenwärtiger digitaler Technologien bedienen. Heute kann so gut wie alles, was Menschen tun, die Form von Daten annehmen. Gleichzeitig entzieht sich dieser Prozess zunehmend der individuellen Kontrolle, was Michael Seemann (2015) dazu veranlasst, diese Entwicklung als einen allgemeinen und unausweichlichen Kontrollverlust (der informationellen Autonomie) zu beschreiben. Dieses Phänomen ist nicht nur ein medientechnisches Epiphänomen, sondern längst von allgemeiner gesellschaftlicher Bedeutung: Wer heute am sozialen Leben teilnimmt, produziert unwillkürlich personengebundene Informationen. Digitale Abstinenz wird zunehmend mit sozialem Ausschluss erkauft (Adolf & Deicke 2015). Im Hinblick auf das Wachstum von personenbezogenen Datenspuren sind drei Aspekte besonders erwähnenswert:

Erstens gehen auf sozialer Ebene die neuen kommunikativen Möglichkeiten der Informations- und Kommunikationstechnologien (IKT), insbesondere der weiter expandierenden Social-Media-Anwendungen, mit neuen Formen der Selbstdarstellung sowie der sozialen Vernetzung einher. Social-Media-Profile sind zu Plattformen für die Formierung und Repräsentation von Identitäten, aber auch für den gesellschaftlichen Diskurs geworden. In vielerlei Hinsicht haben sich soziale Interaktion und Partizipation auf die Plattformen des Internets verlagert, erlangen dort neue Formen und führen dazu, dass sich ein immer größerer Teil der Bevölkerung in digitalen Sozialräumen aufhält. Gleichzeitig geht die Nutzung solcher „Profile“ mit dem Preis persönlicher und interaktioneller Daten einher, deren Informationswert die Ware ist, auf der die digitale Ökonomie basiert (siehe Stalder 2012, Zuboff 2019).

Auf einer medientechnischen Ebene ergibt sich, *zweitens*, die permanente Hervorbringung und die Unmöglichkeit der Einhegung von Daten aus den dispositiven Eigenschaften der Informations- und Kommunikationstechnologie selbst: Computerbasierte, digitale Technologie produziert unwillkürlich Daten, und zwar im Überfluss, denn Bits und Bytes werden an Schnittstellen nicht tatsächlich „übertragen,“ sondern vielmehr kopiert. Computer sind Kopiermaschinen; und Kopien können aufbewahrt, Verbindungen

protokolliert, Örtlichkeiten gespeichert, Kontaktfrequenzen registriert werden. In Kombination mit der enormen Verbreitung von miniaturisierten und günstigen Sensoren zeichnet die digitalisierte Umwelt automatisch alles auf, was sie einfängt. Solche zunächst punktuell und in spezifischen Kontexten aufgezeichnete Datenmengen können später, angesichts der erweiterten Möglichkeiten der Speicherung und Vernetzung von Informationen, zusammengeführt und verarbeitet werden. Die Kombination von zuvor unverbundenen Daten verleiht ihnen eine neue Tiefe und kann, indem neue Zusammenhänge hergestellt werden, Informationen enthalten, die ihre Einzelteilen nicht enthielten.

Ein *dritter* Treiber für den Kontrollverlust über personenbezogene digitale Daten ist der illegitime oder gänzlich illegale – aber kaum zu verhindernde – Zugriff auf personenbezogene Informationen durch Hacker, Sicherheitsdienste oder ausländische, staatliche Akteure. Angriffe auf die Cloudservices oder Datenbanken populärer Digitaldienstleister führen regelmäßig zu enormen Datenverlusten und der Preisgabe persönlicher Information, beispielweise von privaten Fotosammlungen. Auch deutet Vieles von dem, was durch die Enthüllungen des ehemaligen NSA-Mitarbeiters Edward Snowden und andere prominente Datenlecks bekannt wurde, auf eine massive, anhaltende Verletzung von Bürger- und Freiheitsrechten sowie des nationalen und internationalen Rechts hin. Der Verlust der Kontrolle über persönliche Daten ist in dieser Hinsicht jeder anderen Form der Viktimisierung durch eine kriminelle Handlung gleichzusetzen und kann nur bis zu einem gewissen Grad abgewehrt werden.

In immer neuen Lebensbereichen wird das Zurückhalten privater Informationen unmöglich, wodurch gesellschaftliche Teilhabe zusehends an die Preisgabe persönlicher Daten geknüpft wird: Dokumente wie Reisepässe erfordern heute die Herausgabe biometrischer Daten, ebenso wie Mobilität über Grenzen hinweg. Krankenversicherungen sind in vielen Ländern mit Ausweisen verbunden, die neben den biometrischen Daten auch patientenbezogene Daten speichern. In manchen Gefilden rümpft man längst die Nase, wenn Kunden zu Geldscheinen statt zur Debit-Karte greifen; und die Europäische Union hat ein Regelwerk verabschiedet, wonach alle in Europa verkauften Neuwagen verpflichtend mit einem Notrufsystem ausgestattet sein müssen, das im Falle eines Unfalls Daten speichern und senden kann (eCall-System). Dieses Dilemma wird sich weiter verschärfen, da immer mehr ehemals „analoge“ Tätigkeiten digitalisiert werden.

Die hier beschriebenen Entwicklungen scheinen kaum umkehrbar zu sein. Die Gesellschaft profitiert in vielerlei Hinsicht von diesen technologischen und organisationalen Entwicklungen, z.B. durch gesteigerte Effizienz, neue Möglichkeiten der Beobachtung und des Lernens und nicht zuletzt durch persönliche Bequemlichkeit. Vor allem aber leben wir nicht *mit*, sondern eingebettet *in* diesem digitalen informationellen Ökosystem. Viele der Möglichkeiten, die sich durch die Aufzeichnung und die algorithmische Verarbeitung von Big Data ergeben, sind gesellschaftlich wertvoll. Sie machen Zusammenhänge sichtbar, wo vorher nur „weißes Rauschen“ war. Wir gewinnen Einblicke in Phänomene,

die mit konventionellen Mitteln nur mit großem Aufwand zu entdecken gewesen wären. Und wir bezahlen mit unseren Daten: Wir haben Zugang zu Diensten, die sonst für viele unerschwinglich wären, wie zum Beispiel mit Menschen auf der ganzen Welt in Kontakt zu bleiben, umfassende enzyklopädische Informationen abzurufen oder sich mithilfe interaktiver Landkarten in fremden Städten zurechtzufinden.

Dennoch ist eines der Hauptprobleme von Big Data die faktische, stratifizierte Asymmetrie in Bezug auf den Zugang zu und die Verarbeitungsmöglichkeiten von solchen Daten (was Zuboff „epistemische Ungleichheit“ nennt). Nicht nur sind wir uns der fortschreitenden Veränderungen in der Informationsökonomie nur schemenhaft bewusst, auch die darin liegenden Machtgefälle sind uns nicht vollständig gewahr. Der Einzelne hat nur ein begrenztes, oder gar kein Mitspracherecht bei der Sammlung und Weitergabe solcher Informationen und kann über sie nicht auf dieselbe Weise verfügen wie Unternehmen, Behörden und andere institutionelle Akteure.[3]

6. Datenbasierte Teilhabe

Im Zuge globaler Enthüllungen, etwa der Veröffentlichung geheimer diplomatischer Depeschen durch WikiLeaks (die sogenannte „Cablegate“-Affäre) oder der Preisgabe der Überwachungsprogramme nationaler Nachrichtendienste durch Edward Snowden (die „NSA-Affäre“), erhielt der Begriff Big Data eine kritischere Konnotation. Fragen betreffend die Zukunft der Privatsphäre im Internet sind seitdem zu einem wichtigen politischen Thema geworden. Digitale Daten werden längst als Quelle wirtschaftlicher und politischer Macht verstanden, einer informationellen Macht, die in der Erfassung und algorithmischen Verarbeitung riesiger Mengen von Rohdaten liegt.

Ein wesentlicher Punkt ist, *wer* Daten erheben darf und *wo* solche Informationen kumulieren, eine Frage, die seit langem im Zentrum der Debatte über IKT steht. Armin Nassehi (2014, S. 2) erinnert daran, dass der moderne Nationalstaat schon immer auf statistischen Informationen über seine Bürger beruhte: „die Staatlichkeit des modernen Staates seit dem 18. Jahrhundert [gründet] gerade darin, dass er sich mit Daten versorgt, seit es so etwas wie eine zentrale Planung von Bevölkerungen gibt.“ Nassehi behauptet sogar, dass der Begriff des Bürgers selbst erst durch das Wissen, das der Staat über ihn hat, konstituiert wird. Aus dieser Perspektive war Quetelets „homme moyen“ schon immer ein integraler Bestandteil des Regierens und der Machtverhältnisse im modernen Staatswesen, und die digitalen Möglichkeiten von heute sind lediglich eine weitere Stufe dieser Entwicklung: „Es dürfte reichlich naiv sein, so etwas wie eine unbeobachtbare,

3 In jüngster Zeit wurde eine verwandte Kritik am „computational turn“ der Sozial- und Geisteswissenschaften laut, welche unter dem Namen „tool criticism“ eine gründlichere Reflexion der methodologischen Implikationen der Nutzung von Big Data für die Forschung einfordert (van Es et al. 2021).

authentische, autonome Privatheit retten zu wollen – diese hat es nie gegeben.“ (Nassehi 2014, S. 3)

Wird das moderne Individuum generell transparenter in dem Sinne, dass wir mehr übereinander „wissen“? Oder ist der „gläserne Bürger“ vorwiegend ein asymmetrisches Verhältnis zwischen den Mächtigen und den Machtlosen? Eine Gesellschaft der totalen Transparenz ist, wie schon Robert Merton wusste, eine „teuflische“ Gesellschaft (Merton 1957, S. 345). In einer solchen Gesellschaft wäre das Chaos vorprogrammiert: „full visibility of conduct and unrestrained enforcement of the letter of normative standards would convert a society into a jungle. It is this central idea which is contained in the concept that some limits upon full visibility of behavior are functionally required for the effective operation of a society.“ (ebd.)

Die Aussicht auf vollständige Transparenz unter den Mitgliedern einer komplexen Gesellschaft ist nicht nur (funktional wie normativ) problematisch, sie ist auch gering, wie Heinrich Popitz (1968, S. 18) behauptete. Der Widerstand gegen eine zu große Transparenz des eigenen und fremden Verhaltens ist eine strukturbedingte Funktion sozialer Gruppen, z.B. in Form von institutionell sanktionierter Nachsicht in der Durchsetzung bestehender sozialer Normen oder der Tendenz, sich der Preisgabe der eigenen Privatsphäre zu widersetzen (vgl. Popitz 1968, S. 8). Darüber hinaus kennt die Gesellschaft rechtliche und technische Maßnahmen, um der unbegrenzten Sichtbarkeit des Verhaltens und der Überzeugungen entgegenzuwirken. Auch heute erleben wir einen Widerstreit von Kräften, die Überwachungs- und Sicherheitstechnologien propagieren, und solchen, die sie abschwächen und einhegen wollen. So hat beispielsweise San Francisco als erste amerikanische Großstadt im Jahr 2019 den Einsatz von Gesichtserkennungssoftware verboten.

Einige Beobachter, insbesondere Befürworter der Privatsphäre im Zeitalter allgegenwärtiger IKTs, sind weniger überzeugt von der Kontinuität einer liberalen Tradition des begrenzten gegenseitigen und hoheitlichen Wissens. Die Enthüllungen über die globale Dimension digitaler Überwachungsprogramme wie PRISM, die von den Geheimdiensten NSA und GCHQ betrieben wurden, ließen Bürgerrechtsgruppen aus dem Boden schießen, die vor einem drohenden „Tod der Privatsphäre“ angesichts der sich ausbreitenden Werkzeuge zur Sammlung, Speicherung und Verarbeitung von Daten warnen. Zugleich haben viele Regierungen angesichts neuer Formen terroristischer Bedrohungen, und angetrieben von einem Klima der Angst, Gesetze verabschiedet, die einstige Beschränkungen des Zugangs zu privaten Daten lockern. Die klassische Frage nach dem Verhältnis von Sicherheit und Freiheit als grundlegender Kompromiss demokratischen Regierens ist neu entfacht und hat sich als globale Debatte etabliert.[4]

4 Angesichts dieser Herausforderungen sind in vielen Ländern Initiativen, Bewegungen und NGOs wie die Electronic Frontier Foundation (eff.org) oder The Guardian Project (guardianproject.info) entstanden. Ein besonders bemerkenswertes Beispiel ist die Klage des damaligen Jurastudenten Max Schrems gegen Facebook

Anstatt nur zu beschreiben, was in den wachsenden digitalen Spuren unser aller Alltagsleben zu finden ist, erschaffen datenbasierte Informationen längst auch soziale Fakten. Sie verdoppeln die soziale Welt, indem sie diese in Datenform sichtbar und kalkulierbar machen. Diese Repräsentationen stellen jedoch nicht einfach eine Kopie dar, sie sind vielmehr eine zweite, datenförmige Version des gesellschaftlichen Ganzen. Die rasante Ausbreitung digitaler, vernetzter Technik (*Digitalisierung*) und die damit verbundenen kulturellen, ökonomischen und politischen Prozesse (*Informationalisierung*) werfen also wichtige Fragen nach der Rolle von Information und Wissen im Hinblick auf die Verteilung von, und die Mittel zur Ausübung von Macht auf.[5]

Wir teilen die grundsätzliche Besorgnis über gesellschaftliche und politische Entwicklungen, dass sich die Machtverhältnisse in modernen, demokratischen Gesellschaften weiter zugunsten jener bereits mächtigen gesellschaftlichen Akteure und Institutionen verschieben, die sich das Informationspotenzial umfänglicher Daten zunutze machen können. Wir stimmen jedoch nicht mit einem großen Teil des Big Data-basierten „Social Physics"-Diskurses innewohnenden Annahme über die unmittelbare Verwertbarkeit solcher Beobachtungsdaten überein. Dies gilt auch für die Protagonisten der wiederkehrenden „Sozialphysik", denen wir uns im Folgenden zuwenden werden.

7. Von der 'physique sociale' zu 'Social Physics'

Während die Niederlage der „Sozialen Physik" im Kampf mit ihrer Geschwisterdisziplin Soziologie den Begriff fast ein Jahrhundert lang aus dem Mainstream der Sozialwissenschaften verdrängt hatte, ist er, angetrieben von den Versprechungen von Big Data, kürzlich mit neuem Selbstbewusstsein wieder zurückgekehrt. Darüber hinaus scheinen sich die heutigen Befürworter einer Big-Data-basierten Sozialphysik wie Alex Pentland nicht mehr an ihren einst so bedeutenden Vorläufer zu erinnern. Sie sind daher anfällig dafür, seine methodologischen Fehler zu wiederholen. „Just as the goal of traditional physics is to understand how the flow of energy translates into changes in motion, social physics seeks to understand how the flow of ideas and information translates into changes in behavior." (Pentland 2014, S. 5)

Den Anhängern der Idee einer „sozialen Physik" muss das Zeitalter des „ubiquitous computing" wie das Schlaraffenland erscheinen. „In just a few short years we are likely to have incredibly rich data available about the behavior of virtually all of humanity – on a

wegen der Verletzung der Privatsphäre der Nutzer. Sein Erfolg vor dem Europäischen Gerichtshof im Jahr 2015 besiegelte das Schicksal des „Safe Harbor"-Abkommens zwischen der EU und den USA, das den Umgang mit privaten Daten im transatlantischen Austausch regelte. Auch das Nachfolgeabkommen „Privacy Shield" wurde 2020 vom EuGH gekippt.

5 Für einen überaus pessimistischen Ausblick bezüglich dieser Fragen siehe Zuboff (2019, 2021).

continuous basis“ (2014, S. 12), schreibt Pentland in Fortsetzung der Aspirationen seines historischen Vorgängers. Denn Datenspuren sind heute unweigerliche Folge eines digitalisierten Alltags und informationalisierter sozialer Organisation. Während die Sozialstatistiker der Pionierzeit ihre Daten noch mühsam zusammentragen mussten, liegen die Datenschätze von heute am Wegesrand – zumindest für diejenigen, die darauf zugreifen und sie verarbeiten können.

Der Anspruch der zeitgenössischen „Social Physics“ ist genauso universell wie die Daten, auf denen sie basiert. Wie Pentland im Geiste Quetelets feststellt, zielt sie darauf ab, „[to] move beyond merely describing social phenomena to building a causal theory of social structure,“ um zu einer „mathematical explanation of why society reacts as it does“ zu gelangen; und um schließlich „better social systems“ erschaffen zu können (Pentland 2014, S. 6). Ziel ist es letztlich, „to plan the future“ (2014, S. 7). Im Lichte dieser programmatischen Aussagen muss die Sozialphysik als eine „Wissenschaft“ verstanden werden, die die Gesellschaft nicht nur beschreiben, sondern aktiv verändern will. Kombiniert mit dem selbstauferlegten Anspruch, die moderne Gesellschaft auf der Basis allgegenwärtiger Daten nicht nur besser zu verstehen, sondern auch zu lenken, erscheint die Überwachung des alltäglichen menschlichen Verhaltens gleich noch einmal bedrohlicher.

Quetelet war der Überzeugung, dass die Feststellung von Kausalität als Voraussetzung für die Beherrschbarkeit sozialer Phänomene dann möglich sei, wenn die betreffenden Phänomene erschöpfend beobachtet und gemessen werden könnten. Daher führte er Lücken in seinen eigenen Arbeiten oft darauf zurück, dass die Mittel zur umfassenden Erfassung spezifischer individueller wie sozialer Verhaltensweisen einfach nicht vorhanden seien. Das Problem war eines der Ressourcen, nicht der Methode: Sobald es möglich wäre, die Leerstellen mit ausreichenden Informationen zu füllen, würden die naturwüchsigen „Gesetze“ der sozialen Physik in der Lage sein, die Wechselbeziehung zwischen individuellen und sozialen Prozessen zu entschlüsseln. Pentland scheint diese Ansicht zu teilen, jedoch verfügt er über gänzlich neue Mittel. Je größer die Datenmenge, idealerweise gemessen im Millisekundentakt, desto vollständiger die daraus resultierende Information. Vollständige Information bringt vollständige Erklärung: Das ist der Punkt, an dem Quetelet und Pentland gänzlich übereinstimmen, und zugleich der Punkt, an dem beide irren.

So wie die Macht der Information in der Vergangenheit überschätzt wurde, so ist dies auch in diesem Fall zu erwarten. Wie schon bei Quetelet basiert auch Pentlands Anspruch, die soziale Wirklichkeit umfassend abzubilden, auf einem fundamentalen Trugschluss. Da die Klärung von Kausalität und ihr anschließender Einsatz zur sozialen Steuerung notwendig auf einer *totalen* Darstellung komplexer sozialer Phänomene beruhen, ist das Scheitern eines solchen Programms vorprogrammiert. Was bleibt, ist das, was Sozialwissenschaft ohnehin bereits leistet: die Abschätzung von Wahrscheinlichkeiten.

Es gibt zumindest drei Annahmen, an denen eine Kritik der „sozialen Physik“ ansetzen kann: (1) die fälschliche In-Eins-Setzung von Information und Wissen, (2) die Ignoranz der Sozialphysik gegenüber ihren eigenen normativen Grundlagen und, als Folge dieser Einschränkungen, (3) die Gefahr der Verkehrung des Verhältnisses von wissenschaftlicher Vernunft und ihrer praktischen Anwendung und Konsequenzen.

Erstens ist die Sozialphysik praktisch frei von einer Theorie dessen, was sie zu beschreiben versucht. Wie schon Durkheim (1983 [1897], S. 349, unsere Hervorhebung) in seiner Kritik an Quetelets „homme moyen“ in *Der Selbstmord* feststellte: „diese Theorie erscheint sehr einfach. […] Zunächst kann sie erst dann als *Erklärung* anerkannt werden, wenn sie aufzeigen kann, wie es kommt, dass der Durchschnittsmensch in der Mehrzahl der Einzelmenschen in Erscheinung tritt.“ Auch Pentland strebt eine „causal theory of social structure“ (2014, S. 6) an, verabsäumt es jedoch, die tieferreichenden sozialen und kulturellen Gründe für individuelles Handeln und soziale Interaktion zu thematisieren. In ihrer reinsten Form ist Sozialphysik eine bloße Korrelation, die zufällig auf Regelmäßigkeiten trifft, die sie dann verdinglicht. Meistens geschieht dies in Form einer Regression zur Mitte, was einmal mehr beweist, dass der „Mittelweg“ selten falsch ist.[6]

Ein Beispiel ist die viel diskutierte Innovation des „predictive policing“: Anhand von Daten über Art, Ort und Zeit krimineller Handlungen versuchen Polizeibehörden mit Hilfe von „vorausschauender“ Polizeiarbeit, Verbrechen zu verhindern. Doch die verwendeten Algorithmen sagen nichts darüber aus, warum solche Delikte geschehen, oder welche Maßnahmen zu ihrer Verhinderung ergriffen werden sollten – oder gar, wie die Ursachen für eine solche Konzentration von Straftaten bekämpft werden können. Solche Daten sind lediglich probabilistisch, und die Informationen, die sich aus ihrer Aggregation ergeben, sind nicht annähernd das, was als Wissen gelten könnte.[7]

Zweitens erlaubt das offensichtliche Fehlen jeglicher Theorie – also die bloße Fokussierung auf das, was beobachtet werden kann – der Sozialphysik so zu tun, als wäre sie frei von jeglichen normativen Bezugspunkten und Implikationen. In ihrer scheinbaren Objektivität bestätigt sie jedoch lediglich unreflektierte Alltagstheorien und ist damit, wie alle Beobachtungen der sozialen Realität, genauso beobachterabhängig (und damit anfällig

6 Ein Beispiel dafür ist ein Befund in Pentlands Studie, von dem er ausführlich berichtet und der aus seiner Untersuchung von Daytradern auf der eToro-Plattform resultiert: „In summary, people act like idea-processing machines combining individual thinking and social learning from the experiences of others.“ (Pentland 2014, S. 41) Der „Sweet Spot“ für Händlerentscheidungen liegt zwischen sturem Individualismus und gedankenlosem Kopieren der Strategien anderer, mit anderen Worten: genau in der Mitte, zwischen den äußeren Enden der Kurve. Das mag eine hilfreiche, aber sicherlich keine revolutionäre Erkenntnis sein.

7 Anstatt Verwaltungsaufgaben und deren Treffsicherheit, etwa im Rahmen der Polizeiarbeit zu verbessern, stellt ein fehlgeleitetes Vertrauen in datenbasierte Profile ein Risiko „of discrimination against people who have the ‘wrong’ data profile“ dar, und es „may be difficult for a person predicted to be a wrongdoer to prove that the predictions are wrong.“ (Maciejewski 2017, S. 131). Meijer & Wessels (2019, S. 1) stellen zudem in ihrem Überblick über die einschlägige Literatur fest, dass dem „predictive policing“ bis heute „eine klare Evidenzbasis fehlt.“

für normative Formatierungen) wie jede andere, „theoretisch verunreinigte" Darstellung. Dies folgt aus der bloßen Tatsache, dass jede Interpretation der Realität, und sei sie auch algorithmisch abgeleitet, notwendigerweise durch ihren eigenen Ausgangspunkt vorstrukturiert ist. Längst hat sich herausgestellt, dass es auch so etwas wie „algorithmic bias" gibt (Noble 2018), und dass auch algorithmisch erzielte Ergebnisse nur so gut sein können, wie es die Primärdaten, die Programmierung und die Absichten der Anbieter es erlauben.

Dasselbe gilt für Pentlands Ziele, wobei sich seine implizite Weltsicht in dem widerspiegelt, was als evident dargestellt wird: Die Sozialphysik, so behauptet er, „helps us tune communication networks so that we can reliably make better decisions and become more productive" (2014, S. 4). *Ordnung* und *Fortschritt*, die normativen Ziele des klassischen Zeitalters der Sozialstatistik, sind durch *Effizienz* und *Innovation* ersetzt worden, die den Einsatz von Big Data vermeintlich selbsterklärend motivieren.

Allerdings gibt es keinen Ort, von dem aus man die soziale Wirklichkeit beobachten könnte, der außerhalb der sozialen Wirklichkeit liegt: Auch Algorithmen sind von Menschen gemachte Erfindungen, die auf von Menschen gemachten Computern laufen, die mit Daten aus weltlichen Quellen gefüttert und später von Anwendern so interpretiert werden, dass sie sich auf das eine und nicht das andere beziehen. Die Gefahr liegt hier in der technischen, szientistischen oder administrativen Blindheit gegenüber der Voraussetzungshaftigkeit solcher vermeintlich wertfreien Informationen, deren Bedingtheit denjenigen verborgen bleibt, die nur über das Rechenschaft ablegen wollen, „was ist". Was ignoriert wird, ist die Tatsache, dass „was ist" und „was sein soll" im sozialen Kontext niemals objektive Kategorien sein können. Der Ort des Ringens um solche Definitionen ist das Feld des Politischen und nicht das Rechenzentrum.

Und daher laborieren sowohl die alte als auch die neue Variante der „Sozialen Physik" letztlich am selben Übel. Bestimmt man nämlich den „Durchschnittsmenschen" rein numerisch, neigt alles andere dazu, zur Abweichung zu werden. Quetelets Beispiel – etwa seine Empfehlungen zur Abwendung revolutionärer Bestrebungen (Quetelet 1848, S. 295) – zeigt, dass die Pioniere der Sozialphysik nicht nur von einem methodischen Interesse an einer immer präziseren Abbildung der sozialen Wirklichkeit getrieben waren, sondern dass sie, wie auch die zeitgenössischen Protagonisten der Soziotechnik des „nudging", ihre Erkenntnisse in konkrete Politik umgesetzt sehen wollten. Und während Quetelet eifrig bemüht war, die Gefahr dessen abzuwehren, was er die „gefährlichen Klassen" nannte, mögen es heute „gefährliche Individuen" sein, die unter Beobachtung gestellt werden sollen; und zwar auf Basis von datenbasierten Annahmen, die sich stets als nichts anderes als eine Illusion von Wissen entpuppen könnten.

Tatsächlich scheint die größte Gefahr der neuen Möglichkeiten darin zu bestehen, subjektive Präferenzen als objektive Tatsachen zu maskieren. So konstatiert Alex Pentland, dass der von ihm als „reality mining" (Pentland 2014, S. 7) bezeichnete Prozess und die Verarbeitung solcher Daten „crashes, revolutions, [and] bubbles" (2014, S. 9) zu

erklären vermag. Selbst Pentland bezeichnet Big Data und sein soziotechnisches Potenzial als ein „promethean fire", das in den falschen Händen katastrophale Folgen für eine liberale und demokratische Gesellschaft haben kann. Dieser Gedanke hält ihn jedoch nicht davon ab, da sein „New Deal on Big Data", wie er behauptet, dieses geringfügige Problem zu heilen vermag.

Drittens droht die Sozialphysik – in Verkennung der Eigenschaften wissenschaftlichen Wissens – einen entscheidenden Prozess der gesellschaftlichen Praktikabilität und Anwendung von Wissen umzukehren. Neues Wissen, auch wenn es aus der Naturwissenschaft entstammt, ist nur dann handlungsbefähigend, wenn man die Umstände kontrolliert, unter denen es zum Einsatz kommen kann (siehe unsere Ausführungen oben). Das Wissen über die Funktionsweise des Klimawandels, z.B. um die Rolle der Treibhausgase bei der Erwärmung der Erdatmosphäre, ist an sich nutzlos, wenn man den Ausstoß solcher Gase nicht verringern kann. Mit anderen Worten und um eine wichtige Erkenntnis aus den Science and Technology Studies zu wiederholen: Effekte, die unter Laborbedingungen beobachtet wurden, lassen sich außerhalb dieses spezifischen Settings nicht einfach wiederholen. Die Sozialphysik, so ist zu befürchten, wird daher versuchen, die Rahmenbedingungen dahingehend zu verändern, ihren „objektiven", algorithmisch abgeleiteten Erkenntnissen zu entsprechen. Das birgt die Gefahr einer autoritären Verdopplung, die allen rigorosen Big Data-Bestrebungen im gesellschaftlichen Kontext innewohnt: dass sie nämlich politischen, nicht wissenschaftlichen Zwecken dienstbar werden, und damit unter dem Deckmantel der Objektivität die liberale Ordnung demokratischer Gesellschaften unterminieren. Und zwar nicht, weil die verwendeten Daten tatsächlich die Ursachen devianten oder delinquenten Verhaltens abbilden, sondern weil individuelles wie kollektives Verhalten durch Regeln und Vorschriften so beeinflusst werden könnte, der „Wahrheit" der Daten zu entsprechen.[8]

Anstatt kritische Einblicke in die Strukturgebundenheit sozialer, ökonomischer oder kultureller Beziehungen zu gewähren, ist die normative Unbedarftheit eines Programms, die soziale Welt „effizienter" und „produktiver" zu machen, vielmehr dazu angetan, ein soziales Umfeld zu erschaffen, in dem seine impliziten Vorgaben tatsächlich Geltung erlangen. Und sofern es opportun ist, können die Bedingungen, unter denen ein solches datengetriebenes „Wissen" tatsächlich praktikabel ist, in der Folge *ex post* hergestellt werden.

8 Für Evgeny Morozov läuft die in den scheinbar neutralen und rein technologisch motivierten *Big Data*-Anwendungen implizierte (Daten-) Politik auf ein „algorithmisches Regieren" im Sinne von Michel Foucaults gouvernementalité hinaus. Viele der Stimmen, die etwa die Big-Data-basierte Politiken des „nudging" bejubeln, lassen sich seiner Ansicht nach auf eine Ideologie des orthodoxen Liberalismus zurückführen. Aus dieser komfortablen Warte lassen sich strukturelle gesellschaftliche Probleme leicht „individualisieren" und schlicht auf „schlechte Entscheidungen" des Einzelnen zurückführen. Morozov nennt diese politische Mischung aus Technologie und liberalistischer Ideologie „Solutionismus", der immer dann am Werk ist, wenn „deeply political, life-altering issues are recast as matters of improving efficiency" (Morozov 2014, S. 134).

Mit anderen Worten: Die soziale Realität gerät unter Druck, den Beobachtungsparametern der Sozialen Physik zu entsprechen, deren Erkenntnisse sodann – rückwirkend – Geltung erlangen. Dies ist ein Paradebeispiel für eine sich selbst erfüllende Prophezeiung im Sinne von Robert Merton (1948): Eine abstrakte Vorstellung der Wirklichkeit wird zu einer faktischen Realität, indem man sie in ihren Konsequenzen vorwegnimmt und damit erst die Voraussetzungen schafft, unter denen sie entstehen kann. „The specious validity of the self-fulfilling prophecy perpetuates a reign of error." (Merton 1948, S. 195)

8. Conclusio

Letztlich dürften sowohl die Gefahren als auch die Verheißungen der zeitgenössischen, auf Big Data basierenden Sozialphysik übertrieben sein. Selbst wenn es möglich wäre, alle sozialen Interaktionen zu messen und durch wahlloses Korrelieren aller möglichen Variablen Beobachtungsinformationen abzuleiten, würde der Mangel an theoretischer Einsicht in immer neue Sackgassen führen. Die wesentlichen Probleme, die wir mit dieser datenbefeuerten Hybris verbunden sehen, sind anderer Art: Das praktische Vermögen des Wissens liegt nicht darin begründet, jede einzelne Eigenschaft eines Phänomens zu erfassen. Vielmehr ist die praktische Macht des Wissens eine Funktion der Kontrolle des sozialen Kontextes seiner Umsetzung. Die Frage ist also nicht so sehr, ob Big Data und darauf aufbauende, wie auch immer genannte Variationen einer „sozialen Physik" daran scheitern, jene Art von praktischem Wissen zu generieren, auf das sie abzielen, sondern, ob das allgemeine gesellschaftliche und politische Klima dahingehend beeinflusst werden kann, die Bedingungen zu schaffen, unter denen „social physics" zu einer wirkmächtigen Ideologie einer zukünftigen Gesellschaft werden kann. Dies öffnet potenziell die Tür für das, was man als „algorithmische Regulierung" bezeichnen könnte. In dieser Form des Regierens ist die „traditional hierarchical relation between causes and effects […] inverted, so that, instead of governing the causes – a difficult and expensive undertaking – governments simply try to govern the effects. […] If government aims for the effects and not the causes, it will be obliged to extend and multiply control. Causes demand to be *known*, while effects can only be checked and controlled." (Agamben 2013, S. 1, unsere Hervorhebung). Die befremdliche Tendenz aus der Datenwissenschaft eine Datenregierung machen zu wollen, bedarf unser aller kritischen Aufmerksamkeit. Und sie verweist darauf, dass demokratische Gesellschaften längst einer Wissenspolitik bedürfen (Stehr 2003), die auch eine Datenpolitik enthalten muss. Denn Daten umfassen längst nicht alles relevante Wissen. Und Information, egal wie umfangreich, kann den politischen Prozess niemals ersetzen.

Literatur

Adolf, Marian & Stehr, Nico (2018): Information, Knowledge, and the Return of Social Physics. *Administration & Society,* 50(9), S. 1238–1258.

Adolf, Marian (2014): Involuntaristische Mediatisierung. Big Data als Herausforderung einer informationalisierten Gesellschaft. In: Ortner, Heike Daniel; Pfurtscheller, & Rizzolli, Michaela (Hrsg.): *Datenflut und Informationskanäle.* Innsbruck: Innsbruck University Press, S.19-35.

Adolf, Marian & Deicke, Dennis (2015): New modes of integration: Individuality and sociality in digital networks. *First Monday*, 20(1). doi:10.5210/fm.v20i1.5495

Adolf, Marian & Stehr, Nico (2017). *Knowledge*. Key Ideas Series. Second, revised and extended edition. New York and London: Routledge.

Agamben, Giorgio (2013): *"From the State of Control to a Praxis of Destituent Power."* Public lecture, November 16, 2013. Retrieved from: http://roarmag.org/essays/agamben-destituent-power-democracy/ (last accessed: 08/04/16)

Beirne, Piers (1987): Adolphe Quetelet and the Origins of Positivist Criminology. *American Journal of Sociology,* 92(5), S. 1140-1169.

Bell, Daniel (1979): The social framework of the information society. In Dertouzos, Michael L. & Moses, Joel (Hrsg.): *The Computer Age: A Twenty-Year View* (pp. 163–211). Cambridge, MA: MIT Press.

Cortada, James W. (2018): Exploring How ICTs and Administration Are Entwined: The Promise of Information Ecosystems. *Administration & Society*, 50(9), 1213–1237.

Durkheim, Emile ([1897] 1983): *Der Selbstmord.* Frankfurt am Main: Suhrkamp.

Einav, Liran & Levon, Jonathan D. (2013): „The data revolution and economic analysis," *NBER Working Paper* w19035.

Fleck, Christian & Stehr, Nico (2007): "Von Wien nach New York." In: Fleck, Christian & Stehr, Nico (Hrsg.): *Paul F. Lazarsfeld. Empirische Analyse des Handelns.* Frankfurt am Main: Suhrkamp. S.7–58.

Lazarsfeld, Paul Felix (1961): Notes on the History of Quantification in Sociology. Trends, Sources and Problems. *Isis*, 52(2), S. 277–333.

Lynch, Jay (2018): Not even our own facts: Criminology in the era of big data. *Criminology*, 56: S. 437–454.

Maciejewski, Mariusz (2017): To do more, better, faster and more cheaply: using big data in public administration. *International Review of Administrative Sciences*, 83(1_suppl), S. 120-135.

Meijer, Albert & Wessels Martijn (2019): Predictive Policing: Review of Benefits and Drawbacks. *International Journal of Public Administration,* 42:12, S. 1031–1039, DOI: 10.1080/01900692.2019.1575664

Merton, Robert K. (1957): *Social Theory and Social Structure.* New York: Free Press.

Merton, Robert K. (1984): The self-fulfilling prophecy, *Antioch Review*, 8, S. 193–210.

Miller, Amalia R. & Tucker Catherine (2017): "Frontiers of health policy: Digital data and personalized medicine." In: Greenstein, Shane; Lerner, Josh & Stern, Scott (Hrsg.): *Innovation Policy and the Economy.* Band 17. Chicago: University of Chicago Press, S. 49–75.

Morozov, Evgeny (2014): *To Save Everything, Click Here: The Folly of Technological Solutionism.* New York: Public Affairs.

Nassehi, Armin (2014). „Wer hat die privaten Daten verraten?" *Frankfurter Allgemeine Zeitung*, 23.04.2014.

Noble, Safiya Umoja (2018): *Algorithms of Oppression: How Search Engines Reinforce Racism.* New York: NYU Press.

Pentland, Alex (2014): *Social Physics. How good ideas spread – the lessons from a new science.* New York: Penguin.

Popitz, Heinrich (1968): *Über die Präventivwirkung des Nichtwissens.* Tübingen: Mohr.

Quetelet, Adolphe (1831 [1984]): *Research on the Propensity for Crime at Different Ages*. Translated and introduced by Sawyer F. Sylvester. Cincinnati: Anderson.

Quetelet, Adolphe (1842 [1835]): *A treatise on man and the development of his faculties.* Edinburgh: W. and R. Chambers.

Quetelet, Adolphe (1846) : *Lettres a S.A.R., le Duc Regnant de Saxe-Coburg et Gotha, sur la theorie des probabilites*. Brussels: Hayez.

Quetelet, Adolphe (1848). *Du systeme social et des lois qui le regissent.* Paris: Guillaumin

Rosen, Sherwin (1981): The economics of superstars, *American Economic Review*, 71(5), S.845-858.

Seemann, Michael (2015): *Digital Tailspin: Ten Rules for the Internet After Snowden.* Network Notebooks 09, Institute of Network Cultures, Amsterdam.

Stalder, Felix (2012): Between Democracy and Spectacle: The Front-End and the Back-End of the Social Web. In: Mandiberg, Michael (Hrsg.): *The Social Media Reader.* New York: New University Press, S. 242–256.

Stehr, Nico (1994): *Knowledge Societies.* London: Sage.

Stehr, Nico (2003): *Wissenspolitik: Die Überwachung des Wissens.* Frankfurt/Main: Suhrkamp.

van Es, Karin; Schäfer, Mirko Tobias & Wieringa, Maranke (2021): Tool Criticism and the Computational Turn. A "Methodological Moment". In: *Media and Communication Studies*. *Medien & Kommunikationswissenschaft*, Vol. 69/1, S. 46–64.

Zuboff, Shoshana (2021): "The Coup We Are Not Talking About". *The New York Times*, 29.01.2021.

Zuboff, Shoshana (2019): *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* London: Profile Books.

Vom Machiavellismus zur Hospitalisierung – Expertokratie oder Mündigkeit im Zeitalter der Digitalisierung

Hans-Martin Schönherr-Mann

Zusammenfassung

Die von der Medizin gelenkte Politik hat 2020 einen weltweiten Ausnahmezustand ausgelöst, der nicht zuletzt durch digitale Überwachungstechniken besonders medizinischer Art zu einer Hospitalisierung der ganzen Gesellschaft führt. Die Mündigkeit der Bürgerinnen ist dabei weitgehend verloren gegangen. Dass sich viele dagegen nicht zur Wehr setzen können, liegt nicht zuletzt daran, dass sich die Massenmedien in die machiavellistische Politik der Furchterzeugung einklinken und es an seriöser kritischer Information von dieser Seite mangelt. Dadurch konnten viele dieses Defizit an Information auch nicht durch das WWW ausgleichen, in dem es schwerfällt, zwischen Fake News und überzeugender Kritik zu unterscheiden, wenn ein seriöser externer Maßstab fehlt. Damit intensiviert sich die staatliche Biopolitik, so dass die soziale wie politische Macht der Medizin weiter wächst, die Mündigkeit und Menschenrechte so wenig wie die Demokratie achtet. Ob sich die Bürgerinnen dagegen zur Wehr setzen können und werden, lässt sich kaum abschätzen. Man hat mal sein Leben für die Freiheit eingesetzt, jetzt opfert man die Freiheit dem nackten Leben.

1. Der digitale Fortschritt der Biopolitik

Die in Deutschland verbreitete Corona-App wäre für die mündige Bürgerin nicht mal das Problem gewesen. Diese App gaukelt zumindest vor, dass das Individuum selber darüber befindet, ob es sie anwendet oder nicht. Dass es dabei dem Druck der Umwelt ausgesetzt sein kann, ist auch nicht unbedingt dramatisch. Man sollte wirklich nicht alle Lebensprobleme verallgemeinern und dann am Ende staatlich regeln. Das Individuum muss sich selbst überlegen, wie es sich wehren kann, wie es solchen Druck der Umwelt und des Staates hintergeht und untergräbt. Man könnte ja das Mobiltelefon zuhause lassen. Natürlich, sich wehren bereitet Schwierigkeiten, verlangt Kreativität, könnte angesichts einer tristen, vom ‚großen Bruder' kontrollierten Realität aber Spaß machen und die Laune aufhellen.

Im freien Fall befindet sich momentan trotzdem die Mündigkeit der Bürgerinnen angesichts des digitalen wie analogen Überwachungsstaates, der sich seit dem Frühjahr 2020 weltweit ausgebreitet hat. Zum ersten Mal in der Geschichte kann man obendrein vor dem ‚großen Bruder' in kein anderes Land fliehen. Denn das Medizinwesen herrscht nun

mal flächendeckend in allen Staaten auf der ganzen Welt und hat praktisch überall zur Ausrufung des Ausnahmezustands geführt. Es gibt kein Entkommen.

Diese weltweite Verbreitung des Medizinwesens verdankt sich seiner zweifellosen Effizienz, indes leider nicht nur bei der Heilung von Krankheiten, sondern weil die Medizin nach Michel Foucault, ihrem schärfsten Analytiker, vor allem im Dienst einer gouvernementalen, d.h. bürokratisch organisierten und polizeilich durchgesetzten Biopolitik steht, aus der heraus und mit der zusammen sich sowohl der Nationalstaat wie die moderne Medizin seit dem 17. Jahrhundert entwickelten. Foucault schreibt bereits 1963 in seinem Buch *Die Geburt der Klinik* über die Medizin:

> „In der Lebensführung der Menschen beansprucht sie eine normative Rolle, die sie nicht bloß zur Erteilung von Ratschlägen für ein vernünftiges Leben befugt, sondern sie zur Lehrmeisterin für die physischen und moralischen Beziehungen zwischen dem Individuum und seiner Gesellschaft macht. Sie situiert sich in der für den modernen Menschen maßgeblichen Randzone, in welcher ein bestimmtes organisches, leises, leidenschaftsloses und muskulöses Glück ganz eng mit der Ordnung einer Nation, mit der Stärke ihrer Armeen, mit der Fruchtbarkeit eines Volkes und mit dem langsamen Gang seiner Arbeit verbunden ist.“ (Foucault 2005, S. 52)

Bereits 1602 intoniert diese medizinisch basierte Biopolitik der häretische Dominikanermönch Tommaso Campanella mit seiner Utopie *La città del Sole* und zwar mit autoritären sozialistischen und universell katholischen Zügen. Dem *Sonnenstaat*, so berichtet Campanellas Reisender von der fernen Insel,

> „obliegt vor allem die Sorge für die Fortpflanzung, damit Männer und Frauen so miteinander verbunden werden, dass sie den besten Nachwuchs hervorbringen. Sie <die Insulaner> spotten über uns, weil wir der Fortpflanzung der Hunde und Pferde unsere eifrige Sorge widmen, die der Menschen aber vernachlässigen.“ (Campanella 1960, S. 119)

Freilich hat er dabei ein frühes Vorbild, nämlich Platons Politeia, in der schon die Züchtung von Menschen propagiert wird.

2. Ausnahmezustand als Hospitalisierung

Diese also von weither kommende, biopolitische Tendenz der frühneuzeitlichen wie der modernen Staaten realisiert sich im gegenwärtigen Ausnahmezustand, bei dem die Organisationsprinzipien des Hospitals auf die Gesellschaften in ihrer Ganzheit übertragen werden. Damit bewirkt der Ausnahmezustand folglich die Hospitalisierung der Gesellschaft. Im Ausnahmezustand werden gemeinhin die Grundrechte der Bürgerinnen

aufgehoben, wobei es gleichgültig ist, wie man das dann bezeichnet, ob als Katastrophenfall oder als epidemischen Notstand.

Den Ausnahmezustand kann man daher auch nicht rechtlich regeln, und zwar nicht nur, weil das Recht ja aufgehoben wird, sondern weil seine Ausrufung immer auf einer Entscheidung beruht, die in letzter Konsequenz immer ein Akt der Willkür ist. Bei welcher Zahl von Infizierten er ausgerufen wird, muss beschlossen werden. Aber es gibt nun mal keinen methodisch angebbaren Übergang von der Information zur Entscheidung. Carl Schmitt, der wichtigste Theoretiker des Ausnahmezustands schreibt 1922:

> „Die Entscheidung über die Ausnahme ist nämlich im eminenten Sinne Entscheidung. Denn eine generelle Norm, wie sie der normal geltende Rechtsatz darstellt, kann eine absolute Ausnahme niemals erfassen und daher auch die Entscheidung, dass ein echter Ausnahmefall gegeben ist, nicht restlos begründen.“ (Schmitt 2004, S. 13)

Mit dem Ausnahmezustand erzeugt man einen anomischen Zustand, weil nun mal der Nomos aufgehoben ist. Das Gesetz ist nicht mehr in Kraft, so dass man dann auch völlig gesetzesfremde Maßnahmen ergreifen kann, wie das heute genauso der Fall ist wie zu Zeiten des Nationalsozialismus. So zieht Schmitt folgenden Vergleich: „Der Ausnahmezustand hat für die Jurisprudenz eine analoge Bedeutung wie das Wunder für die Theologie.“ (Schmitt 2004, 43) Das Wunder durchbricht den Rahmen der Naturgesetze, der Ausnahmezustand den Rahmen der gesetzlichen Ordnung, herrscht im Ausnahmezustand eine Kraft ohne Gesetz. Parlamentsentscheidungen, die die Ausrufung des Ausnahmezustands absegnen bzw. diesem einen demokratischen Heiligenschein verleihen, ändern an dieser Sachlage nichts: Die Grundrechte sind aufgehoben und dann können Mediziner und Politiker Maßnahmen beschließen ohne Rücksicht auf diese Rechte, wie man das 2020 und 2021 tagtäglich erleben durfte.

Die schwerwiegendsten Aufhebungen der Menschenrechte im Zuge des Ausnahmezustands heute sind dabei Demonstrationsverbote und damit die Aufhebung der Meinungsfreiheit, Freiheitsentzug, den man Quarantäne nennt, Ausgangssperren von einer Dauer, die sich keine frisch gebackene Militärdiktatur leisten könnte, grundrechtsverletzende Reiseverbote, die totale Aufhebung der Unverletzlichkeit der Wohnung, die zwischenmenschliche Kommunikation zerstörenden Kontaktverbote, diskriminierende Verhaltensvorschriften, beleidigender und entstellender Gesichtsverhüllungszwang wie z.B. im Iran oder in Saudi-Arabien, weitreichende Unterbindung von Berufstätigkeit, von Bildung, von Freizeitgestaltung und sportlicher Betätigung, um nur einige wichtige Rechtsfelder zu nennen. Und den verbleibenden Rest an Rechten verschmutzen Hygienezwangsmaßnahmen.

Was jenseits davon einer gelenkten Demokratie als Variante des Überwachungsstaates entspricht, ist die flächendeckende Diskriminierung von Kritikern dieses Maßnahmenstaates, den Ernst Fraenkel im Hinblick auf den Nationalsozialismus vom Normenstaat

unterscheidet, in dem weiterhin das geltende Recht angewendet wird – man denke an das BGB –, während im Maßnahmenstaat Entscheidungen „nach Lage der Sache“ (Fraenkel 2001, S. 113) getroffen werden und damit geltendes Recht aufgehoben wird. Natürlich kann man eine Güterabwägung unternehmen zwischen den Folgen des Krankheitsgeschehens und denen des Ausnahmezustands. Diese nehme ich hier nicht vor, sondern betrachte primär, welche Folgen die Hospitalisierung für die Gesellschaft hat. Über dramatische Situationen in Kliniken wird ja ständig berichtet, wiewohl langsam, sehr langsam (Anfang Mai 2021) die Berichte über die Folgen der Hospitalisierung in den Medien zunehmen.

Zu diesen Folgen der Hospitalisierung gehört die Tatsache, dass man Kritiker des Ausnahmezustands in Deutschland zumeist dem rechtsradikalen Lager zuordnet. In China oder Russland werden Regimekritiker mit derselben Methodik als Terroristen verfolgt. Der Schritt dorthin ist ein kleiner: Wer sich fahrlässig oder vorsätzlich nicht vorschriftsmäßig verhält, gefährdet aus medizinischer Sicht andere, und das könnte man schon als eine Form des Terrorismus qualifizieren. Jede Kritik und jede Form des Widerstands soll im Keim erstickt werden. Man schreibt Demonstrationen gegen Maskenzwang und gegen Mindestabstand vor, dass die Demonstranten Masken tragen müssen, was das bei Demonstrationen übliche Skandieren von Parolen behindert. Und sie müssen den Zwangsmindestabstand einhalten, was auf Demonstrationen praktisch unmöglich ist. Mit diesem Argument wurden Demonstrationen reihenweise verboten. Die freie Meinungsäußerung als Grund- und Menschenrecht ist damit an einer für eine Demokratie entscheidenden Stelle aufgehoben.

3. Der digitalisierte medizinische Überwachungsstaat

Aber das primäre Problem des Überwachungsstaates sind die digitalen Möglichkeiten, die dieser heute hat, obgleich er sie noch nicht völlig nutzt, auch weil die Techniken teilweise noch nicht hinlänglich ausgereift sind. Bewegungsprofile indes liefern die Netzanbieter der Kommunikationsbranche längst an die daran interessierten Behörden, wiewohl nach eigenem Bekunden anonymisiert. Aber jederzeit könnte polizeilich für Leib und Leben Gefahr im Verzug geltend gemacht werden – also eine Variante polizeilich verfügter Ausnahme – und selbstredend wird sich kein Telefonanbieter dem staatsanwaltlichen Zugriff letztlich entziehen können. Ähnlich lässt sich der fleißig empfohlene bargeldlose Zahlungsverkehr zur Überwachung nutzen, wo und wie immer man das macht. Und plötzlich wird man eingesperrt, weil an einer Kasse ein Infektionsrisiko medizinisch rekonstruiert wird und offenbar nicht einmal die Virologen ihren eigenen Geräten zur Gesichtsabdeckung trauen.

Noch ist die Gesichtserkennung bei der Videoüberwachung nicht so weit ausgereift, und womöglich wird das auch durch die Gesichtsverhüllung behindert, was indes dazu führen wird, dass man sich auf die Identifikation der Augen konzentriert. Es nützt also nichts, sein Mobiltelefon zuhause zu lassen. Man könnte sich aber spiegelnde Sonnenbrillen aufsetzen, die dann sicherlich verboten werden, wahrscheinlich das Tragen von Sonnenbrillen an Orten mit Maskenzwang überhaupt. Wer in Deutschland einen Wohnsitz hat oder deutschen Behörden amtlich bekannt ist, kann dann fast wie mit einer Fußfessel überwacht werden. Wer sich außerhalb videoüberwachter Gebiete bewegen will, muss sein Mobiltelefon bei sich tragen, das auch vom Hubschrauber aus identifiziert werden kann. Fehlt dieses, dann wird die nächste Polizeistreife auf die entsprechende Person aufmerksam gemacht. Bewegungs-, Kontakt- und Aufenthaltsverbote lassen sich auf diese Weise zukünftig sehr gut, aber auch heute bereits in einem hohen Maße kontrollieren und mit staatlicher Gewalt wie hohen, existenzvernichtenden Geldstrafen durchsetzen. Also die digitalen Überwachungsmaßnahmen sind vielleicht noch nicht ausgereift. Aber der Weg zur wirklich totalen Überwachung dürfte nicht mehr allzu weit sein, was die totale Hospitalisierung der Gesellschaft dann flächendeckend durchsetzt. Und das Ganze mit medizinisch bestem Gewissen, man wolle ja nur Leben schützen.

Man denke auch an die bereits anwendbaren Methoden zur Gesundheitsüberwachung, die sich die um ihre Gesundheit sich ängstigende Bürgerin bisher freiwillig angedeihen lässt. Der postmarxistische und technologieeuphorische Kritiker des Kapitalismus Paul Mason macht daraus gar eine neue Humanität:

> „Die gesammelten Daten unseres Lebens – zu denen in naher Zukunft unsere Fahrgeschwindigkeit, unsere Ernährungsgewohnheiten, unser Body-Mass-Index und unsere Herzfrequenz zählen werden – könnten selbst eine sehr wirksame ‚soziale Technologie' sein." (Mason 2015, S. 343)

Diese Technologie wird sich aus einem Zusammenspiel von Digitalisierung, medizinischer Betreuung und polizeilicher Überwachung entwickeln, also eine Kooperation verschiedener primär technologischer Expertengruppen. So präsentiert sich gerade die Medizin als ein Bereich, in dem die Medizintechnik durch die Digitalisierung eine immer größere Bedeutung gewinnt, welche die sich perfektionierende Gesundheitskontrolle ermöglicht.

Wie sich zeigt, kann man sich dagegen auch auf keinen Rechtstaat verlassen: Nur in seltenen Fällen geben Gerichte Klägern gegen die Maßnahmen des Ausnahmezustands recht. Der Totalitarismus droht heute somit weniger von Seiten politischer oder religiöser Bewegungen als vielmehr durch eine medizinisch technologische Expertokratie, die sich als wissenschaftliche Macht auf eine Politik des epidemischen Ausnahmezustands als weltlichem Arm stützen kann, was sich mit der mittelalterlichen Zwei-Schwerter-Lehre vergleichen lässt, bei der das weltliche Schwert das geistliche realisierte gemäß der Struktur des Inquisitionsprozesses. Einen derartigen Vergleich zieht der politische Philosoph Michael Walzer 1983 in seinem Hauptwerk *Sphären der Gerechtigkeit*:

> „Zu Zeiten des Mittelalters sah es in Europa wie folgt aus: die Betreuung der Seelen, die Seelsorge, war eine öffentliche Angelegenheit, die der Körper hingegen Privatsache. Heute ist die Situation in den meisten europäischen Ländern umgekehrt; […]. In dem Maße, in dem wir das Vertrauen in die Heilung unserer Seelen verloren, ist unser Glaube, wenn es nicht bereits eine Obsession ist, an die Heilbarkeit unserer Körper gewachsen.“ (Walzer 1992, S. 138)

So formt der medizinisch technologische Komplex die Körper wie die Seelen, um sie so lenken zu können, dass die weltlich staatliche Macht als gerichtlich polizeilicher Komplex nur noch zum Ausführungsorgan der medizinisch technologischen Expertokratie depraviert – die Inquisition konnte von solcher Macht nur träumen. Eine gewisse Eigendynamik wird indes dem Justiz- und Polizeikomplex als sozialem Subsystem so lange erhalten bleiben, solange der staatliche Sicherheitsdiskurs und der medizinische Sicherheitsdiskurs noch unterschiedliche, miteinander inkommensurable Sprachen sprechen. Aber auch hier kann man Angleichungstendenzen beobachten. Die Polizei kontrolliert jede Bürgerin, die ob ihres Körpers für andere Körper als potentiell gefährlich gilt. Überhaupt hat die Hospitalisierung dazu geführt, dass jeder Mensch ein Gefährder ist.

Wenn Widerspruch dagegen diskriminiert wird, dann ist Politik definitiv nicht mehr der Ort des Widerstreits verschiedener Diskurse, wie sie von Jean-François Lyotard bestimmt wird, womit sich vor allem Demokratie umschreiben lässt. Politik ist vielmehr zum Ort geworden, wo sich die Hegemonie des medizinisch technologischen Diskurses durchsetzt und zwar unter Rückgriff auf die staatliche, ob des Ausnahmezustands gesetzlose Gewalt, mögen die Parlamente auch noch so viele Erlasse als Gesetze absegnen.

Damit könnte Lyotards Hoffnung an ihr Ende geraten, der 1983 noch primär den ökonomischen, nicht den medizinischen Diskurs als Bedrohung der Politik begreift: „Das einzige unüberwindliche Hindernis, auf das die Hegemonie des ökonomischen Diskurses stößt, liegt in der Heterogenität der Satz-Regelsysteme und Diskursarten, […].“ (Lyotard 1987, S. 299) Gelingt es dem medizinischen Diskurs andere Diskurse zweitrangig zu machen, was nach Lyotard rein sprachlich betrachtet unmöglich ist, was aber durchaus droht, weil die Masse der Zeitgenossinnen bereitwillig dem medizinischen Diskurs folgt? In der Politik wie unter den Bürgerinnen wird heute ein so digitalisiertes wie anglisiertes Medizinisch gesprochen, wird hier ein Sprachreinigungsprozess fortgeschrieben, wie ihn Jürgen Trabant als Vereinheitlichung und Fixierung der lebendigen Sprache in den modernen Wissenschaften bemerkt: „Das Ende der Sprache wird im Dienste der Wissenschaft nicht nur herbeigesehnt, sondern ernsthaft betrieben.“ (Trabant 2020, S. 210) Gerade in der Medizin findet eine intensive Sprachregulierung statt, die in die Gesellschaft hineinwirkt: Man muss die richtigen medizinischen Begriffe verwenden.

Jedenfalls gibt es jetzt eine Methode, die Konsens herstellt, genauer erzwingt, nämlich diese Hegemonie, indem dieser medizinische Diskurs alle anderen zum Schweigen bringt und dadurch jeden Widerstreit unterdrückt. Sicherlich haben sich Apel und Habermas

ihren Konsens im Stil des zwanglosen Zwangs „aus der Kraft des besseren Arguments“ (Habermas 1976, 73) anders vorgestellt. Aber genau das bildet sich der medizinisch technologische Diskurs ob seiner Wissenschaftlichkeit sogar ein, während die törichten bzw. unvernünftigen Zeitgenossen, welche die medizinisch gouvernementalen Maßnahmen nicht genau befolgen, die Gewaltanwendung gegen sich selber zuzuschreiben haben.

Das Schema dazu hat der konservative politische Philosoph Leo Strauss geliefert, der dem Bürger die Kompetenz abspricht, über seine Sicherheit selber zu urteilen:

> „Wenn aber jeder noch so törichte Mensch von Natur aus darüber richten kann, was für seine Selbsterhaltung notwendig ist, dann kann mit Recht alles als für die Selbsterhaltung unerlässlich angesehen werden: alles ist dann von Natur aus gerecht. Wir können dann von einem Naturrecht der Torheit sprechen.“ (Strauss 1977, S. 192)

Dann müssen sich die Bürgerinnen von den weisen Eliten der Mediziner lenken lassen, d.h. natürlich auch richtig sprechen lernen – geht Strauss in der Tat davon aus, dass es höhere, fähigere, gebildetere Menschen gibt, die keine Führung brauchen und unfähigere Menschen, die sie dringend nötig haben.

4. Das WWW als Informationsquelle und die klassischen Massenmedien

Auf der einen Seite herrscht ein unglaublich weit ins individuelle Leben reichender Ausnahmezustand. Auf der anderen Seite bemüht sich die Politik so zu tun, als herrsche Normalität, als wolle man vorführen, dass alles beim Alten geblieben sei und der politische Betrieb routiniert fortgesetzt wird, dass vor allem also die Demokratie erhalten sei, weil ihre Gremien und Institutionen weiterarbeiten, als gebe es gar keinen Maßnahmenstaat. Aber damit unterstreicht man nur Fraenkels Unterscheidung zum Normenstaat, der den Maßnahmenstaat ja nicht hindert.

Von den Befürwortern des Ausnahmezustands wird dabei auch auf die Presse verwiesen, die weiterhin frei und unabhängig geblieben ist. Und natürlich findet keine offizielle Zensur statt, herrscht anscheinend weiterhin Meinungsfreiheit. Erstaunlich ist freilich, dass nicht nur fast alle demokratischen Parteien im Berliner Bundestag, sondern auch die meisten nichtstaatlichen Medienanstalten die Politik des Maßnahmenstaates unterstützen.

Bei den mehr oder weniger staatlichen, also in der Bundesrepublik öffentlich-rechtlichen Rundfunkanstalten kann man sowieso eine aktive Begleitung der Politik des Ausnahmezustands beobachten, die nicht verwundern sollte. Um nur auf ein bayerisches Beispiel zu verweisen: nicht nur, dass seit der Debatte über die Flüchtlingspolitik seit 2015 der Nachrichtenkanal des Bayerischen Rundfunks ständig verkünden muss, dass er ‚aus Bayern und für Bayern‘ sendet. Das Musikprogramm für junge Leute, nämlich Bayern3,

bezeichnet sich seit 2020 als ‚das wir zusammen Radio', das ihren jüngeren Hörern fleißig erklärt, dass sie genauso bedroht von der Krankheit seien wie Ältere und wie man mit dem Ausnahmezustand zurechtkommt und dass man das fleißig zusammen bewältigen müsse. Und in den Nachrichtensendungen des Bayerischen Rundfunks wird ständig das Adjektiv „hochansteckend" wiederholt, wenn der populäre Name der Krankheit fällt.

Man kann also von einer zumindest freiwilligen Gleichschaltung der Medienanstalten sprechen – wobei die ‚Freiwilligkeit' an der Sache selbst nichts ändert; denn es gibt praktisch keine neutralen, geschweige denn kritischen Medien mehr, so dass es in der Tat schwerfällt, sich unabhängig vom hegemonialen Diskurs zu informieren, der schließlich auch die internationale Politik kontaminiert, so dass selbst die Berichterstattung über Angelegenheiten jenseits des herrschenden Ausnahmezustand in ein fragwürdiges Licht getaucht wird. Fast erübrigt es sich, darauf hinzuweisen, dass diese Sachlage den Produzenten von Fake News massiv in die Hände spielt, hat sich bei einem Teil der Bevölkerung doch das Gefühl ausgebreitet, man würde von den herrschenden Medien nur belogen.

Nicht allein deshalb muss diese Sachlage verwundern, weil es einerseits demokratische Aufgabe der Presse und der Medien ist, die Politik kritisch zu begleiten – werden die Medien auch immer wieder als vierte Gewalt neben Legislative, Exekutive und Judikative bezeichnet. Andererseits gibt es zwar immer regierungsnahe Medien, aber eben auch regierungsferne, die sich ansonsten mit kritischen Kommentaren nicht unbedingt vornehm zurückhalten. Just die Medienanstalten versagen im Ausnahmezustand offenbar bzw. kommen dieser Rolle als kritische Institution einfach nicht nach.

Die Welt aus dem Axel Springer Verlag – nicht gerade als Flaggschiff kritischer Berichterstattung berühmt – bietet ein kostenpflichtiges Online Angebot, das die einen oder anderen kritischen Stellungnahmen zum gegenwärtigen Ausnahmezustand publiziert. Nicht nur weil die meisten Zeitgenossinnen im Internet nur kostenlose Angebote goutieren, erscheint dieses Angebot als Nischenprodukt, wenn nicht gar als Feigenblatt, das aber andere große Medienanstalten offenbar gar nicht für nötig halten. *Die Welt* – als konservativ bekannt – könnte damit vielleicht auch im rechten Lager um Kundschaft buhlen, in dem man jeglicher Regierungspolitik feindlich gesonnen ist, freilich bestimmt nicht dem Ausnahmezustand, mit dem die Rechte immer schon gerne Politik machte. So darf man fragen, ob die Hospitalisierung am Ende einer auch biopolitisch orientierten Rechten nicht nutzen könnte.

Warum aber bleibt die Kritik aus? Weil es um ein medizinisches Problem geht, das nur die Experten verstehen, wie man offiziös gerne beteuert? Nein, dazu sollte es genügend Wissenschaftsjournalisten geben, die sich in der Medizin auskennen und zur Not auch schnell nachlernen können, um nicht nur die Maßnahmen zu hinterfragen, die die Politik umsetzt, sondern auch die wissenschaftlichen Theorien, Hypothesen und Informationen, auf denen diese Maßnahmen beruhen. Sie wären bestimmt auch dazu in der Lage, selbst etwas komplizierte Sachverhalte dem Publikum zu erklären und sehr viele könnten das

auch verstehen, nicht zuletzt weil das Thema Medizin im Allgemeinen und Grippe im Besonderen sehr populär ist, wird dem Thema Gesundheit in praktisch allen Medien – nicht bloß in den speziellen wie der Apothekenrundschau – breiter Raum eingeräumt.

Dasselbe gilt auch für juristisch gebildete Journalisten, die jederzeit die erlassenen Maßnahmen daraufhin kritisieren können, ob sie dem Grundgesetz widersprechen, ob sie die Menschenrechte beachten, ob sie in einer Abwägung der betroffenen Rechtsgüter angemessen erscheinen, also letztlich, welche Risiken eher zu vermeiden sind und welche man durchaus eingehen sollte. Man liefert den Bürgerinnen von medialer Seite kaum kritische Informationen, die eine kritische Haltung gegenüber dem Ausnahmezustand befördern.

Fast möchte man darauf reagieren, wie das im Zeitalter der Digitalisierung ein Problem sein kann. Wenn die klassischen Massenmedien versagen, können sich die Bürgerinnen doch im WWW selber informieren. Dem kann man freilich entgegenhalten, dass hier für viele der Aufwand doch gemeinhin höher ist als in den gewohnten Massenmedien. Aber in einem Ausnahmezustand, der praktisch das Leben aller Bürgerinnen massiv beeinträchtigt, wäre es doch nicht zu viel verlangt, dass sich dann die Bürgerinnen darum eben intensiver kümmern müssten.

Doch daraus ergibt sich eine sehr kuriose Sachlage. Zwar kursieren im WWW diverse, durchaus auch seriöse Informationen. Doch angesichts der Flut von Fake News sind diese häufig nur schwer als solche zu erkennen. Man kann sich ja gerade nicht auf die Internetseite des Robert-Koch-Instituts oder des italienischen Gesundheitsministeriums in Rom stützen, wenn man Medizin und Politik der Hospitalisierung unter eine kritische Lupe nehmen will.

Um die Seriosität von WWW-Quellen beurteilen zu können, fehlt umso mehr die kritische Information aus bekannten seriösen Quellen in den gängigen Massenmedien, auf die man sich bisher verlassen konnte. Und umgekehrt, wenn diese Quellen fehlen, lässt sich derart auch jede seriöse Information im WWW desavouieren. Auf diese Weise – ob vorsätzlich oder fahrlässig – werden die Bürgerinnen in einem Zustand der Desinformation gehalten, die sie umso abhängiger macht von der Politik des Ausnahmezustands, von der sie sich blind und unmündig lenken lassen müssen. Aber da steht man doch in einer guten Tradition. Denn wie bemerkt bereits Platon in Bezug auf sein Züchtungsprojekt: „Es scheint, dass unsere Herrscher allerlei Täuschungen und Betrug werden anwenden müssen zum Nutzen der Beherrschten.“ (Platon 1958, 459 c, S. 181) So stellen sich das Mediziner und Politiker auch vor, dürfen dies aber natürlich nie zugeben.

5. Entmündigung durch Unfähigkeit zur Kritik

Das hat natürlich weitreichende Folgen. Denn damit befinden sich die Zeitgenossinnen gegenüber der aktuellen Politik insgesamt in einer Lage, in der sie auch diese nicht mehr kritisch beurteilen können, da diese de facto unter Bedingungen des Ausnahmezustands stattfindet, so dass der Umgang mit anderen Problemen als dem bekannten Krankheitsgeschehen immer unter diesem Vorbehalt desselben wie des Ausnahmezustands steht. Das zeigt sich beispielsweise in der sozial besonders wichtigen Finanzpolitik, in der plötzlich Schuldenberge aufgehäuft werden dürfen – sogar der Europäischen Union wird jetzt erlaubt, Kredite aufzunehmen –, die die Finanz- und Eurokrise weit in den Schatten stellen. Wie will man als Bürgerin gegenüber einer solchen Alltagspolitik noch eine kritische Haltung einnehmen, wenn diese just von einer Sachlage abhängig ist, die kritisch zu reflektieren die notwendigen Informationen oder das dazu notwendige Hintergrundwissen fehlt?

Denn nicht nur die Wirtschafts- und Finanzpolitik, alle politischen Aktivitäten jenseits der medizinisch gelenkten Politik des Ausnahmezustands stehen unter dem Vorbehalt, wie sich einerseits der Ausnahmezustand weiter entwickeln wird und andererseits, wie weit die durch den Ausnahmezustand verursachten ökonomischen und existentiellen Schäden behoben oder kompensiert werden können. Fast im Predigtton und unter aufgesetztem Optimismus verheißen Wirtschaftspolitiker den kommenden Aufschwung nach dem Ende des Ausnahmezustands, der sogar nach offiziellem Bekunden die größte Wirtschaftskrise seit 1929 verursacht hat. Schließlich ist hier die weitere Entwicklung trotz Impfgeschehen keineswegs vorhersehbar.

Wie viele ökonomische Existenzen vernichtet wurden und noch werden, darüber wird eilig hinweggegangen mit der Verheißung von staatlichen Entschädigungen. Wenn sich die Staaten aber finanziell übernommen haben sollten – was sich kaum anders wird bezeichnen lassen –, dann werden solche Versprechungen schwerlich eingehalten, abgesehen von einer kommenden Sparpolitik, die just jene Bereiche treffen wird, die unter dem Ausnahmezustand bereits am meisten leiden, nämlich die der Kultur, der Bildung, der Gastronomie etc. Bürgerinnen werden weitgehend blind einer solchen Politik zustimmen müssen, noch dazu, wenn sie selbst darunter massiv leiden, also nur auf Hilfen und Wirtschaftsaufschwünge hoffen können.

So profitiert am Ausnahmezustand auch die offizielle Politik, die sich großer Zustimmung erfreuen durfte. Dass die Politik des Ausnahmezustands 2020 in der BRD eine Zustimmungsrate von bis zu 80% genoss, mag deren Protagonisten erfreut und beruhigt haben. Leider spricht diese Rate für keine demokratischen Umstände. Denn derart hohe Zustimmungsraten gibt es nur in gelenkten Demokratien oder in Diktaturen. In Demokratien mit einer kritischen öffentlichen Meinung herrschen immer Dissense, Differenzen und Meinungsstreitereien. Wenn diese ausbleiben, kann es schwerlich mit

rechten Dingen zugehen. Vielmehr fehlt eben die kritische Information und Diskussion, die Demokratie ausmacht und ohne die Demokratie aufgehoben ist.

Und offenbar konnte das WWW diesen Mangel nicht ausgleichen, was eigentlich für die klassischen Medien spricht. Wenn seriöse Information fehlt, dann kann diese durch die Eigeninitiative der Betroffenen nicht ersetzt werden, weil sich zu viele unseriöse Informationen dazwischen tummeln und häufig nicht mit Sicherheit entschieden werden kann, wie seriös eine Quelle ist. Dann kann man sich auf eine solche Information auch nicht stützen.

Dabei handelt es sich ja bei der Medizin wie dem WWW mitnichten um private Angelegenheiten, was man ja auch nicht mal von der Religion sagen kann, sondern um öffentliche. Was aber die Religion von der Medizin wie den Naturwissenschaften unterscheidet, ist, dass die Religion von Autoritäten bestimmt wird, denen die Gläubigen folgen, was sich von fundamentalistischen politischen Ideologien gar nicht so sehr unterscheidet. Religiöser wie auch ideologischer Fundamentalismus verbreitet sich im WWW daher leicht unter den Anhängern und vermag auch erfolgreich zu missionieren. Was wahr und was falsch ist, was seriös ist, das ist klar geregelt. Eine kritische Hinterfragung der Glaubensgehalte gehört natürlich nicht zu einem Fundamentalismus.

Das ist in den Wissenschaften anders, besonders in der Medizin, mit der sich alle irgendwie beschäftigen müssen, weil jeder mal krank ist oder kranke Freunde hat. Sehr viele verfügen durchaus über ein differenziertes Verständnis von Krankheit und sammeln darüber auch viele Informationen. Dazu hat das WWW massiv beigetragen, aber natürlich auch die Massenmedien, die sich gerne mit medizinischen Themen befassen, weil diese beim Publikum zumeist auf großes Interesse stoßen.

Weil fast jeder noch dazu bei Erkältungskrankheiten über eigene Erfahrungen und einen eigenen, zumeist durchaus reflektierten Umgang mit gerade diesen Krankheiten verfügt, durfte das aktuelle Krankheitsgeschehen nicht unter dem bekannten Namen Grippe oder dem weniger bekannten Influenza publik gemacht werden. Indem es von allen offiziellen Stellen medizinischer oder politischer Art als etwas Neues und Unbekanntes qualifiziert wurde, nahm man den Bürgerinnen praktisch jede eigene Kompetenz ab und machte sie zu Unmündigen, die den Anweisungen der Mediziner und den Erlassen der Politik folgen müssen, ohne diese prüfen zu können oder gar zu dürfen.

Hätten die Medien über das jeweils aktuelle Krankheitsgeschehen, die offiziellen medizinischen Interpretationen und die politischen Maßnahmen seriöse, d.h. kritische Informationen und einen Meinungsstreit geliefert, hätten sich die Bürgerinnen selber eigene Bilder vom Geschehen machen können und hätten über ihre Reaktionen selber entscheiden können. Viele Bürgerinnen hätten sich den Maßnahmen des Ausnahmezustands nicht einfach gebeugt. Viele hätten eine kritische Haltung eingenommen, eigene Umgangsformen mit der Krankheit entwickelt, wie sie es ja immer gewöhnt sind. Dann wäre eine autoritäre Lenkung durch die Medizin erheblich schwieriger geworden, wenn sie

nicht gänzlich gescheitert wäre. Womöglich wären dann massive polizeiliche Gewaltmaßnahmen erforderlich gewesen, um mit dem Ausnahmezustand die medizinisch gewünschten Effekte zu erzielen.

6. Die Politik der Furcht

Um es so weit nicht kommen zu lassen, hat man obendrein auf ein weit verbreitetes probates Mittel zurückgegriffen, nämlich auf die Politik der Angsterzeugung, die eine lange Geschichte hat. Sie beginnt mit der *Offenbarung des Johannes*, dem letzten Buch der Bibel, das einen totalen Weltuntergang ankündigt, während im jüdischen Denken der erwartete Messias die Welt nur wieder in Ordnung bringen soll. Im römischen Denken wie in asiatischen Weltbildern spielt der Weltuntergang keine Rolle, im Islam nur eine untergeordnete. Bis etwa 1500 lebte das Christentum unter der Drohung des Weltuntergangs, was für den Einzelnen bedeutete, dass dann niemand mehr für ihn beten, für ihn ein gutes Wort einlegen könnte, so dass er immer schon so leben muss, dass ihn das Jüngste Gericht nicht aburteilt.

Seit 1500 verblasste indes dieses apokalyptische Denken im Christentum. Doch es wurde mit der Entstehung der modernen Wissenschaften von diesen übernommen, drohen die Wissenschaften seither immer wieder mit diversen größeren oder kleineren Untergängen, mit denen sie entweder schlicht Aufmerksamkeit erheischen, Forschungsgelder einsammeln oder das Leben der Menschen beeinflussen wollen. So konstatiert Johannes Fried:

> „Astronomen, Physiker, Biologen oder Chemiker erweisen sich als Kinder ihrer Zeit und sind der Herkunft ihrer Kultur verpflichtet, ständig auf der Suche nach Anfängen und Untergängen, und nun immer häufiger nach neuen Erden für den bevorstehenden Untergang der alten, vertrauten.“ (Fried 2016, S. 251)

Natürlich werden davon gerade auch die Massenmedien beseelt, wobei man ihnen unterstellen darf, dass es ihnen dabei primär darum geht, ihren Umsatz zu erhöhen. Mit Szenarien eines Weltendes erregt man die Aufmerksamkeit der verängstigten Zeitgenossinnen. Dasselbe gilt für die Literatur, die Musik, den Film oder Videospiele wie auch für diverse Zirkel und Seiten im Internet.

In der Politik hat das apokalyptische Denken eine eigene Ausformung erhalten, und zwar um 1500 durch den wichtigsten Vordenker des modernen Staates Niccolò Machiavelli, der zusammen mit seinem Zeitgenossen Leonardo da Vinci wesentlich zum Übergang der Apokalypse in ein säkulares Denken beiträgt. Machiavelli empfiehlt nämlich dem Fürsten, sich nicht auf die freiwillige Zustimmung seiner Untertanen zu verlassen. Aber der Fürst kann mit seiner Macht nach eigenem Gutdünken unter diesen Furcht erzeugen, mit der er sie dann lenken kann. So schreibt Machiavelli den Fürsten und allen ihren Nachfolgern ins

Stammbuch: „Da die Liebe zu den Menschen von ihrer Willkür und die Furcht von dem Betragen des Fürsten abhängt, darf ein kluger Fürst sich nur auf das, was in seiner Macht und nicht in der der andern steht, verlassen." (Machiavelli 1980, 70)

Die Politik des Ausnahmezustands arbeitet besonders intensiv mit diesem Mittel. Man hält kritische Informationen zurück, so dass die Bürger sich nicht selber informieren können. Man erklärt die Krankheit als besonders gefährlich, erzeugt also Furcht. Beides zusammen entmündigt die Bürgerinnen und macht sie zu braven Gefolgsleuten jener, die anscheinend als Einzige ein sicheres Wissen haben. Wer den Erleuchteten nicht grundsätzlich vertraut, wird von seiner Furcht motiviert, diesen Eliten trotzdem zu gehorchen.

Die Bürgerinnen durch Furcht zu entmündigen, sie zu willigen Untertanen zu machen, das ist Machiavellismus, den solche Machiavellisten tunlichst verschweigen und verstecken, und Machiavellismus umdeuten: So liegt der Machiavellismus für Leo Strauss „im machiavellischen Prinzip, dass der gute Zweck jedes Mittel rechtfertigt". (Strauss 1984, S. 13). Man soll ja nach Strauss der Bevölkerung gefährliche Wahrheiten verschweigen, die deren Vertrauen in die Regierung schwächen könnten.

Auch Thomas Hobbes, der Vordenker von Absolutismus und Liberalismus, stützt im 17. Jahrhundert die Politik seines *Leviathan* nicht nur auf die Furcht der Bürger. „Die Leidenschaften, die den Menschen friedfertig machen, sind Todesfurcht, das Verlagen nach Dingen, die zu einem angenehmen Leben notwendig sind und die Hoffnung, sie durch Fleiß erlangen zu können." (Hobbes 1984, S. 98) Damit arbeiten die chinesische Regierung wie die Paten des Maßnahmenstaates: Unterwerfung aus Angst vor Gewalt und Krankheit sowie Hoffnung auf ökonomische Entwicklung und auf ein Ende der Gefahr.

Leider hat Hobbes den Herrschenden auch verraten, wodurch ihre Position gefährdet wird, so dass sie ihrerseits alles unternehmen, dem vorzubeugen. Denn Hobbes schreibt:

> „Die Verpflichtung des Untertanen gegen den Souverän dauert nur so lange, wie er sie auf Grund seiner Macht schützen kann, und nicht länger. Denn das natürliche Recht der Menschen, sich selbst zu schützen, wenn niemand anderes dazu in der Lage ist, kann durch keinen Vertrag aufgegeben werden." (Hobbes 1984, S. 171)

Ob sich jemand sicher fühlt, kann man ihm aber von außen nicht eingeben. Darin liegt immer ein möglicher Kündigungsgrund des Gesellschaftsvertrages und das Individuum fängt an, sich selber zu schützen. Ein solches Sicherheitsbedürfnis ist längst von der körperlichen Unversehrtheit durch staatliche oder private Gewalt in die Gesundheit übergelaufen. Wenn man den staatlichen Lebensmittelkontrollen kein Vertrauen mehr entgegenbringt, sucht man nach vertrauenswürdigeren Versorgungsquellen. Wenn man der Medizin misstraut, sucht man sein Heil in der Alternativmedizin oder in der Esoterik.

Als der Souverän den Ausnahmezustand ausrief – in Deutschland die Bundesländer, die für den Katastrophenfall zuständig waren – sah man sich genau mit diesem Problem

konfrontiert. Wenn man einen erfolgreichen Umgang mit Krankheiten pflegt, wird man sich von niemandem dabei reinreden lassen. Man schützt sich selbst.

Wenn es sich aber um eine neue unbekannte gefährliche Krankheit handelt, die man nicht kennt, muss man aus Angst und Unkenntnis gehorchen, sich also vom Ausnahmezustand schützen lassen, d.h. sich diesem unterwerfen. Das WWW hilft ja auch nicht weiter, weil die seriösen Massenmedien keine kritischen Informationen mehr liefern. Im anderen Fall hätte diese Politik der Furcht nicht so flächendeckend wirken können.

Das Versagen liegt damit primär bei der Presse bzw. den Medien, die das machiavellistische Spiel der Politik und der Medizin unterstützt haben, was auch dazu führte, dass abweichende medizinische Auffassungen in der Öffentlichkeit nicht die notwendige Repräsentation fanden. Denn natürlich ist die Medizin kein einfacher monolithischer Block, was eine der Hoffnungen beseelt, dass sich die Entmündigung der Bürgerinnen durch medizinische Experten unterlaufen lässt. Das ist auch eine Chance für die Politik, nicht weiterhin bloß zum weltlichen Schwert des wissenschaftlichen Geistes zu verkommen.

7. Mündigkeit oder nacktes Leben

Zudem gehört der Machiavellismus zur alltäglichen medizinischen Praxis: Man lenkt die Zeitgenossin, indem man ihr die schlimmsten möglichen Konsequenzen ausmalt, bis sie schließlich in die vom Arzt gewünschte Therapie einwilligt, wie existentiell belastend diese auch sein mag. Hier hatte das WWW eine Weile durchaus eine emanzipatorische Wirkung, indem man sich besser über Krankheiten informieren konnte als vor dem WWW. Und das ließ sich auch mit seriösen Informationen abgleichen, was vielen Medizinern und Gesundheitspolitikern schon lange ein Dorn im Auge ist: Daher die ständigen Beschimpfungen und Verfolgungen alternativer Heilpraktiken, über die man sich vor dem WWW gar nicht so leicht informieren konnte.

Der Hang zur Information, sei es im WWW oder durch die klassischen Medien wie auch die Neigungen zur Alternativmedizin, demonstrieren, dass viele Bürgerinnen ihre Abhängigkeit vom Medizinsystem gerne reduzieren würden, dass sie sich dabei eben um Mündigkeit bemühen, was trotzdem ein schwieriges Unterfangen bleibt. Denn das, was Ivan Illich 1975 schreibt, hat sich bis heute massiv verstärkt:

> „Lebenslange ärztliche Beaufsichtigung […] macht das Leben zu einer ununterbrochenen Folge gefährlicher Altersstufen, von denen jede ihre eigene Form der Bevormundung braucht. Von der Wiege bis ins Büro, vom Ferienlager des Club Méditerranée bis ins Leichenschauhaus wird jede Alterskohorte durch ein Milieu konditioniert, das definiert, was für die einzelnen Altersgruppen als Gesundheit zu gelten hat. […] Für Arme wie

> Reiche wird das Leben zu einer Pilgerfahrt, deren Kreuzwegstationen – Sprechzimmer und Wartezimmer – zurück zum Ausgangspunkt führen: in die Krankenstation.“ (Illich 1981, S. 95)

Die globale Macht der Medizin hat sich seit 2020 zudem auch ökonomisch verstärkt. Während die Weltwirtschaft eine ihrer größten Krisen erlebt – die sich der Politik der Hospitalisierung verdankt – geht es Konzernen blendend, die am Gesundheitswesen beteiligt sind, von diesem selbst ganz zu schweigen, dem jedenfalls bestimmt nicht nur in Deutschland eminente finanzielle Verbesserungen gewährt werden. Nicht nur also, dass sich der politische Einfluss des gesamten Gesundheitswesen durch den von diesem gelenkten Ausnahmezustand unendlich gesteigert hat, auch die ökonomische Macht der daran beteiligten Akteure hat sich massiv verbreitert, so dass nicht nur Konflikte zwischen verschiedenen Wirtschaftsbereichen absehbar sind – das wäre das geringste Übel –, vielmehr dürfte sich die medizinische Lenkung der Bürgerinnen und die Hospitalisierung der Gesellschaft dadurch noch massiv intensivieren – und zwar selbst dann noch, wenn das aktuelle Krankheitsgeschehen medial, politisch und medizinisch in den Hintergrund des allgemeinen Interesses treten sollte.

Mit dem medizinisch begründeten Ausnahmezustand hat sich auch gezeigt, dass Medizin und Demokratie, Medizin und Menschenrechte, sowie Medizin und individuelle Mündigkeit, also Medizin und Freiheit miteinander in einem massiven Konflikt liegen. Wie dekretiert Hannah Arendt: „Der Sinn von Politik ist Freiheit, und ohne sie wäre das politische Leben sinnlos.“ (Arendt 2000, S. 231) Oder um es etwas holzschnittartig zu sagen: Früher hat man sein Leben für die Freiheit geopfert; heute opfert man die Freiheit dem nackten Leben.

Bereits 1995 weist Giorgio Agamben darauf hin, dass sich die Biopolitik zunehmend am nackten Leben orientiert. „Nicht der freie Mensch mit seinen Eigenschaften und seinen Statuten, und nicht einmal schlicht homo, sondern corpus ist das neue Subjekt der Politik “ (Agamben 2015, S. 132) Im Zuge der Medizinisierung und speziell im Ausnahmezustand der Hospitalisierung werden Menschen auf gefährliche Körper reduziert, die daher total kontrolliert und gelenkt werden müssen, was nur funktioniert, wenn das Denken ausgeschaltet wird.

Die Medizin präsentiert sich in jeder Hinsicht als autoritäres hierarchisches System, das sich unter Hinweis auf ihre sozial wie individuell lebenserhaltende Funktion hegemonial ins Sicherheitsdispositiv einschreibt und damit absolutistisch ähnlich wie Hobbes argumentiert: um der Lebenssicherung willen sollen die Bürgerinnen widerspruchslos den Weisungen der weisen, wissenden medizinischen Experten folgen. Die mündige ‚Patientin‘, die die Medizin als ein Dienstleistungsangebot versteht und die nur solche Angebote annimmt, die sie selbst geprüft hat und die ihr taugen, wird von nicht allzu vielen Medizinern geschätzt, geschweige denn von den Gesundheitspolitikern.

Doch während Hobbes noch die individuelle Widerstandskraft anerkannte, unterläuft die Medizin die individuelle Mündigkeit durch eine umfassende Hospitalisierung, die sich auf digitale Technologien stützt und machiavellistisch durch Furchterzeugung Gehorsam schafft. Die Medizin spricht ja von Menschen nur als ‚Patienten', die primär aus Körpern bestehen, denen Seelen zugeordnet werden, für die man auch ständig neue Krankheiten und Steuerungsmechanismen entwickelt.

So hadert die Medizin weniger mit der Demokratie als mit den Menschenrechten. Denn Demokratie besteht nicht nur darin, dass sich Parlamente aus verschiedenen politischen Parteien zusammensetzen, die durch reguläre Wahlen in diese Parlamente gelangt sind. Wider das berühmt gewordene Wort von Viktor Orbán muss Demokratie liberal sein, d.h. sie muss vor allem Menschen- und Minderheitenrechte achten, aber auch die Freiheit der Informationsmedien, der Forschung, Lehre, der Bildung wie der Kultur, darf gerade auch letzterer weder durch einen Ausnahmezustand noch durch eine restriktive Politik die Luft zum Atmen genommen werden. Letzteres praktizieren in der EU vor allem Ungarn und Polen, Ersteres findet sich flächendeckend überall.

Wieweit sich die Bürgerin gegen diese Hospitalisierung zur Wehr setzen wird, ist momentan mehr als ungewiss. Viel zu viele wünschen sich eine umfassende Versorgung und Betreuung. Und auf der technologischen Ebene fördert die Digitalisierung eine solche Abhängigkeit, während sie auf der informationellen unter Bedingung des Ausnahmezustands dieser Entwicklung gerade nicht widerstreitet. Behält der Prophet der Digitalisierung Marshall McLuhan dann recht, wenn er 1964 schreibt: „Die Besitzer von Medien sind immer bemüht, dem Publikum das zu geben, was es will, denn sie spüren, dass ihre Macht im *Medium* liegt und nicht in der *Botschaft* oder dem Programm." (McLuhan 1992, S. 251) Hat die Bürgerin 2020/21 doch einfach bekommen, was sie wollte? Dann darf man sich auf eine fortschreitende Hospitalisierung einstellen, auch nach Corona.

Literatur

Agamben, Giorgio (2015): *Homo sacer – Die souveräne Macht und das nackte Leben* (1995). 10. Aufl. Frankfurt/M.: Suhrkamp.

Arendt, Hannah (2000): Revolution und Freiheit (1962). In: dies.: *Zwischen Vergangenheit und Zukunft – Übungen im politischen Denken I* (1968). 2. Aufl. München: Piper, S. 227–251.

Campanella, Tommaso (1960): Der Sonnenstaat (1602). In: Heinisch, Klaus (Hrsg.): *Der utopische Staat*. Reinbek bei Hamburg: Rowohlt, S. 111–170.

Foucault, Michel (2005): *Die Geburt der Klinik – Eine Archäologie des ärztlichen Blicks* (1963). 7. Aufl. Frankfurt/M.: S. Fischer.

Fraenkel, Ernst (2001): *Der Doppelstaat* (1936–38, 1941). Hamburg: Europäische Verlagsanstalt.

Fried, Johannes (2016): *Dies Irae – Eine Geschichte des Weltuntergangs*. München: C.H Beck.

Habermas, Jürgen (1976): *Strukturwandel der Öffentlichkeit – Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft* (1962), 8. Aufl., Neuwied, Berlin: Luchterhand.

Hobbes, Thomas (1984): *Leviathan oder Stoff, Form und Gewalt eines kirchlichen und bürgerlichen Staates* (1651). Frankfurt/M.: Suhrkamp.

Illich, Ivan (1981): *Die Nemesis der Medizin – Von den Grenzen des Gesundheitswesens* (1975). Reinbek: Rowohlt.

Lyotard, Jean-François (1987): *Der Widerstreit* (1983). München: Wilhelm Fink.

Machiavelli, Niccolò (1980): *Der Fürst* (1532). Wiesbaden: VMA Verlag.

Mason, Paul (2016): *Postkapitalismus – Grundrisse einer kommenden Ökonomie*. Berlin: Suhrkamp

McLuhan, Marshall (1992), *Die magischen Kanäle – „Understanding Media"* (1964). Düsseldorf u.a.O.: Econ.

Platon (1958): *Politeia*. Übers. v. Friedrich Schleiermacher. Werke Bd. 3, Hamburg: Rowohlt.

Schmitt, Carl (2004): *Politische Theologie – Vier Kapitel zur Lehre von der Souveränität* (1922). 8. Aufl. Berlin: Duncker & Humblot.

Strauss, Leo (1977): *Naturrecht und Geschichte* (1953). Frankfurt/M.: Suhrkamp

Strauss, Leo (1984): *Thoughts on Machiavelli* (1958). Chicago, London: University of Chicago Press.

Trabant, Jürgen (2020): *Sprachdämmerung – Eine Verteidigung*. München: C.H. Beck

Walzer, Michael (1998): *Sphären der Gerechtigkeit – Ein Plädoyer für Pluralität und Gleichheit* (1983). Frankfurt/M.: S. Fischer.

Das digitale Panopticon – Wie die NSA-Überwachung unser Verhalten verändert

Elsa-Margareta Venzmer

Zusammenfassung

Als die Überwachungspraktiken der NSA durch den Whistleblower Edward Snowden im Jahr 2013 öffentlich gemacht wurden, rechtfertigte sich die US-amerikanischen Politik damit, dass das massenhafte Sammeln von Daten zur Terrorbekämpfung diene. Aus den Snowden-Dokumenten geht allerdings hervor, dass die Daten von der US-Regierung vielmehr für politische und gesellschaftliche Zwecke genutzt werden. Daten können etwa dafür verwendet werden, um das Verhalten von Menschen vorherzusagen oder zu kontrollieren. So kommen Studien zu dem Ergebnis, dass durch das Gefühl des Beobachtetwerdens Internetnutzer ihr Kommunikationsverhalten verändern und ihre Grundrechte, wie Informations- und Meinungsfreiheit einschränken. Diese und andere Gefahren von Überwachung zu untersuchen sowie Lösungen anzubieten, wie man sich vor Datenspionage schützen kann, dem widmet sich der vorliegende Beitrag. Als theoretischer Rahmen soll hierfür Michel Foucaults Theorie des Panoptismus dienen.

1. Der Panoptismus

> „Der perfekte Disziplinarapparat wäre derjenige, der es einem einzigen Blick ermöglichte, dauernd alles zu sehen. Ein zentraler Punkt wäre zugleich die Lichtquelle, die alle Dinge erhellt, und der Konvergenzpunkt für alles, was gewußt werden muß: ein vollkommenes Auge der Mitte, dem nichts entginge.“ (Foucault 1989, S. 224)

Wie Michel Foucault schon 1976 in seinem Werk *Überwachen und Strafen: Die Geburt des Gefängnisses* feststellte, soll es in unserer modernen Gesellschaft einen Machtmechanismus geben, dessen Ziel es sei, jedes Individuum zu überwachen und sein Verhalten zu kontrollieren, um es letztendlich zu verbessern (vgl. Ruoff 2009, S. 102). Um diese sogenannte Disziplinarmacht zu erläutern, greift er auf Jeremy Benthams Konzept des Panopticons zurück (vgl. Foucault 1989, S. 256-257), nach dem sich Menschen selbst disziplinieren, indem ihnen das Gefühl vermittelt wird, dass ihr Verhalten zu jeder Zeit beobachtet werden könnte (vgl. ebd., S. 258 ff.). Das Panopticon war zunächst als ein Gebäude, genauer gesagt, als ein Gefängnis konzipiert. Es handelt sich dabei um einen ringförmigen Bau, in dessen Mitte ein von außen uneinsehbarer Turm steht. Das Ringgebäude besteht dabei aus Zellen, in denen jeweils ein Individuum untergebracht werden kann wie z.B. ein Schüler oder ein Sträfling. Dieses Individuum ist alleine, ein

Kontakt zu dem Zellennachbarn ist durch die architektonische Besonderheit ausgeschlossen. Es könnte vom Turm aus von einem Wächter ständig beobachtet werden. Da der Zellenbewohner aber nicht in den Turm hineinsehen kann, kann er letztendlich nie wissen, ob er gerade beobachtet wird oder nicht (vgl. ebd., S. 256 ff.).

Das sei letztendlich die Hauptwirkung des Panopticons: „[D]ie Schaffung eines bewußten und permanenten Sichtbarkeitszustandes beim Gefangenen, der das automatische Funktionieren der Macht sicherstellt." (ebd., S. 258) Es gebe also eine Macht, die für sich alleine wirksam ist und von niemandem tatsächlich ausgeübt wird. Dabei sei das Gefühl des Überwachtwerdens permanent, auch wenn die Durchführung tatsächlich nur sporadisch geschehe. Es sei nur von Bedeutung, dass die Macht sichtbar bzw. spürbar ist, aber gleichzeitig uneinsehbar bzw. unsichtbar bleibe (vgl. ebd., S. 258).

Foucault betont, dass das Panopticon nicht immer ein Gebäude sein müsse, sondern es sei ein verallgemeinerungsfähiges Funktionsmodell, das generell Machtbeziehungen im Alltag beschreibe (vgl. ebd., S. 263). Nach Foucault sei es Benthams Ziel gewesen, zu beschreiben, wie man Disziplinen im gesamten Gesellschaftskörper zum Einsatz bringen könne, so dass dieser lückenlos überwacht werden kann. Er konstatiert, dass sich dieser Vorgang im Laufe des 17. und 18. Jahrhunderts schon vollzogen habe: die Disziplinargesellschaft wurde geboren (vgl. ebd., S. 268-269) und es gebe sie auch heute noch (vgl. ebd., S. 285).

Foucault geht davon aus, dass die Voraussetzung für den Panoptismus die Entwicklung in der Gesellschaft und im Strafsystem gewesen sei, dass Individuen nicht länger danach beurteilt würden, was sie getan haben (vgl. ebd., S. 28), sondern danach, „was sie sind, sein werden, sein können". (ebd., S. 28) Die Gesetzesübertretungen stünden nun also nicht länger allein im Mittelpunkt der Beobachtung, sondern die Menschen selbst (vgl. ebd., S. 28). So hält Reiner Ruffing, der sich mit Foucaults Werk beschäftigte, fest: „Die Individuen werden nicht mehr nur im Hinblick auf tatsächliches Verhalten gestraft, sondern auf ihr potentielles Verhalten und Gefährdungspotential hin *geprüft*." (Ruffing 2008, S. 106)

Das Strafsystem gehe also immer mehr von der eigentlichen Bestrafung weg und in die Disziplinierung von Individuen über. Das Ziel der Disziplin sei am Ende, durch Überwachung Verhalten zu steuern und damit Menschen zu verbessern (vgl. Ruoff 2009, S. 102). Die Erfassung von kleinsten Details über Individuen würde Wissen und Daten erzeugen, wodurch wiederum neue Techniken der Überwachung entstünden (vgl. Foucault 1989, S. 181). Es sei schließlich wichtig, zu jeder Zeit zu wissen, wo und auf welche Weise jemand gefunden werden kann (vgl. ebd., S. 183). Die Instrumente dieser Disziplinarmacht seien dabei einfach: Es gebe zum einen den hierarchischen Blick, bei dem jemand sieht, ohne selbst gesehen zu werden, und zum anderen eine normierende Sanktion bzw. Strafen (vgl. ebd., S. 220-221). Strafbar sei alles, was von der Regel abweiche und nicht konform sei wie das Begehen von Fehlern (vgl. ebd., S. 231). Diese Fehler würden wiederum gezählt und die Disziplinarapparate könnten Individuen

daraufhin in die Kategorien „gut“ und „schlecht“ einteilen bzw. hierarchisieren (vgl. ebd., S. 233-234). Foucault fasst an diesem Punkt zusammen: „Das lückenlose Strafsystem, das alle Punkte und alle Augenblicke der Disziplinaranstalten erfaßt und kontrolliert, wirkt vergleichend, differenzierend, hierarchisierend, homogenisierend, ausschließend. Es wirkt *normend, normierend, normalisierend*.“ (ebd., S. 236)

Einerseits wirke diese Normalisierungsmacht homogenisierend, aber gleichzeitig individualisierend, da beispielweise die Besonderheiten von Menschen festgehalten würden. (vgl. ebd., S. 237) Durch solche Einzelbeschreibungen würden Registrierungsverfahren implementiert, die auf den Verhaltensweisen der Beobachteten beruhen. Das Individuum werde klassifiziert, um es daraufhin korrigieren oder normalisieren zu können. (vgl. ebd., S. 246) Die individuellen Unterschiede würden letztendlich fixiert, indem jeder seine charakterisierenden Eigenschaften zugewiesen bekommt. Aus jedem Menschen werde demnach ein Fall, wobei in einem Disziplinarsystem die Anormalen mehr individualisiert würden als die Normalen. (vgl. ebd., S. 246 ff.) Es werde allerorts geprüft, ob jemand der Norm entspreche oder nicht. (vgl. Ruffing 2008, S. 106)

Als durch Edward Snowden 2013 bekannt wurde, dass der US-amerikanische Geheimdienst *National Security Agency* (NSA) die weltweite Online- und Telefonkommunikation überwacht und speichert (vgl. Beuth 2013), wurde deutlich, dass Foucaults Theorie des Panoptismus im Informationszeitalter perfektioniert wurde. Durch Überwachungsprogramme wie PRISM[1] ist der NSA besagter Disziplinarapparat gelungen, indem sie buchstäblich alle Informationen aus dem Internet sammeln, analysieren (vgl. Greenwald 2015, S. 83) und für sich auf einen Blick sichtbar machen kann. (vgl. ebd., S. 236) So erfuhr man durch die Bürgerrechtorganisation *American Civil Liberties Union* (ACLU), dass die NSA in ihren Datenbanken Einzelbeschreibungen über Menschen speichert wie die Krankheitsgeschichte, politische Einstellungen, intime Beziehungen und das allgemeine Online-Verhalten. (vgl. ebd., S. 275) Daraufhin werden die Individuen, wie Foucault es beschreibt, registriert und klassifiziert wie z.B. durch das Programm XKeyscore[2], das sogar Live-Überwachung erlaubt (vgl. Greenwald 2015, S. 229). Wie beim Panopticon können sich Internetnutzer also nie sicher sein, ob sie gerade beobachtet werden oder nicht.

Analog zu Foucaults Ausführungen wird von der NSA der gesamte Gesellschaftskörper lückenlos überwacht. So kommt der Journalist Glenn Greenwald zu dem Schluss:

---

[1] Bei dem NSA-Programm PRISM werden IT-Unternehmen wie Google und Facebook dazu verpflichtet, mit dem Geheimdienst zusammenzuarbeiten und ihm alle Kundendaten zur Verfügung zu stellen (vgl. Greenwald 2015, S. 168 ff.).

[2] Hierbei handelt es sich um ein Tool, mit dem die NSA bestimmte Informationen nicht nur sammeln und sortieren, sondern auch konkret nach ihnen suchen kann. Dabei geht es sowohl um Metadaten als auch um Inhalte. XKeyscore erlaubt zusammengefasst einen direkten Zugang zu allem, was ein herkömmlicher Nutzer im Internet tut und das sogar in Echtzeit (vgl. Greenwald 2015, S. 229).

> „Es ist keineswegs übertrieben zu sagen, dass es das erklärte Ziel des Überwachungsstaates ist, sicherzustellen, dass jegliche elektronische Kommunikation von und zwischen Menschen rund um den Globus von der NSA erfasst, gespeichert, überwacht und analysiert wird. (ebd., S. 151)

Wie aus den Snowden-Dokumenten hervorgeht, werden die Spionagetechniken der NSA – entgegen der Rechtfertigung der US-amerikanischen Regierung – seit dem 11. September nicht mehr vorrangig zum Bekämpfen von Verbrechen eingesetzt, sondern es werden in großem Umfang Daten von Personen gesammelt, ohne dass es Hinweise auf konkrete Straftaten oder andere Gefahren gibt (vgl. Schaar 2014, S. 96-97). Vielmehr dient das Datensammeln des Geheimdienstes heutzutage zur Wirtschaftsspionage (vgl. Greenwald 2015, S. 203), der Vorhersehbarkeit von politischen Unruhen (vgl. Rosenbach/Stark 2015, S. 283-284) sowie gesellschaftlichen Bewegungen (vgl. Ammann/Aust 2015, S. 38) und vor allem dazu, um die Vorherrschaft im Internet sicherzustellen (vgl. Rosenbach/Stark 2015, S. 15).

Durch Letzteres entstanden gravierende soziale Folgen. Wie in diesem Beitrag erläutert werden soll, verändern Menschen durch zunehmende Überwachung im Internet ihr Kommunikationsverhalten und schränken ihre Grundrechte wie ihre Informations- und Meinungsfreiheit aus Angst vor Sanktionen von Seiten der Regierung selbst ein. Die erläuterten Theorien von Foucault sollen dabei helfen, diese Phänomene zu erklären.

2. Veränderung des elektronischen Kommunikationsverhaltens

2.1. Begrenzung der Informationsfreiheit

Wie Foucault schreibt, werden in der Disziplinargesellschaft nicht mehr nur Straftäter überwacht, sondern auch das Verhalten von normalen Bürgern dahingehend überprüft, was diese tun könnten. Sie würden individualisiert, um ihre Denk- und Lebensweisen herauszufinden. Das Ziel sei schließlich, die Individuen zu kontrollieren, zu korrigieren oder zu normalisieren (vgl. Foucault 1989, S. 127). Dieses Phänomen lässt sich seit der NSA-Affäre bei normalen Internetnutzern beobachten. Im Zusammenhang mit der elektronischen Kommunikation spricht man jedoch von so genannten *Chilling Effects*.

Datenschützer verwenden diese Theorie häufig, um auf die Gefahren von Überwachungsprogrammen aufmerksam zu machen. Nach dieser Theorie schränken Menschen, die sich beobachtet fühlen, völlig legale Verhaltensweisen ein, da sie Angst haben, sich verdächtig zu machen. Zu diesen Verhaltensweisen gehört z.B. das Äußern einer Meinung oder die Informationssuche nach stigmatisierenden Krankheiten im Internet. Durch eine Studie aus dem Jahr 2016 wurden diese *Chilling Effects* schließlich nachgewiesen. So haben kanadische Forscher um den Wissenschaftler Jon Penney vom *Citizen Lab* der Universität Toronto ermittelt, dass nach den Snowden-Enthüllungen die Abrufzahlen brisanter

Wikipedia-Artikel wesentlich sanken. Um solche kontroversen Artikel herauszufiltern, hatte Penney eine Liste von verdächtigen Begriffen gebraucht, die vom US-Heimatschutzministerium verfasst wurde. Solche Listen dienen beispielsweise dazu, rechtzeitig terroristische Bedrohungen zu erkennen, indem Soziale Netzwerke nach den Begriffen durchforstet werden. Der Wissenschaftler wählte letztendlich 48 Wikipedia-Artikel aus, die Begriffe wie „schmutzige Bombe“ oder die Namen von Terrororganisationen beinhalten.

Es stellte sich heraus, dass nach den Snowden-Aufdeckungen im Juni 2013 die Abrufe der ausgewählten Artikel nur innerhalb eines Monats um fast 30 Prozent absanken. Der Effekt war also unmittelbar nach der Affäre enorm. Aber auch eine Analyse, die sich über 32 Monate erstreckte, legte offen, dass die ursprünglichen Abrufzahlen vor den Snowden-Veröffentlichungen nie wieder erreicht wurden. Für die Studienautoren ist deswegen klar, dass die NSA-Überwachung einen nachhaltigen Einfluss auf das Verhalten von Wikipedia-Usern hat. Penney betont, sollten sich Bürger künftig davor fürchten, sich über kontroverse Themen zu informieren oder ihre Meinung zu äußern, bedrohe das die politische Willensbildung (vgl. Kleinz 2016). „Um das klarzustellen: Diese Aktivitäten sind nicht nur legal, sondern wohl auch für eine gesunde Demokratie wünschenswert“ (Penney zitiert nach Kleinz 2016, o.S.), so der Forscher.

Zu einem ähnlichen Ergebnis kommt auch eine Untersuchung der norwegischen Datenschutzbehörde NDPA. So sagten 46 Prozent der Befragten aus, dass sie seit den Snowden-Veröffentlichungen Angst um ihre Privatsphäre im Internet hätten. Deswegen schränkten sich ca. 16 Prozent selbst ein und suchten nicht länger nach Dingen im Netz, die sie in die Bredouille bringen könnten (vgl. Steinschaden 2014). Im Sinne Foucaults haben sich die Nutzer selbst diszipliniert, normalisiert und dahingehend verbessert, wie sie denken, dass ihre Beobachter es bevorzugen würden. Im Disziplinarraum des Internets kann die NSA so unerwünschte Verhaltensweisen unterbinden (vgl. Ruoff 2009, S. 105). In diesen konkreten Fällen schränkten Menschen ihre eigene Informationsfreiheit ein. Wie auch Jon Penney erklärte, ist diese allerdings ein wichtiger Wert für eine funktionierende Demokratie.

Problematisch speziell an solchen Listen mit verdächtigen Begriffen ist, dass es völlig legitime Gründe dafür geben kann, warum ein Nutzer auf Wikipedia oder in Suchmaschinen z.B. nach „Bombe“ suchen könnte. Man stelle sich vor, dass ein Schüler für ein Referat im Chemieunterricht recherchieren soll, wie eine Bombe zusammengesetzt ist. Er ist vielleicht von arabischer Abstammung oder gehört dem Islam an. Die NSA registriert daraufhin seine Recherchen im Internet und hat ihn im Visier, da dem Geheimdienst der Kontext für die Suchanfragen nicht klar ist und er dazu noch *Racial*

Profiling[3] betreibt. Somit würde ein unschuldiger Internetnutzer verdächtigt, auch wenn er völlig legal sein Recht auf Informationsfreiheit ausübt. Die NSA macht es damit Foucaults Disziplin nach, indem sie Individuen in die Kategorien „gut" und „schlecht" einteilt, sie also kategorisiert und hierarchisiert. Mit Foucaults Worten wird so „die soziale und moralische Trennung zwischen Unschuldigen und Schuldigen in Frage" gestellt. (Foucault zitiert nach Schneider 2004, S. 120)

Deswegen könnten Minderheiten wie in diesem Fall Muslime ihr Verhalten einschränken, um erst gar nicht verdächtig zu wirken. So fand eine Studie, die bereits im Jahr 2007 veröffentlicht wurde, heraus, dass über 71 Prozent der Muslime in den USA denken, dass speziell ihr Online-Verhalten nach den Anschlägen vom 11. September vom Staat überwacht werde. Deswegen änderten 8,4 Prozent ihr Verhalten im Internet (vgl. Steinschaden 2014). Und ihre Annahme wurde bestätigt. So berichteten Medien im Jahr 2012, dass die CIA ganze muslimische Gemeinschaften, die in den USA leben, überwachen lassen will, sowohl physisch als auch elektronisch, auch wenn es keinerlei Hinweise auf Straftaten gebe (vgl. Greenwald 2015, S. 273).

Neben der Diskriminierung von Minderheiten ist das Problem an solch einem Vorgehen der Nachrichtendienste, wie auch Jan-Peter Kleinhans auffällt (vgl. Kleinhans 2013, S. 103), dass man nie wissen könne, wie ein jeweiliger Staat den Begriff „Terrorismus" definiere. Wenn es in einem Land einen Regierungswechsel gebe, könnte die neue Regierung etwas völlig anderes unter Terrorismus verstehen als die vorherige. Durch das langzeitige Speichern der Daten könnte sie aber noch auf ältere Kommunikationsdaten der Bürger zugreifen und diese nachträglich sanktionieren. So sind unter den verdächtigen Begriffen, nach denen Geheimdienste online suchen auch harmlose Wörter wie „beobachten" oder „Schweinefleisch" (vgl. Heuer/Tranberg 2013, S. 76). Vielleicht wird es inzwischen schon als Terrorismus angesehen, wenn jemand Überwachung in Frage stellt und sich im Internet über die NSA informiert oder nach Aktivistengruppen sucht, die sich für Datenschutz einsetzen.

So wurden nach der Bürgerrechtsorganisation *ACLU* Gegner des Irakkriegs wie Studenten oder gewaltlose Demonstranten vom Pentagon überwacht und Informationen über sie in einer militärischen Antiterror-Datenbank gespeichert (vgl. Greenwald 2015, S. 272). Man kann also nie wissen, wer bei Sicherheitsbehörden als sanktionswürdig gilt. All das passt zu Foucaults Thesen, dass in unserer Gesellschaft durch Einzelbeschreibungen Registrierungsverfahren implementiert würden, die auf den Verhaltensweisen der Beobachteten beruhen. Dabei würden die Anormalen häufiger registriert als die Normalen. Wer allerdings als anormal oder normal gilt, das bestimmt die jeweilige Regierung.

---

[3] Bei der Überwachung wird so genanntes *Racial Profiling* betrieben. Nach diesem werden schwarze oder arabisch aussehende Menschen detaillierter überwacht als weiße Menschen (vgl. Henschke 2017, S. 169-170).

2.2. Einschränkung der Kommunikations- und Meinungsfreiheit

Aber Bürger werden nicht nur davon abgeschreckt, sich zu informieren, sondern auch davon, sich über ihre eigene Regierung zu äußern. Nach einer weiteren Studie aus dem Jahr 2016 von Elizabeth Stoycheff von der Wayne State Universität in Michigan beeinflusst Überwachung auch die Bereitschaft zur Meinungsäußerung auf Facebook. Für die Studie wurde das Verhalten von 225 Personen untersucht. Der Hälfte der Studienteilnehmer wurde mitgeteilt, dass der Staat ihr Online-Verhalten überwacht. Allen Befragten wurde daraufhin ein erfundener Facebook-Post über US-Luftangriffe gegen den Islamischen Staat im Irak gezeigt, der nur ein Bild, eine Überschrift und einen Vorspann beinhaltete, aber keine normative Beurteilung der Angriffe. Danach wurden sie befragt, ob sie bereit sind, öffentlich zu dem Thema ihre Meinung abzugeben und auch darüber, wie andere Amerikaner über das Thema wohl denken. Zudem sollten sie die Frage beantworten, für wie gerechtfertigt sie selbst die Internetüberwachung halten (vgl. Jonjic-Beitter 2016).

Das Ergebnis der Studie war, dass sich generell diejenigen Teilnehmer nicht gern äußerten, wenn ihre eigene Meinung von der wahrgenommenen Mehrheitsmeinung abwich. Speziell waren aber diejenigen Personen eher davon abgeneigt, ihre Minderheitsmeinung zu posten, denen gesagt wurde, dass sie überwacht werden. Interessant war für die Studienleiterin außerdem, dass vor allem Personen, die die staatliche Überwachung für gerechtfertigt halten und denken, nichts zu verbergen zu haben, ihre Minderheitsmeinung nicht öffentlich mitteilen wollten. Nach Stoycheff hätten diese Personen vermutlich weniger Angst davor, sozial von ihren Mitmenschen isoliert zu werden, sondern vielmehr davor, von ihrer Regierung verfolgt, sanktioniert oder benachteiligt zu werden. Die Studienautorin sieht durch diese Ergebnisse die Gefahr, dass durch solche Schweigespiralen Menschen mit abweichenden Meinungen aus der öffentlichen Diskussion verdrängt würden (vgl. Rötzer 2016). „Demokratie gedeiht durch die Verschiedenheit der Ideen, Selbstzensur erstickt sie“, so Stoycheff. (Stoycheff zitiert nach Rötzer 2016, o.S.)

Vergleichbares ergaben auch Umfragen zum allgemeinen Kommunikationsverhalten. So fand das *Pew Research Center* im Jahr 2014 heraus, dass 68 Prozent der amerikanischen Internetnutzer Angst um ihre Sicherheit haben, wenn sie persönliche Informationen über Instant-Messenger oder Chats teilen. Dasselbe unsichere Gefühl haben 57 Prozent bei E-Mail, 58 Prozent bei SMS, 46 Prozent beim Handy und 31 Prozent bei Festnetzanschlüssen (vgl. Kolkmann 2016). In Europa gab es bei Umfragen ähnliche Erkenntnisse. Nach einer Befragung des *Vodafone-Instituts* von 2016 haben 51 Prozent der Europäer Angst um ihre Daten, bei den Deutschen sind es sogar 56 Prozent. Deswegen würden diese 56 Prozent ihre digitale Kommunikation einschränken (vgl. *E-Mail, Facebook, SMS und Co.* 2016). Nach dem Technikforscher Sandro Gaycken geschieht diese Verhaltensanpassung dabei oft ohne Absicht. Er hält fest: „Überwachung fördert die innere Zensur. Sie unterdrückt Widerspruchsgeist. Die große Gefahr ist, dass dies

unterbewusst geschieht. Man passt sich an und merkt es gar nicht.“ (Gaycken zitiert nach Schulz 2007)

Eine hohe Anzahl von Menschen scheint ihr Kommunikationsverhalten also anzupassen bzw. völlig einzustellen. Denn den Menschen wurde im Sinne Foucaults beigebracht, sich selbst zu überprüfen und zu kontrollieren. Sie folgen den Normen, von denen sie denken, dass die Autoritäten sie verlangen (vgl. Ruffing 2008, S. 111). Dadurch würden laut dem Philosophen Individuen geschaffen, die nicht mehr außergewöhnlich, sondern gewöhnlich seien und die eine Machtapparatur ihr Leben regeln ließen – eingeordnet und eingeengt durch Disziplinarmechanismen (vgl. Schneider 2004, S. 127).

Aber warum genau schränken Menschen ihre Kommunikations- und Meinungsfreiheit und damit ihr Verhalten ein? Es liegt wohl daran, dass immer wieder Fälle bekannt werden, bei denen harmloses Online-Verhalten zu harten Konsequenzen führte. So gab es einmal den Fall, dass zwei Briten in den USA Urlaub machen wollten, aber am Flughafen in Los Angeles verhaftet und fünf Stunden lang vom *Department of Homeland Security* verhört wurden. Denn vor ihrer Reise hatten sie aus Spaß ihren Freunden getwittert, dass sie „Amerika zerstören“ sowie „Marilyn Monroe ausgraben“ wollen. Sie meinten damit auf Englisch umgangssprachlich, dass sie eine wilde Party feiern wollen, doch die Software der Behörden interpretierte ihre Posts als Terrorismus. Sie konnten letztendlich nicht in die USA einreisen und wurden wieder nach England zurückgeschickt (vgl. Heuer/Tranberg 2013, S. 75).

Wenn Fälle wie dieser bekannt werden, schränken sich Menschen lieber selbst ein, um nichts zu riskieren und nicht sanktioniert zu werden. Nach Foucault (vgl. Foucault 1989, S. 119 ff.) sollen Strafen einen Abschreckungseffekt haben. Sie sollen ein Exempel statuieren, um zukünftiges Verhalten, das nicht der Norm entspreche, zu verhindern. Die Strafen müssen also auch diejenigen abschrecken, die nicht straffällig geworden sind. Wie man anhand der besprochenen Studien erkennen kann, funktioniert solch eine Abschreckung auch von Seiten der US-amerikanischen Geheimdienste. Ihre Macht dringt mit den Worten Foucaults in das Innere der Individuen ein, wo sie als Kontrollinstanz funktioniert (vgl. Schröder 2010, S. 30). Wie der Philosoph beschreibt, ist zwar das tatsächliche Ausüben der Macht nur sporadisch, das Gefühl des Überwachtwerdens dafür aber permanent.

Wie Foucault erörtert, lässt sich an diesem Punkt resümieren, dass sich Machtwirkungen bei vielen Verhaltensweisen im Alltag erkennen lassen (vgl. Schneider 2004, S. 132). Zuletzt soll noch darauf eingegangen werden, wie durch Überwachung speziell die Persönlichkeitsbildung von Individuen beeinflusst werden kann.

3. Persönlichkeitsentwicklung durch Überwachung

3.1. Privatheit als Bedingung für die Identitätsbildung

Foucault ist der Auffassung, dass die Seele bzw. die Identität eines Menschen erst durch Überwachung konstituiert wird. Der Panoptismus halte eine Maschinerie in Gang, die eine Mächteasymmetrie unterstütze und das moderne Individuum hervorbringe (vgl. Sarasin 2005, S. 143). Durch Strafmaßnahmen wie die Disziplin würden Menschen normalisiert und normiert. So bezieht er seine Machttechnologien auch auf Schulen, in denen Kinder und Jugendliche von jung auf und ein Leben lang diszipliniert würden (vgl. ebd., S. 132). Reiner Ruffing (vgl. Ruffing 2008, S. 59) hält in diesem Zusammenhang fest, dass die moderne Macht nach Foucault das Bewusstsein von Individuen durch Bestrafungen und Belobigungen präge und „ihn mit einer individuellen Biographie, Lebensgeschichte, Fähigkeiten, Charaktereigenschaften“ ausstatte. (ebd., S. 59) Das kann sicherlich positive Auswirkungen haben, wenn Menschen so erzogen werden, dass sie lernen, moralische bzw. ethisch richtige Entscheidungen zu treffen, indem Kindern und Jugendlichen z.B. beigebracht wird, dass man anderen Menschen nicht schaden darf. Durch permanente Überwachung und Disziplinierung könnte die Identität allerdings auch geschädigt oder nicht vollständig ausgeprägt werden.

So gehen Privatheitsforscher wie Alan Westin (vgl. Westin 1970, S. 34) davon aus, dass jeder Mensch Privatheit brauche, um seine eigene Persönlichkeit zu formen. Generell hat Privatheit für ihn vier Funktionen: „[P]ersonal autonomy, emotional release, self-evaluation and limited and protected communication.” (ebd., S. 32) So sei in demokratischen Gesellschaften jeder Mensch individuell und diese Individualität würde durch Autonomie bewahrt – also dadurch, dass Individuen von anderen nicht dominiert oder manipuliert werden. Man brauche Zonen der Privatheit, um sein Innerstes für sich selbst zu offenbaren. Wenn die Autonomie gestört werde, seien Geheimnisse des Individuums wie seine Ängste und Träume nicht mehr geheim und würden es unter die Kontrolle derjenigen Personen bringen, die seine Geheimnisse wissen. Jeder Mensch sollte nach Westin aber selbst darüber entscheiden dürfen, was die Öffentlichkeit von ihm wissen darf und was er nur sich selbst oder seinem Freundes- und Familienkreis vorbehalten will. Es gebe vielleicht Eigenschaften eines Menschen, die er selbst noch nicht versteht und langsam erforscht, während er sich entwickelt. Die durch Privatheit ermöglichte Autonomie sei deswegen fundamental für die Entwicklung der Individualität. Man brauche Privatheit, um seine Gedanken und Gefühle zuerst für sich selbst ausprobieren zu können. Man kann mit seinen Ideen und Meinungen experimentieren und diese eventuell ändern, bevor man sich traue, diese öffentlich zu machen. Dafür sei es von Nöten, dass man diese ohne die Angst erprobt, dass man bestraft oder erniedrigt werden könnte. Individualität und Non-Konformität seien letztendlich wichtig für eine Demokratie, die auf Vielfalt basiere.

Was die Funktion *emotional release* angeht, so sei diese Freilassung von Gefühlen wichtig, um Druck im Alltag abbauen zu können. Man brauche sowohl eine Pause von Rollen und Normen in der Gesellschaft als auch das Recht, man selbst zu sein und sich gehen zu lassen. Man sollte z.B. auch ein Mal fluchen oder Autoritäten kritisieren dürfen, ohne für solche Kommentare verantwortlich gemacht zu werden (vgl. ebd., S. 33 ff.). Ohne diese Gefühlsausbrüche stehe man ständig emotional unter Druck (vgl. ebd., S. 36 ff.).

Zu den letzten beiden Funktionen, der Selbstevaluation und geschützten Kommunikation, hält der Privatheitsforscher fest, dass man Privatheit dafür brauche, um Erfahrungen aus dem Alltag zu verarbeiten, diese zu evaluieren und Schlüsse für sein eigenes Verhalten daraus zu ziehen. Man würde lernen, moralisch zu handeln, indem man sein eigenes Verhalten mit dem anderer vergleiche. Zuletzt sei Privatheit essenziell, um mit Freunden oder der Familie über intime Dinge zu kommunizieren bzw. gebe es auch Situationen, in denen man auch einmal objektive Ratschläge von fremden Personen brauche, etwa von Psychologen (vgl. ebd., S. 36 ff.).

Neuere Forschungen gehen davon aus, dass in unserer heutigen Zeit private Räume von Medien eine wichtige Rolle zur Identitätsbildung spielen (vgl. Schröder 2010, S. 76), etwa Soziale Netzwerke (vgl. ebd., S. 81). So erzählte Edward Snowden dem Journalisten Glenn Greenwald in einem Gespräch, dass Medien wie Videospiele und vor allem das Internet wesentlich dazu beigetragen hätten, wie sich seine Persönlichkeit entwickelte. Das Internet sei ein Raum der Freiheit gewesen, in dem man neue Dinge entdecken und geistig wachsen konnte. So hätte er in seiner Jugend im Netz mit den unterschiedlichsten Menschen kommunizieren können, die weit weg wohnten und die er sonst nicht hätte treffen können. Generell hätte er in der virtuellen Welt seine Gedankenwelt erforschen können. Deswegen sei das Internet extrem wertvoll und seine Möglichkeiten müssten um jeden Preis geschützt werden (vgl. Greenwald 2015, S. 80 ff.). So sagte Snowden gegenüber Greenwald überzeugt:

> „Für viele junge Leute ist das Internet ein Mittel der Selbstverwirklichung. Es ermöglicht ihnen herauszufinden, wer sie sind und wer sie sein wollen, aber das geht nur, wenn wir uns dort anonym und auf einer Basis der Vertraulichkeit bewegen können – und Fehler machen, ohne dass sie uns ewig nachhängen. Meine große Sorge ist, dass meine Generation die letzte sein wird, die in den Genuss dieser Freiheit kommt.“ (Snowden zitiert nach Greenwald 2015, S. 82)

Es gibt Studien aus der Zeit, in der das Internet noch in den Kinderschuhen steckte, die Snowdens Erfahrungen bestätigen.

3.2. Identitätskonstruktion im Internet

Anke Bahl beschäftigte sich in ihrem Buch *Zwischen On- und Offline. Identität und Selbstdarstellung im Internet* damit, welchen Einfluss das Netz und Online-Spiele auf die Persönlichkeitsentwicklung von jungen Erwachsenen hatten. Sie führt aus, dass vor allem das Gefühl der Anonymität in virtuellen Räumen – das es in den Anfangsjahren des Internets noch gab – ein Gefühl der Sicherheit vermittelte, das emanzipierend wirken könne (vgl. Bahl 1997, S. 34-35). Um diese Annahmen zu stützen, führte sie Interviews mit Internetnutzern durch, die alle in ihren jungen Zwanzigern waren (vgl. ebd., S. 50 ff.).

Diese legten konkret dar, dass sie die Anonymität des Internets als befreiend empfanden, da niemand wusste, wer man ist und wo man gefunden werden kann. Man konnte sein, wer man wollte, ohne dass man von anderen Menschen verurteilt oder zurechtgewiesen wurde. Man konnte sich also von den Erwartungen der Offline-Welt befreien und sich mit seiner eigenen Persönlichkeit auseinandersetzen. Zudem nutzten viele Studienteilnehmer das Netz, um sich Ratschläge von neutralen Gesprächspartnern zu holen, wenn sie privat Probleme hatten (vgl. ebd., S. 83).

Andere Vorteile der Anonymität des Internets seien gewesen, dass man mit seiner Identität spielen konnte. So hätte man z.B. seine Nationalität (vgl. Bahl 1997, S. 100) oder sein Geschlecht verstecken können, um daran anheftenden gesellschaftlichen Erwartungen in der wirklichen Welt zu entfliehen. Durch Online-Rollenspiele wie das *Multi User Dungeon (MUD)* konnte man die Rollenerwartungen aus dem Alltag hinter sich lassen und diejenige Rolle übernehmen, die man gerne spielen wollte. Eine Userin erzählte, dass ihr das Spiel auch dabei geholfen habe, die Person zu sein, die sie offline sein wollte. Denn man musste im Internet nicht viel darüber nachdenken, wie man sich zu verhalten hatte (vgl. ebd., S. 105). „[D]as MUD gab ihr den möglichen Handlungs*spiel*raum, um sich freier zu entfalten als ihr dies in der Offline-Welt möglich war“ (ebd., S. 105), resümiert Bahl an dieser Stelle.

Gleichzeitig half das Internet auch einigen Studienteilnehmern dabei, ihre Identität in der wirklichen Welt zu bilden. Denn durch das Wunsch-Ich im Internet konnte man sich langsam dem Ich annähern, das man auch offline sein wollte. Durch den virtuellen Raum konnte man die Online-Identität zunächst ausprobieren und dann offline weiterentwickeln (vgl. ebd., S. 105-106). Eine Spielerin berichtete: „The character that I figured was who I wanted to be […] And the more I played it the more I found that it was easier to be that person in real life. It’s kind of like you have practice.“ („Amy“ zitiert nach Bahl 1997, S. 106) Sich in der wirklichen Welt auszuprobieren könne für manche Individuen Gefahren mit sich bringen, aber online habe man alles unter Kontrolle (vgl. Bahl 1997, S. 131). Allgemein hätte das Spiel mit den Rollen online einen therapeutischen Effekt gehabt, da man mit Problemen umgehen lernte und auch einiges über sich selbst lernen konnte (vgl. ebd., S. 125).

In der Untersuchung werden viele Aspekte angesprochen, die auch Alan Westin formulierte. Die jungen Erwachsenen haben ihre Identität noch nicht vollständig ausgebildet, weswegen sie zunächst Eigenschaften ihrer Persönlichkeit online in einem privaten Raum erproben, bevor sie diese in die wirkliche Welt übertragen. Durch die von Privatheit gewährleistete Autonomie wird ihnen dabei geholfen, ihre Persönlichkeit frei zu entwickeln, ohne dass jemand ihr Verhalten wie in der wirklichen Welt sanktionieren könnte. Ohne Angst, erniedrigt zu werden, können sie mit ihren Meinungen oder Ideen online erst einmal experimentieren und sich so selbst finden.

Ebenfalls wie Westin darlegte, scheinen die Interviewten auch einmal eine Pause von den Normen der Gesellschaft zu brauchen, wie von den Anforderungen an ein bestimmtes Geschlecht oder eine Nationalität, was durch die Anonymität im Internet gewährleistet wurde. Wenn sie Probleme in der wirklichen Welt hatten, hätten sich die User in solchen schwierigen Zeiten Ratschläge von neutralen Personen im Internet geholt, die ihnen zuhörten und die solche Informationen nicht gegen sie verwendeten. Sie konnten über ihre Erlebnisse im Alltag reflektieren, ohne dass sie negative Folgen zu befürchten hatten. Im Internet haben sie sich geschützt gefühlt und konnten ihre Ängste offenbaren. Privatheit kann also auch im virtuellen Raum eine therapeutische Wirkung haben und das Wohlbefinden stärken. Zusammenfassend hatte man im Internet schlicht, wie Westin hinsichtlich privater Räume darstellte, die Möglichkeit gehabt, man selbst zu sein.

3.3. Das Ende der Privatsphäre

Die Zeiten, als man sich anonym im Internet bewegen konnte, sind aufgrund der NSA-Überwachung vorbei. So lässt sich feststellen, dass während in den Anfangsjahren des Internet mehr die Privatheitswerte Alan Westins praktiziert wurden, heutzutage vielmehr die Überwachungskonzepte von Foucault im Einsatz sind. Denn Internetnutzer und vor allem junge Menschen können ihre Persönlichkeit im Identitätsspielraum des Internets nicht mehr durch ein Gefühl der Privatheit bilden, sondern ihre Identität wird vielmehr durch das Gefühl des Beobachtetwerdens beeinflusst und konstruiert.

Wie die Untersuchung von Bahl ergab, nutzten junge Menschen das Internet, um verschiedene Verhaltensweisen und unterschiedliche Rollen auszuprobieren, um so ihre Identität zu bilden. Da Menschen nach der NSA-Affäre ihr Kommunikationsverhalten nun nachweislich anpassen oder einschränken, scheinen sich viele User nicht länger zu trauen, beispielsweise ihre Meinungen oder Werte im Internet zunächst zu erproben. Da alle Daten von der NSA und ihren Partnern erfasst und auf unbestimmte Zeit gespeichert werden, hat man nicht mehr den Luxus, den Edward Snowden beschrieb, dass man auch einmal Fehler begehen darf oder wie es Westin ausführte, dass man seine Meinung später noch ändern dürfte. Denn, wie Foucault erörterte, werden Fehler von der Disziplinarmacht immer erfasst und möglicherweise bestraft.

So bringt Maximilian Sönke Wolf das Beispiel, wenn sich jemand online politisch äußere, diese Einstellung (in diesem Fall von der NSA) registriert, gespeichert und bewertet werde. Diese digitale Identität hafte einem daraufhin ewig an, auch wenn man seine politische Meinung Jahre später vielleicht schon wieder geändert hat (vgl. Wolf 2015, S. 134-135). Das wiederum könne

> „die Entwicklung der Persönlichkeit behindern, wenn der Einzelne sich im Kontakt mit Behörden fortwährend einem Persönlichkeitsbild ausgesetzt sieht, das er selbst nicht mehr als aktuell betrachtet und das es ihm verwehrt, die neu justierten Überzeugungen auch in dem Bild staatlicher Entscheidungsträger vom Selbst zu verankern." (ebd., S. 135)

So haben nach einigen US-amerikanischen Studien viele Jugendliche schon einmal Dinge bereut, die sie im Internet posteten und würden sie gerne wieder löschen (vgl. Heuer/Tranberg 2013, S. 170). Sie begangen also Fehler, die sie jetzt nicht mehr rückgängig machen können. Eine andere Umfrage unter deutschen Nutzern zeigte, dass sich 80 Prozent der Befragten schon einmal mit den Privatsphäreeinstellungen von Sozialen Netzwerken beschäftigten. Wolf schließt daraus, dass Menschen ihre Privatheit letztlich wichtig sei, selbst wenn Soziale Netzwerke zur Selbstdarstellung dienten (vgl. Wolf 2015, S. 99).

Das Problem ist, dass schon die primitivsten Daten Schlüsse auf z.B. die politische Einstellung geben können, wie Filme oder Bücher, die man konsumiert (vgl. ebd., S. 137). Viele Menschen geben aus solchen Gründen nachweislich falsche Informationen bei Sozialen Medien ein, um ihre Identität zu schützen (vgl. Heuer/Tranberg 2013, S. 29). Selbst bei Videospielen lassen sich von der NSA viele Daten abschöpfen, etwa von Gaming-Netzwerken wie *World of Warcraft* oder durch Konsolen, die biometrische Daten sammeln wie die Xbox (vgl. ebd., S. 130). Wie früher bei den *MUDs* kann man also heutzutage nicht länger frei mit Rollen spielen, ohne Angst zu haben, dass diese Daten in Datenbanken der Geheimdienste landen. Aufgrund von Überwachung kann man also seinen Freizeitinteressen am Ende nicht mehr nachgehen und sich auch nicht mehr mit anderen Menschen über seine Interessen austauschen. Man kann Werte und Verhaltensweisen nicht länger ausprobieren und mit anderen Usern vergleichen, um seine Identität zu bilden.

Weiter besteht nun die Gefahr, dass sich Menschen im Internet eventuell keine Ratschläge von anderen Usern mehr einholen, wenn sie denken, dass die Informationen gegen sie verwendet werden können. Menschen, die depressiv sind, suchen vielleicht online keine Hilfe mehr, da sie nicht wollen, dass der Staat zu viele intime Details über sie weiß, sie klassifiziert oder die Informationen für andere Zwecke wiederverwendet werden. Denn selbst durch Pseudonyme kann man sich im Internet inzwischen nicht mehr anonymisieren. Die NSA kann problemlos die IP-Adresse eines Users und somit seine Identität herausfinden (vgl. Wolf 2015, S. 63-64).

Wie Westin ansprach, diene Privatheit auch dazu, dass man Druck aus dem Alltag abbauen kann, etwa den Druck, der durch gesellschaftlich vorgeschriebene Normen oder Rollen entsteht. Wenn man im Internet diesen Druck nicht mehr abbauen kann, wie bei den oben genannten Beispielen, indem man sein wahres Ich auslebt oder sich in schwierigen Zeiten Hilfe sucht, steht man emotional permanent unter Druck. So kann das Gefühl, dass man zu jeder Zeit beobachtet werden kann, nachweislich psychische Schäden verursachen, wie Angstzustände oder Unsicherheit (vgl. Heuer/Tranberg 2013, S. 25). Mit den Worten Bahls können Soziale Medien nun nicht länger therapeutisch wirken.

Ein weiterer Nachteil der staatlichen Überwachung ist, dass User im Sinne des Privatheitsforschers auch nicht mehr die Freiheit haben, im Internet Autoritäten wie z.B. Politiker zu kritisieren. Da man nicht weiß, wo Terrorismus für die Regierung anfängt, schränkt man sich vorsichtshalber selbst ein und behält seine Meinungen für sich. Durch das Einüben solcher Verhaltensregeln und Normierungen würden nach Foucault schließlich widerstandslose Individuen entstehen (vgl. Sarasin 2005, S. 137), die alle derselbe Typ von Mensch sein sollen (vgl. Schröder 2010, S. 37), also ohne jegliche Individualität.

Man könnte argumentieren, dass Menschen auch in anderen privaten Räumen als dem Internet weiterhin ihre Identität bilden können. Bei jungen Menschen ist das Internet allerdings nachweislich Teil des Alltags und eine der beliebtesten Freizeitaktivitäten (vgl. Rövekamp 2016), weswegen es für die Persönlichkeitskonstruktion von großer Bedeutung ist. Wenn sie das Gefühl bekommen, dass ihr Verhalten dort jederzeit überwacht und auf unbegrenzte Zeit gespeichert werden kann, werden sie sich der Norm anpassen und nicht länger ihre Individualität ausleben. Indem sie online mit ihrem fiktiven Ich nicht mehr experimentieren können, haben sie vielleicht nicht den Mut, in der wirklichen Welt so zu sein, wie sie sein wollen. Dadurch wird ihr Verhalten und darüber hinaus ihre Identität im Sinne Foucaults von einer äußeren Macht gebildet und kontrolliert (vgl. Schröder 2010, S. 30). Die Autonomie, von der Westin sprach, wird beschädigt, da User jetzt von anderen dominiert und manipuliert werden können, etwa weil die NSA alle ihre Geheimnisse, Wünsche und Ängste kennt. Die Nutzer können demnach nicht mehr darüber entscheiden, wer ihre intimsten Posts sehen darf und wie sie verwendet werden, wenn die NSA ohnehin komplett alles sammelt und Informationen auch manipulieren kann.

So ist aus den Snowden-Unterlagen ersichtlich, dass der britische NSA-Partner *Government Communications Headquarters* (GCHQ) unter anderem Psychologen für die Entwicklung von Techniken einsetzt, deren Ziel die strategische Einflussnahme im Internet sein soll. So denken die GCHQ-Mitarbeiter, dass sich menschliches Verhalten im Internet durch Anpassung, Spiegelung oder Mimikri steuern lasse, also dass User andere User nachahmen. Dadurch können Geheimdienstmitarbeiter Online-Plattformen wie Soziale Netzwerke infiltrieren, andere Nutzer täuschen sowie deren Verhalten beeinflussen, indem sie sie z.B. zu Straftaten anstacheln. Methoden zur Rufschädigung

oder Manipulation sind bei Geheimdiensten also nicht nur möglich, sondern werden bereits angewendet (vgl. Greenwald 2015, S. 283-284).

Es lässt sich zusammenfassen, dass man sich vor der NSA-Überwachung im Internet frei und privat bewegen konnte, ohne dass jemand wusste, wer oder wo man ist. Heutzutage ist es so, wie Foucault es bezüglich der Disziplin formulierte, dass die NSA immer weiß, wo und auf welche Weise jemand gefunden werden kann. Niemand ist mehr anonym und kann sich ihrem vollkommenen Auge entziehen.

4. Die Ethik des Selbst als Ausweg?

In *Überwachen und Strafen* resümiert Foucault, dass wir alle „in das Räderwerk der panoptischen Maschine [eingeschlossen sind], die wir selber in Gang halten – jeder ein Rädchen." (Foucault 1989, S. 279) In seinen späteren Werken entwickelt er schließlich eine Lösung, wie man aus diesem Kreislauf, dass Individuen durch Überwachung und Korrigierung immer wieder aufs Neue hervorgebracht werden (vgl. ebd., S. 41-42), ausbrechen könne und schlägt die so genannte *Sorge um sich* bzw. *Ethik des Selbst* vor (vgl. Sarasin 2005, S. 192-193).

Diese ist an die antike Ethik angelegt, die aber mit der Moderne gewisse Gemeinsamkeiten habe (vgl. Ruffing 2008, S. 99). „Heute wie damals brach eine Welt zusammen, damals die Poliswelt, gegenwärtig die Welt der kodifizierten Werte. Die Menschen mussten und müssen sich neu orientieren" (ebd., S. 99), fasst Reiner Ruffing zusammen. Die Menschen müssten deswegen sich selbst und ihre Sicht- und Verhaltensweisen ändern. (vgl. ebd., S. 99) „Wir müssen neue Formen der Subjektivität zustande bringen, indem wir die Art von Individualität, die man uns jahrhundertelang auferlegt hat, zurückweisen", so Foucault. (Foucault zitiert nach Sarasin 2005, S. 192). Man müsse sich also gegen eine Macht wie den Panoptismus, der das Verhalten und die Identitätsbildung beeinflusst, wehren. Denn eine Ethik des Selbst bzw. die Beziehung zu sich selbst könne eine Form des Widerstands gegen politische (vgl. Sarasin 2005, S. 195) sowie normierende Macht sein (vgl. Ruoff 2009, S. 53). Das heißt für ihn konkret, dass das Subjekt die Differenz zwischen sich und dem, was es sein soll, erkennen muss und sich durch Selbstpraktiken als ein sich selbst bewusstes und handelndes Subjekt konstituiert (vgl. Sarasin 2005, S. 196). Nur so könne es individuell sein Leben gestalten (vgl. Ruffing 2008, S. 65). Die Autonomie des Individuums steht nun also im Mittelpunkt (vgl. Ruoff 2009, S. 53).

Hinsichtlich der NSA-Überwachung würde das bedeuten, dass die Menschen zunächst erkennen müssten, dass sie durch das Gefühl des Beobachtetwerdens beeinflusst werden und ihr Verhalten unfreiwillig einschränken. Denn, wie bereits erwähnt, scheint diese Begrenzung der eigenen Freiheiten manchmal unterbewusst zu geschehen. Sie müssten also nach Foucaults Ratschlag verstehen, dass sie normiert werden und dass es einen

Unterschied zwischen ihrem wirklichen Ich und ihrem durch Überwachung normalisierten Ich gebe. Dazu müssten sie den Panoptismus zurückweisen und der Selbstdisziplinierung gezielt entgegensteuern, indem sie sich so verhalten, wie sie sich zu Hause ohne einen Beobachter verhalten würden. Nach Foucault müsse man ständig an sich selbst arbeiten (vgl. ebd., S. 60), um Veränderungen herbeiführen zu können (vgl. ebd., S. 54). Bei der Sorge um sich geht es also um eine Verschränkung von Denken und Handeln (vgl. ebd., S. 199).

So gehören beispielweise manche Menschen Netzbewegungen an, deren Devise es ist, völlig transparent zu leben. Einer davon ist Hasan Elahi. Dieser wurde aufgrund eines Fehlers auf eine Anti-Terrorismus-Merkliste der US-amerikanischen Regierung eingetragen und entschied sich daraufhin dazu, mit ungewöhnlichen Mitteln dagegen anzukämpfen. Denn er teilt seitdem jede noch so winzige Kleinigkeit seines Lebens, indem er inzwischen 46.000 Fotos online postete wie Fotos von seinem Essen oder von Toiletten. Durch diese Aktion hat er nun das Gefühl, die Kontrolle über seine Privatsphäre zu haben. Er denkt, wenn viele Menschen es ihm nachmachen würden, müssten sich Nachrichtendienste neu erfinden. Denn durch so eine immense Datenflut würden die Rechner der Sicherheitsbehörden ausgelastet, sodass Geheimdienste abgeschafft würden (vgl. Heuer/Tranberg 2013, S. 33-34).

Das wäre das extremste Szenario der Ethik des Selbst. Es würde aber auch ausreichen, wenn Internetnutzer ihre Rechte nicht selbst einschränken, um sich aus ihrer eigenen Unmündigkeit zu befreien und so zu einer gesunden Demokratie beizutragen. Denn, wenn die NSA merkt, dass Menschen sich von der Überwachung nicht beeindrucken und beeinflussen lassen, würde sie ihre Praktiken vielleicht begrenzen. So könnte das eigene Handeln zu Veränderungen in der Gesellschaft führen.

Man könnte die Sorge um sich aus heutiger Sicht allerdings auch so interpretieren, dass sich Menschen selbst vor Überwachung schützen sollen. Indem sich User anonym im Netz bewegen, können sie sich der Geheimdienstüberwachung zum Teil entziehen und die Spionage nicht mehr wahrnehmen, sodass sie ihr Verhalten nicht einschränken müssen. Zwar denken viele Menschen, dass die Macht der Geheimdienste und IT-Unternehmen so groß ist, dass man gegen sie sowieso nichts ausrichten könne (vgl. Schaar 2014, S. 256). Allerdings machen es sorgfältig eingesetzte Verschlüsselungsverfahren den Spionen schwerer, die Daten mitzulesen.

Um etwa seinen Datenverkehr im Internet zu verschlüsseln, gibt es den Tor-Browser, mit dem die eigene IP-Adresse und somit der Standort verschleiert wird. Da die US-amerikanische Bürgerrechtsorganisation *Electronic Frontier Foundation* (EFF) ermittelte, dass vor allem der Browser viele Auskünfte über die eigene Identität gibt, ist die Wahl des Browsers von Bedeutung. Nach Snowdens Dokumenten hatte die NSA zudem wenig Erfolg damit, das Tor-Netzwerk zu brechen (vgl. Schartner 2014, S. 154 ff.). Eine ähnliche Möglichkeit der Anonymisierung bieten Proxy-Server. Hier werden die Daten nicht über das eigene Gerät versendet, sondern sie werden zuerst an einen Proxy-Server geschickt,

der mit seiner IP-Adresse die Daten dann an den Empfänger weiterleitet, also an die aufgerufene Webseite (vgl. ebd., S. 158).

Nach Snowden sollte man zudem Firmen unterstützen, die sich für Datenschutz einsetzen (vgl. Gurnow 2014, S. 281). Da vor allem durch PRISM viele Informationen gespeichert werden, kann man dieser Spionage entgehen, wenn man Dienste wie Facebook oder Google meidet, die sich direkt durch die Datensammlung ihrer Nutzer finanzieren (vgl. Schaar 2014, S. 267). So haben sich einige Webseiten zum Ziel gesetzt, Alternativen zu den großen Plattformen vorzustellen, etwa die Webseite *Prism-Break.org*. Hier werden Dienste aufgelistet, die keine Daten loggen, wie z.B. die Suchmaschine DuckDuckGo als Alternative zu Google, das Soziale Netzwerk Diaspora anstelle von Facebook oder das Betriebssystem Linux als Gegenvorschlag zu Windows (vgl. Zhong 2021).

Glenn Greenwald (vgl. Greenwald 2015, S. 367) betont, indem man IT-Unternehmen, die mit der NSA zusammenarbeiten, umgeht, übe man Druck auf diese Konzerne aus, diese Zusammenarbeit abzubrechen. Zudem motiviere man deren Mitbewerber dem Datenschutz einen hohen Stellenwert einzuräumen. Dass die informationelle Selbstverteidigung wirkt, sieht man an den finanziellen Verlusten, die die Silicon Valley-Giganten kurz nach der NSA-Affäre erlitten hatten (vgl. Rosenbach/Stark 2015, S. 297). Und auch Snowden, obwohl ihm bewusst ist, dass die NSA immer an neuen Wegen arbeitet, Verschlüsselungen zu knacken (vgl. Gurnow 2014, S. 281), sagt, dass Verschlüsselung funktioniert: „Wenn sie richtig eingesetzt werden, gehören starke Kryptographiesysteme zu den wenigen Dingen, auf die man sich verlassen kann." (Snowden zitiert nach Harding 2014, S. 178) Und wenn es jemand weiß, dann er.

Diese Sorge um sich bzw. Technologien des Selbst, die Foucault herausarbeitete, hätten bei erfolgreicher Anwendung letztendlich drei Dinge vollbracht. Erstens finde man sich selbst und seinen Platz in der Welt. Zweitens könne man immer die Wahrheit sprechen, also müsse man sich selbst nicht zurücknehmen. Und drittens gebe es keine Instanz mehr, die dem Subjekt sage, was es zu tun hätte. Denn diese Instanz sei es nun selbst (vgl. Sarasin 2005, S. 199). Ohne das Gefühl des Überwachtwerdens könnten Menschen also völlig frei ihre eigene Identität bilden, ihre Meinungsfreiheit ausleben und zu einem autonom handelnden Subjekt werden. Nach Foucault kann das Subjekt schließlich nicht nur durch Unterwerfung konstituiert werden, sondern auch durch Praktiken der Befreiung (vgl. Ruffing 2008, S. 111).

Literatur

Ammann, Thomas & Aust, Stefan (2015): *Digitale Diktatur. Totalüberwachung, Datenmissbrauch, Cyberkrieg*. Berlin: Ullstein Buchverlage.

Bahl, Anke (1997): *Zwischen On- und Offline. Identität und Selbstdarstellung im Internet*. München: KoPäd.

Beuth, Patrick (2013): Snowden-Enthüllungen. Alles Wichtige zum NSA-Skandal. *ZEIT ONLINE*. 28. Oktober 2013. Abgerufen unter: https://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal [Stand vom 08-05-2021].

Blumer, Tim (2013): *Persönlichkeitsforschung und Internetnutzung*. Ilmenau: Universitätsverlag Ilmenau.

E-Mail, Facebook, SMS und Co. Ständige Überwachung führt zur Selbstzensur im Internet. (2016): *Forschung und Wissen*. 28. Januar 2016. Abgerufen unter: https://www.forschung-und-wissen.de/nachrichten/psychologie/staendige-ueberwachung-fuehrt-zu-selbstzensur-im-internet-13372255 [Stand vom 08-05-2021].

Foucault, Michel (1989): *Überwachen und Strafen. Die Geburt des Gefängnisses*. Frankfurt am Main: Suhrkamp.

Greenwald, Glenn (2015): *Die globale Überwachung. Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen*. München: Droemer.

Gurnow, Michael (2014): *The Edward Snowden Affair. Exposing the Politics and Media Behind the NSA Scandal*. Indianapolis: Blue River Press.

Harding, Luke (2014): *Edward Snowden. Geschichte einer Weltaffäre*. London: Weltkiosk.

Henschke, Adam (2017): *Ethics in an Age of Surveillance. Personal Information and Virtual Identities*. Cambridge: Cambridge University Press.

Heuer, Steffan & Tranberg, Pernille (2013): *Mich kriegt ihr nicht! Die wichtigsten Schritte zur digitalen Selbstverteidigung*. Hamburg: Murmann Verlag.

Jonjic-Beitter, Andrea (2016): Studie: Online-Überwachung bringt abweichende Meinungen zum Schweigen. *Netzpolitik*. 22. März 2016. Abgerufen unter: https://netzpolitik.org/2016/studie-online-ueberwachung-bringt-abweichende-meinungen-zum-schweigen/ [Stand vom 08-05-2021].

Kleinhans, Jan-Peter (2013): Minority Reports ‘Precrime’ ist das Ziel des MI5 Director General Andrew Parker. In: Beckedahl, Markus & Meister, Andre (Hrsg.): *Überwachtes Netz. Edward Snowden und der größte Überwachungsskandal der Geschichte*. Berlin: Newthinking Communications, S. 101-106.

Kleinz, Torsten (2016): Studie zu Chilling Effects: Wikipedia-Artikel zu Terrorismus werden weniger gelesen. *heise online*. 27. April 2016. Abgerufen unter: https://www.heise.de/newsticker/meldung/Studie-zu-Chilling-Effects-Wikipedia-Artikel-zu-Terrorismus-werden-weniger-gelesen-3191301.html [Stand vom 08-05-2021].

Kolkmann, Thomas (2016): Chilling Effects: Führt Überwachung zur Selbstzensur? *GIGA*. 21. März 2016. Abgerufen unter: https://www.giga.de/extra/ratgeber/specials/chilling-effects-fuehrt-ueberwachung-zur-selbstzensur/ [Stand vom 08-05-2021].

Rosenbach, Marcel &Stark, Holger (2015): *Der NSA Komplex. Edward Snowden und der Weg in die totale Überwachung*. Hamburg: SPIEGEL-Verlag.

Rötzer, Florian (2016): Wie beeinflusst das Wissen über Überwachung die Online-Kommunikation? *heise online*. 02. April 2016. Abgerufen unter: https://www.heise.de/tp/features/Wie-beeinflusst-das-Wissen-ueber-Ueberwachung-die-Online-Kommunikation-3379369.html [Stand vom 08-05-2021].

Rövekamp, Marie (2016): Freizeitverhalten von Jugendlichen. Sie chatten mehr und lesen weniger. *DER TAGESSPIEGEL*. 16. November 2016. Abgerufen unter: https://www.tagesspiegel.de/wirtschaft/freizeitverhalten-von-jugendlichen-sie-chatten-mehr-und-lesen-weniger/14851782.html [Stand vom 08.05.2021].

Ruffing, Reiner (2008): *Michel Foucault*. Paderborn: Wilhelm Fink.

Ruoff, Michael (2009): *Foucault-Lexikon. Entwicklung – Kernbegriffe – Zusammenhänge*. Paderborn: Wilhelm Fink.

Sarasin, Philipp (2005): *Michel Foucault zur Einführung*. Hamburg: Junius Verlag.

Schaar, Peter (2014): *Überwachung total. Wie wir in Zukunft unsere Daten schützen*. Berlin: Aufbau Verlag.

Schartner, Götz (2014): *Vorsicht, Freund liest mit! Wie wir alle seit Jahren ausspioniert werden und wie wir uns wehren können*. Kulmbach: Plassen Verlag.

Schneider, Ulrich Johannes (2004): *Michel Foucault*. Darmstadt: Wissenschaftliche Buchgesellschaft.

Schröder, Bernhard (2010): *Identität im historischen Wandel aus machttheoretischer Perspektive*. Hamburg: Diplomica Verlag.

Schulz, Daniel (2007): Staatliche Überwachung. „Man passt sich an und merkt es nicht". *taz*. 31. Oktober 2007. Abgerufen unter: https://www.taz.de/!5192484/ [Stand vom 08-05-2021].

Steinschaden, Jakob (2014): „Der Chilling Effect": Massenüberwachung zeigt soziale Folgen. *Netzpiloten Magazin*. 07. April 2014. Abgerufen unter: https://www.netzpiloten.de/der-chilling-effect-massenueberwachung-zeigt-soziale-folgen/ [Stand vom 08-05-2021].

Westin, Alan F. (1970): *Privacy and Freedom*. New York: Atheneum.

Wolf, Maximilian Sönke (2015): *Big Data und Innere Sicherheit. Grundrechtseingriffe durch die computergestützte Auswertung öffentlich zugänglicher Quellen im Internet zu Sicherheitszwecken*. Marburg: Tectum Verlag.

Zhong, Peng (2021): All Projects. *PRISM BREAK*. 20. Januar 2021. Abgerufen unter: https://prism-break.org/en/all/ [Stand vom 08-05-2021].

Datenpolitiken ‚von unten' zwischen Aktivismus und Politischer Medienbildung

Valentin Dander

Zusammenfassung

Datenpolitiken werden in diesem Beitrag denkbar weit gefasst. Unter Datenpolitiken ‚von oben' werden kapitalistische und staatliche Datenpolitiken sowie hybride Formen verstanden. Datenaktivismus wird beispielhaft für Datenpolitiken ‚von unten' eingeführt und in reaktive und proaktive Praktiken und Taktiken differenziert, die reaktiv auf verschiedenen Ebenen auf Datenschutz zielen und/oder proaktiv in thematisch weiterreichende politische Projekte eingebettet sind. Für datenaktivistische Praktiken erweisen sich zahlreiche Fähigkeiten als bedeutsam, die in unterschiedlichen Ausprägungen als *(Critical Big) Data Literacy/-ies* modelliert werden. Diese verweisen auf die Schnittstelle von Politischer und Medienbildung in datafizierten Gesellschaften und münden im Text mit Gert Biesta in der Skizze eines *Ignorant Digital/Data Citizen* als erstrebenswerte politische Subjektfigur, die es vermag, zwischen universellem Gleichheitsstreben und weitgehender Unbestimmtheit zu vermitteln.

1. Einleitung

Bereits seit knapp 10 Jahren wird das Thema Big Data Analytics, die damit einhergehenden Überwachungs- und Ausbeutungspraktiken sowie die Verschränkungen mit automatisierten, algorithmischen Prozessen und den auf vielfache Weise in sie eingeschriebenen Diskriminierungsformen wissenschaftlich thematisiert. Unterschiedliche Fachdisziplinen rücken unterschiedliche Aspekte in den Vordergrund. Sie eint dabei eine fundamentale Kritik an den damit verbundenen hegemonialen, quantifizierenden Wissens- und Subjektivationsformen, an der Hervorbringung neuer wie auch der Verstärkung bestehender Ungleichheiten, Machtasymmetrien und Herrschaftsformen. Dieser Komplex wird im Folgenden als *Datenpolitiken von oben* bezeichnet. Der vorliegende Beitrag nimmt in einer selektiven Skizze von einigen dieser Debattenstränge seinen Ausgang (*Kap. 2*) und sodann eine Verschiebung vor: zunächst zu *Datenpolitiken von unten* (*Kap. 3*), worunter individuelle und kollektive, im weitesten Sinne politische Datenpraktiken verstanden werden.

Welche datenbezogenen pädagogischen Konzeptionen hierfür relevante Kategorien darstellen können, wird im darauffolgenden *Kapitel 4* dargelegt. Verschiedene Varianten von *Data Literacy* unterscheiden sich in ihrem politischen Anspruch mitunter deutlich von *(Critical Big) Data Literacy/-ies*, welche stärker auf demokratische Selbst- und Mitbestimmung abheben und entsprechend friktionsfreier mit Digital Citizenship

zusammengedacht werden könnten. Inwieweit Konzeptionen eines Digital Citizen gedacht werden können, ohne auf Kompetenzmodelle beschränkt zu sein oder depolitisierende Festschreibungen vorzunehmen, skizziert abschließend *Kapitel 5*.

2. Datenpolitiken ‚von oben': hybride Konstellationen zwischen Unternehmen und Staat

Wenn in diesem Artikel von ‚Datenpolitiken' die Rede ist, so bezieht sich dieser Ausdruck keineswegs nur auf ein enges Verständnis von Praktiken im Rahmen politischer Institutionen, des demokratischen bzw. des Parteiensystems. Der Text folgt stattdessen einem umfassenden Verständnis von ‚Datenpolitiken' insofern, als darüber hinaus alle datenbezogenen Praktiken verstanden werden, die sich auf die Konstitution, die Gestaltung, die Produktion und Reproduktion aller möglichen Aspekte des sozio-technischen und politischen Lebens beziehen – insbesondere aber auch auf ‚das Politische', also verkürzt gesprochen auf dissensuale Infragestellungen der Konturen von ‚Politik' (vgl. Bröckling/Feustel 2012; Mouffe 2015, S. 22–23).[1] Dieser breit angelegte Zugang umfasst den Beschluss der EU-Datenschutzgrundverordnung (DSGVO) genauso wie außerparlamentarische netzpolitische Initiativen, Tracking durch Online-Plattformen oder den einen Klick, der beim Besuch einer Website nicht-essenzielle Cookies ablehnt. Ruppert, Isin und Bigo (2017, S. 2) konstatieren: "[D]ata and politics are inseperable. Data is not only shaping our social relations, preferences, and life chances but our very democracies."

Ebenso bezieht sich ein solches Verständnis auf grundlegende Fragen des Wissens (bzw. des Wissbaren) und der Erkenntnis, die im Zusammenhang mit Praktiken des Datensammelns und -auswertens einhergehen. Hier setzen erste Kartierungen und Analysen dessen ein, was im sich stets verschiebenden Diskurs mit *Big Data*, *Algorithmisierung*, *Künstliche Intelligenz* (*KI* bzw. *Artificial Intelligence*, *AI*), *Machine Learning* etc. beschrieben wird. Auch wenn damit jeweils spezifische Aspekte in den Vordergrund gerückt werden, befassen sie sich mit einem thematischen Komplex, in welchem das eine das andere bedingt (vgl. Dander 2018, S. 21 ff.). Während eine technik-fokussierte Perspektive zum einen einer IT- und Ingenieurslogik folgt und zum anderen

[1] So schreibt etwa Oliver Marchart (2005, S. 19; Herv. im Original): „Ich schlage also vor, eine analytische Unterscheidung zu treffen zwischen *‚Polizei'*, *Politik* und *dem Politischen*, oder im Englischen: *policy*, *politics* und *the political*" und präzisiert die Differenzierung: „Politik als Debatte, d.h. als Form der *antagonistischen* Austragung des Politischen, von Politik als Teilsystem der Gesellschaft und schließlich von Politik als regulatorischem Verwaltungshandeln, also im Sinne von Politikfeldadministration (*policy*)." Genau genommen bezieht der Ausdruck ‚Datenpolitiken' im vorliegenden Text alle drei Bereiche ein.

mehr oder minder bewusst von einer Ideologie der technischen Lösbarkeit gesellschaftlicher Probleme durchzogen ist (vgl. etwa Morozov 2014; Nachtwey/Seidl 2017), richten sich (kritische) sozial- und kulturwissenschaftliche Perspektiven u.a. auf die Dimensionen Kontext, Macht/(soziale) Gerechtigkeit, Ideologie oder Mythologie (vgl. Boyd/Crawford 2012, S. 663), Praxis oder politische Handlungsoptionen.

Die Wirksamkeit all dieser Datenpolitiken lässt sich an medienkulturellen Entwicklungen ablesen, die Ramon Reichert (vgl. 2014) mit Blick auf den kommerziellen Sektor von Datenpolitiken am Beispiel von Social Media Plattformen und Suchmaschinen beschreibt: Eine „algorithmische Prognostik kollektiver Prozesse" (ebd., S. 40) bildet hierbei die eine Seite, während auf der anderen Seite Personalisierung erfolgt. Statistische Auswertungen bzw. prognostische Modellierungen von ‚Massen' sowie identifizierbare Einzeldatensätze und ihre Analysen ankern im „Profiling" und den dabei generierten Profilen. Einzelne Nutzende der Anwendungen finden sich darin als Individuen und als geteilte Zugehörige von multiplen, dynamischen Profilkategorien wieder (vgl. ebd.).

Die lange Tradition staatlicher Regierungskünste, in welche sich diese statistischen Methoden einschreiben, skizzierte Michel Foucault (vgl. 2004, S. 152–157) bereits 1978. So entwickelte sich die Statistik ab dem späten 16. Jahrhundert zu einer tragenden Säule staatlicher Wissenstechniken. Sie erlaubte es, das „Problem der Bevölkerung" (ebd., S. 157) zu quantifizieren, ihren Zustand und ihre Handlungen zu erfassen, zu analysieren und das Regierungshandeln daran auszurichten (vgl. ebd.).

An Beispielen wie Facebook oder Google wird jedoch deutlich, dass gegenwärtige Datenpolitiken zu großen Teilen von nicht-staatlichen Akteuren vollzogen werden, während sich staatliche Agenturen in antagonistischer (z.B. Gesetzgebung oder Rechtsprechung für Datenschutz), teil-abhängiger (z.B. Strafverfolgungsbehörden, die Daten/sätze von Unternehmen anfordern) oder regulierender (z.B. DSGVO) Position befinden.[2]

Wir haben es demnach mit zwei sich teilweise überlagernden Ebenen von Datenpolitiken zu tun: Zum einen werden Prozesse der Kapitalisierung, der Enteignung, Kommodifizierung und des In-Wert-Setzens von Daten und ihren Beziehungen analytisch in den

[2] Wie am aktuellen „Gesetz zur Änderung des BND-Gesetzes" von April 2021 (vgl. Bundestag der BRD 2021) und insbesondere an dessen Kritik deutlich wird (vgl. etwa die Stellungnahme des DAV – Deutscher Anwaltverein 2021), wird seitens des Staates eine Ausweitung der Befugnisse der Geheimdienste und Strafverfolgungsbehörden (hier etwa des BND, Bundesnachrichtendienst) betrieben – inklusive der Überwachung weltweiter Telekommunikation und der umstrittenen Datenspeicherung. Demokratische Kontrolle und Rechenschaftspflichten werden hierbei vernachlässigt. Dies gilt auch für einen Regierungsentwurf vom Januar 2021, welcher in einem „Gesetz zur Fortentwicklung der Strafprozessordnung (StPO)" deutlich erweiterte Möglichkeiten für Online-Durchsuchungen (auch Staats- oder Bundestrojaner genannt) durch ermittelnde BeamtInnen vorsieht (vgl. Kurz 2021).

Blick genommen und in entsprechende Konzeptionen umgemünzt, die vorrangig die ökonomischen Ebene und damit privatwirtschaftliche Akteure beschreiben und kritisieren. Zum anderen werden staatliche Datenpolitiken analysiert und kritisiert, die in der Verwaltung und Kontrolle verschiedener gesellschaftlicher Felder zum Einsatz kommen und ihre Macht entfalten – neben Sicherheitstechnologien und Strafverfolgung beziehen sich diese z.B. auf das Sozial-, Gesundheits- und Bildungssystem, auf Migrationspolitik oder auch auf bereichsübergreifende Kontroll- und Disziplinierungsmaßnahmen.

2.1. Kapitalistische Datenpolitiken

Beispielhaft für kapitalistische Datenpolitiken kann hier etwa das vielzitierte Konzept des „Überwachungskapitalismus" von Shoshana Zuboff (2019) genannt werden, welches sie u.a. als "rogue mutation of capitalism" definiert (ebd., S. 8). Die Gesamtheit des Überwachungs- und Verwertungsdispositivs ("ubiquitious digital apparatus") bezeichnet sie in Abwandlung des Orwell'schen Big Brother als "Big Other" (ebd., S. 353) und bezeichnet hiermit die oben angesprochene Verschiebung von staatlicher zu privatwirtschaftlicher Überwachung in unmittelbaren Diensten des Kapitals:

> "it is the sensate, computational, connected puppet that renders, monitors, computes, and modifies human behavior. Big Other combines these functions of knowing and doing to achieve a pervasive and unprecedented means of behavioral modification. Surveillance capitalism's economic logic is directed through Big Other's vast capabilities to produce instrumentarian power, replacing the engineering of souls with the engineering of behavior." (ebd.)[3]

Eine ähnliche Stoßrichtung findet sich im Buch "The costs of connection" von Nick Couldry und Ulises A. Mejias (2019). Die Autoren argumentieren, dass die auf Wertschöpfung gerichteten Prozesse der Datensammlung und -auswertung als Datenkolonialismus bezeichnet werden können:

> "Data relations […] are new types of human relations that give corporations a comprehensive view of our sociality, enabling human life to become an input or resource for capitalism. In this neocolonial scheme, the colony is not a geographic location but an 'enhanced reality' in which we conduct our social interactions under conditions of continuous data extraction. The resources that are being colonized are the associations, norms, codes, knowledge, and meanings that help us maintain social connections, the

[3] Auch unabhängig von der durchaus problematischen Marionetten-Metaphorik wurde einige Kritik an Zuboffs Ansatz geübt. Darauf kann hier aus Platzgründen nicht weiter eingegangen werden (vgl. etwa di Bella 2019).

> human and material processes that constitute economic activity, and the space of the subject from which we face the social world." (ebd., S. 85)

Couldry und Mejias sind sich der Unterschiede zum historischen Kolonialismus und zu dessen rassistischen, sexistischen und eurozentristischen Dimensionen bewusst, die im Datenkolonialismus auf andere Weise zum Tragen kommen, und nehmen diese Differenz in ihrer Beschreibung von Datenextraktion als Daten*kolonialismus* in Kauf (ebd., S. 45).[4] Die damit einhergehende, neue Bedeutungsebene von "*digital natives*", die zum Objekt datenkolonialistischer Praktiken und Strukturen gemacht werden (ebd., S. 111; Herv. im Original), trägt diese Einschränkung in der metaphorischen Übertragung ebenfalls in sich.

Im Grunde beschreiben die Autoren einen Prozess, der in der Terminologie einer Kritischen Politischen Ökonomie als „[i]mperialistische Expansion" in Richtung eines nichtkapitalistischen Außens (Luxemburg 1970, S. 754 ff.) oder später als „neue Landnahme" (Dörre 2009) bezeichnet werden kann. Anstatt anderer Weltregionen geraten bisher nicht warenförmige Aspekte von Sozialverhalten, Gefühlen oder sozialen Beziehungen in den Fokus der Kapitalakkumulation.[5]

2.2. Staatliche Datenpolitiken

Staatliche Datenpolitiken werden im Unterschied zu den oben genannten Arbeiten insbesondere im Zusammenhang mit staatlichem Überwachungs-, Kontroll- und Verwaltungshandeln beschrieben, welches in verschiedenen gesellschaftlichen Teilbereichen oder Feldern unter Zuhilfenahme von Datenbanken und Analysesoftware vollzogen wird. Auch hier wird im Folgenden beispielhaft dargelegt, wie diese staatlichen Datenpolitiken konzeptionell-analytisch gefasst und wie sie dadurch problematisiert werden.

Das wohl eindrücklichste Ereignis in dieser Hinsicht waren die *Snowden-Leaks* im Juni 2013, die ein weltweites Netz geheimdienstlicher Spionage in einem bisher nur erahnten Ausmaß offenbarten (vgl. etwa Beckedahl/Meister 2013; Himmelsbach 2015). Anstatt dass dieser Skandal zu Beschränkungen geheimdienstlicher Befugnisse geführt hätte, wurde im Gegenteil festgestellt, dass die rechtlichen Grundlagen dem rechtlich zuvor fraglichen Vorgehen angepasst werden. Mit Blick auf polizeiliche Überwachungs- und Ermittlungsmaßnahmen lässt sich ein ähnliches Bild zeichnen: Das prognostische Versprechen von KI und der automatisierten Auswertung von großen Datenmengen ist unter dem Titel „Predictive Policing" auch in Deutschland im Einsatz, es wird mit automatischer Gesichtserkennung experimentiert (vgl. Galla 2020; Meyer 2020) und auch

---

4 Zu post-/kolonialen Datenregimes im gängigen Wortsinn vgl. den Beitrag von Isin & Ruppert (2019).

5 Bei Dander (2020) findet sich eine Einführung in grundlegende Marx'sche Kategorien sowie ihre Anwendung auf Zusammenhänge von Big Data Analytics am Beispiel von Social Network Sites.

auf EU-Ebene spielen Daten- und Informationssysteme eine wichtige Rolle, etwa in der Überwachung von Migrationsbe-wegungen (vgl. Monroy 2020).

International wird auf das sich anhaltend im Aufbau befindliche Sozialkreditsystem in der Volksrepublik China verwiesen, das als das umfassendste staatliche *Social Scoring* Projekt gilt und dem etwa im Sammelband „Super-Scoring?“ ein thematischer Abschnitt gewidmet ist (vgl. Gapski/Packard 2021). Eine Besonderheit dieses Systems gegenüber europäischen oder nordamerikanischen Bonitätssystemen scheint seine Eigenschaft als Meta-System, welches mehrere Untersysteme umfasst und künftig weitere Überwachungs- und Kontrollprojekte integrieren kann. Während etwa die SCHUFA in Deutschland zum einen privat organisiert ist und zum anderen mit Kreditauskünften einen relativ beschränkten Funktionsbereich bedient, ist das chinesische Meta-System integrativ und transversal verfasst (vgl. Liang u. a. 2018; Ohlberg 2021).

In gesellschaftlichen Teilbereichen finden sich im ‚globalen Norden‘ auch jenseits von Nachrichtendiensten und Strafermittlungsbehörden besorgniserregende Einsätze, etwa im Bereich der Bildung und der Sozialen Arbeit (vgl. Andrejevic/Selwyn 2020; Kutscher 2021), im Sozial- und Fürsorgesektor (vgl. Eubanks 2017; Redden u. a. 2021) oder auch im Umgang mit Erwerbslosen, etwa in Österreich (vgl. Berner/Schüll 2020). Den genannten Analysen ist weithin gemein, dass die verschiedenen Überwachungs- und Kontrolltechnologien nicht nur zu einer panoptischen Atmosphäre führen, die hochgradig von Intransparenz und, seitens der staatlichen Agenturen, vom Mythos der Objektivität geprägt ist, sondern bestehende Ungleichheiten fortschreiben oder neue Diskriminierungsformen hervorbringen.

2.3. Hybride Datenpolitiken

Ein genauerer Blick auf einzelne Einsatzszenarien legt offen, dass die Trennlinie zwischen kapitalistischen und staatlichen Datenpolitiken nicht so scharf gezogen werden kann, wie die Formulierungen suggerieren. So greifen staatliche Akteure vielfach auf kommerzielle Software zurück, wie an einigen Beispielen gezeigt wird. Prominent in der Öffentlichkeit wurden etwa der Einsatz von kommerziellen Prüfungsmanagement- und -überwachungssystemen an Hochschulen, wie jenes von *Proctorio*, insbesondere im angelsächsischen Raum, diskutiert und problematisiert (vgl. Swauger 2020). Kommerzielle Gesichtserkennungssoftware des Unternehmens *Clearview AI* kommt bspw. in den USA in der Strafverfolgung zum Einsatz (vgl. Marks 2021). Schließlich sorgte der Fall des Unternehmens *Cambridge Analytica* für einen Skandal, als über die scheinbar wahlentscheidenden, personalisierten Datenanalysepraktiken und ihren Einsatz 2014-2016 im US-Präsidentschafts(vor)wahlkampf berichtet wurde (vgl. Richterich 2018; Bridle 2019, S. 17).

Umgekehrt schaltet sich der Staat etwa durch gesetzliche Regulierung in die Gestaltung kapitalistischer und nicht-kommerzieller Datenpolitiken ein. Ende 2020 verabschiedeten bspw. die InnenministerInnen der EU-Mitgliedstaaten eine Entschließung, die als Angriff auf verschlüsselte Kommunikation gewertet werden kann (vgl. Krempl 2020). In Deutschland kann das Netzwerkdurchsetzungsgesetz (NetzDG; novelliert im März 2021) als Beispiel genannt werden, das den Umgang der (großen) Social Media Plattformen etwa mit strafbaren Inhalten reguliert (vgl. Eickelmann u. a. 2017; Bundesamt für Justiz 2021). Ende 2020 hat die EU-Kommission (2020) mit dem „Daten-Governance-Gesetz" einen Vorschlag vorgelegt, der auf eine Vermittlung der Interessen von „Dateninhaber", „Datennutzer" und „Datenmittler" zielt. Dies soll einerseits unter Berücksichtigung von Datenschutz erfolgen, andererseits durch diese Regulierung die kommerzielle und nicht-kommerzielle Verwendung von personenbezogenen und Verwaltungsdaten stärken.[6]

Diese Beispiele machen deutlich, dass es sich bei den geschilderten Datenpolitiken ‚von oben' insofern oft um *hybride Datenpolitiken* handelt, als vielfach eine Verschränkung von kommerziellen und staatlichen Infrastrukturen, Technologien und Einsätzen vorliegt. Die Zielsetzungen unterscheiden sich freilich in ihrer primären Zielsetzung auf Kapitalakkumulation einerseits und auf die konkrete Zielbestimmung der staatlichen Akteure andererseits (‚Sicherheit' und ‚Gefahrenabwehr', ‚Bildung', usw.).

3. Datenpolitiken ‚von unten': Datenaktivismus und Data Justice

In jede Datensammlung gehen Verhalten, Gefühlsausdrücke oder soziale Beziehungen konkreter Menschen ein. Ohne dieses Zusammenspiel ist Big Data nicht denkbar (vgl. Kaldrack/Köhler 2014, S. 1), ohne sie sind Datenpolitiken ‚von oben' nicht denkbar. Diese Beteiligung, dieses Verstrickt-Sein in die genannten Prozesse eröffnet stets die Möglichkeit der Gegenwehr, etwas anders oder nicht zu tun – bis hin zu kollektiven Bestrebungen, die Infra/Strukturen dieser Datenpolitiken zu beeinflussen oder zu verändern. Bigo et al. (2019, S. 6) formulieren als eine Annahme in der Einleitung zu ihrem Sammelband "Data Politics":

---

6 U.a. ist in diesem Vorschlag von „Datengenossenschaften" die Rede, welchen in etwa die Rolle einer Interessensvertretung, Beratungs- und Ombudsstelle im Interesse von Einzelpersonen und kleineren Unternehmen zukommen soll (Europäische Kommission 2020, S. 20–21). Die konkrete Ausgestaltung bleibt abzuwarten. Ebenfalls angeführt wird im Dokument der Ausdruck „Datenaltruismus", mit welchem die freiwillige Freigabe von personenbezogenen Daten für gemeinwohlorientierte Nutzungsformen, wie etwa Forschungszwecke, bezeichnet wird (ebd., S. 27 sowie S. 23). Für den Hinweis auf diesen Vorschlag der EU-Kommission gilt Theo Hug herzlicher Dank!

> "that the production of data is a social and often political practice that mobilises agents who are not only objects of data (about whom data is produced) but that they are also subjects of data (those whose engagement drives how data is produced). Our question thus shifts to social practices and agents."

In diesem Zitat wird deutlich, dass die Perspektive der AutorInnen auf Datenpolitiken von einer weiteren Annahme getragen wird: Datenpraktiken wohnt eine performative Kraft inne, die in ihrem Tun jene Strukturen von Wissen und Macht erzeugt, reproduziert und verändert, die in Kap. 2 so hermetisch und allmächtig erschienen (vgl. ebd., S. 4). Eine Subjektposition, die diese Handlungsmacht im eigenen Tun anerkennt und zu nutzen sucht, ist jene von DatenaktivistInnen.

Was in der Literatur als Datenaktivismus beschrieben wird, ist in enger Verbindung mit früheren Varianten eines Informations- und Cyberaktivismus, Hacktivism und anderen medienaktivistischen Spielarten zu begreifen (vgl. Milan/van der Velden 2016, S. 60–61; Sützl/Hug 2012). Im Datenaktivismus werden zwei Varianten unterschieden (siehe hierzu auch den Beitrag von Neuschäfer in diesem Band):

Die erste Form fasst Miren Gutiérrez (2018, S. 63) als *proaktiven Datenaktivismus* zusammen und versteht darunter Formen zivilgesellschaftlicher Betätigung wie das datengestützte Erzählen und Verbreiten unkonventioneller Narrative auf der Grundlage unabhängiger Recherchen und mit dem Ziel alternative (digitale) Öffentlichkeiten zu schaffen (vgl. ebd., S. 63–64), um soziale Ungerechtigkeiten anzuprangern und sozialen Wandel herbeizuführen (vgl. Milan/van der Velden 2016, S. 67). Die zweite Form, *reaktiver Datenaktivismus*, entspricht u.a. dem Modell digitaler Selbstverteidigung: "activists react to exogenous threats trying to defend their values, beliefs and practices and/or underminde those dynamics and mechanisms they reject" (ebd.). Beide datenaktivistische Formen beinhalten individuelles wie kollektives Tun und basieren auf einer involvierenden, anwendungsbezogenen ‚hands-on'-Auseinandersetzung von Information und Technologie als "objects of intervention".

Lina Dencik, Arne Hintz und Jonathan Cable (2016) bringen den Ausdruck "Data Justice" in die Debatte ein, um damit auch in überwachungskritischen Kontexten die Relevanz sozialer Gerechtigkeit herauszustellen. Diese thematische Verbindungslinie erachten sie als bedeutsam, da sie eine Trennung zwischen der Beschäftigung mit der Überwachungsthematik und anderen, breiter angelegten Themen sozialer Gerechtigkeit beobachten. (vgl. ebd., S. 8) Data Justice ist so angelegt, dass der gesellschaftliche Felder durchziehende Charakter datenbezogener Kampfzonen hervortritt:

> "[H]ow society is and *ought to be* organized in relation to digital infrastructures – on social, political, economic, cultural and ecological terms – that can consider and develop the meaning of justice in this context. This would include questions of how to think about notions such as security,

> autonomy, dignity, fairness and sustainability in a data-driven society and make us ask what, for example, the implications are for workers' rights, or for community cohesion and discrimination; for welfare and inequality; or for the environment, for poverty, and for conflict. Most importantly, advancing this agenda would transform surveillance from a special-interest 'issue' into a core dimension of social, political, cultural, ecological and economic justice, and thus respond to the central position of data-driven processes in contemporary capitalism." (ebd., S. 9; Herv. im Orig.)

Eine ähnliche Stoßrichtung verfolgen Catherine D'Ignazio und Lauren F. Klein in ihrem Buch "Data Feminism" (2020). Sie sprechen zwar von Feminismus, explizieren aber zu Beginn, dass sie darin im Sinne eines intersektionalen Ansatzes das Anliegen aufgehoben sehen, jegliche gesellschaftliche Ungleichheit zu bekämpfen – egal, ob in Bezug auf gender, "race, class, ability, and more." Sie sehen sich in diesem Anliegen der Idee der "co-liberation" verpflichtet, welche Herrschaftssysteme als schädlich für alle Menschen und Befreiung als ein relationales Geschehen zwischen allen in Machtbeziehungen verstrickten begreift (vgl. ebd.).

Die Autorinnen strukturieren ihr Konzept von Datenfeminismus wie auch ihr Buch anhand von sieben Prinzipien, die einen Überblick über ihren Ansatz vermitteln: Macht(strukturen) untersuchen, Macht(strukturen) herausfordern, Gefühle und verkörperte Wissensformen anerkennen, Binaritäten und Hierarchien überdenken, Pluralitäten (z.B. von Perspektiven) einbeziehen, Kontext beachten, Arbeit sichtbar machen (vgl. ebd.; Übers. VD).

Im letzten Abschnitt geht es schließlich um die Aufforderung: "Let's multiply now." (ebd., Conclusion), wobei anhand einiger Kampagnen und Initiativen aufgezeigt wird, welche Ver/Handlungsmacht kollektive Kämpfe gegen datenbasierte Ungerechtigkeiten an den Tag legen können; insbesondere, wenn die ArbeiterInnen, die unabkömmliche Rollen in digitalen Infrastrukturen einnehmen, selbst aktiv werden oder ihre Arbeit niederlegen. So wird bspw. die Geschichte von Streikenden bei Google im Jahr 2018 erzählt, die auf Berichte über sexuelle Belästigung reagierten und strukturelle Änderungen im Unternehmen einforderten. Weiters wird auf eine Plattform verwiesen, die Gig-Workern ermöglicht, sich zur Verbesserung ihrer Arbeitsbedingungen zu organisieren (*Coworker.org*). Die *design justice group* verweist auf bildungsbezogene Fragen, insofern Workshops und Bildungsforen zu ihren Aktivitätsformen gehören, in denen DesignerInnen für Ungleichheiten in Designentscheidungen sensibilisiert werden. Als Beispiel aus dem deutschsprachigen Kontext kann das *Berliner Register* zur Dokumentation von u.a. rassistischen, antisemitischen, homo- und transphoben Übergriffen eingebracht werden. Das Register speist sich aus einzelnen Meldungen, die über Polizeiberichte deutlich hinausreichen und eröffnet verschiedene Niveaus der Beteiligung und Ermächtigung (vgl. Dander/Macgilchrist i.E.; Kap. 5).

Gleichwohl sind datenaktivistische oder -feministische Praktiken vielfach stärker unter solchen Personengruppen vertreten, die sich durch tiefreichende technische und andere Kenntnisse und Fertigkeiten, mitunter durch einen hohen Bildungsgrad und einen gesicherten sozio-ökonomischen Status auszeichnen, wie am Beispiel von Open Data AktivistInnen in Deutschland festgestellt wurde (vgl. Dander 2014, S. 125; Baack 2015, S. 8). Wenn Stefan Baack diese (Open Data) Eliten oder ExpertInnen als "empowering intermediaries" beschreibt (2015, S. 6), beinhaltet die Bezeichnung eine aktive Auseinandersetzung und den Einbezug von nicht-expertisierten BürgerInnen. Dadurch werden sie zu "important supporters of agency in datafied publics." (ebd.) Hierin deutet sich etwas an, was D'Ignazio und Klein (vgl. 2019, Kap. 2) als einen zentralen Aspekt des Prinzips ‚Macht(strukturen) herausfordern' formulieren: Machtstrukturen und asymmetrische Wissensbestände sollen auch innerhalb aktivistischer Gruppen und Netzwerke herausgefordert werden. Der Schlüssel dafür liegt in einem pädagogischen Verhältnis, einer Kultur des gemeinsamen Lernens von relevanten Fähigkeiten – ‚Data Literacy' – auf dem Weg zu einer ‚Digital Citizenship'.

4. Mit *(Critical Big) Data Literacy/-ies* zu *Digital/Data Citizenship*

Data Literacy erweist sich in seiner Verwendung, in der Literatur und Forschungslandschaft als schillernder Begriff, der von verschiedenen AkteurInnen und Disziplinen auf sehr verschiedene Weise modelliert und eingesetzt wird (vgl. Dander 2018, S. 77–78). Der Schwerpunkt liegt hier auf zwei Linien, deren Differenz quasi analog zur Unterscheidung von proaktivem und reaktivem Datenaktivismus verläuft:

Proaktiver Datenaktivismus verlangt insbesondere nach einem Bündel von Fähigkeiten, welche die produktive Arbeit mit Daten (generieren, finden, bereinigen, analysieren, interpretieren, visualisieren) und die öffentliche Kommunikation von Ergebnissen in den Vordergrund rücken. Diese Variante von Data Literacy findet sich etwa in Modellen, die im Kontext von Open Data Initiativen Anwendung finden (vgl. Dander/Macgilchrist i.E.; Deahl 2014). *Reaktiver Datenaktivismus* erfordert insbesondere einen versierten Umgang mit Techniken des Anonymisierens, Verschleierns und Verschlüsselns, wie sie von überwachungskritischen Tech-ExpertInnen etwa in Cryptoparties einem breiteren Publikum nähergebracht werden (vgl. https://www.cryptoparty.in). In seinen technisch versiertesten Formen beziehen beide Varianten das Programmieren oder Modifizieren von Software mit ein: etwa für die Datenanalyse oder -visualisierung einerseits, andererseits für Zwecke des Datenschutzes und der Datensicherheit.

Doch gehen einige Konzepte über technisches Wissen und Können hinaus.[7] Ina Sander (2020, S. 3; Herv. im Original) etwa schlägt einen eher *reaktiv* ausgerichteten Ansatz vor:

> "*critical big data literacy* in practice should mean an *awareness*, *understanding* and ability to *critically reflect upon big data collection practices, data uses and the possible risks and implications* that come with these practices, as well as the *ability to implement* this knowledge for a *more empowered internet usage*."

Mit diesem Konzept zielt Sander auf ein breiteres Publikum, auch jenseits von ExpertInnen oder Bildungsinstitutionen, und bezieht explizit Aspekte eines kritischen Denkens in liberaler angelsächsischer Tradition ohne moralische Aufladung ein (vgl. ebd., S. 4). Wenngleich eingeräumt wird, dass individuelle Verantwortung zur Bearbeitung der Problematik datafizierter Umwelten nicht ausreicht, legt die Konzeption einen Schwerpunkt auf lehr- und erlernbares individuelles Können und Wissen, um als handelndes Subjekt entscheidungs- und handlungsfähig zu werden (vgl. ebd., S. 4–5). Über rein technische Fertigkeiten digitaler Selbstverteidigung reicht Critical Big Data Literacy hinaus, insofern der strukturellen Dimension von Big Data hohe Relevanz zugeschrieben wird (vgl. ebd., S. 4).

Einen in mehrfacher Hinsicht differenten, *proaktiven* Ansatz wählt Aristea Fotopoulou (vgl. 2020), indem zum einen zivilgesellschaftliche Organisationen AdressatInnen der im Projekt durchgeführten und untersuchten *Datahub Workshops* waren und zum anderen konsequent von der Singularform ‚Data Literacy' abgesehen wird. Stattdessen betont Fotopoulou den transversalen Charakter von Literacies und hält fest: "data literacies should be understood as 'social literacies', because of the real-life material conditions within which learning takes place […]." (ebd., S. 3)

Die Gruppen und Organisationen, mit denen gearbeitet wurde, weisen thematisch keinen überwachungskritischen Schwerpunkt und kaum datenbezogene Expertise auf. Die *Datahub Workshops* beinhalteten neben allgemeinen Aspekten wie dem Verhältnis von Daten und Wissen insbesondere datenanalytische bzw. -journalistische Fähigkeiten, wie u.a. das Finden, Bereinigen, Analysieren, Visualisieren und Narrativieren von Daten sowie ihren Einsatz in Kampagnen. Der Ablauf der Workshops und die einbezogenen Workshopmodule weisen damit große Schnittmengen mit der Arbeit von Open Data Projekten wie der Datenschule in Berlin auf. Die dort genutzte "data pipeline" entspricht in etwa diesem Workflow (vgl. Dander/Macgilchrist i.E., Kap. 4). Deutlicher als die *data pipeline* stellt Fotopoulou aufgrund der Studienergebnisse heraus, dass sich diese (eher

[7] Auch hier finden nur wenige ausgewählte Konzeptionen Eingang. Mit verschiedenen Schwerpunktsetzungen kann an anderen Stellen über Literacy-Konzepte weitergelesen werden: z.B. zu Daten und Infrastrukturen (vgl. Gray u. a. 2018), personenbezogenen Daten (vgl. Pangrazio/Selwyn 2019) oder Online-Privatheit (vgl. Trepte/Masur 2015).

instrumentellen) Data Literacies in den Workshops mit "critical awareness about the ideological and power aspects of data" verbinden ließen (Fotopoulou 2020, S. 15).

Ähnlich wie Fotopoulou fokussieren Carmi, Yates, Lockley und Pawluczuk (vgl. 2020, S. 11) in ihrer Konzeption von Data Literacy (hier im Kontext von *dis-/mis-/mal-information*) community-basierte Fähigkeiten "beyond the individual." Sie schreiben in diesem Zusammenhang von "'networks of literacy', meaning how people engage with others, where and with which media to gain the understanding, skills and competencies in a way that fits them." (ebd., S. 12) Individualisierenden und instrumentalisierenden Konzeptionen von Data Literacy attestieren sie hingegen problematische ideologische Lagerungen (vgl. ebd. S. 9–10). Wie Sander argumentieren sie für eine kritische Haltung gegenüber algorithmischen Systemen und digitalen Datenökonomien (ebd., S. 13), die über technische Fertigkeiten hinausreicht. Schließlich betten sie ihre Überlegungen zu Data Literacy/-ies in eine übergreifende Konzeption von "data citizenship" (ebd., S. 15) ein, welche anhand der Dimensionen *Data thinking*, *Data doing*, *Data participation* (vgl. ebd., S. 10) auf eine aktive BürgerInnenrolle abzielt: "proactive skills to protest, object, unionise and conduct other collective actions against various civic issues." (ebd., S. 15)

Konzeptionen von (Critical Big) Data Literacy/-ies ließen sich probeweise anhand der folgenden Ebenen differenzieren:

(1) *Re/Aktivität* (proaktiver/reaktiver Schwerpunkt)

(2) *AdressatInnen/Subjekt des Lernens* (nicht-/expertisierte Individuen oder Kollektive wie zivilgesellschaftliche Organisationen, Communities etc.)

(3) *Normativität/Politizität* (Gleichheit, Inklusion, Data Justice oder ‚nur' kritisches Denken)

(4) *Bildungskontext* (formal, non-formal, informell)

(5) *Themenschwerpunkte* (Technik und Überwachung und/oder nicht-technische Themen)

(6) *Datenarten* (Schwerpunkt auf Open Data, personenbezogene Daten etc.)

(7) *Konzeptionelle Kontextualisierung* (alleinstehende Fähigkeit oder relational zu anderen Fähigkeiten und Konzepten)

(8) *Lokalisierung* (lokale und/oder supra-/nationale bzw. globale Datenassemblages)

5. Politische Medienbildung zu einem *Ignorant Digital/Data Citizen*?

Sofern Data Literacy/-ies nicht auf das engere Terrain medienpädagogischer Überlegungen beschränkt gedacht wird/werden, sondern in enger Verzahnung mit Politischer Bildung und mit einer politischen Subjektivität in Form von Digital oder Data Citizens, liegt es nahe, auf den genannten Ebenen sowohl den relationalen Charakter von

datenbezogenen Politiken zu verschiedenen Themen, verschiedenen Datenarten, Fähigkeiten/Kompetenzen und Relevanzebenen (lokal, global) zu berücksichtigen als auch den performativen Charakter von Data Literacy/-ies und Digital Citizenship. Demnach müssten Bildungskontexte eröffnet werden, die konkrete, relevante (daten)politische Fragen zumindest auch proaktiv bearbeiten. Letzteres kann in Auseinandersetzung mit zivilgesellschaftlichen Organisationen, aber genauso in formalen Bildungskontexten stattfinden.

Gestärkt wird ein solcher Ansatz durch eine aktualisierte Konzeption von Digital Citizenship, wie in Hintz, Dencik und Wahl-Jorgensen in ihrem Buch "Digital Citizenship in a Datafied Society" erarbeiten (2018, S. 40): Die Subjektposition des Digital Citizen wird demnach durch Datenpolitiken ‚von oben' wie ‚von unten' ko-konstituiert:

> "Digital citizenship is […] constituted, partly, through the enactment of users but also, partly, through data analysis by the state and the private sector. Digital citizens, we argue, are both self-constructed and created by new (the data-driven economy) and traditional (the state) institutions."

Offen bleibt bis hier der oben genannte Aspekt der *Normativität/Politizität* in Data Literacies, der freilich stark von der paradigmatischen Positionierung abhängt. Wird diesbezüglich – ähnlich wie etwa bei Hintz et al. (vgl. ebd., S. 22 ff.) – ein an neuerer politischer Philosophie geschulter Zuschnitt gewählt, der sich von liberalen Ansätzen abgrenzt, lässt sich eine mehr oder minder universelle Zielsetzung wie Gleichheit begründen.[8]

Gert Biesta (2011) stellt – ohne explizite Bezüge zu digitalen Technologien – das Konzept eines "Ignorant Citizen" zur Diskussion. Er begründet es in Auseinandersetzung mit dem Denken von Chantal Mouffe und Jacques Rancière in den Unbestimmtheiten und Dynamiken politischer Ordnungen und, damit einhergehend, mit der Unbestimmtheit dessen, was 'a good citizen' sein sollte, obwohl für Mouffe, Rancière und Biesta gleichermaßen die Prinzipien Freiheit und Gleichheit die Stoßrichtung des demokratischen Projekts darstellen:

> "The ignorant citizen is the one who is ignorant of a particular definition of what he or she is supposed to be as a 'good citizen.' The ignorant citizen is the one who, in a sense, refuses this knowledge and through this, refuses to be domesticated, refuses to be pinned down in a pre-determined civic identity." (ebd., S. 152)

In Konsequenz bedeutete das für Lernen und (Politische) Bildung, dass sie sich keineswegs in der Aneignung von Kompetenzen erschöpfen können, sondern als "an

---

[8] Am Beispiel von Open Data Projekten wird in einem anderen Zusammenhang für eine "ethics of care" argumentiert, welche für konkrete lokale, community-basierte Kontexte eine ähnliche Stoßrichtung aufweist (vgl. Wylie u. a. 2019).

inherent dimension of the ongoing experiment of democratic politics" (ebd.) gedacht werden sollten. Dies könne nicht als ein rein kognitives Unterfangen umgesetzt, sondern lediglich als leidenschaftliches, lustvolles und sehnsüchtiges Geschehen (vgl. "desire for democracy"; ebd.) unterstützt werden. Ich halte es für ein relevantes Unterfangen die Rolle eines *Ignorant Digital/Data Citizen* ernst zu nehmen und um über Prozesse Politischer Medienbildung jenseits von Kompetenzmodellen und domestizierenden Festschreibungen nachzudenken.

Literatur

Andrejevic, Mark & Selwyn, Neil (2020): Facial recognition technology in schools: critical questions and concerns. *Learning, Media and Technology*, 45 (2), S. 115–128, doi: 10.1080/17439884.2020.1686014.

Baack, Stefan (2015): Datafication and empowerment: How the open data movement re-articulates notions of democracy, participation, and journalism. *Big Data & Society*, 2 (2), S. 1–11, doi: 10.1177/2053951715594634.

Beckedahl, Markus & Meister, Andre (Hrsg.) (2013): *Überwachtes Netz. Edward Snowden und der größte Überwachungsskandal der Geschichte*. Berlin: Newthinking Communications.

di Bella, Sam (2019): Book Review: The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power by Shoshana Zuboff. LSE Review of Books, 4. November 2019. Abgerufen unter: https://blogs.lse.ac.uk/lsereviewofbooks/2019/11/04/book-review-the-age-ofsurveillance-capitalism-the-fight-for-the-future-at-the-new-frontier-of-power-byshoshana-zuboff/ [Stand vom 09-07-2021].

Berner, Heiko & Schüll, Elmar (2020): Bildung nach Maß. Die Auswirkungen des AMS-Algorithmus auf Chancengerechtigkeit, Bildungszugang und Weiterbildungsförderung. *Magazin erwachsenenbildung.at*, pedocs, (40).

Biesta, Gert (2011): The Ignorant Citizen: Mouffe, Rancière, and the Subject of Democratic Education. *Studies in Philosophy and Education*, 30 (2), S. 141–153, doi: 10.1007/s11217-011-9220-4.

Bigo, Didier; Isin, Engin & Ruppert, Evelyn (2019): Data Politics. In: Bigo, Didier; Isin, Engin F. 6Ruppert, Evelyn Sharon (Hrsg.): *Data politics: worlds, subjects, rights*. Abingdon, Oxon; New York, NY: Routledge, S. 1–17.

Boyd, Danah 6 Crawford, Kate (2012): Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, communication & society*, 15 (5), S. 662–679.

Bridle, James (2019): State to stateless machines. A trajectory. In: Colakides, Yiannis; Garrrett, Marc & Gloerich, Inte (Hrsg.): *State machines: reflections and actions at the edge of digital citizenship, finance, and art*. Amsterdam: Institute of Network Cultures, S. 14–21.

Bröckling, Ulrich & Feustel, Robert (2012): Einleitung: Das Politische denken. In: Bröckling, Ulrich & Feustel, Robert (Hrsg.): *Das Politische denken. Zeitgenössische Positionen*. 3., unv. Aufl. Bielefeld: transcript, S. 7–18.

Bundesamt für Justiz (2021): *NetzDG – Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken. gesetze-im-internet.de*, Abgerufen unter https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html [Stand vom 03-05-2021].

Bundestag der BRD (2021): Gesetz zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts. *Bundesgesetzblatt Teil I*, (17), S. 771.

Carmi, Elinor; Yates, Simeon J.; Lockley, Eleanor & Pawluczuk, Alicja (2020): Data citizenship. Rethinking data literacy in the age of disinformation, misinformation, and malinformation. *Internet Policy Review*, 9 (2). https://doi.org/10.5210/fm.v25i7.10847

Couldry, Nick & Mejias, Ulises Ali (2019): *The costs of connection: how data is colonizing human life and appropriating it for capitalism*. Stanford, California: Stanford University Press.

Dander, Valentin (2014): Datendandyismus und Datenbildung. Von einer Rekonstruktion der Begriffe zu Perspektiven der sinnvollen Nutzung. In: Ortner, Heike; Pfurtscheller, Daniel; Rizzolli, Michaela & Wiesinger, Andreas (Hrsg.): *Datenflut und Informationskanäle*. Innsbruck: Innsbruck University Press, S. 113–129.

Dander, Valentin (2018): Medienpädagogik im Lichte | im Schatten digitaler Daten. Manteltext. In: *MedienPädagogik: Zeitschrift für Theorie und Praxis der Medienbildung*, S. 1–134, doi: 10.21240/mpaed/diss.vd.01.X.

Dander, Valentin (2020): Grundzüge einer Kritischen Politischen Ökonomie von Big Data Analytics – und ihre bildungstheoretischen Implikationen. In: Iske, Stefan; Fromme, Johannes; Verständig, Dan & Wilde, Katrin (Hrsg.): *Big Data, Datafizierung und digitale Artefakte*. Wiesbaden: Springer Fachmedien, S. 75–95.

Dander, Valentin & Macgilchrist, Felicitas (i.E.; geplant für 2021): School of Data and shifting forms of political subjectivity. In: Bettinger, Patrick (Hrsg.): *Educational Perspectives on Mediality and Subjectivation. Discourse, Power and Analysis*. London: Palgrave Macmillan.

DAV – Deutscher Anwaltverein (2021): *DAV-Stellungnahme 23/21 zur Änderung des BND-Gesetzes*. Dipl.-Jur. Jens Usebach LL.M │Rechtsanwalt & Fachanwalt │Kündigungsschutz & Arbeitsrecht, Abgerufen unter https://www.jura.cc/rechtstipps/dav-stellungnahme-23-21-zur-aenderung-des-bnd-gesetzes/ [Stand vom 30-04-2021].

Deahl, Erica Sachiyo (2014): *Better the Data You Know. Developing Youth Data Literacy in Schools and Informal Learning Environments*. Master Thesis Cambridge, Massachusetts: MIT Massachusetts Institute of Technology.

Dencik, Lina; Hintz, Arne & Cable, Jonathan (2016): Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society*, 3 (2), S. 205395171667967, doi: 10.1177/2053951716679678.

D'Ignazio, Catherine & Klein, Lauren F. (2020): Introduction. In: dies., *Data feminism*. Cambridge, Massachusetts: The MIT Press. Abgerufen unter: https://data-feminism.mitpress.mit.edu/pub/frfa9szd/release/4 [Stand vom 14-05-2021].

Dörre, Klaus (2009): *Die neue Landnahme. Dynamiken und Grenzen des Finanzmarkt-Kapitalismus.* Paper für die gemeinsame Tagung „Kapitalismustheorien" von ÖGPW und DVPW, Sektion Politik und Ökonomie Wien.

Eickelmann, Jennifer; Grashöfer, Katja & Westermann, Bianca (2017): #NETZDG #MAASLOS. *Zeitschrift für Medienwissenschaften*, 9 (17–2), S. 176–185, doi: 10.14361/zfmw-2017-0218.

Eubanks, Virginia (2017): *Automating inequality: how high-tech tools profile, police, and punish the poor*. First Edition. New York, NY: St. Martin's Press.

Europäische Kommission (2020): *Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance* (Daten-Governance-Gesetz). Abgerufen unter: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX: 52020PC0767 [Stand vom 03-05-2021].

Fotopoulou, Aristea (2020): Conceptualising critical data literacies for civil society organisations: agency, care, and social responsibility. *Information, Communication & Society*, Routledge, S. 1–18, doi: 10.1080/1369118X.2020.1716041.

Foucault, Michel (2004): *Geschichte der Gouvernementalität. 1. Sicherheit, Territorium, Bevölkerung. Vorlesung am Collège de France 1977 - 1978*. 1. Aufl. Frankfurt am Main: Suhrkamp.

Galla, Nina (2020): KI in der Polizeiarbeit. Der Mythos vom vorhersagbaren Verbrechen. *CILIP*, (Bürgerrechte&Polizei/CILIP 121), S. 46–56.

Gapski, Harald & Packard, Stephan (Hrsg.) (2021): *Super-Scoring? Datengetriebene Sozialtechnologien als neue Bildungsherausforderung*. München: kopaed.

Gray, Jonathan; Gerlitz, Carolin & Bounegru, Liliana (2018): Data infrastructure literacy: *Big Data & Society* 5(2), S. 1–13, doi: 10.1177/2053951718786316.

Gutiérrez, Miren (2018): *Data activism and social change*. Cham: Palgrave Macmillan.

Himmelsbach, Sabine (2015): Poetics and Politics of Data. Die Ambivalenz des Lebens in der Datengesellschaft. In: Himmelsbach, Sabine & Mareis, Claudia (Hrsg.): *Poetics and Politics of Data: Die Ambivalenz des Lebens in der Datengesellschaft / The ambivalence of life in a data-driven society*. Basel: Christoph Merian Verlag, S. 25–41.

Hintz, Arne; Dencik, Lina & Wahl-Jorgensen, Karin (2018): *Digital citizenship in a datafied society*. Medford, MA: Polity Press.

Isin, Engin & Ruppert, Evelyn (2019): Data's Empire. Postcolonial data politics. In: Bigo, Didier; Isin, Engin F. & Ruppert, Evelyn Sharon (Hrsg.): *Data politics: worlds, subjects, rights*. Abingdon, Oxon; New York, NY: Routledge, S. 207–227.

Kaldrack, Irina & Köhler, Christian (2014): Das Datenhandeln – Zur Wissensordnung und Praxeologie des Online-Handels. In: *Mediale Kontrolle unter Beobachtung* 3 (1), 1-13. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-40019.

Krempl, Stefan (2020): Crypto Wars: EU-Staaten beschließen Resolution zu Entschlüsselung. *heise online*, Abgerufen unter: https://www.heise.de/news/Crypto-Wars-EU-Staaten-beschliessen-Resolution-zu-Entschluesselung-4988717.html [Stand vom 03-05-2021].

Kurz, Constanze (2021): Staatstrojaner im Gesetzentwurf: Mehr Befugnisse zur heimlichen „Online-Durchsuchung". *netzpolitik.org*, 26. Januar.

Kutscher, Nadia (2021): Ethische Dimensionen des Einsatzes von algorithmenbasierten Enscheidungen und Scoring in pädagogischen und sozialpolitischen Kontexten. In: Gapski, Harald & Packard, Stephan (Hrsg.): *Super-Scoring? Datengetriebene Sozialtechnologien als neue Bildungsherausforderung*. München: kopaed, S. 177–190.

Liang, Fan; Das, Vishnupriya; Kostyuk, Nadiya & Hussain, Muzammil M. (2018): Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure. *Policy & Internet*, 10 (4), S. 415–453, doi: https://doi.org/10.1002/poi3.183.

Luxemburg, Rosa (1970): Die Akkumulation des Kapitals. In: *Das Kapital. Kritik der Politischen Ökonomie. Band II*: *Der Zirkulationsprozeß des Kapitals*, Frankfurt am Main: Ullstein, S. 713–756.

Marchart, Oliver (2005): Der Apparat und die Öffentlichkeit. Zur medialen Differenz von „Politik" und „dem Politischen". In: Gethmann, Daniel& Stauff, Markus (Hrsg.): *Politiken der Medien*. Zürich-Berlin: Diaphanes, S. 19–38.

Marks, Paul (2021): Can the biases in facial recognition be fixed; also, should they? *Communications of the ACM*, 64 (3), S. 20–22, doi: 10.1145/3446877.

Meyer, Roland (2020): Ein unaufhaltsamer Aufstieg: Zur Geschichte der automatisierten Gesichtserkennung. *CILIP*, (Bürgerrechte&Polizei/CILIP 121), S. 57–66.

Milan, Stefania & van der Velden, Lonneke (2016): The Alternative Epistemologies of Data Activism. *Digital Culture & Society*, 2 (2), S. 57–74.

Monroy, Matthias (2020): 220 Abfragen pro Sekunde. Das Schengener Informationssystem wächst dynamisch. *CILIP*, (Bürgerrechte&Polizei/CILIP 121), S. 67–74.

Morozov, Evgeny (2014): *To save everything, click here: technology, solutionism and the urge to fix problems that don't exist*. London: Penguin Books.

Mouffe, Chantal (2015): *Agonistik. Die Welt politisch denken*. Bonn: Bundeszentrale für Politische Bildung (Lizenzausgabe).

Nachtwey, Oliver & Seidl, Timo (2017): Die Ethik der Solution und der Geist des digitalen Kapitalismus. *IfS Working Papers*. IfS – Institut für Sozialforschung an der Johann Wolfgang Goethe-Universität, S. 1–36.

Ohlberg, Mareike (2021): Sieben Punkte zu Chinas gesellschaftlichem Bonitätssystem. In: Gapski, Harald & Packard, Stephan (Hrsg.): Super-Scoring? *Datengetriebene Sozialtechnologien als neue Bildungsherausforderung*. München: kopaed, S. 53–65.

Pangrazio, Luci & Selwyn, Neil (2019): 'Personal data literacies': A critical literacies approach to enhancing understandings of personal digital data. *New Media & Society*, 21 (2), S. 419–437, doi: 10.1177/1461444818799523.

Redden, Joanna; Dencik, Lina; Hintz, Arne & Warne, Harry (2021): „Data Scores as Governance": Katalog und Analyse neuer Verwaltungsverfahren in Großbritannien. In: Gapski, Harald & Packard, Stephan (Hrsg.): *Super-Scoring? Datengetriebene Sozialtechnologien als neue Bildungsherausforderung*. München: kopaed, S. 111–118.

Reichert, Ramón (2014): Big Data: Medienkultur im Umbruch. In: Ortner, Heike; Pfurtscheller, Daniel; Rizzolli, Michaela & Wiesinger, Andreas (Hrsg.): *Datenflut und Informationskanäle*. Innsbruck: Innsbruck University Press, S. 37–54.

Richterich, Annika (2018): How Data-Driven Research Fuelled the Cambridge Analytica Controversy. *Partecipazione e conflitto*, 11 (2), S. 528–543, doi: 10.1285/i20356609v11i2p528.

Ruppert, Evelyn; Isin, Engin & Bigo, Didier (2017): Data politics. *Big Data & Society*, 4 (2), S. 2053951717717749, doi: 10.1177/2053951717717749.

Sander, Ina (2020): What is critical big data literacy and how can it be implemented? *Internet Policy Review*, 9 (2).

Sützl, Wolfgang & Hug, Theo (Hrsg.) (2012): *Activist Media and Biopolitics. Critical Media Interventions in the Age of Biopower*. Innsbruck: Innsbruck University Press.

Swauger, Shea (2020): Our Bodies Encoded: Algorithmic Test Proctoring in Higher Education. In: Critical Digital Pedagogy, Hybrid Pedagogy Inc. Abgerufen unter: https://hybridpedagogy.org/our-bodies-encoded-algorithmic-test-proctoring-in-higher-education/ 02 April 2020. [Stand vom 03-05-2021].

Trepte, Sabine & Masur, Philipp K. (2015): *Privatheitskompetenz in Deutschland. Ergebnisse von zwei repräsentativen Studien*. Stuttgart: Universität Hohenheim.

Wylie, Caitlin; Neeley, Kathryn & Ferguson, Sean (2019): Beyond Technological Literacy. Open Data as Active Democratic Engagement? In: Reichert, Ramón & Wenz, Karin; Abend, Pablo; Fuchs, Matthias & Richterich, Annika (Hrsg.): *Digital Culture & Society, Vol. 4, Issue 2/2018/ Digital Citizens*. Bielefeld: transcript, S. 157–181.

Zuboff, Shoshana (2019): *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. New York: PublicAffairs.

Datenaktivismus und Digital Citizenship

Anna-Maria Neuschäfer

Zusammenfassung

Im Beitrag wird das Konzept des Digital Citizenship vorgestellt. Unter Digital Citizenship versteht man gesellschaftliche Teilhabe über digitale Medien. Dahinter steht die Annahme, dass der Begriff des Digital Citizen gleichzeitig Medienkompetenzen als auch Handlungsräume beschreibt, die für Datenaktivismus von Interesse sind. Datenschutz ist ein abstraktes Schlagwort, weshalb unterschiedliche Ausprägungen und Möglichkeiten vorgestellt werden, wie man sich seiner eigenen Daten ermächtigen kann. Unabhängig davon, ob es sich um den Staat oder multinationale Konzerne handelt, besteht im Internet großer Bedarf an persönlichen Daten. Als mögliche Reaktionen auf Datensammlung werden Clicktivismus, politischer Konsum und Hacktivism auf Basis der Arbeit von Jordana J. George und Dorothy E. Leidner präsentiert.

1. Digital Citizenship

Bei Digital Citizenship handelt es sich um die Erweiterung Thomas Marshall's Citizenship Modell. (Klaus/Lünenborg 2004, S. 193; Klaus/Zobl 2019, S. 27–28) Sein dreidimensionales Modell unterteilt in Civil, Political und Social Citizenship. (Klaus/Lünenborg 2004, S. 193) Mit dem Konzept des Citizenship wird die Befähigung zur Freiheit, politischer Partizipation und ökonomischer Sicherheit[1] verstanden. (Marshall 1992, S. 10) Die deutsche Übersetzung ‚Staatsbürgerschaft' wird dem Citizenship nur unzureichend gerecht. (Kaun 2015, S. 182; Klaus/Lünenborg 2004, S. 194) Im Laufe der Zeit wurde das dreidimensionale Modell um die Kategorie des Cultural Citizenship ergänzt. Digital Citizenship kann als Unterordnung des Cultural Citizenship gesehen werden, einem Kernbereich der Cultural Studies. (Marchart 2018, S. 12)

Die Erweiterung um die Kategorie des Digital Citizenship fasst den Aspekt der Partizipation mit der Handlungsfähigkeit im Netz zusammen. Per Definition können Menschen, die täglich das Internet nutzen, als Digital Citizens gelten, allerdings reicht das Betreiben von Social-Network-Accounts dazu nicht aus. (Akarçeşme/Pachner/Prlić 2019, S. 6–7) Von Bedeutung ist, dass der digitale Austausch der gesellschaftlichen Teilhabe dient. (Lünenborg 2015, S. 257) Hintz et al. (2017, S. 731) fassen zusammen:

[1] Klaus und Lünenborg (2004, S. 194) führen die Gedanken Marshalls detaillierter aus und benennen für Civil Cititizenship die Freiheit der Person, Rede-, Gedanken-, Glaubens- und Pressefreiheit, die Freiheit des Eigentums sowie das Recht auf ein Gerichtsverfahren. Political Citizenship beinhaltet unter anderem das passive und aktive Wahlrecht. Ein staatliches Sozialsystem, welches Erziehungswesen und Wohlfahrt berücksichtigt, umfasst das Social Citizenship.

„Digital Citizenship is typically defined as the (self-)enactment of people's role in society through the use of digital technologies. It therefore has empowering and democratizing characteristics. "

Gerade der partizipative Charakter, beziehungsweise „doing citizenship"[2] wie es Dahlgren (2008, S. 282) nennt, verdeutlicht die Bedeutung des Rezipierens und Produzierens.

Die technologischen Rahmenbedingungen des Internet ermöglichen ein geändertes Mediennutzungsverhalten. Deutlich wird die neue Rolle des Internetusers durch die Wortkreuzung „produsage" von Axel Bruns (2008 zit. n. Deterding 2015, S. 377). Produsage, zusammengesetzt aus den englischen Wörtern produce und usage deutet auf die vielfältigen Gestaltungsmöglichkeiten von Onlineinhalten hin. Beispielhaft können hier Websites, Blogs und Wikis genannt werden, welche ebenfalls die Informationsbeschaffung der Internetnutzenden transformieren. Jugendliche stehen nicht nur mit den bisher genannten Onlineangeboten im Austausch, sie nutzen vor allem Soziale Netzwerke, um zu interagieren und produktiv zu sein. Jugendliche finden zudem über Soziale Medien Selbstbestätigung und können soziale Werte erlernen – beziehungsweise Elemente des Citizenship entwickeln. (Gleason/Gillern 2018, S. 201) Hier lassen sich Interferenzen zwischen Digital Citizenship und Medienpädagogik beschreiben. Medienpädagogik kann das verbindende Glied zwischen Digital Citizenship und einen selbstbestimmten, rücksichtsvollen Umgang mit Medien sein.

2. Datafizierung und Datenmonopole

Die Datafizierung der Privatsphäre mit ihren prognostischen und vorverurteilenden Mitteln kann negative Konsequenzen mit sich bringen. (Helbig 2016, o. S.) Dies bedeutet eine Machtasymmetrie zugunsten privatwirtschaftlich orientierter Internetunternehmen. Weitere Einschränkungen, wie die Entstehung von Datenmonopolen, Filterblasen, der Ausbau der Staatsmacht oder die Vorverurteilung von Personengruppen aufgrund von Daten, die über sie verfügbar sind, werden hier als Beispiele angeführt. Unternehmen wie Google, Facebook, Amazon und Apple schaffen durch Datenwirtschaft Netzwerkeffekte, von denen sie unzählige personale Daten abschöpfen. Dies ist nicht nur unangenehm für die Menschen, die nicht wissen, welche Daten von ihnen erhoben werden, es bedeutet auch einen Wettbewerbsnachteil für kleinere Unternehmen. Mit der Datafizierung hat sich auch die Relation zwischen diesen großen Institutionen und KonsumentInnen gewandelt. Unternehmen, die auf individuelle Bedürfnisse ausgerichtet sind, konnten sich im Internet durchsetzen. Es ist eine wechselseitige Abhängigkeit zwischen Internetnutzenden und den marktdominierenden Internetanbietern entstanden.

[2] Im gleichnamigen Artikel fordert Dahlgren eine intensivere Auseinandersetzung zwischen Kulturwissenschaften und Überlegungen zu Citizenship. (Dahlgren 2006, S. 282)

> Dabei „[…] benötigen sie große Mengen an personenbezogenen Daten, die entweder explizit von Nutzern zu Verfügung gestellt werden (etwa wenn diese ein Formular ausfüllen, um sich zu registrieren, das eigene Adressbuch hochladen, einen online Kalender nutzen, Bookmarks anlegen etc.) oder implizit, in ihre Handlungen beobachtet, aufgezeichnet und analysiert werden." (Stalder 2019, S. 105)

Diese Daten, die nicht nur Suchmuster und Kaufvorlieben umfassen, werden zugunsten von Werbeanzeigen und personalisierten Nachrichten erhoben. NutzerInnen finden sich nicht selten in einer Filterblase[3] wieder. Filter-Bubbles widersprechen der Mündigkeit des Digital Citizenship. Gerade für Jugendliche, deren Persönlichkeitsentwicklung noch im Entstehen ist, stellt die Filterblase eine Einschränkung von „Selbst- und Weltverhältnis und damit Bildungschancen und Entwicklungsoptionen" dar. (Zorn 2017, S. 23)

3. Ausbau der Staatsmacht und Vorverurteilung

Durch die Fragmentierung der Gesellschaft wird es für politische AkteurInnen immer schwieriger Menschen zu erreichen. Parteien können über Soziale Netzwerke sogenanntes Microtargeting vornehmen. Dabei erstellen Algorithmen über Informationen Sozialer Netzwerke Profile über die jeweiligen Personen. Im US-Wahlkampf 2016 wurden durch Microtargeting demokratische WählerInnen demobilisiert, um Donald Trump eine Stimmenmehrheit zu verschaffen.[4] Über Soziale Netzwerke, insbesondere Facebook, wurden in diesem Fall maßgeschneidert abschreckende Inhalte an WählerInnen zugespielt. (Ballweber/Dachwitz 2020, o.S.)

Diese Entwicklung basiert auf geänderter Mediennutzung, die mit einer Krise der staatlichen Einflussnahme einher geht. Denn lose gemeinschaftliche Zusammenschlüsse sind gegenwärtig eher temporär, weshalb es Autoritäten durch Online-Überwachung und Profiling ermöglicht wird, eine regierbare Zielgruppe zu definieren. (Hintz et al. 2017, S. 733) Dies stellt eine Diskrepanz in Hinsicht auf Bürgerrechte dar, da die staatliche Datenerfassung für BürgerInnen intransparent bleibt. (Hintz et al. ebd.) Diese Datensammlung ist vergleichbar mit dem Abschöpfen personenbezogener Daten durch Firmen. Big Data bedeutet auch die Kombination von gesundheitsbezogenen und ortsspezifischen Daten, aus denen beispielsweise die Kreditwürdigkeit Konsumierender abgeleitet wird. Diese Daten weisen Menschen eine zweite Identität zu. (Hintz et.al. 2017, S. 734) Es entsteht ein sogenanntes *Data-Double* (Poster 1990; Haggerty/Ericson 2000

[3] Filterblasen sind problematisch, weil damit unterschiedliche Ansichten und divergierende Informationen schwerer zugänglich gemacht werden. (Zorn 2017, S. 23)

[4] Netzpolitik.org bezieht sich mit dieser Information auf ein Leak, welches dem britischen TV-Sender Channel 4 vorgelegt wurde. Laut dieser Quelle wurden WählerInnen kategorisiert, um nicht unnötige Gelder in Wahlwerbung investieren zu müssen und möglichst effektiv Zielgruppen anzusprechen.

zit. n. Steinbicker 2019, S. 91) Hier werden durch die Rekombination von Daten statistische Gruppen konstruiert, die real nicht existieren, aber bei Betroffenen zu finanziellen Nachteilen führen können. (Nassehi 2019, S. 66)

4. Datenaktivismus

Digital Cititzenship impliziert eine produktive Teilnahme an politischer Meinungsbildung. Dazu ist die Nutzung von digitalen Medien charakteristisch. Jordana J. George und Dorothy E. Leidner vertreten die These, dass es mehrere Facetten des digitalen Aktivismus gibt. Um Onlineaktivismus mit traditionellem Aktivismus vergleichbar zu machen schlagen sie drei Stufen der Partizipation vor. Die Grafiken und Überlegungen im Artikel „from Clicktivsm to Hacktivism" lehnen sich an Milbraths Hierarchie zur Politischen Partizipation an. Er unterscheidet zwischen „spectator", „transitional" und „gladiatorial" activities. George und Leidner nennen ihre Pyramide „hierarchy of digital activism" und visualisieren damit nicht nur Milbraths adaptierte Version, sondern stellen auch ein Verhältnis von AktivistInnen und deren Handlungsfeldern her (s. Abb. 1).

Auf unterster Stufe sind es Beobachtende, die durch verhaltene Äußerungen – Clicktivism, Metavoicing und Assertion agieren. „Die Funktion des Teilens, die in der einfachsten Form ein Klick oder ein Retweet darstellt, ist Teil einer Partizipationskultur, die inzwischen den Eingang in die Wirtschaft gefunden hat" (Aigrain 2012 zit. n. Thimm 2017, S. 203) So lassen sich auf der zweiten Ebene der Hierarchie Menschen verorten, die bewusst Kaufentscheidungen treffen oder Firmen boykottieren, die mit ihren Ansichten nicht im Konsens stehen. (George/Leidner 2019, S. 8) Auf dieser Ebene werden außerdem Spendenaufrufe organisiert und Petitionen via digitaler Medien gestartet. Auf oberster Stufe befinden sich Aufdeckende, darunter HacktivistInnen[5] und DatenaktivistInnen. (vgl. George/Leidner 2019, S. 7) Datenaktivismus ist aufwändig und bedarf analytischer Kenntnisse. (Baack 2015) AktivistInnen, die sich für „open data" einsetzen, machen unter anderem Regierungsdaten zugänglich und müssen dementsprechend mit Sanktionen rechnen. (George/Leidner 2019, S. 10) Digitalem Aktivismus liegt ein Problembewusstsein zu Grunde. Ballenthien et al. (2015, S. 5) vertreten hingegen die Auffassung, dass sich zu wenige um Selbstdatenschutz kümmern „– weder gegenüber staatlichen noch gegenüber privatwirtschaftlichen Akteur_innen." Das Beispiel Social Media zeigt die Sorglosigkeit gegenüber Nutzungsbedingungen. Von denen behauptet Leistert (2016, S. 42), dass Terms of Services […] regelmäßig und ohne Ankündigung von Unternehmen

[5] Der Ursprung des Begriffs wird mit der Mitte der 90er Jahre angegeben und mit der Bildung der Hackergruppe „Cult of the Dead Cow" in Verbindung gebracht (Jordan/Taylor2004 zit.n. Füllgraf 2015, S. 81)

geändert [werden; Anm. AN.] sie werden von den Juristen/innen der Unternehmen ausschließlich im Sinne der Unternehmen formuliert […]“.

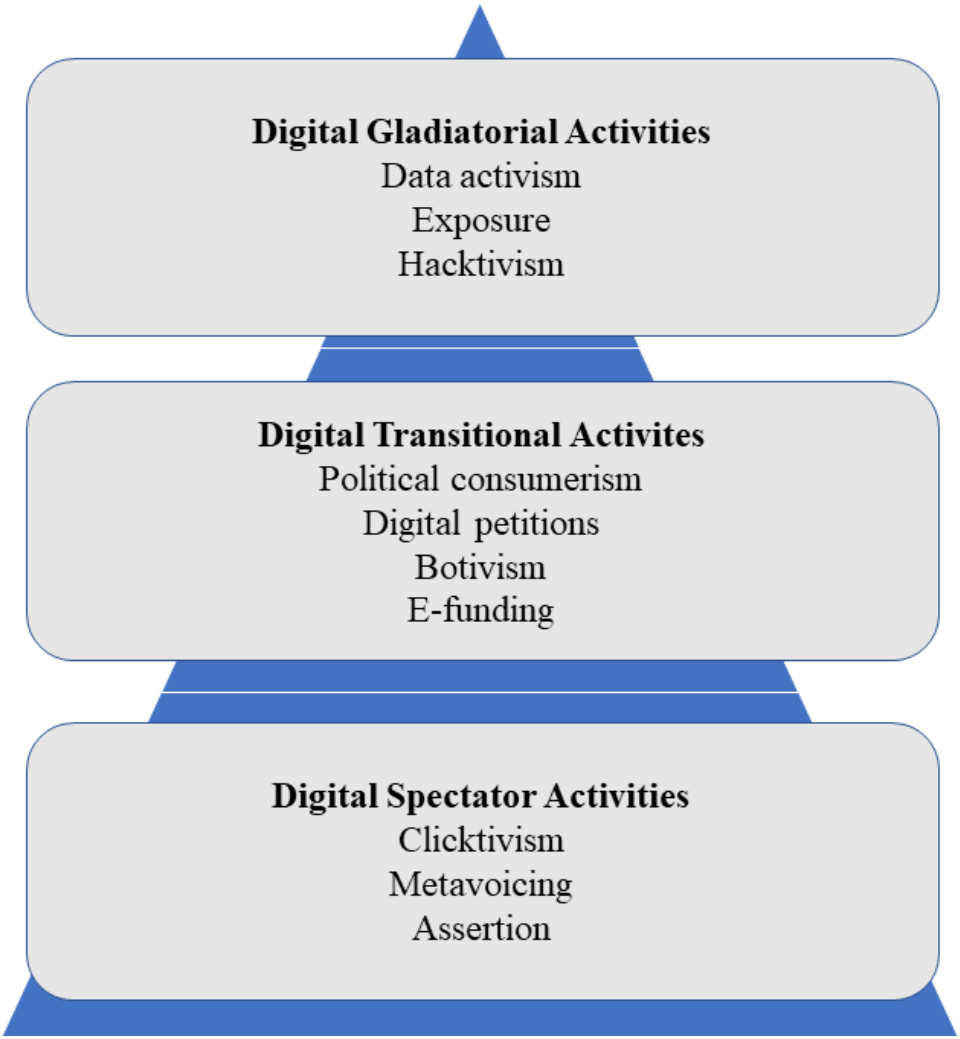


Abbildung 1: Hierarchy of digital activism (George/Leidner 2019: 7)

Verglichen mit den USA bietet das Europäische Datenschutzgesetz Privatpersonen mehr Schutz. In dieser europäischen Datenschutzgrundverordnung findet sich unter Artikel 4 das Verbot der Verarbeitung von personenbezogenen Daten. Im Wortlaut ist unter Paragraph 2 folgende Formulierung zu lesen:

> „das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;“ [von Daten ist untersagt. Anm. AN].

Allerdings ist der Staat laut Artikel 10 dieses Gesetzes zu Gunsten der Kriminalitätsbekämpfung zu jeglicher Einsichtnahme befähigt. Kriminalitätsbekämpfung ist ein weitreichendes Feld – das sehr viel Spielraum lässt.

5. Clicktivism

Clicktivism kann vielfältige Ausprägungen annehmen. In einem großen Netzwerk kann ein Click einer Influencerin, eines Influencers weitreichende Kreise ziehen. Inhalte sind per se Kommunikate, die kontextabhängig eine große Reichweite annehmen können. Ein gut verfasster Kommentar kann meinungsbildend auf die Netzgemeinde wirken. Dementsprechend einflussreich kann ‚political consumerism‘ werden. Wie zuvor angedeutet, werden hier Kaufentscheidungen durch persönliche Kriterien eines Digital Citizen getroffen. Diese Haltung kann, wenn sie im Internet viral geht, kommerzielle Organisationen beeinflussen. (George/Leidner 2019, S. 8) Wer sich näher mit Datenschutz auseinandersetzen möchte, aber nicht gerade ‚gladiatorial activities‘ beherrscht, kann sich einer größeren Interessensgemeinschaft anschließen. Eine solche europäische Initiative ist My Data.

My Data hat seinen Ursprung in unterschiedlichsten datenaktivistischen Vereinigungen. Die Non-Profit Organisation ist darin bestrebt eine zugängliche Art des Datenschutzes zu etablieren. Dabei ist die Partizipation im Internet obligatorisch, offline zu bleiben ist keine Option. Ausgehend von der Beobachtung, dass Datenschutzgesetze zu wenig bekannt und nur selten durchsetzbar sind, wird „Zugang, Richtigstellung, Portierbarkeit und das Recht auf Vergessenwerden als *Ein-Klick Rechte*“ (Poikola et al., 2020) gefordert. Man könnte eine Parallele zwischen Ein-Klick Rechten und der passiveren Gruppe an ClicktivistInnen (George/Leidner 2019, S. 5) ziehen. Denn das Lesen von umfangreichen Datenschutzvereinbarungen ist vielen NutzerInnen von Apps zu aufwändig und macht sie in Bezug auf ihre Daten gleichgültig. „Die direkte Convenience der Techniken digitaler Selbstvermessung scheint in vielen Fällen also schwerer zu wiegen als die abstrakten Nachteile, die

in Form geteilter Daten durch die Nutzung dieser Techniken entstehen könnten." (Leger/Panzitta/Tiede 2018, S. 35)

Dennoch versucht My Data allen Nutzenden Autonomie über die Entscheidung zurückzugeben, was mit den eigenen, vorliegenden Daten passiert. Damit möchte My Data einen unbeschränkten Datenfluss gewährleisten, um Vorteile gegenwärtiger Monopole zu beschränken. Dabei geht es um Internetgiganten, insbesondere Google, Apple, Facebook und Amazon – kurz GAFA (Lehtiniemi/Haapoja 2020, S. 96). My Data denkt Datenschutz aus der Position von Individuen und kleineren (im Vergleich zu GAFA) Unternehmen, um einen eigenen Absatzmarkt zu lukrieren. (Lehtiniemi/Haapoja 2020, S. 88) Gleichzeitig zielt My Data auf die Standardisierung von Privatheit, Datensicherheit und Datensparsamkeit ab. Dies setzt voraus, dass Organisationen leicht verständliche Datenschutzerklärungen verfassen. Nutzende könnten etwa über ihr Einverständnis darüber in Kenntnis gesetzt werden „für was, wie und über welchen Zeitraum ihre Daten genutzt werden". (Poikola et al. 2020, o. S.)

My Data animiert Personen und Unternehmen dazu, die *declaration* zu unterschreiben, zu kommentieren und Inhalte der My Data Seite weiterzuverbreiten. Dieses kollaborative Vorgehen berücksichtigt die Meinungen der Unterzeichnenden, da die *declaration* fortlaufend adaptiert wird. Ein Aspekt der My Data Erklärung ist die Portierbarkeit[6] von Daten. Des Weiteren achtet My Data auf Datentransparenz, also der Auskunftspflicht vor, während und nach den Verarbeitungsschritten. „Wir wollen Individuen in die Lage versetzen, zu verstehen, wie und auf welche Weise Entscheidungen auf Grundlage ihrer Daten getroffen wurden." (Poikola et al. 2020, o. S.)

6. Hacktivism

Die Modelle von George und Leidner sehen HacktivistInnen an der Spitze der Aktivismus-Hierarchie. HacktivistInnen wollen eine Veränderung nicht nur beeinflussen, sie streben die aktive Beeinflussung der Gesellschaft an. (George/Leidner 2019, S. 9) Dabei ist die Trennschärfe zwischen den Begriffen HackerIn und HacktivistIn unklar. Sowohl Hacking als auch Hacktivismus stellt unter Umständen eine Straftat dar. Hacktivismus kann aber auch als Eintreten für ideelle Ziele gesehen werden. Das deutsche Bundeskriminalamt hält zum Thema Cyberkriminalität fest: „Während Hacker von Eigeninteressen geleitet werden, verfolgen Hacktivisten oft soziale oder politische Ziele." (Füllgraf 2015, S. 21) In diesem Zitat wird die begriffliche Unschärfe deutlich. Das Bundeskriminalamt fasst unter dem Begriff Eigeninteressen illegale, gewinnbringende Tätigkeiten, wie etwa Phishing zusammen. (Füllgraf 2015, S. 20)

[6] Die eigenen Personendaten sollen an andere Dienste übermittelt, oder heruntergeladen werden können. Das soll den Internetnutzenden zur Datenautonomie verhelfen.

> „Gemein ist allen Definitionen, dass es sich bei Hacktivisten um „gewaltfreie“ Aktivisten handelt, die sich der technischen Möglichkeiten von Internet und Computern auf vielfältige Art und Weise bedienen, um ideologisch motivierte Ziele zu verfolgen.“

Missomelius hebt die Ursprünge des Hacking in der Bastlerbewegung der Fünfzigerjahre hervor. Denn BastlerInnen ging es damals um das Erkunden neuer Technologien (2018, S. 3). Der Wortstamm „hack“ stammt aus dem studentischen Eisenbahnclub am MIT. Für kreative Lösungen bei auftretenden technischen Limitierungen benutzten sie das Wort hack. (Post 2016, S. 7 zit. n. Mülling 2019, S. 67) Ein hack beschreibt demnach das Arbeiten mit unüblichen Mitteln. (Liebl/Düllo/Kiel 2000, S. 13) Die Differenzierung zwischen Hackern und HacktivistInnen ist in Zusammenhang mit Digital Citizenship von Bedeutung, weil im Zuge des Hacktivism keine Einzelpersonen geschädigt werden sollen. Vielmehr geht es um die diskursive Beteiligung an der digitalen Gesellschaft, in der HacktivistInnen die Auseinandersetzung mit politischen und kulturellen Belangen für andere ermöglichen.

Es gibt diverse Möglichkeiten um selbstbezogene Daten zu schützen. George und Leidner haben gezeigt, dass Protest auf höchst unterschiedlichen Ebenen stattfinden kann, weshalb sich der Begriff Clicktivism als Synonym für zurückhaltenden Protest etabliert hat. (Thimm 2017, S. 203) Soziale Netzwerke bieten eine Plattform, um mehr Menschen zu erreichen und damit Digital Citizenship provozieren zu können. Digital Citizenship ist in diesem Zusammenhang nicht nur ein Modell, welches versucht mit den neuen Kulturtechniken des Digitalen umzugehen. Es ist auch die Forderung nach kritischem Denken, die sowohl von PädagogInnen als auch von AktivistInnen erhoben wird.

Literatur

Aigrain, Philipp (2012): *Sharing: Culture and the economy in the internet age*. Amsterdam: University Press.

Akarçeşme, Dilara; Pachner, Timna & Prlić, Sonja (2019): *Das Handy als Erzeugung von Utopien*. in: P/art/icipate, Salzburg, S. 1–10.

Baack, Stefan (2015): Datafication and empowerment: How the open data movement re-articulates notions of democracy, participation, and journalism. *Big Data & Society*, 2 (2).

Ballenthien, Jana; Hensel, Alexander; Hoeft, Christoph; Ulbrich, Maren; Rohde, Markus; Rohwerder, Jan & Urich, Karin (2015): Editorial: Zwischen Sichtbarkeit und Anonymität. Protest, Bewegung und digitale Kultur. In: *Forschungsjournal Soziale Bewegungen* 28 (3), S. 3–7.

Ballweber, Jana & Dachwitz, Ingo (2020): *Wie Trump Millionen Schwarze Amerikanerinnen mit gezielter Werbung vom Wählen abhalten wollte*. Abgerufen unter: (https://netzpolitik.org/2020/microtargeting-wie-trump-millionen-schwarze-amerikanerinnen-mit-gezielter-werbung-vom-waehlen-abhalten-wollte/) [Stand vom 30-01-2021]

Bruns, Axel (2008): *Blogs, Wikipedia, Second Life, and beyond: From production to produsage (digital formations)*. New York: Peter Lang.

Dahlgren, Peter (2006): Doing citizenship. In: *European Journal of Cultural Studies* 9 (3), S. 267–286.

Füllgraf, Wendy (2015): *Hacktivisten. Abschlussbericht zum Projektteil der Hellfeldbeforschung.* Abgerufen unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2015HacktivistenProjektteilHellfeldbeforschung.html. [Stand vom 10-04-2021]

George, Jordana J. & Leidner, Dorothy E. (2019): From clicktivism to hacktivism: Understanding digital activism. In: *Information and Organization* 29 (3), S. 1–45.

Gleason, Benjamin & Gillern Von, Sam (2018) Digital Citizenship with Social Media. *Educational Technology & Society* 21 (1) S. 200–212.

Haggerty, Kevin, Ericson, Richard V. (2000): The surveillant assemblage. *British Journal of Sociology* 51(4): S. 605–622.

Helbig, Christian (2016): Partizipation und Kulturelle Medienbildung in einer digitalen Medienwelt. In: *KULTURELLE BILDUNG ONLINE*. Abgerufen unter: https://www.kubi-online.de/artikel/partizipation-kulturelle-medienbildung-einer-digitalen-medienwelt. [Stand vom 11-04-2021]

Hintz, Arne; Dencik, Lina & Wahl-Jorgensen, Karin (2017): Digital Citizenship and Surveillance Society. In: *International Journal of Communication* 1932–8036/20170005 11 (11), S. 731–739.

Jordan, Tim.& Taylor, Paul. (2004*). Hacktivism and Cyberwars. Rebels with a cause?*. London: Routledge.

Kaun, Anne (2015): Citizenship und Partizipation. In: Hepp, Andreas; Krotz, Friedrich; Lingenberg, Swantje & Wimmer, Jeffrey (Hrsg.): *Handbuch Cultural Studies und Medienanalyse*. Wiesbaden: Springer Fachmedien, S. 181–189.

Klaus, Elisabeth; Lünenborg, Margreth (2004): *Cultural Citizenship. Ein kommunikationswissenschaftliches Konzept zur Bestimmung kultureller Teilhabe in der Mediengesellschaft*. In: M&K 52 (2), S. 193–213.

Klaus, Elisabeth; Zobl, Elke (2019): Kritische kulturelle Produktion im Kontext von Cultural Studies und Cultural Citizenship. In: Zobl, Elke; Klaus, Elisabeth; Lang, Siglinde; Moser, Anita; & Baumgartinger, Persson Perry (Hrsg): *Kultur produzieren. Künstlerische Praxen und kritische kulturelle Produktion*. 1. Auflage. Bielefeld: transcript (Edition Kulturwissenschaft, 200), S. 19–31.

Leger, Matthias; Panzitta, Susanne & Tiede, Maria (2018): Daten-Teilen? Digitale Selbstvermessung aus praxeologischer Perspektive. In: Houben, Daniel & Prietl, Bianca (Hrsg.): *Datengesellschaft.* Bielefeld: transcript-Verlag, S. 35–59.

Lehtiniemi, Tuukka & Haapoja, Jesse (2020): Data agency at stake: MyData activism and alternative frames of equal participation. In: *New Media & Society* 22 (1), S. 87–104.

Leistert, Oliver (2013): *Der Beitrag der Social Media zur Partizipation*. In: Forschungsjournal Soziale Bewegungen 26 (2), S. 39–48.

Liebl, Franz; Düllo, Thomas & Kiel, Martin (2005): Before and After Situationism — Before and After Cultural Studies: The Secret History of Cultural Hacking. In: Düllo, Thomas &

Liebl, Franz (Hrsg.): *Cultural Hacking: Kunst des Strategischen Handelns*. Wien: Springer, S. 13–46.

Lünenborg, Margreth (2015): Rethinking Cultural Citizenship. Zur Teilhabe in der (digitalen) Mediengesellschaft. In: Drüeke, Ricarda; Kirchhoff, Susanne; Thomas, Steinmaurer & Thiele, Martina (Hrsg.): *Medien, Öffentlichkeit und Geschlecht.* Bielefeld: transcript Verlag, S. 251–262.

Marchart, Oliver (2018): *Cultural Studies*. München: Utb, Web.

Marshall, Thomas H. (Hrsg.) (1992): *Citizenship and Social Class*. London: Pluto Press, S. 8–17. Abgerufen unter: https://pages.nyu.edu/jackson/analysis.of.inequality/Readings/Marshall%20-%20Development%20of%20Citizenship.pdf [Stand vom 10-05-2021]

Missomelius, Petra (2018): Widerständige Praktiken – Cultural hacking als Form politischen Protests. In: *Medienimpulse*, Bd. 56 Nr. 2 (2018), S. 1–5.

Mülling, Eric (2019): *Big Data und der digitale Ungehorsam*. Dissertation. Universität Potsdam. Wiesbaden: Springer Fachmedien.

Nassehi, Armin (2019): Die Zurichtung des Privaten in: Stempfhuber, Martin & Wagner, Elke (Hrsg.): *Praktiken der Überwachten. Öffentlichkeit und Privatheit im Web 2.0*. Wiesbaden: Springer Fachmedien, S. 63–78.

Poikola, Antti; Kuikkaniemi, Kai; Kuittinen, Ossi; Honko, Harri; Knuutila Aleksi & Lähteenoja, Viivi (2020): *My Data. an introduction to human-centric use of personal data*. Abgerufen unter: https://mydata.org/papers/ [Stand vom 11-04-2021]

Post, Leslie (2016): *Kleine Kulturgeschichte des Hackens*. Hamburg: Bachelor + Master Publishing.

Poster, Mark (1990): *The Mode of Information.* Cambridge: Polity Press.

Stalder, Felix (2019): Autonomie und Kontrolle nach dem Ende der Privatsphäre. In: Stempfhuber, Martin & Wagner, Elke (2019) (Hrsg.): *Praktiken der Überwachten. Öffentlichkeit und Privatheit im Web 2.0.* Wiesbaden: Springer Fachmedien, S. 97–110.

Steinbicker, Jochen (2019): Überwachung und die Digitalisierung der Lebensführung. In: Stempfhuber, Martin & Wagner, Elke (Hrsg.) *Praktiken der Überwachten. Öffentlichkeit und Privatheit im Web 2.0.* S. 79-96.

Thimm, Caja (2017): Soziale Medien und Partizipation. In: Schmidt, Jan-Hinrik & Taddicken Monika (Hrsg.): *Handbuch Soziale Medien*. Wiesbaden: Springer S. 191–201.

Wimmer, Jeffrey (2018): Partizipation und (Gegen-)Öffentlichkeit. In: Hoffmann, Dagmar & Winter, Rainer (Hrsg.): *Mediensoziologie*: Nomos, S. 247–254.

Zorn, Isabel (2017): Wie viel „App-Lenkung" verträgt die digitalisierte Gesellschaft? Herausforderungen digitaler Datenerhebungen für die Medienbildung. In: Eder, Sabine; Mikat, Claudia & Tillmann, Angela (Hrsg.) (2017): *Software takes command. Herausforderungen der „Datafizierung" für die Medienpädagogik in Theorie und Praxis.* München: kopaed (Schriften zur Medienpädagogik, 53). S. 19–34.

Learning Analytics – Datenschutzrechtliche Bestimmungen als Ausgangspunkt einer verantwortungsvollen Nutzung von Bildungsdaten

Silvia Lipp

Zusammenfassung

Die fortschreitende Digitalisierung führt zu einer Virtualisierung zahlreicher Lebens- und Arbeitsbereiche. Auch für den Bereich des Lehrens und Lernens erschließen sich angesichts zunehmend elaborierter digitaler Lernmanagementsysteme neue Möglichkeiten der Ausgestaltung von Lehr-Lernarrangements. Dies bezieht sich nicht nur auf die Nutzung von Lernplattformen selbst, sondern auch auf die Nutzung der damit generierten Daten. Mit Bildungstechnologien, wie Learning Analytics, die sich einem originär pädagogischen Zweck verschrieben haben, werden generierte Daten von Lernenden adressiert. Damit nehmen Daten einen wichtigen Stellenwert zur Verbesserung von Lehr-Lernprozessen ein. Allerdings heiligt auch der altruistischste Zweck nicht die Mittel. Der Drang, unbedingt Nutzen aus Bildungsdaten ziehen zu wollen, vernachlässigt eine zentrale Komponente: die Rechte der betroffenen Personen, deren Schutz einer Datennutzung nicht nach-, sondern vorgereiht werden muss. Im vorliegenden Beitrag wird daher der Einsatz von Learning Analytics an Hochschulen aus datenschutzrechtlicher Perspektive diskutiert, um den nicht regulierten und damit verantwortungsrelevanten Handlungsspielraum zur verantwortungsvollen Nutzung von Bildungsdaten aufzuzeigen.

1. Einleitung

Die Digitalisierung, die digitale Transformation, das digitale Zeitalter oder auch die digitalen Medien sowie das digitale Lernen sind Begrifflichkeiten, die mittlerweile in unseren alltäglichen Sprachgebrauch übergegangen sind. Damit wird eine mehr oder weniger digitale Prägung zahlreicher Lebens- und Arbeitsbereiche wie auch die Übergangsphase von einer Wissens- in eine Datengesellschaft verdeutlicht (Hengstschläger 2020, S. 9). Jegliche Interaktionen in digitalen Räumen verursachen Datenspuren. Diese Flut an Daten nimmt exponentiell zu und es ist längst unmöglich geworden, auch nur einen Bruchteil davon zweckmäßig zu nutzen. Damit splitten sich Datenmengen in genutzte und ungenutzte Daten. Ein ungenutztes respektive unerforschtes und sodann in Vergessenheit geratenes Datenkontingent wird als *Dark Data* bezeichnet (Hand 2020; Krotova 2020). Die Verwendung dieser vorhandenen und bislang ungenutzten Dark Data versprechen neues Innovationspotenzial beispielsweise im Rahmen von Prozessoptimierungen (Gimpel 2020). Auch im Bildungskontext rückt die Nutzung vorhandener, aber brachliegender, digitaler Datenkonvolute in den Vordergrund. Spätestens seit Auftreten der COVID-19 Pandemie stellen virtuelle Lehr-Lernsettings einen integrativen

Bestandteil der Bildungslandschaft Österreichs dar. Datenverkehr entsteht dabei auf verschiedenen Ebenen des Bildungssektors, der Makroebene (Bildungssystem), der Mesoebene (Bildungsmanagement) wie auch auf der Mikroebene (Ebene von Lehr-Lernprozessen). In Hinblick auf die Verarbeitung, Analyse und Auswertung von Bildungsdaten werden vor allem die bildungstechnologischen Konzepte Learning Analytics, Educational Data Mining und Academic Analytics diskutiert. Während *Educational Data Mining* auf die automatisierte Analyse aller verfügbaren Daten des Bildungskontextes setzt (U.S. Department of Education, Office of Educational Technology 2014, S. 8; Siemens/Baker 2012), haben *Academic Analytics* eine datengestützte Betrachtung von Bildungseinrichtungen aus einem politischen und wirtschaftlichen Blickwinkel zum Ziel (Romero/Ventura 2020, S. 2). *Learning Analytics* hingegen konzentrieren sich stärker auf Daten der Lehr-Lernprozessebene und deren Potenzial zur Unterstützung Lehrender und Lernender (Mandausch/Meinhard 2018, S. 24–26).

Bildungstechnologien wie Learning Analytics beruhen auf der Intention, Daten als individuelle Lernunterstützung sprechen zu lassen und damit Lehr-Lernprozesse zu unterstützen. Der Blick wird somit vorwiegend auf potenzielle Vorteile dieser Technologien gelenkt bzw. wird der lernförderliche Zweck in den Mittelpunkt gestellt. Die mit dem Einsatz von Learning Analytics verbundenen Herausforderungen und Risiken der Datennutzung werden hingegen nachrangig behandelt. Damit wird eine zentrale Thematik – Schutz der Personenrechte von Lernenden – vernachlässigt, die einem Einsatz von Learning Analytics allerdings vorausgehen sollte. Ausgehend von diesem Problemfeld liegt der Fokus dieses Beitrags daher – unabhängig von der Zielsetzung und Ausrichtung von Learning Analytics – in der Grundsatzfrage, welchen rechtlichen Rahmenbedingungen ein Einsatz von Learning Analytics im Hochschulkontext in Österreich zugrunde liegt. Hierfür erfolgt zunächst eine fragmentarische Betrachtung des Forschungsfelds Learning Analytics. Anschließend werden die datenschutzrechtlichen Regeln zur Datennutzung in den Blick genommen und der Schutz personenbezogener Daten diskutiert. Darüber hinaus werden die Rechte und Pflichten der betroffenen Personen sowie das Abschätzen möglicher datenschutzrechtlicher Folgen behandelt. Im den Beitrag abschließenden Fazit wird insbesondere deutlich, dass die Skizzierung und Abgrenzung des Rechtsrahmens erst den Ausgangspunkt einer verantwortungsvollen Nutzung von Bildungsdaten darstellt und den verantwortungsrelevanten Handlungsspielraum und damit das Ausmaß einer Eigenverantwortung bei Einsatz von Learning Analytics offenlegt.

2. Learning Analytics – Datengestützte Hilfe zur Selbsthilfe

Nutzen Lernende digitale Lernumgebungen, so verursacht ihr Nutzungsverhalten die Produktion von Datenspuren. Ist Learning Analytics in diese digitalen Lernumgebungen eingebunden, so werden sämtliche Interaktionen der Lernenden als Datenspuren erfasst,

gesammelt, aggregiert, in Echtzeit analysiert und visualisiert. Diese datenbasierten Einsichten in Lehr-Lernprozesse sollen in weiterer Folge Ansatzpunkte zur Verbesserung des Lehrens und Lernens liefern (Höfler/Kopp 2018, S. 560; Ifenthaler/Schumacher 2016, S. 176–177). Das vermeintliche Potenzial wird dabei unterschiedlichen Datentypen zugeschrieben (Grandl et al. 2017, S. 7; Khalil/Ebner 2015, S. 1329):

- Kommunikationsdaten (u. a. E-Mails, Foreneinträge)
- Interaktionsdaten mit fester Struktur (u. a. Up- und Downloads, Anzahl der Logins in Lernmanagementsysteme, Social Network-Aktivitäten, Logfiles)
- Persönliche Daten (u. a. demografische Daten)
- Spezifische Lernendendaten (je nach Bildungsinstitution u. a. Prüfungsergebnisse, Informationen zum Bildungsweg)

Der Einsatz von Learning Analytics bezweckt somit die Unterstützung und Optimierung von Lehr-Lernprozessen. Lernende sollen beispielsweise durch individuelle Lernmaterialien, Empfehlungen erfolgreicher Lernpfade oder Peer-Vergleiche profitieren (Ifenthaler/Schumacher 2016, S. 177; Chatti et al. 2012b, S. 22). Lehrenden wird eine Echtzeitbetrachtung des Lernstandes und -fortschrittes sowie der Nutzung des Lernangebotes ermöglicht. Eine bedarfsgerechte Adaptierung der Lehre kann daran anschließen (Johnson et al. 2012, S. 26). Auch wenn durch den Einsatz von Learning Analytics den (aggregierten) Daten ein hohes Gewicht zugeschrieben wird, bleibt die Relevanz der pädagogischen Rolle der Lehrenden erhalten (Grandl et al. 2017, S. 1). Learning Analytics kann lediglich das pädagogische Handeln unterstützen. Bisherige Einsichten in das Lehr-Lerngeschehen werden um die Perspektive einer digitalen Lernangebotsnutzung ergänzt. Diese datengestützte Hilfe zur Sammlung von Informationen über Lehr-Lernprozesse soll Lehrenden und Lernenden wiederum als Selbsthilfe zur Verbesserung ihrer Lehr-Lernprozesse dienen (Ebner/Ebner 2018, S. 5–6; Grandl et al. 2017, S. 1).

Allerdings heiligt der Zweck von Learning Analytics auch bei noch so guten Absichten nicht die Mittel. Daten unreflektiert und bedingungslos heranzuziehen, um beispielsweise Lernende automatisiert als *Problemfall* zu kennzeichnen (um diese frühzeitig zu fördern), löst Diskussionen über das zugrundeliegende Verständnis aus. Geht es um die Förderung des persönlichen Wachstums (Parkes et al. 2020, S. 113) oder treibt uns diese Entwicklung in eine gegensätzliche Richtung und führt letztlich zu Bestrebungen einer bestmöglichen digitalen Selbstinszenierung? Die zwischen befürwortenden und kritischen Parteien geführten Debatten eines Einsatzes von Learning Analytics werfen allesamt die Problematik eines möglichen Datenmissbrauchs auf (Buckingham Shum 2012, S. 9). Die Auseinandersetzung mit Datenschutzrichtlinien und deren Bedeutung für den Einsatz von Learning Analytics ist daher unerlässlich und wird im Folgenden dargelegt.

3. Alles was Recht ist – Regeln zur Datennutzung

Die Diskussion um Datenschutz, Vertraulichkeit, Privatsphäre und eine dementsprechend ethisch vertretbare Verwendung von Lernendendaten (im gegenständlichen Beitrag werden Studierendendaten fokussiert) gewinnt zunehmend an Bedeutung. Auch wenn Studierende beispielsweise der Verwendung ihrer Daten zustimmen, ist nicht außer Acht zu lassen, dass der dahinterstehende Zweck für sie mangels Transparenz unklar sein kann. Obendrein kann zwar das intendierte Ziel offensichtlich erkennbar sein, die tatsächliche Nutzung kann hingegen von der ursprünglichen Zielsetzung abweichen (beispielsweise aufgrund der Änderung von Analysemethoden), was eine rechtlich legitime und auch ethische Verwendung dieser generierten Daten fraglich erscheinen lässt (Arnold/Sclater 2017; Slade/Prinsloo 2013, S. 1520).

Rechtliche Fragestellungen, die mit einem Einsatz von Learning Analytics einhergehen, betreffen u. a. nachfolgende Themengebiete (Drachsler/Greller 2016, S. 96; Bock/Meissner 2012, S. 425; Buckingham Shum/Ferguson 2012):

- Zugriff auf Daten (Voraussetzungen eines Datenzugriffs; Notwendigkeit einer Zustimmung; Zugriffsberechtigungen)
- Zweckgebundenheit der Datennutzung (Voraussetzung eines legitimen Zwecks)
- Aufzeichnung von Daten (Zeitrahmen der Datenspeicherung)
- Analyse von Daten (Auswahl bestimmter Verfahren und Instrumente)
- Gewährleistung der Datensicherheit (Schutz vor dem Zugriff unbefugter Personen)
- Persönlichkeitsrechte und Schutz der Privatsphäre der betroffenen Personen (Notwendigkeit einer Anonymisierung)

Grundsätzlich besteht in Österreich lt. § 1 DSG ein Grundrecht auf Datenschutz. Jede Person entscheidet demnach selbst über den Umfang der Weitergabe und die Verwendung ihrer personenbezogenen Daten (Lachmayer/Lewinski 2019, S. 10). Datenschutzrechtliche Bestimmungen bzw. Richtlinien zur Handhabe personenbezogener Daten finden sich (Datenschutzbehörde 2018):

(1) in der Charta der Grundrechte der Europäischen Union,
(2) in der seit 25.05.2018 EU-weit geltenden Datenschutz-Grundverordnung (DSGVO) sowie
(3) im ergänzenden nationalen Datenschutzgesetz (DSG).

In der DSGVO wird die (teil-)automatisierte und nicht automatisierte Verwendung personenbezogener Daten geregelt (Schmidl 2019, S. 6). Personenbezogene Daten werden dabei lt. Art. 4 Z 5 DSGVO verstanden als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“ (Europäisches Parlament und Rat 2018, S. 33). Aus diesem Datentyp personenbezogener Daten, der einen

Rückschluss auf einzelne Personen zulässt, ergibt sich die Notwendigkeit, die Privatsphäre betroffener Personen zu schützen, was folglich Belange einer (Pseudo-)Anonymisierung darstellen. Daten, welche Ausgangspunkt für die Anwendung von Learning Analytics sind, fallen unter diese Definition der personenbezogenen Daten. Learning Analytics bedienen sich der Nutzungsdaten eines Lernmanagementsystems. Nutzungsdaten entstehen, wenn Studierende in digitalen Lehr-Lernsettings auf eingebettete Lernanlässe zugreifen, wie beispielsweise durch Lösen von Quizaufgaben, Erstellen von Forenbeiträgen oder Ansehen bereitgestellter Lernvideos. Die Maßnahme zum Schutz dieser personenbezogenen Daten stellt die Pseudonymisierung dar. Ist aus diesen Daten ohne weitere Information keine Identifikation einer bestimmten Person möglich, wird von pseudonymen Daten gesprochen (Holst et al. 2018, S. 8). Die Pseudonymisierung wird im Art. 4 Z 5 DSGVO behandelt, und besagt, dass eine gesonderte Aufbewahrung sowie technische und organisatorische Maßnahmen in Bezug auf diese Daten mit identifizierbarem Charakter vorgenommen werden müssen – kurzum personenbezogene Daten sollen aus restlichen (Inhalts-)Daten entfernt werden. Dadurch sollen verantwortliche Personen keine Möglichkeiten mehr haben, spezifische Personen zu identifizieren (Europäisches Parlament und Rat 2018, S. 33). Der Begriff der pseudonymen Daten grenzt sich dabei von anonymen Daten insoweit ab, dass bei anonymen Daten keinerlei Möglichkeit besteht, oder nur unter Einsatz eines beträchtlichen Aufwandes, auf spezifische Personen zurückschließen zu können. Sobald dies von Grund auf nicht ausgeschlossen werden kann, handelt es sich um pseudonyme Daten (Holst et al. 2018, S. 9). Dabei stellt sich allerdings die Frage, ob eine solch (vollständige) Anonymisierung in Hinblick auf Möglichkeiten, die sich aus Big Data, Data Mining und Künstlicher Intelligenz ergeben, überhaupt noch garantiert werden kann (Drachsler/Greller 2016, S. 93; Barocas/Nissenbaum 2014), oder ob die Pseudonymisierung aus diesem Blickwinkel nicht eher nur einen mäßig erfolgreichen Versuch einer Rechtfertigung darstellt oder sogar ein Umgehen der DSGVO ermöglicht (beispielsweise durch ausgeklügelte Datenverschlüsselungstechniken) (Marnau 2016, S. 430–433).

4. Pseudonymität – Schutz personenbezogener Daten

Ungeachtet dessen stellt die Pseudonymisierung ein wichtiges Konzept der Datenanonymisierung im Rahmen der DSGVO dar (siehe beispielsweise Art. 25 Abs. 1 DSGVO). Die Pseudonymisierung wird als eine Art der Datenverarbeitung aufgefasst. Diese Verarbeitung personenbezogener Daten ist grundsätzlich verboten und nur unter Einhaltung der Bestimmungen des Art. 6 und Art. 9 DSGVO erlaubt. Rechtmäßig ist eine Verarbeitung von Daten demgemäß nur dann, wenn zumindest eine der aufgelisteten Voraussetzungen lt. Art. 6 DSGVO zutrifft. Aus Learning Analytics Perspektive sind zwei Möglichkeiten der Auflistung lt. Art. 6 DSGVO relevant, um das grundsätzliche Verbot der Pseudonymisierung aufzuheben:

(1) Bei Vorliegen einer rechtsgültigen Einwilligung der Betroffenen zur Verwendung deren personenbezogener Daten für einen bestimmten festgelegten Zweck.
(2) Bei der Datenverarbeitung für wissenschaftliche Zwecke, sofern auch die Anforderungen gem. Art. 89 Abs. 1 DSGVO (Vorschriften für besondere Verarbeitungssituationen u. a. im Hinblick auf wissenschaftliche Forschungszwecke) erfüllt werden (Europäisches Parlament und Rat 2018, S. 33, S. 36 und S. 85).

Die grundsätzliche Privilegierung einer Datenverarbeitung für wissenschaftliche Zwecke bezieht sich jedoch nicht auf die *reale* Lehre. Forschungstätigkeiten im Bereich Learning Analytics bedingen allerdings den Einsatz von Learning Analytics. Die Erforschung kann daher beispielsweise nur im Rahmen einer forschungsgeleiteten Lehre im Hochschulkontext erfolgen. Die Verarbeitung für Forschungszwecke wird im § 7 DSG noch weiter konkretisiert (Schmidl 2019, S. 52), ist aber für die Rechtfertigung eines Einsatzes von Learning Analytics nach wie vor als unzureichend anzusehen.

Der Blick auf eingesetzte Lernplattformen an österreichischen Hochschulen zeigt einen weit verbreiteten Einsatz des Lernmanagementsystems Moodle (Bratengeyer et al. 2016, S. 32–33 und S. 45–46). Moodle als Lernplattform integriert per se bereits Learning Analytics Funktionalitäten (Bösch 2020). Die Freischaltung bzw. Nutzung dieser Funktionalitäten setzt die Einhaltung der datenschutzrechtlichen Regeln voraus. Auch im deutschen Hochschulraum wird Moodle als Lernplattform eingesetzt sowie deren Learning Analytics Werkzeuge erforscht. Forschungstätigkeiten von beispielsweise Kiy und Lucke zeigen auf, dass ein Einsatz von Learning Analytics auf der Lernplattform Moodle keine Pseudonymisierung gewährleisten kann, ohne dass nicht auch die pädagogische Zielsetzung, die mit Learning Analytics erreicht werden soll (z. B. die Unterstützung eines personalisierten individuellen Lernens), abgeschwächt wird (Kiy/Lucke 2014, S. 109). Das Umgehen dieser Limitation, durch beispielsweise Visualisierung ausschließlich aggregierter (statt namentlich gekennzeichneter) Studierendenaktivitäten, verfehlt jedoch die Intention von Learning Analytics. Das vermeintliche Potenzial von Learning Analytics, datengestützt einer Lernendenzentrierung und Individualisierung näher zu kommen, verblasst damit allerdings schon vor dem eigentlichen Einsatz (Gaaw/Stützer 2017, S. 149; Kiy/Lucke 2014, S. 110).

Der Hinweis auf die Zweckgebundenheit im Umgang mit personenbezogenen Daten als Ergänzung zur Einwilligung der Betroffenen (Art. 6 Abs. 1 DSGVO) schränkt erneut die Nutzung von Learning Analytics ein. Learning Analytics kann als ein iterativer Prozess mit den Phasen der Sammlung, Aufbereitung, Analyse und Auswertung von Daten beschrieben werden, dessen Annäherung an ein intendiertes Ziel Veränderungen im Laufe des Einsatzes notwendigerweise bedingen. Diese Veränderungen können sich auf nahezu alle Phasen beziehen. Daten aus verschiedensten Datenquellen werden gesammelt, aufbereitet und mit ausgewählten Methoden analysiert (Grandl et al. 2017, S. 12; Chatti et al. 2012a, S. 322–323). Die Ergebnisse werden meist auf Dashboards visualisiert, die dann

als Ausgangspunkt pädagogischer Handlungen dienen (Leitner/Ebner 2017). Dashboards sind grafische Benutzeroberflächen zur Visualisierung der wesentlichsten Informationen – ähnlich einem virtuellen Cockpit (Few 2006). Die Nachbereitungsphase, ist vor allem für die kontinuierliche Verbesserung von Learning Analytics wesentlich. Diese kann die Einbindung neuer Daten aus zusätzlichen Datenquellen enthalten, das Verfeinern des Datensatzes, das Ändern der Analysevariablen oder auch das Auswählen einer neuen Analysemethode (Chatti et al. 2012a, S. 323). Daraus geht hervor, dass sich z. B. durch die Analyse weiterer Daten oder der Änderung der Analysemethode auch die Zwecke von Learning Analytics erweitern/verändern können. Learning Analytics kann sich beispielsweise auf die Vorhersage von Studierendenleistungen beziehen. Die Speicherung der Daten für deren Wiedernutzung für eine spezifischere Ausrichtung, z. B. zur Modellierung erfolgreicher Lernpfade – was jedoch zum Zeitpunkt der ursprünglich eingeholten Einwilligungserklärung nicht absehbar war – ist rechtlich gesehen nicht zulässig. Hierzu müsste die Einwilligung für jeden vom definierten Ursprungszweck abweichenden Zweck erneut eingeholt werden. Drachsler und Greller zufolge würde andernfalls eine Verletzung von persönlichen Informationsrechten vorliegen (Drachsler/Greller 2016, S. 93). Die Einhaltung der lt. DSGVO geforderten Zweckgebundenheit kann demnach nur bei starrem Einsatz von Learning Analytics erfolgen, was wiederum deren Zielsetzung entgegensteht.

Die ausgeführten Möglichkeiten zur Verwendung personenbezogener Daten stellen gleichzeitig wesentliche Limitationen von Learning Analytics dar, welche die Brauchbarkeit und Intention massiv einschränken. Die Datenminimierung stellt einen weiteren Grundsatz für die Verarbeitung personenbezogener Daten dar (Art. 5 Abs. 1 lit. c DSGVO). Damit kommt zum Ausdruck, dass nur notwendige sowie auf den Zweck abgestimmte und angemessene Daten erhoben werden sollen. Dies begrenzt wiederum Möglichkeiten einer kontinuierlichen Verbesserung des Learning Analytics Einsatzes.

5. Rechte, Pflichten und Folgenabschätzung

Die Verarbeitung personenbezogener Daten beinhaltet auch die Einhaltung von Pflichten gegenüber betroffenen Personen sowie die Berücksichtigung derer Rechte. Tangiert wird hier beispielsweise

- die Informationspflicht gegenüber den Betroffenen (z. B. Lernenden) (Art. 13 und Art. 14 DSGVO),
- das Auskunftsrecht beteiligter Personen (Art. 15 DSGVO),
- das Recht auf Berichtigung unrichtiger oder unvollständiger personenbezogener Daten (Art. 16 DSGVO),
- das Recht auf Löschung der Daten (Art. 17 DSGVO),
- das Recht auf Einschränkung der Datenverarbeitung (Art. 18 DSGVO),

- das Recht auf Mitteilungen in Hinblick einer Berichtigung, Löschung oder Datenverarbeitungseinschränkung (Art. 19 DSGVO) sowie
- das Recht, die eigenen personenbezogenen Daten an andere verantwortliche Personen übertragen zu können (Art. 20 DSGVO).

Demnach sind betroffene Lernende bereits vor einer Datenerhebung über den Zweck der Datenerhebung und über daran beteiligte bzw. dafür verantwortliche Personen zu informieren. Auch die Art und Weise der Datenverarbeitung (z. B. Maßnahmen der Pseudonymisierung) ist transparent darzulegen. Hinzu kommt die Pflicht zur Sicherstellung der Datensicherheit durch technische und organisatorische Anordnungen und die Löschung der Daten nach dessen ursächlichem Zweck.

Darüber hinaus kann für Learning Analytics vorab die Notwendigkeit einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) bestehen. Hinweise darauf hat die Datenschutzbehörde in Form von Verordnungen veröffentlicht. Während die ‚white list' (BGBl. II Nr. 108/2018) die Ausnahmen einer Datenschutz-Folgenabschätzung beschreibt, kennzeichnet die ‚black list' dessen verpflichtende Ausstellung. Eine Datenschutz-Folgenabschätzung ist beispielsweise für eine datenbasierte und automatisierte Erstellung von Profilen und Prognosen erforderlich, welche negative Auswirkungen nach sich ziehen können. Oder auch, wenn der Einsatz einer neuen Technologie vermutlich eine Auswirkung auf datenbezogene Rechte der Betroffenen hat (Europäisches Parlament und Rat 2018, S. 53; § 2 BGBl. II Nr. 278/2018). Learning Analytics oder deren verwandte Forschungsbereiche wie Educational Data Mining oder Academic Analytics sind begrifflich nicht dezidiert auf einer der beiden Listen angeführt. Die in den Verordnungen spezifizierten Kriterien können außerdem je nach Einsatzgebiet unterschiedlich ausgelegt werden. Ungeachtet dessen wäre die vorsorgliche Erstellung einer Datenschutz-Folgenabschätzung für den Einsatz von Learning Analytics an Hochschulen zu empfehlen. Dies allein schon als Zeichen sich dem verantwortungsvollen Umgang mit sensiblen Daten im Bildungskontext bewusst zu sein. An dieser Stelle lässt sich noch hinzufügen, dass sich neben gesetzlichen Regulierungen unter Umständen auch Regelungen in den Satzungen oder Richtlinien (z. B. Compliance-Richtlinien) der Hochschulen finden lassen, die es im Anwendungsfall zu berücksichtigen gilt.

6. Fazit

In diesem Beitrag wurden die rechtlichen Rahmenbedingungen, denen der Einsatz von Learning Analytics im österreichischen Hochschulraum unterliegt, skizziert. Die Gewährleistung einer rechtskonformen Datenverwendung bedingt zumindest die Beachtung und Einhaltung der Rechte und Pflichten der EU-weit geltenden DSGVO sowie des österreichischen DSG und gegebenenfalls der Regelungen der relevanten Hochschule. Auf Schulebene sind ebenfalls die Bestimmungen der DSGVO und DSG relevant. Hinzu

kommt hier noch eine notwendige Einbeziehung der gesetzlichen Aufgaben der Schule, die in den Schulgesetzen geregelt sind und Regelungen für Datenverarbeitungen enthalten (BMBWF 2021).

Durch eingehende Auseinandersetzung mit Datenschutzregeln können Unsicherheiten in Bezug auf eine ordnungsgemäße Datenverarbeitung verringert werden. Diese Vorschriften zielen u. a. darauf ab, eine diesbezüglich intensive Beschäftigung nicht erst im Zuge einer Datenerhebung, sondern dieser bereits vorgelagert, sicherzustellen. Eine unter Umständen erforderliche Verfassung einer Datenschutz-Folgenabschätzung bietet zudem die Gelegenheit datenschutzrechtliche Lücken aufzudecken. Das ermöglicht a priori die Vorwegnahme potenzieller Datenmissbrauchsrisiken. Auch die Zustimmungseinholung der betroffenen Lernenden ist unbedingt vor dem Beginn einer Datensammlung erforderlich. Das Vorhandensein von Datenschutzregeln garantiert dennoch nicht deren Einhaltung. Außerdem setzen die Auslegung und Umsetzung datenschutzrechtlicher Bestimmungen fundierte Kenntnisse verantwortlicher Personen voraus (Ebner et al. 2020, S. 270). Ungeachtet der Regelbefolgung und profunder datenschutzrechtlicher Kenntnisse reicht der gesetzliche Rahmen für einen verantwortungsvollen Umgang mit Bildungsdaten nicht aus (Hartong 2019, S. 18). Gerade auch, da die Rechtsprechung technischen Entwicklungen naturgemäß hinterherhinkt. Der trotz gesetzlicher Regulierung weiterhin bestehende Handlungsspielraum kann durch zusätzliche Berücksichtigung ethischer Aspekte auf das Fundament der moralischen Grundnormen der Gesellschaft gestellt werden. Eine Richtung, wie sich im Bereich Learning Analytics Ethik und Recht ergänzen können, zeigt beispielsweise das Konzept der *Trusted Learning Analytics* (Hansen et al. 2020, S. 9). Den Orientierungsrahmen der Trusted Learning Analytics liefert ein Verhaltenskodex, der rechtliche und ethische Aspekte einer Bildungsdatennutzung behandelt und damit als Leitfaden eines rechtlich korrekten und gleichzeitig verantwortungsvollen Einsatzes von Learning Analytics dient. Datenschutzrechtliche Bestimmungen stellen demnach *nur* den Ausgangspunkt einer verantwortungsvollen Nutzung von Bildungsdaten dar.

Literatur

Arnold, Kimberly E. & Sclater, Niall (2017): Student perceptions of their privacy in leaning analytics applications. In: LAK ‘17 (Hrsg.): *Proceedings of the Seventh International Learning Analytics & Knowledge Conference*. New York: ACM, S. 66–69.

Barocas, Solon & Nissenbaum, Helen (2014): Big data’s end run around procedural privacy protections. *Commun ACM* 57(11), S. 31–33. DOI: 10.1145/2668897.

BGBl. II Nr. 108/2018: *Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung,* vom 25.05.2018. Abgerufen unter: https://

www.ris.bka.gv.at/GeltendeFassung/Bundesnormen/20010206/DSFA-AV%2c%20Fassung%20vom%2008.06.2018.pdf [Stand vom 27-04-2021].

BGBl. II Nr. 278/2018: *Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist,* vom 09.11.2018. Abgerufen unter: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010375 [Stand vom 27-04-2021].

BMBWF (2021): *Datenschutz in Schulen. Datenschutzinformation gemäß Art. 12ff DSGVO im Rahmen der Schulverwaltung an österreichischen Schulen gemäß Art. 14 B-VG*. BMBWF – Bundesministerium für Bildung, Wissenschaft und Forschung. Abgerufen unter: https://www.bmbwf.gv.at/Themen/schule/schulrecht/ds.html [Stand vom 28-04-2021].

Bock, Kirsten & Meissner, Sebastian (2012): Datenschutz-Schutzziele im Recht. *Datenschutz und Datensicherheit* 36 (6), S. 425–431.

Bösch, Luca (2020): *Moodle Dokumentation 3.10 - Learning Analytics*. Abgerufen unter: https://docs.moodle.org/310/de/index.php?title=Learning_Analytics&oldid=21736 [Stand vom 27-04-2021].

Bratengeyer, Erwin; Steinbacher, Hans-Peter; Friesenbichler, Martina; Neuböck, Kristina; Kopp, Michael & Gröblinger, Ortrun (2016): *Die österreichische Hochschul-E-Learning-Landschaft. Studie zur Erfassung des Status quo der E-Learning-Landschaft im tertiären Bildungsbereich hinsichtlich Strategie, Ressourcen, Organisation und Erfahrungen*. Norderstedt: Books on Demand.

Buckingham Shum (2012): *Learning Analytics*. Moscow: UNESCO Institute for Information Technologies in Education, S. 1–12. Abgerufen unter: https://iite.unesco.org/pics/publications/en/files/3214711.pdf [Stand vom 16-03-2021].

Buckingham Shum, Simon & Ferguson, Rebecca (2012): Social learning analytics. *Educational Technology and Society* 15 (3), S. 3–26.

Chatti, Mohamed Amine; Dyckhoff, Anna Lea; Schroeder, Ulrik & Thüs, Hendrik (2012a): A reference model for learning analytics. *IJTEL* 4 (5–6), S. 318–331.

Chatti, Mohamed Amine; Dyckhoff, Anna Lea; Schroeder, Ulrik & Thüs, Hendrik (2012b): Forschungsfeld Learning Analytics. Learning Analytics Research Challenges. *i-com* 11(1), S. 22–25. DOI: 10.1524/icom.2012.0007.

Datenschutzbehörde (2018): *Datenschutzrecht in Österreich*. Abgerufen unter: https://www.dsb.gv.at/recht-entscheidungen/gesetze-in-oesterreich.html [Stand vom 21-01-2021].

Drachsler, Hendrik & Greller, Wolfgang (2016): Privacy and Analytics – it's a DELICATE Issue. A Checklist for Trusted Learning Analytics. In: LAK '16 (Hrsg.): *Proceedings of the Sixth International Learning Analytics & Knowledge Conference*. New York: ACM, S. 89–98.

Ebner, Markus & Ebner, Martin (2018): Learning Analytics an Schulen – Hintergrund und Beispiele. *Medienimpulse* 56 (1), S. 1–28. DOI: 10.21243/mi-01-18-06.

Ebner, Martin; Leitner, Philipp & Ebner, Markus (2020): Learning Analytics in der Schule - Anforderungen an Lehrerinnen und Lehrer. In: Christine Trueltzsch-Wijnen & Gerhard Brandhofer (Hrsg.)*: Bildung und Digitalisierung. Auf der Suche nach Kompetenzen und Performanzen*. Baden-Baden: Nomos (Medienpädagogik), S. 255–272.

Europäisches Parlament und Rat (2018): *Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG*. Abgerufen unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE [Stand vom 21-01-2021].

Few, Stephen (2006): *Information Dashboard Design. The Effective Visual Communication of Data*. Beijing: O'Reilly.

Gaaw, Stephanie & Stützer, Cathleen M. (2017): Learning und Academic Analytics in Lernmanagementsystemen (LMS): Herausforderungen und Handlungsfelder im nationalen Hochschulkontext. In: Thomas Köhler et al. (Hrsg.): *Wissensgemeinschaften in Wirtschaft, Wissenschaft und öffentlicher Verwaltung.* Tagung Gemeinschaften in Neuen Medien. Dresden: TUDpress, S. 145–161.

Gimpel, Gregory (2020): Bringing dark data into the light: Illuminating existing IoT data lost within your organization. *Business Horizons* 63 (4), S. 519–530. DOI: 10.1016/ j.bushor.2020.03.009.

Grandl, Maria; Taraghi, Behnam; Ebner, Markus; Leitner, Philipp & Ebner, Martin (2017): Learning Analytics. In: Karl Wilbers & Andreas Hohenstein (Hrsg.): *Handbuch E-Learning. Expertenwissen aus Wissenschaft und Praxis – Strategien, Instrumente, Fallstudien*. Köln: Wolters Kluwer, S. 1–16.

Hand, David J. (2020): *Dark data. Why what you don't know matters*. Princeton: University Press.

Hansen, Jan; Rensing, Christoph; Herrmann, Oliver & Drachsler, Hendrik (2020): *Verhaltenskodex für Trusted Learning Analytics. Version 1.0. Entwurf für die hessischen Hochschulen*. Frankfurt am Main: Innovationsforum Trusted Learning Analytics, S. 1–18.

Hartong, Sigrid (2019): Learning Analytics und Big Data. Zur notwendigen Entwicklung eines datenpolitischen Alternativprogramms. In: Gewerkschaft Erziehung und Wissenschaft (Hrsg.): *Bildung in der digitalen Welt*. Frankfurt am Main: gew, S. 1–32. Abgerufen unter: https:// www.gew.de/index.php?eID=dumpFile&t=f&f=91791&token=702ec8d5f9770206a4aa8a1079750ec9021b90bf&sdownload=&n=Learning-analytics-2019-web-IVZ.pdf [Stand vom 16-03-2021].

Hengstschläger, Markus (2020): Vorwort. In: Markus Hengstschläger & Rat für Forschung und Technologieentwicklung (Hrsg.): *Digitaler Wandel und Ethik*. Salzburg: ecowin, S. 8–19.

Höfler, Elke & Kopp, Michael (2018): MOOCs und Mobile Learning. In: Claudia de Witt & Christina Gloerfeld (Hrsg.): *Handbuch Mobile Learning*. Wiesbaden: Springer VS, S. 543–564.

Holst, Sonja; Schütze, Bernd & Spyra, Gerald (2018): Arbeitshilfe zur Pseudonymisierung / Anonymisierung. In: GMDS Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (Hrsg.): *Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“*. Köln: GMDS, S. 1–43. Abgerufen unter: https://www.gesundheitsdatenschutz.org/download/Pseudonymisierung-Anonymisierung.pdf [Stand vom 21-03-2021].

Ifenthaler, Dirk & Schumacher, Clara (2016): Learning Analytics im Hochschulkontext. *WIST* 45 (4), S. 176–181. DOI: 10.15358/0340-1650-2016-4-176.

Johnson, Larry; Adams, Samantha & Cummins, Michele (2012): *Horizon Report: 2012 Higher Education Edition*. Austin: NMC.

Khalil, Mohammad & Ebner, Martin (2015): Learning Analytics: Principles and Constraints. In: *Proceedings of World Conference on Educational Multimedia, Hypermedia and Telecommunication*. Chesapeake: AACE, S. 1326–1336.

Kiy, Alexander & Lucke, Ulrike (2014): Learning-Analytics-Werkzeuge im Praxisvergleich. In: Christoph Rensing & Stephan Trahasch (Hrsg.): *Proceedings of DeLFI Workshops 2014 co-located with 12th e-Learning Conference of the German Computer Society*. Freiburg: Ges. für Informatik, S. 104–111.

Krotova, Alevtina (2020): *Datennutzung: Offensive Großunternehmen, defensiver Mittelstand*. Köln: Institut der deutschen Wirtschaft (IW-Kurzbericht).

Lachmayer, Konrad & von Lewinski, Kai (2019): Einleitung. In: Konrad Lachmayer & Kai von Lewinski (Hrsg.): *Datenschutz im Rechtsvergleich. Deutschland – Österreich* (Schriften zum internationalen und vergleichenden öffentlichen Recht). Wien: Facultas, S. 9–13.

Leitner, Phillip & Ebner, Martin (2017): Development of a dashboard for learning analytics in higher education. In: Panayiotis Zaphiris & Andri Ioannou (Hrsg.): *Learning and Collaboration Technologies. Technology in Education. Fourth International Conference, LCT*. Cham: Springer, S. 293–301.

Mandausch, Martin & Meinhard, David B. (2018): Learning Analytics – ein hochschuldidaktischer Diskurs zu Datenanalysen in der Lehre. In: Martina Schmohr et al. (Hrsg.): *Gelingende Lehre: erkennen, entwickeln, etablieren: Beiträge der Jahrestagung der Deutschen Gesellschaft für Hochschuldidaktik (dghd) 2016*. Bielefeld: wbv, S. 19–33.

Marnau, Ninja (2016): Anonymisierung, Pseudonymisierung und Transparenz für Big Data. *DuD – Datenschutz und Datensicherheit* 40 (7), S. 428–433. DOI: 10.1007/s11623-016-0631-9.

Parkes, Sarah; Benkwitz, Adam; Bardy, Helen; Myler, Kerry & Peters, John (2020): Being more human: rooting learning analytics through resistance and reconnection with the values of higher education. *Higher Education Research and Development* 39 (1), S. 113–126. DOI: 10.1080/07294360.2019.1677569.

Romero, Cristobal & Ventura, Sebastian (2020): Educational data mining and learning analytics: An updated survey. *WIREs Data Mining Knowledge Discovery* 10 (3), S. 1–21. DOI: 10.1002/widm.1355.

Schmidl, Matthias (2019): *Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung, Leitfaden*. Datenschutzbehörde Republik Österreich.

Siemens, George & Baker, Ryan S. J. d. (2012): Learning analytics and educational data mining. In: LAK'12 (Hrsg.): *Proceedings of the Second International Learning Analytics & Knowledge Conference*. New York: ACM, S. 252–254.

Slade, Sharon & Prinsloo, Paul (2013): Learning Analytics: Ethical Issues and Dilemmas. *American Behavioral Scientist* 57 (10), S. 1510–1529. DOI: 10.1177/0002764213479366.

U.S. Department of Education, Office of Educational Technology (2014): *Enhancing Teaching and Learning Through Educational Data Mining and Learning Analytics: An Issue Brief*. Washington: U.S. Department of Education, S. 1–60.

Umgang mit (digitalen) Forschungsdaten: Rahmungen, Effekte und Herausforderungen

Michaela Rizzolli

Zusammenfassung

Der planvolle und nachhaltige Umgang mit (digitalen) Forschungsdaten hat in den letzten Jahren immer mehr Aufmerksamkeit erfahren. Hochschulen, Universitäten, Forschungsgemeinschaften sowie Forschungsverbünde haben vermehrt Leitlinien und Empfehlungen zum Umgang mit Forschungsdaten erlassen. Auch von Förderinstitutionen, wie beispielsweise der Deutschen Forschungsgemeinschaft, werden zunehmend Angaben zum Datenmanagement bei der Antragstellung gefordert. Wesentliche Aspekte hierbei sind die Herkunft der Daten, die Maßnahmen für ihre angemessene Sicherung und ihre mögliche Nach- und Weiternutzung.
Der Beitrag nimmt das Handlungsfeld Forschungsdatenmanagement, seine Rahmungen, Effekte und Herausforderungen in den Blick. Er gründet auf der Annahme, dass mit den gegenwärtigen Entwicklungen und den zahlreichen Bemühungen zur Dissemination von Forschungsdatenmanagement auch Momente von Kontextsteuerung, Diskursnormierungen und Verschiebungen von Normalitätserwartungen einhergehen.

1. Digitaler Wandel: Forschungsdaten gewinnen an Bedeutung

Die voranschreitende Digitalisierung beeinflusst und verändert die Praktiken wissenschaftlicher Arbeit. Neue Technologien, digitale Werkzeuge und Infrastrukturen haben in den letzten Jahren vermehrt Einzug in nahezu alle Wissenschaftsdisziplinen gehalten und laden zur Entwicklung neuer Methoden und Arbeitsweisen ein.

Die Deutsche Forschungsgemeinschaft (DFG) hat dies im Oktober 2020 zum Anlass genommen, ein Impulspapier zum digitalen Wandel in den Wissenschaften zu formulieren. Darin werden die wichtigsten Merkmale des digitalen Wandels identifiziert, die wesentlichen Auswirkungen des digitalen Wandels auf die Forschung benannt und zukünftige Handlungsfelder der DFG abgesteckt. Unter dem Begriff „digitaler Wandel" fasst die DFG

> „alle relevanten Veränderungen und Auswirkungen in epistemischer, ethischer, rechtlicher, technischer, infrastruktureller, organisatorischer, finanzieller und auch sozialer Hinsicht […], die sich durch die Entwicklung und Nutzung digitaler Technologien in den Wissenschaften ergeben." (Deutsche Forschungsgemeinschaft 2020, S. 4)

Aus Sicht der DFG (ebd.) ist der digitale Wandel kein „wissenschaftsinternes Phänomen". Vielmehr sehen sich alle Bereiche der Gesellschaft und Wirtschaft durch den Einzug digitaler

Technologien und der Etablierung digitaler Arbeitsweisen grundlegenden Veränderungen[1] ausgesetzt. Die Wissenschaft ist aber laut DFG in ganz besonderer Weise befähigt und gefordert, den digitalen Wandel aktiv zu gestalten, seine Chancen zu nutzen und die vielfältigen Herausforderungen zu bewältigen. Klicken oder tippen Sie hier, um Text einzugeben.

Wandel infolge von Digitalisierungsprozessen fordert jedoch nicht nur wissenschaftliche Arbeitspraktiken und elaborierte Verfahren wissenschaftlicher Gemeinschaften heraus, sondern schlägt sich folgenreich auf Grundprinzipien und Normen guter wissenschaftlicher Praxis sowie Diskursen von Wissenschaft und ihren Öffentlichkeiten nieder. Ganz besonders deutlich wird dies im Hinblick auf die Forschungsdaten. Hierfür lassen sich mehrere Beispiele nennen wie z.B. Änderungen in den Anforderungen zum Umgang mit Forschungsdaten (siehe Deutsche Forschungsgemeinschaft 2019), die zunehmende Anerkennung von (digitalen) Forschungsdaten als wertvolle Quelle und eigenständige Wissenschaftsleistung (vgl. Jensen 2019, S. 31), die Entwicklung und Etablierung von institutionellen Policies[2] oder der Aufbau einer nationalen Forschungsdateninfrastruktur (NFDI)[3].

Der folgende Abschnitt folgt dem Gedanken, dass digitale Forschungsdaten in allen Wissenschaftsdisziplinen immer mehr an Bedeutung gewinnen und fragt danach, was Forschungsdaten eigentlich sind und wie wir mit ihnen umgehen.

2. Forschungsdaten und Forschungsdatenmanagement: Ein „neues“ Handlungsfeld für Wissenschaft und Forschung

Der Begriff „Forschungsdaten“ umfasst grundsätzlich alle (analogen und digitalen) Informationen und Daten, die „während des Forschungsprozesses entstehen oder ihr Ergebnis sind“ (Kindling et al. 2013, S. 45). Ein großer Teil der Forschungsdaten liegt heute in digitaler Form vor. Selbst in Disziplinen und Forschungsvorhaben, in denen analoge Arbeitsweisen mit „Stift und Papier“ (Imeri 2018b, S. 213) weiter Anwendung finden, spielen digitale Forschungsdaten und Methoden eine immer größer werdende Rolle. Auch in Wissenschaftsdisziplinen, die gewöhnlich mit Texten, Objektbeschreibungen und Bilder zu tun

---

1 Die DFG (2020, S.6) unterscheidet drei Typen des Wandels: *Erstens* die Transformation analoger Daten in digitale Formate (transformativer Wandel). *Zweitens* die Nutzung datenintensiver Technologien zur Bearbeitung von Forschungsfragen (ermöglichender Wandel) und *drittens* die Ablösung von grundlegenden Arbeitsweisen und Grundprinzipien (substituierender Wandel).

2 So wurde beispielsweise am 5. Mai 2021 eine Policy für das Forschungsdatenmanagement an der Freien Universität Berlin und eine Aktualisierung der Open-Access-Policy durch den Akademischen Senat verabschiedet. Eine allgemeine Übersicht über institutionelle Policies ist unter https://www.forschungsdaten.org [Stand vom 07-05-2021] zu finden.

3 https://www.nfdi.de/ [Stand vom 07-05-2021].

haben, finden diese nun verstärkt in digitaler Form Verwendung.[4] Gleichwohl wird nach wie vor nicht in jeder Forschung das gesamte Material digital erzeugt bzw. in eine digitale Form überführt. Wie Jane Kamensky, eine amerikanische Historikerin und Professorin für Geschichte an der Harvard University 2017 im Rahmen eines Symposiums zur digitalen Transformation des Sammelns an wissenschaftlichen Bibliotheken treffend formuliert, „in an era where it is fashionable to talk about the power and promise of 'big data,' much scholarship is still 'tiny data,' gathered by hand, and involves touching and noticing small details." (Malpas und Proffitt 2017, S. 14)

Doch was genau sind Forschungsdaten und was bedeutet es, sie zu managen? Diese Frage lässt sich nach Fabian Cremer et al. (2015, S. 14) „konkret nur aus Sicht der Fachdisziplinen oder Fach-Communities" beantworten. Während sich aber in den Naturwissenschaften ein allgemein geteiltes Verständnis davon, was Forschungsdaten sind, bereits etablieren konnte, hat sich in den geisteswissenschaftlichen Fächern noch keine gemeinsame Begriffsdefinition herausgebildet (vgl. Andorfer 2015, S. 4; Cremer et al. 2018, S. 153). Auch in den ethnologischen Fächern steht eine Reflexion des Datenbegriffs noch aus (vgl. Imeri 2018a, S. 72; Deutsche Gesellschaft für Sozial- und Kulturanthropologie 2019, S. 2), sodass mithin unklar bleibt, was genau durch den Begriff bezeichnet wird und „bei welchem Bearbeitungsstand von ‚Daten' gesprochen werden kann oder sollte" (Imeri 2019, S. 53).[5] Ausgehend davon, dass die Bedeutung des Datenbegriffs zunächst aus der eigenen Disziplin heraus begriffen werden muss, gibt der vorliegende Artikel zu bedenken, *dass*, wenn dem so sein sollte, die *Frage* womöglich *falsch gestellt* sei. Die Frage ist vielleicht gar nicht, was Forschungsdaten eigentlich sind, sondern wohl eher: Was wollen individuelle Forschende, einzelne Fachdisziplinen oder künftige *data communities*[6] als (Forschungs-)Daten auffassen?

Die DFG (2015) begreift Forschungsdaten als eine „wesentliche Grundlage für das wissenschaftliche Arbeiten". Entsprechend werden Forschungsdaten nicht als Nebenprodukt, sondern vielmehr als Basis einer jeden Forschungstätigkeit betrachtet. Zu Forschungsdaten zählt die DFG etwa Texte, Objekte aus Sammlungen oder Proben, Umfragedaten, Messdaten, Laborwerte und methodische Testverfahren wie z.B. Fragebögen, Software und Quellcode. Aber auch Interviewdaten, Audio- und Videoaufnahmen, Bilder, Protokolle und vieles andere mehr werden unter den Begriff Forschungsdaten gezählt. Zentral ist in diesem Zusammenhang nun, dass Forschungsdaten in den letzten Jahren einen „völlig neuen und gesteigerten Stellenwert" (Putnings et al. 2021, S. 115) erhalten haben. Sabine Imeri (2018b, S. 213) argumentiert, dass Forschungsdaten aus Sicht der Förderinstitutionen in allen Disziplinen

4 Zu Forschungsdaten in der (digitalen) Geschichtswissenschaft vgl. Hiltman 2018.

5 Besonders schwierig erweist sich der Begriff des „Datums" für die qualitative Sozialforschung, sofern er Daten mit Informationen gleichsetzt oder die Vorstellung von Daten als Fakten (‚data as hard numbers') voraussetzt.

6 Danielle Cooper und Rebecca Springer (2019, S.16) definieren „data communities" als „a loosely connected group of scholars who all work with a particular type of data, often linked by professional relationships". Data Communities zeichnen sich durch gemeinsame formelle oder informelle Praktiken des Teilens und Nachnutzens von Daten aus.

„künftig nicht nur abgelegt, ausgewertet, kombiniert und interpretiert, sondern auch gemanagt, langfristig archiviert, möglichst frei ausgetauscht und zur weiteren Verwendung zur Verfügung gestellt werden".

Unter dem Label „Forschungsdatenmanagement" werden ganz allgemein alle Aktivitäten und Maßnahmen gefasst, die mit der „Aufbereitung, Speicherung, Archivierung und Veröffentlichung von Forschungsdaten verbunden sind" (Simukovic et al. 2013, S. 6). Imeri et al. (2018, S. 72-73) unterscheiden drei Ebenen, anhand derer sich das Forschungsdatenmanagement und die damit verbundenen Erfordernisse beschreiben und kategorisieren lassen: Die erste Ebene – das *prozessbegleitende Datenmanagement* – umfasst zunächst einmal alle organisatorischen und technischen Maßnahmen und Entscheidungen, die zu treffen sind, um im Forschungsprozess einen adäquaten Umgang mit Forschungsdaten zu gewährleisten. Dazu zählen beispielsweise die Organisation und Ablage, Speicherung und Sicherung sowie der projektinterne Austausch von Forschungsdaten. Auf der Ebene der *Langzeitarchivierung* geht es darum, Forschungsdaten nach Projektende und unter Einhaltung datenschutzrechtlicher Vorgaben dauerhaft für einen angemessenen Zeitraum abzulegen. Langzeitarchivierung geht dabei über das reine Backup oder die Ablage auf Festplatten hinaus. Im Sinne der Langzeitarchivierung müssen Daten stets „lesbar" erhalten werden, z.B. auch über eine lange Speicherdauer und etwaige Dateiformatänderungen hinweg. Die dritte Ebene des Datenmanagements betrifft die Bereitstellung und *Nachnutzung* von Forschungsdaten. Hier geht es darum, Wissen nicht nur zu sammeln und aufzubewahren, sondern mit anderen zu teilen und für weitere Forschung nutzbar zu machen. Forschungs-datenmanagement fungiert hier als ein umfassender Begriff, um eine Menge von Aktivitäten und Erfordernissen zu beschreiben, die im Umgang mit (digitalen) Forschungsdaten derzeit neu ausgehandelt werden.

Auch wenn digitale Forschungsdaten über alle Fächer hinweg immer mehr an Bedeutung gewinnen und das Thema Forschungsdatenmanagement mittlerweile in allen Fachdisziplinen Eingang gefunden hat, lassen sich bei der konkreten Umsetzung von Forschungsdatenmanagement und der Entwicklung geeigneter Verfahren und infrastruktureller Lösungen in den Fachdisziplinen „jedoch (noch) unterschiedliche Geschwindigkeiten" (Cremer et al. 2015, S. 14) feststellen. Während sich in einigen Disziplinen bereits geeignete Best-Practice-Lösungen, Daten-Infrastrukturen und verbindliche Vorgehensweisen etabliert haben, stehen andere Fach-Communities noch am Anfang bzw. sehen sich mit ganz besonderen Herausforderungen konfrontiert.[7]

Darüber hinaus unterliegt der „adäquate" Umgang mit Forschungsdaten wiederum gesellschaftlichen Wertungen, Normen sowie institutionellen Anforderungen. Mittlerweile wurde der Umgang mit Forschungsdaten in Richtlinien und Policies von wissenschaftlichen Institutionen und Förderorganisationen verankert. In anderen Worten, Forschungsdatenmanagement ist das Ergebnis wissenschaftspolitischer Forderung nach einem zeitgemäßen Management, einer nachhaltigen Aufbewahrung und einem offenen Austausch von

[7] So stellt beispielsweise die Ebene der Nachnutzung ein besonders schwieriges Terrain für ethnografische Forschung dar (vgl. Imeri et al. 2018, S. 73).

wissenschaftlichen Daten. Im Folgenden werden die wissens- und förderpolitischen Rahmungen des Umgangs mit Forschungsdaten in Deutschland, insbesondere die entscheidenden Impulse der DFG zum Umgang mit Forschungsdaten näher beleuchtet. Darin zeigen sich die verbindlichen Regeln, Anforderungen und Erwartungen, die aktuell von Wissenschaft und Politik im Handlungsfeld „Forschungsdatenmanagement" verhandelt werden.

3. Wissenschaftspolitische Rahmungen: Regulierung und Standardisierung des Umgangs mit Forschungsdaten

Mit der Denkschrift zur „Sicherung guter wissenschaftlicher Praxis" legt die DFG (1988) den Grundstein für ein nachhaltiges Forschungsdatenmanagement an wissenschaftlichen Einrichtungen in Deutschland. Darin heißt es (siehe Empfehlung 7, S. 12, Herv. im Original): *„Primärdaten als Grundlagen für Veröffentlichungen sollen auf haltbaren und gesicherten Trägern in der Institution, wo sie entstanden sind, für zehn Jahre aufbewahrt werden."* Wie in den Erläuterungen zur Empfehlung 7 ausgeführt wird, sollen die Arbeitsschritte auf dem Weg zum wissenschaftlichen Ergebnis so nachvollziehbar dargelegt werden, dass sie an anderer Stelle „nachvollzogen" bzw. „reproduziert" werden können. Einerseits werden arbeitsökonomische Gründe hierfür als maßgebend betrachtet, andererseits wird die langfristige Archivierung von Forschungsdaten als Voraussetzung für die prinzipielle Nachvollziehbarkeit und Überprüf-barkeit wissenschaftlicher Ergebnisse betrachtet.

2003 wurde die „Berliner Erklärung über den offenen Zugang zu wissenschaftlichem Wissen" veröffentlicht und seither von zahlreichen Wissenschaftsorganisationen unterzeichnet.[8] Die Empfehlungen zum „offenen Zugang" (Open Access) richten sich nicht nur an Forschungs- und Förderinstitutionen, sondern auch an kulturelle Einrichtungen wie Bibliotheken, Archive und Museen. In der Berliner Erklärung wird das Ziel formuliert, die neuen Möglichkeiten des Internets zu nutzen, um Wissen einer möglichst breiten Öffentlichkeit zugänglich zu machen. Betont wird, dass „unsere Aufgabe Wissen weiterzugeben […] nur halb erfüllt [ist], wenn diese Informationen für die Gesellschaft nicht in umfassender Weise und einfach zugänglich sind". Im Zitat finden sich Hinweise darauf, dass Veröffentlichung und Zugänglichmachung als Aufgabe und Verantwortung gegenüber einer Öffentlichkeit verstanden und eingefordert werden. Gewünscht wird nicht weniger als ein „Kulturwandel" (vgl. Imeri 2018b, S. 217), der in der Berliner Erklärung als ein „Prozess des Übergangs zu einer Kultur des offenen Zugangs" umschrieben wird. Als Objekte, die nach dem „Prinzip des offenen Zugangs" frei zugänglich

[8] Aktueller Stand der Unterzeichner abgerufen unter: http://oa.mpg.de/lang/de/berlin-prozess/signatoren/ [Stand vom 07-05-2021].

gemacht werden sollen, werden nicht nur wissenschaftliche Forschungsergebnisse, sondern auch Forschungsdaten[9] genannt.

Seit 2007 gibt es im Rahmen von DFG-Sonderforschungsbereichen die Möglichkeit, ein Infrastrukturprojekt (kurz: INF) zu beantragen (vgl. Engelhardt 2013). Damit wurde ein wichtiger Schritt gesetzt, um Forschungsdatenmanagement in größeren Forschungsverbünden lokal einzubetten[10] und Lösungen und Maßnahmen im direkten Austausch mit Forschenden zu entwickeln. Zu den Kernaktivitäten von INF-Projekten zählen neben der Planung und Umsetzung eines nachhaltigen Datenmanagementkonzepts auch der Aufbau und der Betrieb der dafür notwendigen Infrastruktur. Dazu arbeiten INF-Projekte eng mit Informationseinrichtungen am Standort, z.B. den Bibliotheken oder Rechenzentren, zusammen. Sie nehmen daher eine wichtige Mittlerposition zwischen den vorhandenen Infrastruktureinrichtungen und den spezifischen Bedarfen der Forschenden ein. Dass Forschungsdatenmanagement nicht nur eine Frage der Infrastruktur ist, zeigt die unterschiedliche Ausgestaltung und Schwerpunktsetzung innerhalb der INF-Projekte.[11]

Im Jahr 2010 hat die Allianz der deutschen Wirtschaftsorganisationen „Grundsätze zum Umgang mit Forschungsdaten" verabschiedet. Darin hält sie fest: „Qualitätsgesicherte Forschungsdaten bilden einen Grundpfeiler wissenschaftlicher Erkenntnis." Die Allianz spricht sich darin für eine langfristige Sicherung und Zugänglichkeit von Forschungsdaten aus. Weitere Themenfelder, die im Grundsatzpapier aufgegriffen werden, sind Unterschiede der wissenschaftlichen Disziplinen, wissenschaftliche Anerkennung, Lehre und Qualifizierung, Verwendung von Standards und Entwicklung von Infrastrukturen. Die Allianz-Grundsätze gelten als wichtiger Meilenstein in der damaligen Diskussion um den zeitgemäßen Umgang mit Forschungsdaten.

Die DFG verabschiedet am 30. September 2015 die „Leitlinien zum Umgang mit Forschungsdaten". Darin greift die DFG die „Grundsätze" der Allianz auf und konkretisiert diese hinsichtlich der DFG-Fördervorgaben. In den Leitlinien schreibt die DFG den Gedanken fort, dass Forschungsdaten einen Grundpfeiler wissenschaftlichen Arbeitens darstellen und Grundlage für weiterführende Forschung sein können. Die nachhaltige Sicherung und Bereitstellung der Forschungsdaten eröffnet aus Sicht der DFG nicht nur Anschlussmöglichkeiten für weitere Forschung, sondern ist zugleich bedeutsam für die „Qualitätssicherung" wissenschaftlicher Arbeit. Mit der Veröffentlichung der Leitlinien ist zugleich eine Aufforderung an die Fachgemeinschaften gerichtet, ihren Umgang mit Forschungsdaten zu reflektieren.

Im Juli 2019 hat die DFG einen Kodex „Leitlinien zur Sicherung guter wissenschaftlicher Praxis" beschlossen. Dieser ist am 1. August 2019 in Kraft getreten und ersetzt die ehemalige Denkschrift zur „Sicherung guter wissenschaftlicher Praxis", die zuletzt 2013 überarbeitet

---

9 Als Forschungsdaten sind z.B. Ursprungsdaten, Quellenmaterialien, bildliche und graphische Materialien sowie multimediale Darstellungen aufgelistet.

10 Wird auch als „Embedded Data Management" bezeichnet. Siehe dazu Cremer et al. 2015.

11 Zur unterschiedlichen Ausgestaltung und Schwerpunktsetzung von INF-Projekten siehe Engelhardt 2013.

worden war. Der Kodex der Deutschen Forschungsgemeinschaft richtet sich sowohl an WissenschaftlerInnen als auch an die Hochschulen und außerhochschulischen Forschungseinrichtungen. Die Wissenschaftseinrichtungen in Deutschland sind aufgefordert, die Leitlinien in den eigenen Satzungen zur guten wissenschaftlichen Praxis bis zum 31. Juli 2022 rechtsverbindlich umzusetzen, um auch in Zukunft Fördermittel durch die DFG erhalten zu können. Inhaltlich fasst der Kodex die zentralen Standards guter wissenschaftlicher Praxis zusammen und beschreibt das Verfahren im Falle wissenschaftlichen Fehlverhaltens. In mehreren Leitlinien des Kodex finden sich Angaben zum Umgang mit Forschungsdaten. Dabei spielen neben einer Reihe forschungspraktischer Aspekte des Managements von Daten insbesondere die Forschungsdatenpublikation und die Aufbereitung von Forschungsdaten hinsichtlich der weiteren Nachnutzung eine zentrale Rolle.[12]

So findet sich in der Leitlinie (L) 13 die Annahme, dass die Herstellung von öffentlichem Zugang zu Forschungsergebnissen grundsätzlich zur guten wissenschaftlichen Praxis von Forschenden gehöre. Aus Gründen der „Nachvollziehbarkeit, Anschlussfähigkeit der Forschung und Nachnutzbarkeit“ (Erläuterungen zu L13, S. 19) sollen aus Sicht der DFG künftig neben den Ergebnissen auch „die den Ergebnissen zugrunde liegenden Forschungsdaten, Materialien und Informationen, die angewandten Methoden sowie die eingesetzte Software verfügbar“ (ebd.) gemacht und Arbeitsverfahren und Abläufe nachvollziehbar dargelegt werden. Gleichzeitig erkennt L13 (S. 18) an, dass es „im Einzelfall […] aber Gründe geben [kann], Ergebnisse nicht öffentlich zugänglich […] zu machen“ oder nur unter bestimmten Bedingungen nach außen zu geben. Forschende sind demnach aufgefordert, die den Publikationen zugrunde liegenden Forschungsdaten, wo immer „möglich und zumutbar“ (Erläuterungen zu L10, S. 16) zu veröffentlichen, um so im Sinne einer transparenten Wissenschaft einen Beitrag zu Open Science zu leisten. Forschungsdaten sollen gemäß der FAIR[13] Prinzipien auffindbar (Findable), zugänglich (Accessibe), interoperabel (Interoperable) und wiederverwendbar (Reusable) sein.

Als Publikationsorgane (L15, S. 21) sollen neben Büchern und Zeitschriften auch Fach-, Daten- oder Softwarerepositorien in Betracht gezogen werden. Die Entscheidung, ob, wie und wo Ergebnisse öffentlich zugänglich gemacht werden, soll laut DFG von Forschenden „in eigener Verantwortung – unter Berücksichtigung der Gepflogenheiten des betroffenen Fachgebiets“ (L13, S. 18) getroffen werden. In der L17 werden über die WissenschaftlerInnen hinaus auch die wissenschaftlichen Einrichtungen in die Pflicht genommen, die für die nachhaltige Sicherung erforderliche Infrastruktur bereitzustellen. Forschungsdaten, die einer Publikation zugrunde liegen, sollen in „adäquater Weise“ gesichert und für einen „angemessenen Zeitraum“ aufbewahrt werden (L17, S. 22). Daten sollen an der Einrichtung, wo sie

[12] Heinz Pampel hält am 10.07.2020 im Gemeinschaftsblog zu wissenschaftlicher Kommunikation im Netz dazu fest, dass es bemerkenswert sei, „wie tief die Forderung nach Open Science den Kodex durchdringt“. https://wisspub.net/2010/07/10/grundsatze-zum-umgang-mit-forschungsdaten-veroffentlicht/ [Stand vom 07-05-2021].

[13] Siehe auch https://www.go-fair.org/fair-principles/ [Stand vom 07-05-2021].

entstanden sind oder in standortübergreifenden Repositorien zugänglich gemacht und nachvollziehbar gespeichert werden.

Die überblicksartige Darstellung der wissenschaftspolitischen Rahmenbedingungen und der bestehenden Regelungen, Leitlinien und Empfehlungen zeigt, dass der Ruf nach einem adäquaten Forschungsdatenmanagement vonseiten der Politik und Wissenschaft immer lauter wird. Sie gibt Aufschluss darüber, wie der Umgang mit (digitalen) Forschungsdaten von Politik und Wissenschaft verhandelt und zu unterschiedlichen Zeiten schriftlich fixiert wird: Forschungsdatenmanagement wird in erster Linie als *Mittel und Zweck zur Herstellung von Transparenz und Nachvollziehbarkeit* erkennbar. So sollen die den Forschungsergebnissen zugrunde liegenden Informationen im Sinne guter wissenschaftlicher Praxis dokumentiert und archiviert werden. Darüber hinaus wird Forschungsdatenmanagement als *Instrument zur Förderung von Nachhaltigkeit in Wissenschaft und Forschung* an verschiedenen Stellen eingefordert. Es gilt als explizites Ziel (und Erwartung) des Forschungsdatenmanagements, wissenschaftliche Ergebnisse und die ihnen zugrunde liegenden Daten so offen wie möglich mit der Scientific Community bzw. einer Öffentlichkeit zu teilen und damit die Entstehung weiterer Erkenntnisse zu ermöglichen. Als *Instrument der Kontrolle und Qualitätssicherung* zielt Forschungsdatenmanagement auf die Reproduzierbarkeit und Überprüfbarkeit von Forschungsergebnissen ab. Die sorgfältige Dokumentation und Archivierung von Forschungsdaten sollen dazu dienen, weitere Auswertungen bzw. Replikationen von Ergebnissen zu ermöglichen.

Darüber hinaus ist Forschungsdatenmanagement auch ein *Instrument der Regulierung und Standardisierung*, das Effekte freisetzt und Herausforderungen – insbesondere für die qualitative Sozialforschung – beinhaltet. Die fachübergreifenden Regelungen, Empfehlungen und Leitlinien sehen sich mit der Kritik konfrontiert, dass diese nicht vollends mit bisherigen Arbeitsweisen von Forschenden bzw. Disziplinen im Einklang stehen. Die DFG hat daher bereits 2015 einen Appell an alle Wissenschaftsdisziplinen gerichtet, „ihren Umgang mit Forschungsdaten zu reflektieren und angemessene Regularien zur disziplinspezifischen Nutzung und ggf. offenen Bereitstellung von Forschungsdaten zu entwickeln“. (Deutsche Forschungsgemeinschaft 2015, S. 2) Mittlerweile sind verschiedene Fachgesellschaften diesem Auftrag nachgekommen und haben differenzierte Beurteilungen der Anforderungen an einen nachhaltigen Umgang mit Forschungsdaten in Form von Positionspapieren und Empfehlungen[14] vorgelegt. Darin werden sowohl Möglichkeiten und Herausforderungen der Bereitstellung und Nachnutzung von Forschungsdaten thematisiert, Zielkonflikte und Passungsprobleme artikuliert sowie Bedarfe und Forderungen an Förderorganisationen formuliert. Der nächste Abschnitt widmet sich schwerpunktmäßig den Herausforderungen des Umgangs mit (digitalen) Forschungsdaten in der qualitativen Sozialforschung.

[14] In Anlehnung an Maike Altenrath et al. (2020) wird davon ausgegangen, dass Förderrichtlinien dem aktuellen politischen Diskurs entsprechen bzw. etwas darüber aussagen.

4. Effekte und Herausforderungen: Forschungsdatenmanagement in der qualitativen Sozialforschung

Auch qualitativ Forschende sehen sich zunehmend mit der Erwartung konfrontiert, ihre heterogenen Forschungsdaten und -materialien zu archivieren und wenn möglich zur Nachnutzung, z.B. im Rahmen von Sekundäranalysen zur Verfügung zu stellen. Als Ausgangspunkt und Hintergrund der folgenden Erörterung dient exemplarisch[15] für die qualitative Sozialforschung das „Positionspapier zum Umgang mit ethnologischen Forschungsdaten" der Deutschen Gesellschaft für Sozial- und Kulturanthropologie (DGSKA) (2019), das „Positionspapier zur Archivierung, Bereitstellung und Nachnutzung von Forschungsdaten" der Deutschen Gesellschaft für Volkskunde (dgv) (2018) und die Stellungnahme des Vorstands und Konzils der Deutschen Gesellschaft für Soziologie (DGS) (2019) zur „Bereitstellung und Nachnutzung von Forschungsdaten". Der folgende Abschnitt geht der Frage nach, vor welche Herausforderungen das Datenmanagement die qualitative Sozialforschung stellt. Zugleich gerät in den Fokus, welche Verschiebungen, Normalitätserwartungen und Diskursnormierungen einhergehen, geprägt und vonseiten der Fördergeber vorangetrieben werden. Nach Sichtung der Papiere lassen sich vier gemeinsame Schnittpunkte im Hinblick auf die Archivierung, Bereitstellung und Verfügbarmachung von qualitativen Forschungsdaten bestimmen:

Nicht alle qualitativen Forschungsdaten können einer Nachnutzung zugänglich gemacht werden.

Blickt man zunächst auf Aussagen zur Bereitstellung und Nachnutzung von Forschungsdaten, ist allen Positionspapieren die Annahme inhärent, dass die Verfügbarmachung von Forschungsdaten im Kontext qualitativer Forschungsvorhaben nur begrenzt möglich ist. Während die DGS (2019) im Positionspapier ganz grundsätzlich festhält, dass „nicht alle wissenschaftlich erhobenen Forschungsdaten (…) einer Nachnutzung zugänglich gemacht werden" können, verweist die DGSKA (2019) auf die Schwierigkeit der Veröffentlichung und freien Verfügbarmachung von ethnologischen Forschungsdaten. Die dgv nimmt noch feingranularer auf die Daten Bezug, die im Zuge ethnografischer Verfahren entstehen. Sie hält fest: „Eine regelrechte Veröffentlichung ethnografischer Daten wird in der überwiegenden Zahl der Fälle nicht möglich sein." (Deutsche Gesellschaft für Volkskunde 2018, S. 5)

Entsprechend darf die Nachnutzbarkeit von Daten nicht als „Normalmodell" von Forschung gelten.

---

[15] Auswahlkriterien für diese Dokumente war die eigene Verortung im Sonderforschungsbereich (SFB) 1171 „Affective Societies – Dynamiken des Zusammenlebens in bewegten Welten" an der Freien Universität Berlin. Der SFB 1171 versammelt insgesamt zehn Disziplinen aus den Geistes-, Kultur-, Sozial-, und Naturwissenschaften. Schwerpunktmäßig liegt der Fokus meiner Arbeit im integrativen Service- und Forschungsprojekt „Datenmanagement und Informationsinfrastruktur" auf dem FDM in den ethnologischen bzw. ethnografischen Teilprojekten.

Die Feststellung, dass nicht alle Forschungsdaten gleichermaßen für die Nachnutzung wissenschaftlich zugänglich gemacht werden kann, ist nicht als generelle Ablehnung des Datenmanagements und Data Sharing zu lesen. Vielmehr machen die Fachgesellschaften darauf aufmerksam, dass unter Umständen der Verzicht auf die Veröffentlichung von Daten als sinnvoll und erforderlich erachtet werden kann, wie der folgende Textausschnitt aus dem dgv-Positionspapier verdeutlicht: „Forschende sollen unterstützt werden, die mit der Archivierung verbundenen Chancen zu nutzen, aber auch das Recht haben, die Nachnutzung der Daten einzuschränken." (ebd., S. 4) Aus dem Zitat geht gleichermaßen hervor, dass in den Papieren Forschungsdatenmanagement als Chance und gleichzeitige Verpflichtung verhandelt wird. Entsprechend heißt es im Positionspapier der DGS (2019) auch: „Die Sekundärnutzung von Daten [darf] nicht als ‚Normalmodell' von Forschung gelten." Dies gilt es auch vonseiten der Fördergeber anzuerkennen. Entsprechend soll die Nachnutzbarkeit der Daten, die Vergabe durch Forschungsmitteln nicht beeinflussen. Darüber hinaus wird die Entwicklung von Standards und Kriterien gewünscht, die den in den Fächern etablierten Arbeitsweisen, methodischen Zugängen und Spezifika entsprechen (vgl. Deutsche Gesellschaft für Sozial- und Kulturanthropologie 2019, S. 1).

Die Vielfalt empirischer Zugänge und die Heterogenität der Forschungsdaten widersetzt sich per definitionem einer Standardisierung und Regulierung des Umgangs mit Forschungsdaten.

Die Vielfalt und Unterschiedlichkeit qualitativer Verfahren und Forschungsfelder führen in der Regel dazu, dass Forschungsdaten „heterogen, wenig standardisiert und multimodal" (Deutsche Gesellschaft für Volkskunde 2018, S. 2) sind. Um dieser Vielfalt gerecht zu werden und diese zu erhalten, fordert die DGSKA (2019, S.2) eine Berücksichtigung der Heterogenität von Forschungsdaten bei Prozessen der Datenarchivierung und -nachnutzung. Aufgrund der Vielgestaltigkeit von qualitativer Forschung wird eine „gleichmäßige und bedingungslose Verpflichtung" (Deutsche Gesellschaft für Volkskunde 2018, S. 4), Forschungsdaten zu veröffentlichen und nachnutzbar zu machen abgelehnt. Vielmehr sollen die Möglichkeiten und Grenzen der Bereitstellung und Nachnutzung von Forschungsdaten differenziert und stets unter ethischen Gesichtspunkten abgewogen werden. Folgende Aspekte werden konkret benannt, die dabei ebenso berücksichtigt werden sollen: das Wesen qualitativer Daten, die Besonderheiten qualitativer Forschungsprozesse, der Aufwand der Aufbereitung sowie der Schutzbedarf qualitativer Daten. Die Frage, ob und welche Forschungsdaten frei zugänglich gemacht werden können, kann demnach nicht standardmäßig, sondern nur „einzelfallbezogen" (Deutsche Gesellschaft für Volkskunde 2018, S. 5) beantwortet werden.

Die wünschenswerte Offenheit qualitativer Forschungsprozesse konfligiert mit der wissenschaftspolitischen Forderung nach Planungssicherheit und Berechenbarkeit.

Offenheit ist ein zentrales Moment qualitativer Sozialforschung. Das Prinzip der Offenheit gilt sowohl gegenüber dem Forschungsgegenstand als auch gegenüber der jeweiligen Forschungsmethode (vgl. Rieker und Seipel 2006). Entsprechend müssen Forschende flexibel sein und ihre Methoden und geplanten Arbeitsschritte immer wieder neu an zuvor nicht vorhersehbare Entwicklungen des Gegenstandes und Erfordernissen der Situation anpassen. Die dgv (2018, S.1) hält schwerpunktmäßig mit Blick auf die ethnografische Forschung fest,

dass diese als „offener Prozess“ konzipiert sei, der situations- wie beobachterabhängig verläuft. Zwar führen diese Offenheit und Flexibilität gegenüber dem Untersuchungsgegenstand und der Bereitschaft, ggf. geplante Arbeitsschritte zu modifizieren, zu besonders differenzierten Einsichten in die Komplexität und Dynamik sozialer Situationen und Prozesse. Mit Blick auf die Anforderungen des Datenmanagements entstehen aber auch Spannungen, wenn bereits bei Antragstellung Angaben zu den anfallenden Daten und den geplanten Umgang erwartet bzw. zunehmend auch in Form eines Datenmanagementplans (DMP)[16] eingefordert werden. Die gut gemeinte Merkregel „always remember to plan ahead“ widerspricht der gängigen Forschungspraxis bei offenen Formen der Datenerhebung.

Entscheidungen über die Archivierung und Verfügbarmachung von qualitativen Forschungsdaten können nur schwer im Vorfeld getroffen werden und es muss möglich sein, Entscheidungen auch zu einem späteren Zeitpunkt zu revidieren (vgl. ebd., S. 3). Entsprechend wird gefordert, dass die Flexibilität auch im Hinblick auf den Umgang mit Daten im gesamten Forschungsprozess bewahrt und sichergestellt wird (vgl. Deutsche Gesellschaft für Sozial- und Kulturanthropologie 2019, S. 6). Um diese Offenheit und Flexibilität zu erreichen, sollen alternative Möglichkeiten (z.B. Exit-Strategien bei der Datenarchivierung) geschaffen werden.[17]

5. Zusammenfassung und Ausblick: Daten(management) und Politik

Wissenschaftliches Arbeiten ist seit dem Einzug des Digitalen einem Wandel unterzogen. Immer mehr Forschungsdaten liegen in digitaler Form vor, werden im Laufe des Forschungsprozesses ins Digitale überführt oder werden ausschließlich digital produziert. Dem Thema Forschungsdaten wird im wissenschaftspolitischen Diskurs aktuell ein hoher Stellenwert beigemessen. Forschungs- und Förderinstitutionen wie die DFG haben in den letzten Jahren wiederholt Anforderungen an die Handhabung von digitalen Forschungsdaten formuliert.

Die Leitlinien, Empfehlungen und Richtlinien geben einen Rahmen vor, wie Daten effizient, nachhaltig und verantwortungsvoll im Kontext von Wissenschaft und Forschung gehandhabt werden. Die Forderung, mit (digitalen) Forschungsdaten auf bestimmte Weise umzugehen, ist

---

[16] Datenmanagementpläne sind ein zentrales Instrument des Forschungsdatenmanagements. Ein DMP beschreibt, wie während und nach der Projektlaufzeit mit den im Forschungsprojekt anfallenden Forschungsdaten verfahren wird. Vereinfacht gesagt beschreibt ein DMP, welche Daten im Zuge eines Forschungsprojektes entstehen bzw. verwendet werden und was während des Forschungsverlaufs mit ihnen geschehen soll. Darüber hinaus werden in einem DMP Verantwortlichkeiten und Rechte geregelt sowie datenschutzrechtliche wie forschungsethische Aspekte berücksichtigt.

[17] Am Forschungsdatenzentrum Qualiservice werden aktuell Möglichkeiten und Wege der Archivierung exploriert und erarbeitet, um künftig auch ethnologische Forschungsdaten zu archivieren und für die Weiternutzung in der Forschung und für die Lehre zugänglich zu machen. Weitere Informationen unter https://www.qualiservice.org/de/ [Stand vom 08-05-2021].

für alle Wissenschaftsdisziplinen herausfordernd – insbesondere auch für die qualitative Sozialforschung. Schließlich gehen mit diesen Entwicklungen Standardisierungs- und Regulierungsprozesse einher, die der Vielfalt, Flexibilität und Offenheit qualitativer Sozialforschung zuwiderlaufen.

Forschungsdatenmanagement ist daher mehr als eine Agenda. Der Datenbegriff und in Erweiterung dazu das Forschungsdatenmanagement sind offene und umkämpfte Felder, in denen Akteurinnen und Akteure mit höchst divergenten Interessen, Erwartungen und Arbeitsweisen aufeinandertreffen. Dabei zeigt sich, dass Daten(management) und Politik untrennbar miteinander verbunden sind (vgl. Ruppert et al. 2017, 2). Entsprechend gilt es, Forschungsdatenmanagement nicht zuletzt auch als politische Form der Regulierung und Standardisierung in den Blick zu nehmen und zu hinterfragen.

In diesem Sinne bedarf das Thema weiterer Auseinandersetzung, die im Modus konsequenter Analyse und Reflexion von Möglichkeiten und Herausforderungen FDM-bezogener Prozesse und Praktiken realisiert werden soll. Speziell zu den konkreten Effekten, die das Forschungsdatenmanagement (Maßnahmen und Infrastrukturen) auf die Arbeitspraktiken und die Wissensproduktion haben, fehlen noch empirische Befunde: Wie verändert Forschungsdatenmanagement eigentlich die Art und Weise, wie, wo, wann und mit wem geforscht wird? Wie genau ereignen und stabilisieren sich Praktiken und Gewissheiten des Umgangs mit Forschungsdaten? Und wie gehen Forschende mit den Transformationsprozessen konkret um?

Literatur

Allianz der deutschen Wissenschaftsorganisationen (2010). Grundsätze zum Umgang mit Forschungsdaten. *RatSWD Working Paper* 156. Berlin: Rat für Sozial- und Wirtschaftsdaten. Abgerufen unter: https://www.konsortswd.de/wp-content/uploads/RatSWD_WP_156.pdf [Stand vom 07-05-2021].

Altenrath, Maike; Helbig, Christian & Hofhues, Sandra (2020): Deutungshoheiten. Digitalisierung und Bildung in Programmatiken und Förderrichtlinien Deutschlands und der EU. *MedienPädagogik: Zeitschrift für Theorie und Praxis der Medienbildung,* 17 (Jahrbuch Medienpädagogik), S. 565–594. DOI: 10.21240/mpaed/jb17/2020.05.22.X.

Andorfer, Peter (2015): Forschungsdaten in den (digitalen) Geisteswissenschaften. Versuch einer Konkretisierung. *DARIAH-DE Working Papers*, 14, S. 4–27.

Berliner Erklärung über den offenen Zugang zu wissenschaftlichem Wissen (2003): 22. Oktober 2003. Abgerufen unter: https://openaccess.mpg.de/68053/Berliner_Erklaerung_dt_Version_07-2006.pdf [Stand vom 07-05-2021].

Cooper, Danielle & Springer, Rebecca (2019): Data Communities. A New Model for Supporting STEM Data Sharing. *ITHAKA S+R Issue Brief*. DOI: 10.18665/sr.311396.

Cremer, Fabian; Engelhardt, Claudia & Neuroth, Heike (2015): Embedded Data Manager – Integriertes Forschungsdatenmanagement. Praxis, Perspektiven und Potentiale. *Bibliothek Forschung und Praxis* 39 (1), S. 13–31. DOI: 10.1515/bfp-2015-0006.

Cremer, Fabian; Klaffki, Lisa & Steyer, Timo (2018): Der Chimäre auf der Spur. Forschungsdaten in den Geisteswissenschaften. *O-Bib. Das Offene Bibliotheksjournal* 5 (2), S. 142–162. DOI: 10.5282/O-BIB/2018H2S142-162.

Deutsche Forschungsgemeinschaft (DFG) (1988): *Vorschläge zur Sicherung guter wissenschaftlicher Praxis. Denkschrift.* Abgerufen unter: https://mpimet.mpg.de/fileadmin/download/Good_scientific_practice_at_MPI-M/Sicherung_guter_wissenschaftlicher_Praxis_DFG.pdf [Stand vom 07-05-2021].

Deutsche Forschungsgemeinschaft (DFG) (2015): Leitlinien zum Umgang mit Forschungsdaten. 30. September 2015. Abgerufen unter: https://www.dfg.de/download/pdf/foerderung/grundlagen_dfg_foerderung/forschungsdaten/richtlinien_forschungsdaten.pdf [Stand vom 07-05-2021].

Deutsche Forschungsgemeinschaft (DFG) (2019): *Leitlinien zur Sicherung guter wissenschaftlicher Praxis. Kodex.* Deutsche Forschungsgemeinschaft. DOI: 10.5281/zenodo.3923602.

Deutsche Forschungsgemeinschaft (DFG) (2020): *Digitaler Wandel in den Wissenschaften*. 28. Oktober 2020. Impulspapier. DOI:10.5281/zenodo.4191345.

Deutsche Gesellschaft für Sozial- und Kulturanthropologie (DGSKA) (2019): *Positionspapier zum Umgang mit ethnologischen Forschungsdaten. Unter Mitarbeit von Röttger-Rössler, Birgitt; Dilger, Hansjörg; Imeri, Sabine & Huber, Elisabeth. 01. Oktober 2019.* Abgerufen unter: https://www.dgska.de/wp-content/uploads/2019/11/Positionspapier_Bearbeitet-fu%CC%88r-MV_24.09.2019.pdf [Stand vom 07-05-2021].

Deutsche Gesellschaft für Soziologie (DGS) (2019): *Bereitstellung und Nachnutzung von Forschungsdaten in der Soziologie. Stellungnahme des Vorstands und Konzils der DGS. 08. Jänner 2019.* Abgerufen unter: https://soziologie.de/fileadmin/user_upload/stellungnahmen/DGSStellungnahme_zum_Forschungsdatenmanagement_08.01.2019.pdf [Stand vom 07-05-2021].

Deutsche Gesellschaft für Volkskunde (dgv) (2018): *Positionspapier zur Archivierung, Bereitstellung und Nachnutzung von Forschungsdaten.* Deutsche Gesellschaft für Volkskunde. 19. November 2018. Abgerufen unter https://www.d-g-v.de/wp-content/uploads/2020/03/dgv-Positionspapier_FDM-1.pdf [Stand vom 07-05-2021].

Engelhardt, Claudia (2013): Forschungsdatenmanagement in DFG-Sonderforschungsbereichen. Teilprojekte Informationsinfrastruktur (INF-Projekte). *LIBREAS. Library Ideas* 23, S. 106–130. DOI: 10.18452/9045.

Hiltman, Torsten (2018): Forschungsdaten in der (digitalen) Geschichtswissenschaft. Warum sie wichtig sind und wir gemeinsame Standards brauchen. In: *Das Blog der AG Digitale Geschichtswissenschaft im VHD (Digitale Geschichtswissenschaft)*. 27. September 2018. Abgerufen unter: https://digigw.hypotheses.org/2622 [Stand vom 07-05-2021].

Imeri, Sabine (2018a): Archivierung und Verantwortung. Zum Stand der Debatte über den Umgang mit Forschungsdaten in den ethnologischen Fächern. In: Hollstein, Betina & Strübing, Jörg (Hrsg.): Archivierung und Zugang zu Qualitativen Daten. *RatSWD Working Paper* 267. Berlin: Rat für Sozial- und Wirtschaftsdaten, S. 69-79.

Imeri, Sabine (2018b): Ordnen, archivieren, teilen. Forschungsdaten in den ethnologischen Fächern. *Österreichische Zeitschrift für Volkskunde* LXXII/121 (2), S. 213–243.

Imeri, Sabine (2019): ‚Open Data' in den ethnologischen Fächern. Möglichkeiten und Grenzen eines Konzepts. In: Klingner, Jens & Lühr, Merve (Hrsg.): *Forschungsdesign 4.0. Datengenerierung und Wissenstransfer in interdisziplinärer Perspektive.* Dresden: Institut für Sächsische Geschichte und Volkskunde, S. 45–59.

Imeri, Sabine; Sterzer, Wjatscheslaw & Harbeck, Matthias (2018): Forschungsdatenmanagement in den ethnologischen Fächern. Bericht aus dem Fachinformationsdienst Sozial- und Kulturanthropologie. *Zeitschrift für Volkskunde* 114 (1), S. 71–75.

Jensen, Uwe (2019): Forschungsdaten und Forschungsdatenmanagement in den Sozialwissenschaften. In: Jensen, Uwe; Netscher, Sebastian & Weller, Katrin (Hrsg.): *Forschungsdatenmanagement sozialwissenschaftlicher Umfragedaten. Grundlagen und praktische Lösungen für den Umgang mit quantitativen Forschungsdaten.* Opladen: Verlag Barbara Budrich, S. 13–35.

Kindling, Maxi; Simukovic, Elena & Schirmbacher, Peter (2013): Forschungsdatenmanagement an Hochschulen. Das Beispiel der Humboldt-Universität zu Berlin. *LIBREAS. Library Ideas* (23), S. 43–63. DOI: 10.18452/9041.

Malpas, Constance & Proffitt, Merrilee (2017): *The Transformation of Academic Library Collecting: A Synthesis of the Harvard Library's Hazen Memorial Symposium*. Dublin, OH: OCLC Research. DOI: 10.25333/C3J04Z

Putnings, Markus; Neuroth, Heike & Neumann, Janna (2021): *Praxishandbuch Forschungsdatenmanagement*. Berlin, München, Boston: De Gruyter Saur.

Rieker, Peter & Seipel, Christian (2006): Offenheit und Vergleichbarkeit in der qualitativen und quantitativen Forschung. In: Rehberg, Karl-Siegbert (Hrsg.): *Soziale Ungleichheit, kulturelle Unterschiede. Verhandlungen des 32. Kongresses der Deutschen Gesellschaft für Soziologie in München 2004*. Frankfurt am Main, New York: Campus, S. 4038–4046. Abgerufen unter: https://nbn-resolving.org/urn:nbn:de:0168-ssoar-142320 [Stand vom 07-05-2021].

Ruppert, Evelyn; Isin, Engin & Bigo, Didier (2017): Data politics. *Big Data & Society* 4 (2), 1-7. DOI: 10.1177/2053951717717749.

Simukovic, Elena; Kindling, Maxi & Schirmbacher, Peter (2013): Umfrage zum Umgang mit digitalen Forschungsdaten an der Humboldt-Universität zu Berlin. Abgerufen unter: http://nbn-resolving.de/urn:nbn:de:kobv:11-100213001[Stand vom 07-05-2021]

Funktionsweisen von Verschwörungserzählungen auf Social Media und der parallel aufkeimende Antisemitismus

Andre Wolf

Zusammenfassung

Verschwörungserzählungen sind nichts Neues. Doch im Zuge der Coronapandemie haben sie eine menschenfeindliche Renaissance erfahren. Alte antisemitische Ritualmordlegenden finden in einem hochdynamischen neuen Erzähluniversum eine neue Verbreitung. Sie liefern in Krisenzeiten Feindbilder, vereinen dadurch Menschen unterschiedlicher Gruppierungen und stellen (falsch-) einfache Lösungen bereit.
Eine nicht unwesentliche Rolle spielt darin das QAnon-Erzähluniversum, in dem teils absurde Verschwörungsnarrative von gequälten Kindern auf der Metaebene für eine Radikalisierung und Selbstlegitimierung der Gewaltanwendung führen. Diese stetige Radikalisierung, auch auf Basis von Verschwörungserzählungen, stellt am Ende eine reale Gefahr für die Demokratie dar.[1]

1. Antisemitische Verschwörungserzählungen und das Coronavirus: Eine Gefahr für die Demokratie?

Vor wenigen Jahren noch hätten wir auf Podien oder in Diskussionsrunden gesessen und über die Gefahren von Fake News auf Social Media gesprochen. Darüber sind wir mittlerweile jedoch hinaus und diskutieren nun über Verschwörungserzählungen. Fake News können wir recht unproblematisch mit Fakten widerlegen. Verschwörungserzählungen hingegen bieten ein Erzähluniversum, das Fakten ignoriert oder sie sogar in ihre Immunitätsmechanismen integriert. Verschwörungserzählungen wurden auf Social Media über lange Jahre hinweg belächelt, waren es in der Vergangenheit doch häufig absurde Geschichten von der hohlen Erde, von einer flachen Erde, oder von Außerirdischen aus dem Aldebaran-System. Hin und wieder ging es um Reptiloide oder auch um Chemtrails. Diese Verschwörungserzählungen waren im Großen und Ganzen gesellschaftlich nicht weiter gefährlich. Es konnte lediglich vorkommen, dass jene Personen, die sie verbreiten, einen persönlichen Reputationsschaden erlitten haben. Parallel zu diesen Mythen existierten jedoch auch immer schon antisemitische Verschwörungserzählungen, die explizite Feindbilder beinhalten. In diesen Mythen sind generell Juden, aber auch einzelne Personen stellvertretend für Juden als Feindbilder aufgetaucht. Besonders bekannt sind

[1] Der Beitrag basiert auf Überlegungen aus dem Buch: Angriff auf die Demokratie (Wolf 2021, S. 137–164),

hierbei Verschwörungserzählungen rund um George Soros oder um die Familie Rothschild.

Doch seit mehreren Monaten hat sich etwas geändert. Die Corona-Pandemie hat dazu geführt, dass es eine Art Renaissance der antisemitischen Verschwörungserzählungen gibt. Diese Verschwörungserzählungen haben häufig uralte Ritualmordlegenden zum Vorbild oder stützen sich generell auf bereits bestehende Narrative. Auf den ersten Blick und einzeln betrachtet ergeben antisemitische Verschwörungsmythen im Umfeld des Coronavirus wenig Sinn und wirken absurd. Nach näherer Betrachtung fällt allerdings auf, dass diese neuen Mythen ein eigenes, gefährliches Erzähluniversum aufbauen.

Die Initialzündung der antisemitischen Verschwörungserzählungen in Bezug auf das Coronavirus können wir auf den Anfang April 2020 verorten. Genauer gesagt war ein Video des Künstlers Xavier Naidoo ein wichtiger Auslöser. Viele Menschen haben dieses Video gesehen oder zumindest in den Medien davon erfahren. Naidoo, vor seinem Smartphone sitzend, berichtet von Kindern in unterirdischen Höhlen. Er spricht davon, dass tausende Kinder von sogenannten „Eliten“ in diesen unterirdischen Gefängnissen gefangen gehalten werden und sich dort grausamen Ritualen unterwerfen müssen.

2. Am Beispiel der „Adrenochrom-Legende“

Durch genau dieses Video haben zwei Dinge in Österreich und Deutschland eine große Bekanntheit gewonnen, die bis dato kaum Gehör erhalten haben, da es sich um absurde Verschwörungsszenerien handelte: QAnon und Adrenochrom.

Kommen wir zuerst auf das Video zu sprechen. Naidoo erzählt darin weinend von Kindern, die „in diesem Moment“ weltweit aus den Händen von Pädophilen befreit werden. Kryptisch nennt er auch das Stichwort „Adrenochrom“, ohne es weiter auszuführen. Er sagt:

> „Adrenochrom… geht auf Adrenochrom … Bilder … wenn ihr das ertragen könnt, und ich weiß seit mindestens 15 Jahren, was los ist.“ (Xavier Naidoo, 2020, selbst veröffentlichtes Video auf Telegram)

Wer Naidoos Rat folgt und nun „Adrenochrom“ in die Google-Bildersuche eintippt, stößt in der Tat auf eine Menge Behauptungen, Kern ist: Der Stoff soll eine Verjüngungsdroge sein, welche die „Hollywood-Elite“ aus den Körpern entführter und gefolterter Kinder gewinnt. Diese, nicht näher erläuterten Eliten werden in der Erzählung zu Feindbildern stilisiert. Die Kinder dienen laut der Verschwörungserzählung als Nutztiere, die gefoltert werden, um qualitativ hochwertiges Adrenochrom zu gewinnen, mit denen sich Eliten auf ewig jung halten. Dieser erzählerische Kniff ist notwendig, um den Feindbildern etwas Schlimmes vorzuwerfen. Und das ist ein wichtiger Punkt: Kinder als Opfer der Feinde.

Denn es gibt kaum etwas sagbar Schlimmeres, als Kindern (alternativ jungen, unschuldigen Frauen oder aber auch Haustieren) etwas Grauenvolles anzutun.

Jene Infos über die gefangenen Kinder hat Naidoo anscheinend aus einer der zahlreichen QAnon-Gruppen, die auf Telegram existieren. QAnon ist angeblich ein Insider der US-Regierung, der solcherlei Informationen leakt. Doch dazu später mehr.

Zunächst interessiert erst einmal die Frage: Was ist Adrenochrom eigentlich? Wo kommt es her, was soll es bewirken, warum werden zur Gewinnung angeblich Kinder entführt? Adrenochrom ist eine seit Jahrzehnten bekannte Verbindung, die im Körper durch die Oxidation von Adrenalin entsteht. Also ist weder der Begriff noch diese chemische Verbindung eine Erfindung. Die Verbindung kann jedoch ohne weiteres im Labor hergestellt und käuflich erworben werden. Menschen sind dafür nicht notwendig, eine Folter ebenso wenig.

Eine halluzinogene Wirkung hat die Verbindung nicht, eine verjüngende Wirkung schon gar nicht. Ebenso ist die Idee der Gewinnung von Adrenochrom aus Adrenalindrüsen von Menschen eine reine Erfindung des Autors Hunter S. Thompson für den Film „Fear and Loathing in Las Vegas“. Insofern macht es auch absolut keinen Sinn, warum „Hollywood-Eliten“ Kinder entführen sollten, um aus ihnen Adrenochrom zu zapfen. Selbst wenn sie es für eine halluzinogene Droge halten würden, könnten sie es einfach kaufen oder mit genügend Geld im Labor selbst herstellen. Dies wäre auch effektiver.

Doch um das alles geht es am Ende nicht. Es geht vielmehr um gewisse Symbole und Narrative, die ihre Bedeutung auf der Metaebene entfalten und deren Wirkungsweise und Ablauf sich in mehreren Falschmeldungen und Verschwörungserzählungen während der Corona-Pandemie wiederfinden. Die Elemente, die wir in der Geschichte Naidoos und der Adrenochrom-Legende finden, sind weder neu noch einzigartig. Sie folgen einem wichtigen und wiederkehrenden Muster.

3. Adrenochrom: Eine uralte Ritualmordlegende der Gegenwart

Das Muster in der Geschichte lässt sich leicht erklären: Wie erschafft man sich ein Feindbild, an dessen Ende man sich absolut dazu legitimiert sieht, dieses Feindbild zu verfolgen, ja sogar töten zu dürfen? Die Lösung ist so einfach wie leider auch immer wieder funktionierend: indem man dieses Feindbild entmenschlicht und ihm die schlimmsten Gräueltaten unterstellt, die man zwar nicht beweisen kann, die aber anhand bestehender Narrative glaubwürdig klingen und anhand von Indizien oder Bündelungen von sinnstiftenden Erzählungen vermeintlich bewiesen werden. So funktionieren Ritualmordlegenden.

Diese Legenden sind bereits uralt und teilweise extrem antisemitisch. Ritualmordlegenden basieren auf dem Narrativ, dass eine gesellschaftliche Minderheit im Geheimen

Gräueltaten, ja gar Morde, an der Mehrheit der Bevölkerung ausübt. Das Gefährliche an diesen Ritualmordlegenden ist das Ergebnis: Angestachelt von diesem Mythos wird die verleumdete Minderheit verfolgt. Zunächst wird sie kriminalisiert, dann durch die Erzählungen entmenschlicht und am Ende physisch verfolgt.

Ritualmordlegenden haben eine lange Geschichte und wurden verwendet, um eine gesellschaftliche Minderheit verfolgen zu können. In Europa waren das häufig antisemitische Legenden, so wie beispielsweise die Behauptung, Juden entführten christliche Kinder, um sie für rituelle Zwecke grausam zu ermorden. Mithilfe dieser Darstellungen wurden häufig unerklärbare Phänomene versucht zu erklären, man erkennt also auch hier deutlich den Drang dazu, hinter allem einen Plan vermuten zu müssen, auch wenn dieser Plan grauenvoll ist.

Die Ritualmordlegenden selbst gleichen sich ebenfalls. Die (teils geheimen) Minderheiten verüben grauenvolle Taten an den ihnen unterlegenen Personen aus der stärkeren Mehrheit. Hierbei handelt es sich zumeist um Kinder, aber es kann sich durchaus auch um kranke, gebrechliche oder alte Menschen handeln. Wichtig dabei ist lediglich, dass die vermeintliche Tätergruppe sich unmenschlich verhält und unbedingt dafür verurteilt, ja am besten ermordet werden muss.

Die Tätergruppe bleibt dabei recht unspezifisch. Es wird entweder lediglich eine Ethnie generell beschuldigt oder eine gewisse Gruppe von Menschen angeprangert. Eine konkrete Benennung von Personen findet selten statt, was auch für die Ritualmordlegende an sich wichtig ist, da sie so unkonkret wie möglich gehalten werden muss, um die Minderheit als Ganze verfolgen zu können.

Die wohl bekanntesten mittelalterlichen Ritualmordlegenden sind die Erzählungen um William von Norwich und Simon von Trient. Beide Geschichten weisen die typischen Merkmale dieser Legenden auf. Wer die Geschichten nicht kennt, hier eine kurze Beschreibung:

In der Legende um William von Norwich heißt es, dass der junge Mann William, ein Kürschnerlehrling, im Jahre 1144 in der Karwoche (was wir uns an dieser Stelle einfach merken) von Juden heimlich auf rituelle Weise hingerichtet wurde. Das zumindest wurde in den Schriften eines Mönches unter dem Titel „De Vita et passione sci Willelmi martiris norwic („Leben und Passion des Märtyrers Wilhelm von Norwich“)“ in mehreren Bänden veröffentlicht. Den Juden vor Ort konnte das natürlich nie nachgewiesen werden, es gab entsprechend auch kein Urteil. Interessant ist jedoch, dass sich laut Schriften die klagenden Personen auf „Traumgesichter“ oder ihre innere Überzeugung bzw. ihren Glauben beriefen. Beweise gab es schlichtweg nicht. Aus William von Norwich wurde aufgrund der entstandenen Ritualmordlegende ein Märtyrer.

Abbildung 1: Ritualmordlegenden. Bild: Martyrium des Simon von Trient, Darstellung aus der Nürnberger Weltchronik von Hartmann Schedel. Datum:1493; Quelle: Hartmann Schedels Weltchronik (Nürnberg 1493); Urheber: Woodcuts by Michel Wolgemut, Wilhelm Pleydenwurff (Text: Hartmann Schedel); Lizenz: Dies ist eine originalgetreue fotografische Reproduktion eines zweidimensionalen Kunstwerks. Das Kunstwerk an sich ist aus dem folgenden Grund gemeinfrei: Public domain. Dieses Werk ist gemeinfrei, weil seine urheberrechtliche Schutzfrist abgelaufen ist. Dies gilt für das Herkunftsland des Werks und alle weiteren Staaten mit einer gesetzlichen Schutzfrist von 100 oder weniger Jahren nach dem Tod des Urhebers.

Die später entstandene Ritualmordlegende um Simon von Trient ist da schon extremer. Auch hier spielt die Karwoche erneut eine Rolle, jedoch geht es nicht allein um einen Mord, sondern die rituelle Komponente rückte mehr in den Vordergrund. Neben dieser gewann das Blut der Opfer immer mehr an Bedeutung, denn die neuen Ritualmordlegenden sprachen auf einmal davon, dass die Täter, in diesem Fall Juden, das Blut für bestimmte Zwecke benötigten. Diese Zwecke sollten angeblich medizinischer Natur sein (auch das merken wir uns an dieser Stelle).

4. Antisemitischer Hintergrund!

Worum ging es nun bei der Ritualmordlegende um Simon von Trient? Effektiv gesehen ging es auch bei dieser Legende nur darum, Juden als Minderheit in der Gesellschaft generell zu kriminalisieren und ihnen schlichtweg ein bestialisches Image zu verpassen. Der Jude als Ritualmörder an sich, der im Geheimen irgendwelche Fäden zieht und schuld am Übel der Gesellschaft ist.

Kommen wir nun auf die Geschichte selbst zu sprechen. Im Jahr 1475 verschwand der Legende entsprechend dabei der zweijährige Simon von Trient. Der Sohn eines Gerbers verschwand nicht Mitte September oder irgendwann im Februar, sondern auch hier angeblich in der Karwoche. Wir erkennen also die Gleichheiten, die auf Ostern und damit indirekt auf den Tod Christi verweisen. Ritualmorde als eine Form des Racheakts, die nun einhergehen mit der Verwendung des Blutes der Opfer.

Wie ging nun die Geschichte um Simon von Trient aus? Laut Überlieferung wurde das Kind in einem Rinnstein an einem Ostersonntag von einem Juden gefunden, der den Fund ordentlich meldete. Das ging für ihn nicht gut aus, denn er stand direkt unter Verdacht und es kam zu einer grauenvollen Folter, unter der der Mann sich beugte und am Ende eine Schuld eingestand, die er jedoch nicht trug. Er sagte schlichtweg unter der Folter aus, was seine Verhörer von ihm hören wollten.

Auch wenn es im Nachhinein durch Papst Sixtus IV eine Untersuchung gab, so war diese nicht wirklich auf eine Aufklärung bedacht. Laut dieser war am Ende die Verfahrensweise in Ordnung, jedoch verbot Papst Sixtus IV, Juden deswegen zu verfolgen. Zu spät jedoch, denn der Verdächtigte sowie 12 weitere Personen wurden bereits umgebracht. Man bemerkt an dieser Stelle, dass Ritualmordlegenden durchaus einen Mord legitimieren sollen.

Die Ritualmordlegenden zogen sich über das gesamte Mittelalter bis in die Neuzeit. Sie waren auch Bestandteil im Holocaust, wirklich bewiesen wurde so ein Ritualmord jedoch nie. Natürlich nicht, denn es handelt sich um eine Legende, die zu einer sinnstiftenden Erzählung gewachsen ist und am Ende immer plausibel klingt, sobald sie auftaucht. Ein Beweis ist aufgrund ihrer vermeintlichen Glaubwürdigkeit also nicht mehr notwendig.

5. Was hat die Ritualmordlegende mit dem Coronavirus bzw. den Mythen rund um das Coronavirus zu tun?

Hier wird es spannend, da wir uns auf einer Metaebene befinden, auf der es nicht mehr direkt um Juden, sondern über den indirekten Weg mittels „Eliten" geht, die letztendlich in Verschwörungslegenden um Juden ebenso ihren Platz haben. Die Adrenochrom-Legende ist eine dynamische Weiterentwicklung der Ritualmordlegenden und hat in ihrem Ursprung auf den ersten Blick wenig mit Juden oder Ritualmorden zu tun. Doch dieser Schein trügt.

Die Adrenochrom-Legende spricht zwar nicht von getöteten, jedoch von gefangenen und gefolterten Kindern, denen in Ritualen ein Hormon abgenommen wird. Wir reden also von einem schweren Verbrechen, einer Gräueltat gegenüber Kindern.

War es im Mittelalter das Blut von Kindern, das durch perverse Rituale von „gesellschaftlichen Minderheiten" auf verbrecherische Weise gewonnen wurde, stellt Adrenochrom exakt dieselbe Ritualmordlegende in einem modernen Gewand dar. Kindern wird angeblich eine Körperflüssigkeit (Blut entspricht hier dem Hormon Adrenochrom) entnommen, die zu medizinischen Zwecken der teuflischen Minderheit dient. Nichts hat sich also am Narrativ selbst geändert, lediglich in der Art der Darstellung hat eine Veränderung stattgefunden.

Adrenochrom allein reicht nicht für die moderne Adaption der Ritualmordlegenden, sondern die Adrenochrom-Erzählung ist nur ein Teil des Ganzen. Daneben gibt es Geschichten um Kinder in unterirdischen Gefängnissen, die extrem eng an die Adrenochrom-Legende geknüpft sind, da es eben diese Kinder sein sollen, denen man das Hormon abnimmt. Auch hier finden sich mehr als deutliche Parallelen zu den ältesten Ritualmordlegenden: Es soll sich um entführte Kinder handeln, die durch eine Minderheitenelite gequält werden und denen man zu „medizinischen Zwecken" Flüssigkeiten abnimmt.

Die modernen Erzählungen zu gefangenen Kindern haben teils ebenso absurde und groteske Elemente wie ihre Pendants aus der fernen Vergangenheit. Ein Beispiel: Angeblich befinden sich tausende gefangene Kinder unter dem Central Park in New York in unterirdischen Tunneln. Man erkennt einfach das Muster wieder, das hier zum Tragen kommt. Wenn auch an dieser Stelle erneut unbewiesene Tunnel in den Erzählungen vorkommen, so merken wir uns diese Tunnel ein weiteres Mal.

Kommen wir wieder auf den Central Park und auf die Kinder zurück. Zurückzuführen ist diese Geschichte auf die Behelfskrankenhäuser, die zu Beginn der Coronakrise in New York in Zelten im Central Park errichtet wurden. New York kämpfte mit dem Coronavirus. Gleichzeitig wurde das Behelfskrankenhaus im Central Park bewusst falsch interpretiert und der Befreiung von tausenden Kindern zugeschrieben.

Was in New York zu Beginn der Coronakrise der Fall war: Das Krankenhausschiff Comfort der US-Marine war im Hafen von New York City angedockt. New York wurde im April 2020 als „Epizentrum des Virusausbruchs“ in den Vereinigten Staaten dargestellt, das Schiff sollte die Kapazitäten in den zivilen Krankenhäusern der Stadt entlasten, damit sich die Krankenhäuser auf Coronavirus-Patienten konzentrieren können. Gleichzeitig wurde im Central Park in New York eine Art Feldkrankenhaus errichtet (Central Park Samaritan’s Purse Field Hospital), mit dem andere Krankenhäuser der Stadt entlastet werden sollten. So weit, so plausibel. Aber alles Plausible kann man mithilfe von Narrativen und ein wenig gewolltem Verschwörungsglauben in eine andere Realität ummünzen.

Und genau das geschieht im QAnon-Erzähluniversum. Die Adrenochrom-Legende ist nur eine von vielen Geschichten aus dem QAnon-Erzähluniversum. An dieser Stelle wäre es daher wichtig, einen Exkurs zu dem Begriff QAnon zu unternehmen und darauf zu schauen, wie die einzelnen Mythen in dem Erzähluniversum aufgebaut sind und welches Ziel die Geschichten haben.

6. QAnon

QAnon spielt in den USA bereits seit 2016 eine Rolle, in Österreich oder Deutschland ist dieses Erzähluniversum seit dem Frühjahr 2020 bekannter geworden. Daher verwundert es nicht, dass die älteren Verschwörungserzählungen Bilder und Mythen aus den USA transportieren und dass die symbolischen Feindbilder für uns auf den ersten Blick nicht immer verständlich sind. So zum Beispiel, warum die Kinder angeblich in New York gefangen sind und nicht irgendwo im verlassenen mittleren Westen.

Denn es hat einen Grund, warum ausgerechnet New York ein Tunnelsystem mit gefangenen Kindern haben soll. New York ist ein sogenannter „Blauer Staat“. Das bedeutet, er ist klassischerweise ein Bundesstaat der Demokraten. Diese Blauen Staaten liegen hauptsächlich im Nordosten der USA, sowie entlang der Westküste. Dementsprechend ist es logisch, dass New York, aber auch beispielsweise Hollywood, immer wieder Verschwörungsmythen zum Opfer fallen, da es sich bei diesen Mythen um einen Angriff auf politische Gegner handelt. Wir erkennen auch hier den Aufbau von Feindbildern und deren Entmenschlichung zur Selbstlegitimierung vollstreckerischen Handelns.

Zunächst auf die USA bezogen erkennt man die typischen Feindbilder: Linksliberale Eliten (von ihren politischen Gegnern abwertend als Libtards = liberal bastards bezeichnet) sind Verbrecher. Auf der Metaebene haben wir es mit dem Bild des Judentums aus den Ritualmordlegenden zu tun, auf das später noch eingegangen wird.

Ausschlaggebend für die Bezeichnung „Q“ war ein Eintrag im Internet-Forum 4Chan eines Nutzers mit dem Nickname „Q“. „Q“ sollte hier wohl den Sicherheitsstatus „Q

Clearance“ andeuten: die höchste Freigabestufe für geheime Informationen. Nutzer im Forum 4Chan tragen die Bezeichnung „Anonymous“, so wurde „Anon“ beigefügt und zeigt wiederum die Anonymität, unter der dieser Nutzer agiert. Der Autor im Forum behauptete, hochrangiger Regierungsmitarbeiter zu sein und seine Informationen unter dem Deckmantel der Anonymität weiterzugeben.

Die meisten Ausführungen sind kryptisch und vage formuliert. So werden sie weiter interpretiert und wachsen zu den Legenden an, denen wir mittlerweile immer öfter im Internet und in sozialen Medien begegnen.

QAnon Mythen arbeiten stark mit anlassbezogenen Inhalten. Das bedeutet, sie nutzen reale Vorkommnisse und interpretieren sie innerhalb der Grenzen des Bedeutungsrahmens im eigenen Erzähluniversum. Hier können wir wieder auf den Einsatz der Schiffe vor New York sowie des Behelfskrankenhauses im Central Park schauen. Beide Elemente wurden bewusst in einen Verschwörungsmythos eingearbeitet. Wir sind hier wieder bei den gefangenen Kindern angekommen und müssen in Bezug auf QAnon uns in Erinnerung rufen, dass im Zuge des QAnon-Narratives Donald Trump ein Heilsbringer ist, der linksliberale Eliten in die Knie zwingt.

Somit findet an dieser Stelle in Bezug auf das Schiff sowie auf das Behelfskrankenhaus eine massive Umdeutung statt: Das Behelfskrankenhaus sowie das Schiff seien Teil einer großangelegten Kinderbefreiung – so der Mythos. Diese Kinder, die von Pädophilen missbraucht worden sein sollen, seien angeblich in Tunneln unter dem Central Park gefangen gewesen und Trump hätte die Rettung angeordnet. Es soll sich dabei um viele tausend Kinder gehandelt haben, die Zahlen variieren.

Bei dieser Interpretation handelt es sich in keinster Weise um eine einmalige Deutung. Als vor wenigen Wochen im Suez Kanal das Containerschiff Ever Given den Kanal blockierte, kam dasselbe Narrativ zur Anwendung. Auf dem Schiff sollen sich angeblich ebenfalls versklavte Kinder befunden haben. Der QAnon-Mythos spricht an dieser Stelle davon, dass das Schiff absichtlich im Suez Kanal festgesetzt wurde, um die Kinder zu befreien.

Wir erkennen an dieser Stelle wieder die typischen Erzählstrukturen, die von Eliten, geheimen Ritualen, Feindbildern und Kindern sprechen und immer wieder anlassbezogen auftauchen. Dadurch zeigt sich das hochdynamische Potenzial, welches das QAnon Erzähluniversum bietet und dass es am Ende nicht mehr zwingend mit den USA verbunden sein muss.

7. Warum ausgerechnet Kinder?

Die Ritualmordlegenden aus der Vergangenheit tragen eine interessante neuzeitliche Dynamik in sich. Das Motiv der Kinder, welches bereits in diesen Legenden verwendet wird, wird über Ort und Zeit hinweg als regelmäßig wiederkehrendes Element genutzt. Hier geht es nämlich darum, die Feindbilder zu entmenschlichen. Das ist ein wichtiger Schritt innerhalb der Verschwörungserzählungen.

Der Schritt, bereits ein bestimmtes Feindbild aufgebaut zu haben, geht grundsätzlich voran. Dieses Feindbild kann eine Regierung oder eine gewisse Gruppe innerhalb einer Gesellschaft sein. Nun geht es zwingend darum, dieses Feindbild zu entmenschlichen. Eine ideale Entmenschlichung wird erschaffen, indem dem Feindbild das schlimmste aller Übel vorgeworfen wird. Eines dieser schlimmsten Übel ist es, Kinder zu quälen oder zu foltern.

Das wird exakt in diesen klassischen Verschwörungserzählungen angewendet. Aber auch in anderen, nicht so detaillierten Narrativen finden wir das Bild der gequälten Kinder. So gab es im letzten Herbst in Deutschland mehrere Behauptungen, dass Kinder sterben, wenn sie Masken tragen. Das war natürlich nicht der Fall, doch dieser Vorwurf wurde genutzt, um der Regierung Kinderquälerei als größtmögliches Übel vorwerfen zu können. Hier findet also eine Entmenschlichung statt, um im nächsten Moment einen Angriff oder einen Aufstand (in welcher Weise auch immer) gegenüber einer demokratisch gewählten Regierung zu legitimieren.

Diese Effekte zeigen sich auch. Im Sommer 2020 kam es in Deutschland während einer Demonstration gegen die Coronamaßnahmen zum „Sturm“ der Treppen des Reichstags in Berlin. Im Herbst gab es einen Brandanschlag auf das Robert-Koch-Institut. Das Institut ist zuständig für die Informationen rund um die Zahlen der Coronainfektionen in Deutschland. Mit dem Anschlag sollte eine ablehnende Haltung gegenüber den Maßnahmen der Coronakrise zum Ausdruck gebracht werden. Nicht zuletzt gab es auch in Österreich aggressive Tendenzen auf den sogenannten Coronademos. Teilweise sind im Vorfeld verschiedene Chatnachrichten aufgetaucht, die von (gewaltsamen) politischen Umstürzen sprechen.

8. Die Gefahr für die Demokratie

Doch sind diese Einzelaktionen bereits die große Gefahr für die Demokratie? Nein, eher nicht. Die größere Gefahr, die über Verschwörungserzählungen transportiert wird, liegt in der Erschaffung von Feindbildern in Bezug auf gesellschaftliche Gruppen. An dieser Stelle kommt der Antisemitismus der Verschwörungserzählungen zum Tragen. Als im Frühjahr 2020 die ersten Verschwörungserzählungen während der Coronapandemie aufgetaucht

sind (wie die Adrenochrom-Legende), hatten diese noch keinen direkten Bezug zur Corona-Thematik und der darin enthaltene Antisemitismus kam nur vage und auf der Metaebene zum Vorschein.

Mittlerweile wird der Antisemitismus dieser Verschwörungserzählungen auch in Bezug auf das Coronavirus recht offen kommuniziert, auch wenn oftmals ein Antisemitismus im Nachhinein bestritten wird. Die Verschwörungserzählungen bilden ihre klassischen Feindbilder anlassbezogen auf die aktuelle Situation ab. Regierungen werden nicht allein zum Feindbild erklärt, sondern hinter den Regierungen werden geheime Drahtzieher vermutet. Diese Drahtzieher, auch als Eliten bezeichnet, finden ihren Ursprung in der Erzählung des sogenannten Weltjudentums. Innerhalb dieser Erzählung wird pauschal dargestellt, dass „Juden" als fiktives Kollektiv im Geheimen die Weltherrschaft anstreben. In diesem Umfeld erscheinen auch immer wieder Begriffe wie „Zionismus" oder „Weltregierung" auf. Ebenso werden die Namen Soros, Rothschild oder Rockefeller als Symbol für diese Verschwörungserzählung genutzt.

Gleichzeitig finden wir auf den sogenannten Coronademos eine massive Holocaust-Relativierung. Impfungen werden mit dem Holocaust gleichgesetzt. Tafeln und Transparente mit Sprüchen wie „Impfen macht frei" tauchen regelmäßig auf den Demonstrationen auf und bauen eine gekünstelte und überzogen falsche Opferdarstellung der Demoteilnehmenden auf. Dieses verdrehte Opferbewusstsein geht einher mit einem neu entfachten Judenhass, der nicht nur in Österreich, sondern auch in Deutschland während der Demonstrationen beobachtet werden konnte. Sowohl eine Täter-Opfer-Umkehr als auch die unterschwellige Schuldzuweisung gegenüber Juden aufgrund antisemitischer Verschwörungserzählungen führten bis dato zu einem weit verbreiteten Antisemitismus, der im Jahresbericht 2020 der Meldestelle Antisemitismus deutlich erwähnt wird. Im Abschnitt „Corona-Verschwörungsmythen" lautet es:

> „Antisemitismus mit Coronabezug
>
> Diese ad-hoc eingeführte Subkategorie tritt nicht im Vakuum auf, sondern stets im Verbund mit Verschwörungsmythen und/oder Shoah-Relativierung und/oder mit dem Thema Israel.
>
> Der Anstieg der gemeldeten Fälle Ende des Jahres ist – wie auch an anderer Stelle erläutert – vor allem auf die immer aggressiver auftretenden Gegnerinnen und Gegnern der Coronamaßnahmen zurückzuführen, jedoch auch auf die erhöhte Sensibilität und dadurch gestiegene Zahl an Meldungen, vor allem von Seiten anderer Organisationen der Zivilgesellschaft." (Bericht: Antisemitische Vorfälle 2020, Seite 9; 2021, Antisemitismus Meldestelle)

Bereits im dazu erschienenen Vorbericht wurde verdeutlicht, dass in den aufgetretenen Verschwörungserzählungen verkalkulierte Begriffe und Namen stellvertretend angewendet wurden. Hier lautet es:

> „Beispielhaft anzuführen sind hier die obszön antisemitischen Aussagen einer seit Anbeginn der Corona-Demos präsenten wie wortführenden Aktivistin aus dem rechten Milieu, Jennifer Klauninger, welche Ende Mai in einem selbst aufgenommenen Video unter anderem Soros und Rothschild als Führer der Weltelite bezeichnete – beide Namen dienen Verschwörungstheoretikern als antisemitischer Code für den „mächtigen Juden" […]" (Bericht: Gemeldete antisemitische Vorfälle im 1. Halbjahr 2020, Seite 3; 2021, Antisemitismus Meldestelle)

Hier liegen die tatsächlichen Gefahren. Ab dem Moment, in dem Teile einer Bevölkerung, einzelne Gruppen oder Ethnien angefeindet, bedroht oder gar verfolgt werden, ist die Demokratie in Gefahr. Bei diesem Prinzip spielt es keine Rolle, ob wir von Juden, Homosexuellen oder bestimmten politischen Richtungen sprechen. Die Verschwörungserzählungen bauen an dieser Stelle bewusst ihre einfach gestalteten Feindbilder auf, deren Eliminierung am Ende eine einfache Lösung eines komplexen Problems bieten soll.

Literatur

Gensing, Patrick (2020): „*Sturm*" *auf Reichstagsgebäude – Mit gezielten Falschmeldungen aufgehetzt.* 31. August 2020. Abgerufen unter: https://www.tagesschau.de/faktenfinder/reichstag-berlin-sturm-fakenews-101.html [Stand vom 30-04-2021].

Gemeldete antisemitische Vorfälle im 1. Halbjahr 2020. (2021): Antisemitismus Meldestelle. Abgerufen unter: https://fca755ac-004d-4a98-bf62-6ebd5ba1ecc3.filesusr.com/ugd/0a9e18_64f4d46da51346d6b13ece884bfd7b70.pdf [Stand vom 05-02-2019].

Habermalz, Christiane (2020): *Warnung vor Judenhass bei den Corona-Protesten*. 24. November 2020. Abgerufen unter: https://www.deutschlandfunk.de/antisemitismus-warnung-vor-judenhass-bei-den-corona.1766.de.html?dram:article_id=488068 [Stand vom 30-04-2021].

Huld, Sebastian (2020): *Verschwörungstheorie QAnon; Horrormärchen der Kinderfolterer geht um*. 21. Mai 2020. Abgerufen unter: https://www.n-tv.de/politik/Horrormaerchen-der-Kinderfolterer-geht-um-article21776816.html [Stand vom 30-04-2021].

Lorenz, Laurin; Pucher, Johannes; Schmidt, Colette M. & Schmid, Fabian (2021): *"Querdenker" diskutierten vor Demo in Wien „Übernahme des Parlaments*". 19. Jänner 2021. Abgerufen unter: https://www.derstandard.at/story/2000123431741/querdenker-diskutierten-vor-demo-in-wien-uebernahme-des-parlaments [Stand vom 30-04-2021].

Michel, Anke (2021): *Polizei sucht nach Anschlag auf RKI-Gebäude mit Foto nach Verdächtigem.* 16. April 2021. Abgerufen unter: https://www.rbb24.de/panorama/beitrag/2021/04/brandanschlag-rki-fahndung-verdaechtiger-foto.html [Stand vom 30-04-2021].

Sulzbacher, Markus (2021): *Der bizarre Antisemitismus auf den Corona-Demos.* 18. April 2021. Abgerufen unter: https://www.derstandard.at/story/2000125773958/der-bizarre-antisemitismus-auf-den-corona-demos [Stand vom 30-04-2021].

Wolf, Andre (2020): *Befreite Kinder im Central Park / New York?* 07. April 2020. Abgerufen unter: https://www.mimikama.at/aktuelles/kinder-new-york/ [Stand vom 30-04-2021].

Wolf, Andre (2021): *Angriff auf die Demokratie*. Wien: Edition A.

Ölstandsanzeiger: Über die Unsichtbarmachung und Naturalisierung der Produktion personenbezogener Daten

Tobias Stadler

Zusammenfassung

In der gegenwärtigen Debatte über Daten und Datafication wird nicht mit Beschreibungen gespart, in denen diese Informationen als natürliche Ressourcen imaginiert werden: *Data as the new Oil* evoziert den Reichtum globaler Ölkonzerne, *Data Mining* erzeugt Bilder vom glückssuchenden Goldschürfenden und die *Cloud* lässt die Materialität von Infrastrukturen verpuffen.
Diese Bilder haben eine *ideologische* Funktion, die die zugrunde liegenden Produktionsbedingungen dieser Daten naturalisieren und verdecken. Sie sorgen dafür, dass eine solche Produktion als *natürlich*, *selbstverständlich* und *unausweichlich* betrachtet wird. Dementsprechend bleiben viele Umgangsformen mit den ungewünschten Seiten dieser Produktion – von technischen Lösungsansätzen bis legislativen Regulationsversuchen – bei der Verwaltung *bestehender* Daten stehen, ohne die *Produktion* dieser Daten in Frage zu stellen.
Dieser Aufsatz schlägt eine ideologiekritische und polit-ökonomische Perspektive vor, um die Aktivität der NutzerInnen von digitalen Systeme besser begreifen zu können.

1. Einleitung

Öl wird gewonnen und in Minen wird geschürft. Es werden natürliche Ressourcen abgebaut, die später als Rohstoffe in den weiteren globalen Produktionsprozess einfließen. Mit *Data Mining* oder *Data as the new Oil* wird das Bild der natürlichen Ressource auch auf Daten angewendet. Damit wird die Gewinnung dieser Ressource, die *Produktion* dieser Daten, als natürlicher Prozess positioniert, dessen konkrete Ausgestaltung rein technischen Überlegungen geschuldet wäre. Tatsächlich lässt sich jedoch zeigen, dass die Gestaltung des Produktionsprozesses von ganz bestimmten ökonomischen Interessen geprägt ist.

Dass diese Daten wertvoll sind, ist heute unbestritten. Die größten gegenwärtigen Technologie-Unternehmen hantieren fast ausschließlich mit personenbezogenen Daten, deren Wert sie auf unterschiedliche Weisen realisieren. Die effektivste und am weitesten verbreitete davon ist der Verkauf von personalisierten Werbeflächen. Der direkte Verkauf von Daten an Versicherungs- und Finanzunternehmen nimmt überdies zu, so wie auch das Trainieren von KI-Systemen mit diesen Daten, deren Funktionen später als Services verkauft werden.

Es macht also Sinn, Daten als Waren zu betrachten, die in einem größeren Wertschöpfungsprozess direkt verkauft oder weiter verarbeitet werden können. Diese Daten sind nicht beliebig, sondern beschreiben etwas Konkretes: Personen, deren Erfahrungen, deren Interaktionen, Interessen, Ängste und Gefühle – deren *Subjektivität.* Kommerzielle soziale Netzwerkplattformen produzieren diese Daten nicht selbst. Sie stellen das Umfeld – die Produktionsmittel – zur Verfügung, in denen sich solche Ausdrücke der Menschlichkeit ihrer NutzerInnen artikulieren können, und zwar auf eine Art, durch die personenbezogene Daten entstehen. Manche „Datenwaren" werden danach weiter verarbeitet, um die bereits erwähnten Formen der Realisierung ihres Wertes zu ermöglichen, aber *Facebook* selbst produziert genauso wenige Daten wie *Google* oder *Twitter* das tun – aber wer produziert hier dann? Wo passiert die *produktive Arbeit*, die laut der politischen Ökonomie nach Marx notwendig ist, um Waren und schließlich Mehrwert zu produzieren?

Im medien- und kommunikationswissenschaftlichen Diskurs hat sich die Auseinandersetzung mit dieser Frage rund um den Begriff *Digital Labour* organisiert, der unter anderem von Christian Fuchs stark geprägt wurde. Auf die obige Frage weiß dieser Folgendes zu antworten:

> "Commodities have producers who create them; otherwise they cannot exist. So if the commodity of the mentioned Internet platforms is user data, then the process of creating these data must be considered to be value-generating labour. This means that this type of Internet usage is productive consumption or prosumtion in the sense that it creates value and a commodity that is sold." (Fuchs, 2014, S. 246)

Damit ist der Kern der *Digital Labour* Debatte beschrieben: Die Tätigkeiten von NutzerInnen auf sozialen Netzwerkplattformen (und in vielen anderen digitalen Kontexten der Produktion personenbezogener Daten) ist *produktive Arbeit* im marxschen Sinne, also Waren- und Mehrwert produzierende Arbeit. Daraus ergeben sich verschiedene Konsequenzen für die Analyse dieses Verhältnisses, und den Umgang mit den daraus entstehenden Daten.

Zum einen können wir von kommerziellen sozialen Netzwerkplattformen als *Ausbeutungsverhältnis* sprechen, denn der von den NutzerInnen produzierte Mehrwert wird ihnen vorenthalten und stattdessen für die Akkumulation des Unternehmens genutzt (Andrejevic 2011). Der Arbeitsprozess lässt sich daran anschließend auch als *entfremdet* beschreiben. Die NutzerInnen werden vom *Objekt der Arbeit* entfremdet, weil die Plattformen durch ihre Nutzungsbedingungen Eigentumsrechte an deren Interaktionen und Erzählungen bekommen (Fuchs 2014). Sie sind von den *Produktionsmitteln* entfremdet, denn die Interfaces treten ihnen unbeeinflussbar und fremdbestimmt gegenüber, während Werbeschaltungen und algorithmische Sortierung die Organisation dieser sozialen Erfahrungen bestimmen (Galloway 2012). Und schließlich entfremdet der Produktionsprozess die NutzerInnen zu einem gewissen Grade von sich selbst: *Habit-forming Design*

will NutzerInnen unbewusste Praktiken antrainieren, während die Form der sozialen Interaktion sich in Ideen des Selbst und der Selbstdarstellung einschreibt. Die Summe der Interaktionen der NutzerInnen sowie des kollektiv produzierten Wissens und der daraus entstehenden kulturellen Artefakte fasse ich unter dem Sammelbegriff *Sozialität*, deren Produktion durch die Plattformen eingehegt und auf eine Art (re-)organisiert wird, die gleichzeitig Mehrwert produziert.

Dieser Beitrag kann an dieser Stelle jedoch keine vollständige Aufarbeitung der *Digital Labour* Debatte leisten,[1] sondern will die Frage stellen, welche Konsequenzen für den gesellschaftlichen Umgang mit Daten aus so einer Analyse entstehen. Dafür beleuchte ich zunächst die ideologische Unsichtbarmachung dieses Ausbeutungsverhältnisses und seiner Produkte. Daran anschließend skizziere ich einige der sozialen und ökologischen Folgen dieser Produktionsweise. Am Ende dieses Beitrages ziehe ich daraus einige politische Konsequenzen und skizziere eine Position zur Plattformregulierung oder *Data Governance*.

2. Einhegen und optimieren

Im Gegensatz zu klassischen Lohnarbeitsverhältnissen ist der Zwang zur Arbeit auf sozialen Netzwerkplattformen nicht so offensichtlich wie die Armut, die bei der Verweigerung anderer Ausbeutungsformen droht. Historisch war es meist physische Gewalt, Enteignung und Vertreibung, mit der sich die kapitalistische Produktionsweise in neuen Sektoren durchgesetzt hat (Federici 2012a). Soziale Netzwerkplattformen arbeiten hier mit subtileren Methoden, um ihre NutzerInnen dazu zu bringen, ihre Sozialität in einem Rahmen auszuleben, der gleichzeitig personenbezogene Daten als Waren für die Plattform produziert. Durch verschiedene Arrangements von Netzwerkeffekten, Monopolstellungen und lizenzrechtlichen wie netzwerktechnischen Ein- und Ausschlüssen hat es das Konzept *Plattform* geschafft, weite Teile kollektiver sozialer Prozesse einzuhegen.

Informations- und Austauschfunktionen, die einmal von schwarzen Brettern an gemeinsamen Orten erfüllt wurden; Community-Building, das einmal auf spezialisierten Websites mit konkretem Fokus passierte; Ankündigung und Bewerbung von politischen oder kulturellen Veranstaltungen, die bisher über mehrere E-Mail-Verteiler, Flyer oder Plakate organisiert wurden; Familien, die die Fotos des letzten Zusammenkommens nicht mehr direkt verschicken, sondern in einer gemeinsamen Chatgruppe posten. All diese sozialen Interaktionen finden zunehmend innerhalb geschlossener und proprietärer Netzwerke statt. Die Plattformen müssen uns nicht mit physischer Gewalt zwingen, unsere aller Leben über

[1] Ein gute Übersicht über verschieden Diskussionsstränge bietet etwa Sevignani (2017). Der Band von Fuchs (2014) eignet sich gut zur vertiefenden Einführung.

sie zu organisieren – sie sind es bereits, und das völlig verständliche Interesse ein Teil dieser sozialen Prozesse zu sein, drängt uns zur immer weiteren Integration von Plattform-Services in unsere Leben. Ein Heraustreten aus diesen Kommunikationsformen ist zwar prinzipiell möglich, jedoch nur auf Kosten einer Einschränkung verschiedener sozialer Beziehungen, gesellschaftlicher Teilhabe und kulturellem Anschluss. Wir sind von diesen digitalen Infrastrukturen abhängig, sich daraus auszuloggen ist ein Privileg.

Mark Andrejevic bezeichnet dies in Anschluss an James Boyle als „Digital Enclosure", als Einhegungsprozess zur „Errichtung von Eigentumsrechten über Ressourcen, die dadurch in den Markt gelangen, um gekauft und verkauft zu werden" (Andrejevic 2011, S. 36). Die hiermit gemeinten Ressourcen sind einerseits die personenbezogenen Daten, die die NutzerInnen der sozialen Netzwerkplattformen generieren, in dem sie ihre normale Sozialität innerhalb derer Interfaces und Netzwerke ausleben – und andererseits die dort artikulierte, letztlich auch *produzierte* Sozialität zwischen den NutzerInnen.

Durch den inhärenten Drang zur konsequenten Steigerung der Profite haben Plattformen ein Interesse an erhöhten Produktion personenbezogener Daten. Die arbeitsförmige Organisation unserer Sozialität wird durch die konkrete Ausgestaltung der Interfaces, Funktionen und Services sozialer Netzwerkplattformen vorangetrieben, die uns zu besonders datenintensiven Sozialpraktiken drängen und sich in immer mehr Bereiche unseres Alltags einweben. Damit verändern sich unsere Sozialpraktiken unhinterfragt entlang von Kapitalinteressen, wenn Plattformen eher die Anliegen ihrer AnlegerInnen als die ihrer NutzerInnen ernst nehmen. Andrejevic beschreibt dies als:

> „rationalisierenden Instrumentalismus: die Durchdringung sozialer Netzwerke durch die quantifizierende Logik des Tauschwerts und die Erschaffung einer Welt, in der sich jeder Akt der Kommunikation und der sozialen Interaktion als Werbung und als Marketing Datenpunkt verdoppelt." (Andrejevic 2011 S. 34)

Dass diese Sozialität nun nach den Interessen der Mehrwertproduktion umgestaltet wird, verschwindet dabei in der Selbstverständlichkeit unserer dominanten Art der Computernutzung. Marx nennt diese Umgestaltung des konkreten Arbeitsprozesses die *reelle Subsumtion*, in der die konkrete Tätigkeit im Arbeitsprozess auf die Mehrwert-produktion hin optimiert wird (Marx & Engels 2014, S. 533). Das Drängen auf daten- und zeitintensive Kommunikationspraktiken ist genauso Teil dieser Veränderung wie die Normalisierung von Tracking-Devices und Capture-Strukturen in allen Lebensbereichen.

Dass soziale Netzwerkplattformen einen Raum zum Ausdruck unserer Sozialität bieten, wird oft als ihr *Service* verhandelt. Doch all die Timelines, Threads, Kommentarspalten und Pages wären ohne die Arbeit der NutzerInnen leer. Auch dies ist eine Form der Entfremdung: Die Arbeit der NutzerInnen wird vor ihnen unsichtbar gemacht, ideologisch abgespalten und ihnen dann als Service der Plattform zurück*gespiegelt.* Von den Produkten ihrer eigenen Arbeit getrennt, müssen sie die Nutzungsbedingungen der

Plattform – und damit die gesamte Produktionsweise – immer wieder akzeptieren um ihr soziales Umfeld weiter pflegen zu dürfen.

3. Unsichtbar machen

Die Unsichtbarmachung ihrer Arbeit lässt sie dankbar für die Möglichkeit sein, überhaupt digital kommunizieren zu dürfen. Die Darstellung der Organisation dieser Arbeit als *natürlich* und *selbstverständlich* trägt zur Akzeptanz dieses Verhältnisses bei, eine Parallele zu den Analysen, die durch den materialistischen Feminismus in Bezug auf Hausarbeit in den 1970ern diskutiert wurden (Dalla Costa &James 2005). Auch dort ging es darum, die Organisation der sozialen Reproduktion als Teil des gesamten Produktionsprozesses zu markieren. Laurel Ptak hat diese Parallele aufgenommen und mit "WAGES FOR FACEBOOK" eines der politischen Manifeste der damaligen Diskussion (Federici 1975) auf die hier analysierten Verhältnisse angepasst:

> „Capital had to convince us that it is a natural, unavoidable and even fulfilling activity to make us accept unwaged work. In its turn, the unwaged condition of facebook has been a powerful weapon in reinforcing the common assumption that facebook is not work, thus preventing us from struggling against it." (Ptak 2014)

Der Eindruck der Natürlichkeit und Unausweichlichkeit dieser Organisation unserer Sozialität wird durch die medialen und technologischen Verhältnisse untermauert. Alexander Galloway beschreibt ausführlich, wie (meistens grafische) Interfaces versuchen, sich selbst unsichtbar zu machen, sich jedem hinterfragenden Blick zu entziehen (Galloway 2012, S. 54). Wenn Galloway meint, das Interface „facilitates the way of thinking that tends to pitch things in terms of "levels" or "layers" in the first place", verweist er damit auf die wortwörtlich rahmende Funktion, auf das *Framing*. Denn die innere und äußere Gestaltung besonders kommerzieller sozialer Netzwerkplattformen hat die Aufgabe der Optimierung der Metriken von *Engagement* – also Interaktion mit präsentiertem Content und Werbungen – und der Datenproduktion. Die emotionale Lenkung hin zu Affekten wie Wut oder Empörung hat sich dafür als besonders effizient herausgestellt.

Wendy Chun beschreibt ähnliche ideologische Effekte in unseren gegenwärtigen digitalen Infrastrukturen. Sie analysiert die funktionalen Analogien zwischen Ideologie und Software und verortet sie in tieferliegenden Abstraktionsebenen der gegenwärtigen Informatik: „Software, or perhaps more precisely operating systems, offer us an imaginary relationship to our hardware: they do not represent transistors but rather desktops and recycling bins. Software produces 'users.'" (Chun 2014, S. 43). Damit ist ein Prozess der *Subjektivierung* beschrieben. Die digitalen Systeme, mit denen wir interagieren, durch die wir kommunizieren, anhand derer wir uns gegenüber anderen selbst darstellen, formen uns als Subjekte, unsere Weltbeziehung, unsere Selbstwahrnehmung, unsere materiellen und

ideologischen Handlungsräume. Als *User* ist dieser Subjektstatus im hier beschrie-benen Produktionsprozess immer passiv, wir haben nur die Wahl, entweder die Platt-formen so zu nutzen, wie sie sind, oder gar nicht. Und damit müssen wir den Ausschluss von zentralen sozialen Prozessen akzeptieren.

Für solche sozio-technischen Komplexe hat Philipp Agre schon Anfang der 1990er Jahre den Begriff *Capture* stark gemacht (Agre 1994). Mit einer doppelten Bedeutung von Capture als *einfangen*, aber auch als *erfassen*, im Sinne von *verstehen*, beschrieb Agre damit techno-soziale Systeme, in denen Abläufe so formalisiert, automatisiert und überwacht werden, dass ihre Zustände allesamt maschinenlesbar sind. Um beide Anforde-rungen zu erfüllen, werden "grammars of action" definiert, die Tätigkeiten, Handelnde und Zustände beschreiben und in unterschiedlichen Zusammensetzungen fassen können. Solche *Grammars of Action* sorgen in den Interfaces, Protokollen, Normen und Sortierungen kommerzieller sozialer Netzwerkplattformen für die Subjektivierung als passivierte UserInnen und die Rekonfiguration unserer Sozialität, die für die effiziente Produktion personenbezogener Daten notwendig ist. Mit digitalen Artefakten außerhalb ihrer eigenen Plattformen, etwa als Plug-ins in der Fitness-App, als Cookies setzender Share-Button auf ganz anderen Webseiten, oder als fixer Bestandteil von mobilen Betriebssystemen können die Capture-Systeme kommerzieller Plattformen sich in immer mehr Bereiche unserer alltäglichen Lebensführung und Sozialität einweben, und diese für ihre Produktion umgestalten.

4. Unsichtbare Konsequenzen

Diese Veränderungen in unseren sozialen Beziehungen und den Räumen, in denen wir diese ausleben, bringen teils gravierende Folgen mit sich. Im folgenden Abschnitt skizziere ich einige der sozialen, gesellschaftlichen und ökologischen Konsequenzen der bisher beschriebenen Weise der Produktion von personenbezogenen Daten und gleichzeitig ihre Art, sich in der Offensichtlichkeit zu verstecken, denn die Komplexität, Undurchsichtigkeit und Allgegenwärtigkeit unserer digitalen Infrastruktur lässt ihre naturalisierenden Beschreibungen besonders effektiv sein.

Die *Cloud* als immaterieller Ort ist aber immer eine Form von materiellem Datenzentrum – mit konkretem Stromverbrauch, Hardwareverschleiß und menschlichen ArbeiterInnen (Ensmenger 2020). Und Beiträge, die *viral gehen*, tun dies nicht aufgrund ihrer biologischen Eigenschaften als memetische Vehikel, sondern meistens, weil bestimmte Marketinginteressen dahinter stehen, die die algorithmische Sortierung auf kommerziellen Plattformen geschickt zur Aktivierung anderen NutzerInnen benutzen können (Stadler 2017). Solche ideologischen Bilder der Naturalisierung und Unsichtbarmachung rechtfertigen zum einen die Praktiken, mit denen personenbezogene und andere Daten produziert werden. Es erscheint uns mittlerweile völlig normal, Familienbilder auf

Facebook und anderswo zu teilen, es wird suggeriert, das sei eine *natürliche* Art, dies zu tun. Zum anderen Verdecken sie aber auch die materiellen Bedingungen dieser Art der Produktion und die daraus entstehenden Konsequenzen – und damit die Besitzverhältnisse, Verantwortlichkeiten und die sich formenden Interessen.

Das Bild von den Daten als das neue Öl hat zumindest eine brauchbare Seite, wenn auch eine unerwartete. Die Auswirkungen einer auf fossilen Brennstoffen basierenden Produktions- und Wirtschaftsweise sind ähnlich gravierend, manchmal schwierig zu sehen, weil immer nur inkrementell und vor allem global ungleich verteilt. Wenn Jathan Sadowski von diesen Auswirkungen spricht, dann stellt er fest: „The outcomes of smart tech are not evenly distributed. The harms are disproportionately felt by the poor and people of color" (Sadowski 2020, S. 133). Es ist also wichtig, nicht nur die offensichtlichsten Effekte der glatten Oberflächen zu betrachten, mit denen uns kommerzielle soziale Netzwerkplattformen und andere Technologieunternehmen konfrontieren, wenn sie uns unsere eigene Sozialität als ihren Service spiegeln. Eine Kritik an der hier beschriebenen Produktionsweise muss tiefer greifen, anstatt bei der Skandalisierung von Brüchen der bürgerlichen Privatsphäre und staatlicher Überwachung stehen zu bleiben.

Die Kritik an der marktförmigen Reorganisation unserer Öffentlichkeiten und Aufmerksamkeitsverteilung nähert sich daran an. Die strukturelle Logik von *Likes*, *Shares* und Kommentaren intensiviert den sozialen Wettbewerb und weitet die offensichtliche Marktförmigkeit in unsere engeren sozialen Kreise hinein aus. Um die ständige Zirkulation von *Content* und die darin stattfindende Datenproduktion am Laufen zu halten, ist viel manuelle Arbeit nötig – nicht nur von NetzwerktechnikerInnen, ProgrammiererInnen oder eben *Content* kreierende NutzerInnen, sondern auch von noch viel versteckteren ArbeiterInnen.

Commercial Content Moderation (CCM) beschreibt die Arbeit von vielen tausenden Menschen, die über den ganzen Globus verteilt in verschiedensten Settings – aber oft in fabrikartigen Großraumbüros – damit beschäftigt sind, die Beiträge von den abermillionen NutzerInnen auf kommerziellen Netzwerkplattformen zu kontrollieren. Diese ModeratorInnen entscheiden nach geheim gehaltenen Regelwerken, welche Inhalte auf den jeweiligen Plattformen unerwünscht sind und welche gelöscht werden müssen. Die Plattformen weigern sich ihre Richtlinien öffentlich zu machen. Die Arbeit der ModeratorInnen beinhaltet die tägliche stundenlange Konfrontation mit gewaltvollem, übersexualisiertem und menschenverachtendem Material, das die ArbeiterInnen oft mit psychischen Traumata zurück lässt (Roberts 2019). Auch dies ist eine Folge der Organisation unserer Sozialität auf riesigen, zentralisierten Plattformen: Anstatt die Arbeit der Moderation zu verteilen und den betroffenen Communities Mitbestimmungsrechte einzuräumen, wird diese notwendige Arbeit zentralisiert und möglichst kostengünstig organisiert, wobei das Mitspracherecht von NutzerInnen oder mikrokulturelle Besonderheiten einzelner Communities auf der Strecke bleiben.

Aus den ideologischen Bildern der Körperlosigkeit, der Immaterialität und der Ephemeralität, die immer noch in allen gesellschaftlichen Imaginationen und Bezugsweisen auf digitale Infrastrukturen eingeschrieben sind, entsteht eine besonders effektive Art der Unsichtbarmachung und Naturalisierung dieser Verhältnisse. Dadurch kann die Ausbeutung und Zerstörung von Menschen und Natur direkt hinter unserer Vorstellung der *Cloud* verschwinden: Es erscheint nämlich nur digital, nur virtuell. Diese Unsichtbarmachung ist jedoch gefährlich, denn gerade jetzt sollte unsere Produktionsweise und der daraus entstehende CO2-Ausstoß kritischer betrachtet werden denn je. Thomas Mullaney schreibt deswegen eindringlich über Datenzentren als zentrale Punkte unserer Infrastrukturen:

> „They are physical machines, propelled by fire both material and metabolic. When they run, they run hot; and when they work hard, they run hotter. Data centers alone account for more than 2 percent of global energy use, energy consumption predicted to grow with the expansion of the Internet of Things. (Google emitted over 50 kilograms of CO2 in the time it took for you to read this sentence.)“ (Mullaney 2020, S. 5)

Doch die Einhegung und reelle Subsumtion unserer Sozialität bringen nicht nur zermürbende Formen der Ausbeutung und eine Intensivierung der globalen ökologischen Krise mit sich, sondern auch gesellschaftliche Verwerfungen durch die Reformatierung unserer sozialen Reproduktion.

So zeigt zum Beispiel Mar Hicks auf, dass der in unseren Alltagstechnologien eingebettete Sexismus kein Zufall, kein Flüchtigkeitsfehler unwissender EntwicklerInnen ist. Im Gegenteil, weist sie doch auf die tiefe Verankerung frauenverachtender Strukturen in den Wurzeln des Silicon Valley nach: „These gendered harms are also built in to platforms at their core. One of the most highly valued companies in Silicon Valley started out as a site that stole women’s pictures without their consent and asked users to rate their attractiveness.“ (Hicks 2020, S. 136)

In diesem Umfeld fanden die neofaschistischen Gruppen, die gerne unter dem Label *alt-right* zusammengefasst werden, einen fruchtbaren Boden für ihre Propaganda und darauf folgende Rekrutierungen und Radikalisierungen. Joanne McNeil sieht eine Erklärung dafür in den „feedback loops“, die sich in den Plattform-Algorithmen zeigen lassen, die für die Optimierung, Verbreitung und Kommodifizierung von *viral content* gebaut wurden. Der Fokus auf *engagement*, in welcher Form auch immer, fördert hierbei jedoch authoritäre Tendenzen: „As platform incentivice conflict, they forment hate, providing entry points, from the alt-light (Jordan Peterson) to the unambiguously dangerous (Alex Jones and Richard Spencer)“ (McNeil 2019, S. 183) McNeil unterstreicht jedoch auch, dass diese politischen Bewegungen und ihre AkteurInnen nicht erst durch soziale Netzwerkplatt-formen entstanden sind, auch wenn dies oft ihre eigene Erzählung ist.

In eine ähnliche Kerbe schlägt Ruha Benjamin, wenn sie auf die historischen Kontinuitäten von Technologie-gestützter Repression und Überwachung von Schwarzen Menschen verweist – lange bevor *big data* zum Buzzword wurde. Trotzdem betont sie auch die Intensivierung, die von Rassismen betroffene Menschen durch neue Technologien der Sichtbarkeit in ihrer Unterdrückung erfahren (Benjamin 2019).

Silvia Federici hat in ihren Untersuchungen historischer und gegenwärtiger Prozesse der kapitalistischen Einhegung immer wieder festgestellt, dass diese stets Phasen der verstärkten sexualisierten und rassistischen Gewalt waren, die insbesondere mit der Disziplinierung von Frauen* und Angriffen auf deren Rechte im öffentlichen Raum einhergingen (Federici 2012b, S. 96) Dieses Phänomen spiegelt sich in den gerade beschriebenen, zunehmend normalisierten Übergriffen auf sich öffentlich äußernde Frauen, People of Colour oder Personen abseits der patriarchalen Norm. Patriarchale und rassistische digitale Gewalt scheinen hier als Konsequenzen unserer gegenwärtigen Produktionsweise auf, dabei ist jedoch zu unterstreichen, dass diese Verwerfungen nicht rein technisch bedingt sind, also keine ausschließliche Konsequenz der Digitalisierung sind, aber durchaus davon befeuert werden.

5. Den Apparat anzweifeln

Die Erkenntnis, dass unsere Sozialität kommodifiziert ist, also die Form von Waren annimmt, hat weitreichende Konsequenzen – besonders dafür, wie wir mit diesen Waren und ihrer Produktion umgehen wollen. Denn durch die Warenform bekommen Dinge einen neuen Charakter. Marx stellt fest, dass sie „die gesellschaftlichen Charaktere ihrer eignen Arbeit als gegenständliche Charaktere der Arbeitsprodukte selbst“ (Marx & Engels 2014, S. 86) zurückspiegelt, und die Rolle der NutzerInnen im gesamten Produktionsprozess – und damit das Ausbeutungsverhältnis verschleiert. Mein Argument ist nun, dass diese Form einerseits die bereits beschriebenen Unsichtbarmachungen und Naturalisierungen ermöglicht und dadurch die sozialen und ökologischen Katastrophen zusätzlich befeuert. Andererseits kann uns diese Analyse helfen, das Produktions- und Ausbeutungsverhältnis sichtbar zu machen.

Salome Viljoen beschreibt die doppelte Rolle, die die Kommodifizierung in verschiedenen Kritiken an der *Datafication* einnimmt, als „both a process of production and a form of injustice“ (Viljoen 2020). Damit beschreibt sie zwei verschiedene Stränge der Diskussion, die sich in verschiedenen Bereichen der Diskussion um *Data Governance* ausdrücken. Im „propertarian approach“ wird zwar das Produktionsverhältnis anerkannt, dieses soll aber über Eigentumrechte und vor allem Lohnverhältnisse gelöst werden. Den zweiten Strang der Diskussion nennt Viljoen „dignitarian“, und dort wird das extraktive Moment der Datenproduktion betont, und die Lösungsvorschläge übersehen in ihrem Drang zur

Unterbindung dieser Extraktion viele positive Aspekte, die ein selbstbe-stimmter Umgang mit bestimmten Formen von Daten bringen könnte. (Viljoen 2020)

Ihr Vorschlag einer „democratic data governance“ versucht dagegen, personenbezogene Daten als geteilte und produktiv hergestellte Ressource zu verstehen. Dieser Ansatz wird auch in anderen Positionen geteilt und oft unter dem Begriff der *commons* diskutiert (vgl. Papadimitropoulos 2020). Viljoen stellt deswegen richtig fest, dass individualisierende Lösungen dieses Problem nicht lösen können, ohne auch die eventuellen gesellschaftlichen Vorteile, die wissenschaftlichen Erkenntnisse, das gemeinsam erarbeitete Wissen über Bord werfen zu müssen (Viljoen 2020).

Viljoens Trennung von „production“ und „injustice“ hilft vielleicht in der Kategorisierung bestimmter Diskussionen, ist aber für die Analyse unpraktisch: Als Ausbeutungsverhältnis ist unsere gegenwärtige Produktionsweise nämlich beides. Die Einhegung und reelle Subsumtion unserer Sozialität auf kommerziellen sozialen Netzwerkplattformen hat die Tätigkeiten der Reproduktion unseres Soziallebens zentralisiert und auf eine Weise umorganisiert, die sie zu Waren produzierender Arbeit werden lassen. Damit werden konkrete Bedürfnisse von NutzerInnen ausgenutzt und gegen sie positioniert: Sei es das Bedürfnis nach sozialem Austausch, nach politischer Diskussion oder nach gemeinsamer Information. Digitale soziale Netzwerke beruhen darauf, diese Aktivitäten in Form von Daten abzuspeichern, um Teile davon anderen NutzerInnen zur Verfügung zu stellen. In *kommerziellen* sozialen Netzwerkplattformen werden die selben Aktivitäten – durch *capture*-Systeme und sozio-technischen Druck – auf eine Weise organisiert und umgeformt, die gleichzeitig Gebrauchswerte entstehen lässt, die die Tauschwerte für die Plattform realisierbar machen: Detaillierte Aufzeichnungen über Interaktionen, Verhalten, Vermutungen und Kategorisierungen, die keine Bedürfnisse der NutzerInnen befriedigen, sondern nur den eingangs genannten Formen der Realisierung des Mehrwerts für die Plattformen dienen.

Die Plattform als Struktur ist für diese Einhegungen notwendig, denn erst durch die dort entstehenden Netzwerkeffekte kann die Zentralisierung mittels sozialem Zwang funktionieren. Wenn ich die Nutzung von *social media* als Produktionsprozess verstehe, dann ist die Plattform eine Fabrik – deren Arbeitsprozesse, Disziplinierungen und Einschlüsse nicht Teil der Lösung sein können. Denn erst dadurch konnten die oben skizzierten sozialen, ökologischen und ausbeuterischen Verwerfungen entstehen und normalisiert werden. Daran muss sich eine nachhaltige Form der *Data Governance* abarbeiten – nicht nur Fragen, was mit toxischen Daten zu tun ist, als wäre ihre Entstehung ein unentrinnbares Naturverhältnis – sondern schon bei der Produktion dieser Daten hinterfragen, ob unsere Gesellschaft sie für nützlich hält und wie sie damit umgehen will, beziehungsweise ob deren Produktion überhaupt an sich zulässig sein sollte.

Daran anschließend argumentiere ich, dass bestimmte Formen der Datenproduktion immer schädlich sein werden. Die gegenwärtige Produktion personenbezogener Daten, mit der Metrik des *engagement* und *habit forming design* ist nicht alleine Schuld an der globalen

autoritären Wende und der sozio-ökologischen Krise, trägt aber zu deren Normalisierung und Verschärfung bei. Deswegen wird es nicht reichen, kommerzielle Plattformen und undurchsichtige Daten-Aggregatoren mit kleineren oder größeren Beschränkungen zu belegen. Gewisse Formen der Produktion personenbezogener Daten und daraus entstehendem Targeting sind ihre Gefahr nicht wert, und sollten abgeschafft werden.

Gleichzeitig kann diese Forderung nicht bedeuten, dass es keine sozialen Netzwerke mehr geben darf. Die Feststellung, dass dort konkrete Bedürfnisse der NutzerInnen nach Sozialität befriedigt werden, unterstreicht, dass viel eher die gegenwärtige arbeitsförmige Organisation, die zentralisierte Einhegung und die ökonomische Motivation dahinter die Probleme sind.

6. Andere Netze

Ansätze zur Lösung dieser Probleme werden gegenwärtig anhand von dezentralen Modellen diskutiert, die nicht mehr unter der ökonomischen, technischen und rechtlichen Kontrolle einzelner privater Akteure stehen. Ein Beispiel dafür ist das *Fediverse*, ein loses Netzwerk verschiedenster Server, die über die Implementierung verschiedener Netzwerkprotokolle – allen voran das *ActivityPub*-Protokoll – miteinander verbunden sind. Der Name spielt auf die *föderierte Netzwerkstruktur* an, in der es keine zentralen Knoten gibt, und unterschiedliche Instanzen für sich bestimmen können, auf welche Art sie mit dem Rest des Netzwerks oder auch nur mit ganz bestimmten anderen Knoten interagieren wollen. Eines der meist genutzten digitalen Kommunikationssysteme basiert auf diesem Prinzip: Es gibt keinen zentralen E-Mail-Server über den jeder *Traffic* laufen muss,[2] sondern viele unterschiedliche Server, die das E-Mail-Protokoll implementiert haben und ihre eigenen Regeln der Nutzung, von Zugang über Moderation bis Spam-Filterung, definieren können. Dadurch entsteht ein soziales Netzwerk ohne die einschließenden und monopolisierenden Tendenzen der Plattformstruktur.

Dabei ist es hier wichtig, nicht bei individuellen oder privaten Lösungen stehen zu bleiben. Viel eher ist ein anderes Verhältnis zu gemeinsamen Infrastrukturen, Institutionen, Gemeinschaftlichkeit und Öffentlichkeit notwendig. Alternative Produktionsformen, die eine solidarische Infrastruktur aufbauen wollen, können hierfür einen Beitrag leisten, sind aber gegenwärtig meist von individueller Initiative und Freiwilligenarbeit abhängig – all die Arbeit der Serverwartung, Moderation und des Supports, die kommerzielle Plattformen leicht durch die Einnahmen, die durch die Produktion personenbezogener Daten gemacht werden, zahlen können, wird beispielsweise im *Fediverse* meist ehrenamtlich geleistet. Dies ermöglicht zwar Communities, in denen die NutzerInnen in strukturelle

[2] Auch wenn Microsofts Outlook und Googles Gmail sehr erfolgreich in der Zentralisierung bestimmter Teile des Email-Netzwerks sind, gibt es noch viele kleine Knoten.

Entscheidungen der Verwaltung mit eingebunden werden und dadurch selbst Verantwortlichkeit ihrem Umfeld und den von ihnen genutzten Infrastrukturen gegenüber übernehmen können, verbleibt aber im Kleinen und setzt nicht wenig Wissen voraus, was für potentielle NutzerInnen eine große Barriere darstellen kann.

Diese Verantwortung könnte jedoch von nicht-kommerziellen und bestenfalls auch nicht-staatlichen Institutionen übernommen werden. In diesem Kontext spricht Mark Andrejevic etwa von Universitäten als Orte, die solche Infrastrukturen zur Verfügung stellen könnten (Andrejevic 2011, S. 48). Es ist kein Zufall, dass sich das klassische Web und das E-Mail-System durch anfangs akademische Nutzung etabliert haben, weil beide oft von Universitäten betrieben wurden. Joanne McNeil nutzt ein ähnliches Bild, wenn sie von Bibliotheken als öffentlichen Orten spricht, in denen Austausch und Information, aber auch einfach niederschwelliger Aufenthalt möglich ist. In vielen Städten stellen Bibliotheken Ressourcen jenseits von Büchern und Datenträgern zur Verfügung, und eignen sich dafür als Ausgangspunkt einer nicht kommerziellen digitalen Infrastruktur. Das unterstreicht sie mit der Notwendigkeit von BibliothekarInnen: „… a person who might meet users where they are and help provide what they need. (…) people on task to care about the past, with respect to the past and also to what it shall bequeath to the future.“ (McNeil 2019, S. 257)

Mit sozio-technischen Ansätzen der föderierten Interoperabilität müssen solche Institutionen auch anderen Arten, Knoten im offenen Netzwerk zu betreiben, nicht im Wege stehen. Es kann weiterhin möglich sein, kleine Instanzen selbst zu betreiben oder sogar kommerzielle Knoten bereit zu stellen, mit unterschiedlichsten Formen von Selbstregulierung, Moderation oder Community. Damit können die digitalen Ein- und Ausschlüsse des Plattform-Modells umgangen werden, ohne eine vereinheitlichte Art der Interaktion mit dem Netzwerk vorzuschreiben, während gleichzeitig auf einen niederschwelligen Zugang zu den kollektiven Ressourcen geachtet wird.

Die hier skizzierte Analyse einer kommodifizierten Sozialität zeigt aber auch auf, dass die Konsequenzen unserer gegenwärtigen Produktionsweise mit einer direkten Übersetzung in dezentrale, föderierte Strukturen nicht von alleine behoben werden. Durch mehr als zwei Jahrzehnte der reellen Subsumtion unserer Sozialität sind Normen und Gewohnheiten in der Nutzung sowie der inneren und äußeren Gestaltung unserer Kommunikationsmittel entstanden, in die sich die Ausbeutung und Kommodifizierung tief eingeschrieben haben. Deswegen werden viele der Probleme dieser Produktion von Sozialität nicht verschwinden, wenn nur die Verwertungsprozesse abgeschafft werden, die konkreten Tätigkeiten der bisherigen Arbeitsprozesse aber gleich bleiben – und viele alternative soziale Netzwerke versuchen diese zu imitieren. Der Umbau der Infrastrukturen entlang kommunaler, interoperabler und dezentraler Ideen ermöglicht demgegenüber einen Raum zur Erkundung anderer Annäherungen an digitale Sozialität, und eröffnet zumindest die Möglichkeit des Entstehens einer solidarischen digitalen Zukunft.

Literatur

Agre, Philip. E. (1994): ‘Surveillance and capture: Two models of privacy’. *The Information Society*, 10(2), pp. 101–127. doi: 10.1080/01972243.1994.9960162.

Andrejevic, Mark (2011): ‘Facebook als neue Produktionsweise’, in Rohle, Theo and Leistert, Oliver (Hrsg): *Generation Facebook. Über das Leben im Social Net*. Bielefeld: Transcript, S. 31–48.

Benjamin, Ruha (2019): *Race after technology: abolitionist tools for the new Jim code*. Medford, MA: Polity.

Chun, Wendy H. K. (2014): ‘On Software, or the Persistence of Visual Knowledge’. *Grey Room* (18), S. 26–51.

Dalla Costa, Mariarosa & James, Selma (2005): *The Power of Women and the Subversion of the Community*. New York: Pétroleuse Press.

Ensmenger, Nathan (2020): ‘The Cloud is a Factory’. In Hicks, Mar et al. (Hg): *Your Computer Is on Fire*. Cambridge, MA: MIT Press, S. 29–50.

Federici, Silvia (1975): *Wages against Housework*. Bristol: Falling Wall Press.

Federici, Silvia (2012a): *Caliban und die Hexe: Frauen, der Körper und die ursprüngliche Akkumulation*. Edited by Martin Birkner. Translated by Max Henninger. Wien: Mandelbaum (Kritik & Utopie).

Federici, Silvia (2012b): ‚Der Feminismus und die Politik der Commons (2010)‘. In *Aufstand aus der Küche - Reproduktionsarbeit im globalen Kapitalismus und die unvollendete feministische Revolution*. Münster: Edition Assemblage (Kitchen Politics. Queerfeministische Interventionen, 1), S. 87–105.

Fuchs, Christian (2014): *Digital Labour and Karl Marx*. New York: Routledge.

Galloway, Alexander R. (2012): *The interface effect*. Cambridge: Polity.

Hicks, Mar (2020): ‘Sexism is a Feature’. In Hicks, Mar et al. (Hg.): *Your Computer Is on Fire*. Cambridge, MA: MIT Press, S. 3–11.

Marx, Karl & Engels, Friedrich (2014): *Das Kapital: Bd. 1*. (MEW). Berlin: Dietz Verlag.

McNeil, Joanne (2019): *Lurking: how a person became a user*. First edition. New York: MCD, Farrar, Straus & Giroux.

Mullaney, Thomas S. (2020): ‘Your Computer Is on Fire’. In Hicks, M. et al. (eds): *Your Computer Is on Fire*. Cambridge, MA: MIT Press, S. 3–11.

Papadimitropoulos, Vangelis (2020): *The Commons: Economic Alternatives in the Digital Age*. University of Westminster Press. doi: 10.16997/book46.

Ptak, Laurel (2014): *WAGES FOR FACEBOOK*. Abgerufen unter: http://wagesforfacebook.com/ (Stand vom 22-04-2016).

Roberts, Sarah T. (2019): *Behind the screen: content moderation in the shadows of social media*. New Haven: Yale University Press.

Sadowski, Jathan (2020): *Too Smart: How Digital Capitalism is Extracting Data, Controlling Our Lives, and Taking Over the World*. Cambridge, MA: MIT Press.

Sevignani, Sebastian (2017): 'Facetten der Debatte über das digitale Arbeiten – Herausforderungen für eine kritische Theorie des informationellen Kapitalismus', *PROKLA*, 186(47), S. 43–62.

Stadler, Tobias (2017) 'The Whitest Charleston Milk Shake – Weltweites Tanzfieber, globale Einheiten und cultural appropriation'. In Binder, Sarah et al. (Hg.): *Tanz im Film. Über das politische in der Bewegung.* Berlin: Verbrecher Verlag, S. 133–146.

Viljoen, Salmoné (2020): 'Data as Property?'. *Phenomenal World*, 16 October 2020. Abgerufen unter: https://phenomenalworld.org/analysis/data-as-property (Stand vom: 20-01-2021).

Digitale Mündigkeit im Spannungsfeld zwischen ich und wir – Ein Ratgeber in zehn konkreten Schritten

Leena Simon

Zusammenfassung

Die Digitalisierung droht uns zu entgleiten. Der Mensch ist viel zu selten dazu befähigt, in Bezug auf die Digitaltechnik, die er betreibt, die Verantwortung zu übernehmen. Das liegt einerseits daran, dass die äußeren Bedingungen dafür kaum gegeben sind, andererseits aber auch, dass digitale Mündigkeit im Lebensalltag nicht trainiert wird. Die absehbaren Folgen für Demokratie und Gesellschaft sind fatal. Der Text versucht darzulegen, dass mit nur zehn Schritten jede Person ihre eigene digitale Mündigkeit trainieren kann.

1. Digitale Mündigkeit im Spannungsfeld zwischen ich und wir

Je mehr die Digitalisierung voranschreitet, desto mehr werden die gesellschaftlichen Versäumnisse im Zusammenhang mit ihrer Gestaltung offensichtlich. Die Corona-Krise führt uns vor Augen, dass es an belastbaren Gestaltungsprinzipien für die Digitalisierung in Schule, Gesundheitssystem und Sicherheitspolitik fehlt. Der Trend geht zu mehr und mehr Kontrolle seitens der „großen Player“ (staatlich und privat) und zunehmendem Kontrollverlust (vgl. Simon 2020) auf Seite der Benutzenden. Die Folgen dieser, auf leichte Antworten und schnellen Erfolg ausgelegten Digitalpolitik spüren wir zunehmend in Form von politischer Polarisierung, Verschwörungserzählungen und schwindendem Vertrauen in die Demokratie und ihre Repräsentanten.

Der Fehlschluss liegt bereits in den 90er Jahren, als bei der Vermittlung von Computerfertigkeiten ausschließlich auf Anwendungskompetenz Wert gelegt wurde, während die wichtigen Reflexionskompetenzen weitgehend außer Acht gelassen wurden. Wenn man bei einem Office-Kurs nur lernt, wie man ein Dokument anlegt, löscht, ausdruckt, wie man Text fett markiert oder ein Inhaltsverzeichnis anlegt, kann man das Programm zwar bedienen, aber die Folgen des eigenen Handelns nicht verstehen und reflektieren. Reflexionskompetenz würde in diesem Zusammenhang bedeuten, dass auch darüber gesprochen wird, dass die Wahl des Dateiformats entscheidende Konsequenzen haben kann und warum offene Formate denen von Microsoft und Co vorzuziehen sind.

Wer ein Dokument als .docx abspeichert, setzt damit andere unter Druck, ebenfalls Microsoft-Produkte zu nutzen und die dazu notwendigen Lizenzbedingungen zu akzeptieren. Dies ist bei offenen Formaten nicht der Fall, da diese von diversen Programmen ohne Störungen geöffnet werden können.

Folge dieser einseitigen Vermittlung von Computerwissen ist auch, dass wir über keinerlei Kriterien mehr verfügen, wem und was wir eigentlich Vertrauen schenken dürfen. Wer sich diese Frage stellt, bemerkt schnell, dass es nicht einmal ansatzweise ausreichend Information dazu gibt. Wenn Menschen so vor Augen geführt wird, wie unmündig sie in Wahrheit sind, neigen sie dazu, schnell darüber hinweg zu sehen. So ist es zum Normalzustand geworden, dass Allgemeine Geschäftsbedingungen (AGB) ungelesen akzeptiert, Apps ungeprüft installiert und Cookie-Banner unbesehen weggeklickt werden (vgl. Kling 2017). Würden wir nur die Dienste nutzen, denen wir wirklich vertrauen können, könnten wir an der digitalen Welt kaum teilhaben. Den damit verbundenen Kontrollverlust nehmen wir aber durchaus wahr. Dieser untergräbt das Vertrauen in unsere Gemeinschaft.

Die notwendige Reflexion der Folgen des eigenen digitalen Handelns haben wir uns als Gesellschaft nie wirklich anerzogen. Und so geht auch heute der Trend hin zu immer mehr Vereinfachung, die uns gleichzeitig einen verantwortlichen Umgang mit digitalen Werkzeugen zunehmend verbaut. Digitale Mündigkeit ist der Ausgang aus diesem selbstverschuldeten Zustand.

2. Mündigkeit ist ein Muskel, der trainiert werden will

Doch was bedeutet „Digitale Mündigkeit“? Im deutschen Sprachraum haben wir, dank Immanuel Kant, mit dem Begriff der Mündigkeit einen Sonderfall. Denn Kant gab dem ursprünglichen Rechtsbegriff eine weitere Bedeutung. Bisher hatte es sich bei Mündigkeit um die Fähigkeit gehandelt, Verantwortung für das eigene Leben zu tragen (im Sinne von engl. „mature“). Ebenso müsse auch eine Gesellschaft insgesamt die Verantwortung für das eigene Fortbestehen tragen. Der Begriff der Mündigkeit wurde um den Wert der Verantwortung für die Gemeinschaft (im Sinne von engl. „responsible“) erweitert. Entsprechend ist digitale Mündigkeit das Übernehmen von Verantwortung für die digitale Kommunikationsgemeinschaft und damit auch für sich selbst.

Hierfür muss sowohl auf gesellschaftlicher (d.h. politischer) Ebene, als auch auf individueller (d.h. persönlicher) Ebene ein Umdenken stattfinden. Die Reflexion der Folgen unseres Handelns muss in unseren digitalen Alltag Einzug halten. Sie darf nicht in kleine Expertengremien ausgelagert werden. Jede Person ist mit ihren Handlungen Vorbild für andere und prägt das Gesicht unserer digitalen Gesellschaft mit den kleinsten Handlungen mit. Mündigkeit ist hier mehr eine Haltungsfrage als eine Sache von Wissen. Sie ist Übungssache. So wie die Muskeln in unseren Körpern nicht wachsen, wenn man sie nur einmal im Jahr anstrengt, muss auch Mündigkeit als Muskel betrachtet werden, der regelmäßig trainiert werden will.

Die Verantwortung hierfür liegt nicht ausschließlich beim Individuum, das schon längst den Überblick verloren hat und – wie es scheint – diesen im Zuge des entfesselten

Überwachungskapitalismus (vgl. Zuboff 2018) gar nicht wiedererlangen soll. Auch gesamtgesellschaftlich müssen die Voraussetzungen für einen mündigen Umgang mit Digitaltechnik geschaffen werden. Mündigkeit bedeutet allerdings auch, dass das Individuum nicht darauf warten darf, dass ihm die Ketten der Entmündigung abgenommen werden.

3. Zehn Schritte zur digitalen Mündigkeit

Im Folgenden werden zehn Schritte zu digitaler Mündigkeit auf individueller Ebene gezeigt. Diese sollen freilich nicht darüber hinwegtäuschen, dass es ein gesamtgesellschaftliches Umdenken braucht und hierzu Druck auf Politik und Wirtschaft ausgeübt werden muss.

Schritt 1: Die 30 Minuten-Regel

Ob Computeranfängerin oder Profi – niemand versteht alles, was in einem Computer passiert, vollumfänglich. Entscheidend ist, wie wir mit dieser Erkenntnis umgehen. Wer sich von dem Überforderungsgefühl abschrecken lässt, wird ein Problem ausspucken, ehe er oder sie sich wirklich darauf eingelassen hat. Der Schlüssel besteht darin, sich nicht abschrecken zu lassen und sich zunächst auf das zu konzentrieren, was man versteht – und sei es auch noch so wenig. Um dies zu trainieren, gibt es die 30-Minuten Regel: Versuchen Sie ein Computerproblem immer erst 30 Minuten lang alleine (z.B. unter Zuhilfenahme einer Suchmaschine) zu lösen. Holen Sie sich erst nach Ablauf dieser Zeit Unterstützung. Sie werden erstaunt sein, wie viele Probleme Sie alleine lösen können, wenn Sie sich nur darauf einlassen. Und die Menschen, die Ihnen helfen, werden es Ihnen danken. So trainieren Sie im Alltag Ihren Mündigkeits-Muskel und lernen von Tag zu Tag mehr dazu.

Schritt 2: Kontrollanspruch entwickeln

Entwickeln Sie die Haltung, dass Sie die Kontrolle über Ihre Geräte behalten wollen: Geben Sie Passwörter nicht weiter, weil das bequemer ist. Wenn andere darauf Zugriff haben, treten Sie Verantwortung an diese ab, die Sie eigentlich selbst tragen müssten. Wenn Sie Ihre Passwörter hingegen nicht preisgeben, und dennoch jemand anderem Ihr Gerät überlassen, z.B. um Einstellungen daran vorzunehmen, sitzen Sie unausweichlich daneben, weil Sie ja regelmäßig selbst Ihre Passwörter eingeben müssen. Legen Sie Wert darauf, dass Sie zumindest ansatzweise nachvollziehen können, was dort gerade passiert. Am besten behalten Sie das Gerät ganz in der Hand und lassen sich anleiten. So lernen Sie am meisten. Denken Sie immer daran: Wenn etwas schiefgeht, tragen Sie die Verantwortung dafür, nicht die Person, die Ihnen hilft. Holen Sie sich genügend Informationen, damit Sie diese Verantwortung auch tragen können.

Schritt 3: Sichere Passwörter

Passwortsicherheit ist von großer Bedeutung. Indem Sie sichere Passwörter wählen, stellen Sie sicher, dass die Macht über Ihr digitales Leben auch in Ihren Händen bleibt. Passwörter müssen lang genug sein (mindestens 14 Zeichen), dürfen nur für jeweils einen Account verwendet werden, sollten keine Namen, Geburtstage sowie Jahrestage beinhalten oder auch nicht in einem Wörterbuch stehen! Machen Sie sie aber auch nicht zu kompliziert. Denn dann halten Sie es nicht durch. Tipp: Wählen Sie 4 bis 6 zufällige Wörter und trennen Sie diese mit einem Sonderzeichen. Ein Passwort könnte dann z.B. so lauten: „Hund.Teekanne.rot. Kopfstand“. So werden die Passwörter sehr lang und komplex, sind aber dennoch leicht zu merken und einzugeben. Damit Sie nicht den Überblick verlieren, nutzen Sie eine Passwortverwaltungsdatenbank (die nicht in der Cloud liegt).

Schritt 4: Cloud-Dienste vermeiden

Es gibt keine Cloud. Wenn etwas in der Cloud liegt, dann ist das eine schöne Umschreibung dafür, dass es auf den Computern anderer Menschen gespeichert ist. Dort haben Sie entsprechend wenig Kontrolle über Ihre Daten. Wenn Sie auf die Cloud nicht verzichten können, gestalten Sie das aktiv. Betreiben Sie (mit Freunden, Arbeitskolleginnen oder Bekannten) eine eigene Cloud (z.B. mit Nextcloud). Sollten Sie kommerzielle Cloudanbieter nutzen, legen Sie nur Daten dort ab, die Sie vorher verschlüsselt haben (z.B. mit Veracrypt).

Denken Sie daran, dass manche Smartphones automatisch Ihre Daten (besonders die Fotos) in die jeweilige Cloud kopieren. Wenn Sie dies deaktivieren, bedenken Sie, dass Sie nun für Datensicherung selbst sorgen müssen. Das können Sie tun, indem Sie Back-ups auf Datenträgern erstellen, über die Sie Kontrolle haben (z.B. einem USB-Stick oder einer externen Festplatte).

Schritt 5: AGB wenigstens oberflächlich prüfen

Zugegeben: Es ist heute nicht mehr realistisch, alle AGB vollständig zu lesen. Das sollte aber nicht dazu führen, dass Sie es gleich resigniert ganz aufgeben. Wer AGB akzeptiert, unterzeichnet einen Vertrag. Und den sollte man wenigstens überflogen haben, wenn man ihn schon nicht vollständig liest. Gehen Sie diesem Versuch einer Entmündigung durch Überforderung nicht auf den Leim. Dafür reichen meist fünf Minuten aus. Denn anhand zweier Faktoren lässt sich schnell erkennen, wes Geistes Kind ein AGB-Text ist: Prüfen Sie die AGB vor dem Akzeptieren auf Länge und Verständlichkeit. Kopieren Sie die AGB (mitsamt ggf. ausgelagerten Cookie-Richtlinien und der Datenschutzerklärung) in ein Office-Dokument und vergleichen Sie die Länge mit anderen AGB (bei gleichen Dokumenteneinstellungen). Wählen Sie dann zwei zufällige Abschnitte und prüfen Sie diese auf Verständlichkeit. Je länger und unverständlicher AGB sind, desto größer ist die Wahrscheinlichkeit, dass diese geschrieben wurden, damit Sie sie nicht lesen.

Schritt 6: Haltung des Eigensinns

Wer verantwortlich handelt, wird im Alltag im Zusammenhang mit Gruppenaktivitäten nicht selten in Situationen geraten, mit denen man nicht einverstanden ist. Vertrauen Sie Ihrem Urteil, lassen Sie sich nicht unter Druck setzen und gestehen Sie sich die dafür notwendige Portion Eigensinn zu. Wenn Sie nach der Prüfung der AGB von WhatsApp keine Lust mehr haben, diese App zu nutzen, dann lassen Sie es auch. Muten Sie Ihrem Umfeld zu, dass es andere Wege findet, mit Ihnen zu kommunizieren. Wenn Menschen nicht bereit sind, sich einer problematischen Gruppenaktivität anzupassen, finden sich meistens andere Wege.

Schritt 7: Verantwortlich veröffentlichen und Quellen prüfen

Wer öffentlich kommuniziert, trägt besondere Verantwortung. Journalistinnen und Journalisten haben deshalb einen eigenen Kodex (den Pressekodex), der ihnen helfen soll, keine falschen Informationen zu verbreiten. Da neuerdings alle Menschen publizieren können, sollten wir einen ähnlichen Anspruch entwickeln. Ein Blick in den Pressekodex kann inspirieren. Übernehmen Sie keine Informationen, deren Quelle nicht nachvollziehbar ist, prüfen Sie Quellen nach Möglichkeit selbst – wenigstens stichprobenartig. Die Presse verlangt sogar zwei voneinander unabhängige Quellen, ehe sie etwas als „wahr" ansieht. Seien Sie skeptisch bei unbelegten Aussagen und fragen Sie nach einer Quelle. Besonders kritisch sollten Sie übrigens solche Aussagen betrachten, die besonders gut in Ihr Weltbild passen. Diese werden Ihnen algorithmisch maßgeschneidert und sodann zugespielt, müssen aber deshalb nicht wahr sein. Allerdings sind Sie damit viel einfacher manipulierbar, als mit Informationen, die Ihrem Weltbild nicht entsprechen. Wenn Sie sich unsicher sind, ob es sich bei einer Nachricht um einen „Fake" handelt, geben Sie den Titel des Artikels zusammen mit dem Wort „Hoax" (das ist der Internetjargon-Fachausdruck für Falschmeldung) in eine Suchmaschine ein und bringen Sie in Erfahrung, ob schon einmal jemand diese Nachricht als Falschmeldung markiert hat.

Schritt 8: Freie Software nutzen

Einen analogen Wecker kann man aufschrauben, um zu sehen, was darin passiert, eine Software in der Regel nicht. Freie Software legt Wert darauf, in diesem Sinne „aufschraubbar" zu sein und die Nutzenden nicht in ihrer Freiheit einzuschränken. Deshalb darf man Freie Software zu jedem Zweck nutzen, untersuchen, wie sie funktioniert, sie mit anderen Menschen teilen und sie besser machen (vorausgesetzt, man teilt sie wieder als Freie Software). Bekannte Beispiele sind der Browser Firefox, das E-Mail-Programm Thunderbird, das Betriebssystem GNU/Linux und das Smartphone-System Android. Zu all diesen Programmen liegt der so genannte Quellcode vor. Also der Code, der nicht nur für Maschinen, sondern auch für Menschen verstehbar ist. Das gibt uns die Möglichkeit, Programme zu prüfen und herauszufinden, ob ein Programm versteckte Funktionen hat, die es gar nicht haben soll. Entsprechend seltener findet man solche ungewollten

Funktionen in freier Software. Eine Garantie ist das freilich nicht. Informatik-kenntnisse sind natürlich von Vorteil, aber nicht zwingend nötig, um von freier Software zu profitieren. Betrachtet man den Quellcode eines Programms als das Gesetz, das ihm zu Grunde liegt (vgl. Lessig 2006), wird klar, weshalb dieser zugänglich sein muss. Als Nicht-Juristin verstehe ich ganz sicher nicht alles, was im Strafgesetzbuch steht. Doch ich habe die Möglichkeit, mir juristischen Beistand zu holen. Ein System, dessen Gesetze nicht offen einsehbar sind, ist totalitär. Analog befindet man sich beim Gebrauch von unfreier (proprietärer) Software in einem totalitären System. Der Mündigkeit dient das ganz sicher nicht.

Schritt 9: Verschlüsseln, wann immer es geht

Datenträger und Kommunikationsmedien sollten nach Möglichkeit verschlüsselt sein. Das ist manchmal etwas mühsam, sorgt aber dafür, dass kein unbefugter Zugriff auf Ihre Daten stattfindet. Viele Messenger (nicht so Telegram) verschlüsseln schon standardmäßig. Aber auch E-Mail-Verschlüsselung ist wichtig, funktioniert aber nur, wenn beide Kommunikationsseiten diese bereits eingerichtet haben. Festplattenverschlüsselung ist ebenfalls wichtig, kann aber auch zu Datenverlust führen (z. B. wenn man das Passwort vergisst). Entsprechend ist auch hier wichtig, dass man eigenverantwortlich für Sicherungs-kopien sorgt. Diese sollten am besten ebenfalls verschlüsselt gelagert werden.

Damit dies auch weiterhin möglich ist, sollte ein Recht auf Verschlüsselung in die Verfassung aufgenommen werden.

Schritt 10: Solidarität

Verantwortung für die Kommunikationsgemeinschaft zu tragen, bedeutet natürlich auch, sich solidarisch mit den Kommunikationspartnern zu zeigen. Dabei geht es vor allem darum, mehr Augenmerk auf die kleinen Alltagssituationen zu richten, die andere betreffen. Viele Menschen überkleben mittlerweile die Frontkamera ihres Smartphones. Doch auch die Rückkamera sollte man überkleben. Denn diese ist im öffentlichen Leben (z.B. im Wartezimmer oder in der U-Bahn) häufig auf andere Menschen gerichtet, die nicht wissen können, ob man gerade Solitär spielt oder ein Foto von ihnen aufnimmt. Wer WhatsApp installiert, gibt damit nicht nur die eigenen Daten an die Firma Facebook weiter, sondern erlaubt dem Datengiganten auch Zugriff auf das Adressbuch zu nehmen. Die Daten darin sind jedoch Daten anderer Menschen (meist inklusive Foto, Geburtsdatum, Postadresse usw.) und nicht die eigenen, über die man auch selbst entscheiden dürfte. Aber wer hat schon alle Kontakte im Adressbuch um Erlaubnis gefragt, ehe er WhatsApp installiert? Damit mir jemand eine verschlüsselte E-Mail schicken kann, muss ich dies erst eingerichtet haben und die notwendigen Informationen (meinen „öffentlichen Key“) kommunizieren. Wenn ich die AGB von Facebook nicht akzeptieren will, komme ich nicht an Informationen, die ausschließlich dort abgelegt

wurden. Es geht – kurz gesagt – darum, sich die Frage zu stellen, ob man möglicherweise jemand anderen mit einer Handlung Schaden zufügt, ihn unter Druck setzt oder ausgrenzt.

Digitale Mündigkeit ist ein Haltungsanspruch. Haltung ist eine dauerhafte Angelegenheit. Deshalb ist es auch viel „bequem[er] unmündig zu sein“ (Kant 1967, S. 55). Und genau deshalb ist es vor allem eine individuelle Aufgabe, dieser Bequemlichkeit nicht nachzugeben.

Literatur

Kant, Immanuel (1967): Beantwortung der Frage: Was ist Aufklärung? In: Zehbe, Jürgen (Hrsg.): *Was ist Aufklärung? Aufsätze zur Geschichte und Philosophie.* Göttingen: Vandenhoeck & Ruprecht, S. 55-61.

Kling, Marc-Uwe (2017): *Qualityland*. Berlin: Ullstein.

Lessig, Lawrence (2006): *Code – And Other Laws of Cyberspace, Version 2.0*. New York: Basic Books.

Simon, Leena (2020): Kontrollverlust und digitale Entmündigung. In: Wenn KI, dann feministisch. Hg Netzforma e.V. Berlin 2020

Zuboff, Shoshana (2018): *Das Zeitalter des Überwachungskapitalismus*. Frankfurt/New York: Campus Verlag.

Weiterführende Literatur

Beck, Roman & Greger, Vanessa & Hoffmann, Christian & König, Wolfgang & Krcmar, Helmut & Weber, Jasmin & Wunderlich, Nico & Zepic, Robert (2018): Digitale Mündigkeit – Eine Analyse der Fäigkeiten der Bürger in Deutschland zum konstruktiven und souveränen Umgang mit digitalen Räumen. NEGZ e.V.

Hoffmann, Christian & Weber, Jasmin & Zepic Robert & Greger, Vanessa & Krcmar, Helmut (2019): Dimensionen digitaler Mündigkeit und politische Beteiligung im Netz. In: I. Engelmann, M. Legrand & H. Marzinkowski (Hg). Politische Partizipation im Medienwandel (S.79-99). Berlin https://doi.org/10.17174/dcr.v6.4

Petsche, Hans-Joachim & Simon, Leena (2014): „Der ganze Strudel strebt nach oben; Du glaubst zu schieben, und du wirst geschoben.“ (Goethe, Faust I). – Technikpaternalismus und Digitale Mündigkeit. In: Banse, Gerhard & Rothkegel, Annely (Hrsg.): *Neue Medien – Hoffnungen, Befürchtungen, Realitäten*. Berlin: trafo Wissenschaftsverlag, S. 71-83.

Simon, Leena (2020): „Digitale Mündigkeit – Eigenverantwortlich im 21. Jahrhundert. Eine Handreichung. Bielefeld: Art d‘Ameublement.

Spiekermann, Sarah (2019): *Digitale Ethik. Ein Wertesystem für das 21. Jahrhundert*. München: Droemer Verlag.

Kurzbiografien der Autorinnen und Autoren

Marian Adolf, Prof. Dr., ist Kommunikationswissenschaftler und Mediensoziologe und widmet sich in seiner Arbeit den Auswirkungen der Mediatisierung auf die zeitgenössische Gesellschaft. Zuletzt hatte er den Lehrstuhl für Medienkultur an der Universität Friedrichshafen inne.

Martina Bachor, BA, ist studentische Mitarbeiterin und organisiert das Projekt Medientag sowie die gekoppelte Ringvorlesung mit Übung. Sie ist seit März 2020 am Institut für Medien, Gesellschaft und Kommunikation beschäftigt und Teil des Forums Innsbruck Media Studies. Sie studiert Erziehungs- und Bildungswissenschaften im Master an der Universität Innsbruck.

Valentin Dander, Prof. Dr., ist Erziehungswissenschaftler und Professor für Medienbildung und pädagogische Medienarbeit an der Fachhochschule Clara Hoffbauer Potsdam. Seine Forschungsinteressen liegen im Feld medienpädagogischer Bildungs- und Wissenschaftstheorie, mit Schwerpunktsetzungen auf Politischer Medienbildung, digitalen Daten, Medien*Kritik und Open Education.

Theo Hug, Dr. phil., Professor für Erziehungswissenschaft mit Schwerpunkt Medienpädagogik und Kommunikationskultur, Leiter des Instituts für Medien, Gesellschaft und Kommunikation und Sprecher des interfakultären Forums Innsbruck Media Studies an der Universität Innsbruck.

Oliver Leistert, Dr., Leuphana Universität Lüneburg; Arbeitsschwerpunkte: Digitale Kulturen, Überwachung und Protest, Affekte und Algorithmen, Blockchains und programmierbares Geld, Technologien der Kontrolle.

Silvia Lipp, BSc MSc, ist wissenschaftliche Mitarbeiterin im Rahmen des Projektes Learning Analytics am Institut für Wirtschaftspädagogik an der Karl-Franzens-Universität Graz und hat auch ihr Dissertationsvorhaben im Bereich Learning Analytics verankert.

Tilmann D. Märk, Univ.-Prof. Dr. Dr. hc.mult., Rektor der Universität Innsbruck.

Anna-Maria Neuschäfer, Mag., ist Lehrerin für Bildnerische Erziehung am Gymnasium Kufstein. Sie schreibt eine Dissertation zum Thema Augmented Reality im Kunstunterricht bei Franz Billmayer (Mozarteum Salzburg) und zieht unter anderem kommunikationswissenschaftliche Positionen heran.

Günther Pallaver, Dr. jur., Dr. phil., em. Professor für Politikwissenschaft am Institut für Medien, Gesellschaft und Kommunikation sowie am Institut für Politikwissenschaft der Universität Innsbruck. Derzeit Senior Researcher am Institut für vergleichende Föderalismusforschung/Eurac Research in Bozen.

Hermann Petz, Mag., Jahrgang 1961, ist seit 2003 Vorstandsvorsitzender des Tiroler Medienhauses Moser Holding AG sowie Mitglied des Vorstandes und des Präsidiums des Verbands Österreichischer Zeitungen (VÖZ), Vorstandsvorsitzender der Austria Presse Agentur (APA) und Österreich-Delegierter der ENPA (European Newspaper Publishers Association).

Clemens Pig, Dr., ist Vorsitzender der Geschäftsführung und geschäftsführender Vorstand der APA – Austria Presse Agentur Unternehmensgruppe (Wien) und Vize-Präsident des Verwaltungsrates der Keystone-SDA-ATS AG (Bern) sowie Präsident der Vereinigung der unabhängigen Nachrichtenagenturen Europas.

Michaela Rizzolli, PhD, Freie Universität Berlin, SFB Affective Societies; Arbeitsschwerpunkte: Forschungsdatenmanagement, Datenbegriff, Wissenschaftliches Arbeiten im Digitalen.

Hans-Martin Schönherr-Mann, Professor für politische Philosophie an der Universität München; Arbeitsschwerpunkte: Ethik, Philosophie der Technik, Medien und Bildung. Existentialismus, Poststrukturalismus.

Leena Simon, MA, ist graduierte Philosophin, IT-Beraterin und Netzpolitologin und beschäftigt sich mit digitaler Mündigkeit und Technikpaternalismus. Sie arbeitet u.a. für das Anti-Stalking-Projekt im Frieda Frauenzentrum in Berlin und für Digitalcourage e.V.

Tobias Stadler, MA, studierte Theater-, Film- und Medienwissenschaft an der Universität Wien. Er promoviert derzeit an der Universität Oldenburg und arbeitet zu digitalem Kapitalismus, patriarchaler Informatik und alternativen Konzeptionen von digitaler Sozialität.

Nico Stehr, Prof. PhD, forscht und lehrt an zahlreichen in- und ausländischen Universitäten, zuletzt als Karl Mannheim-Professor für Kulturwissenschaften an der Zeppelin Universität (Friedrichshafen). Seine Arbeitsschwerpunkte sind u.a. die Theorie der Wissensgesellschaft, der Zusammenhang von Gesellschaft und Klima und die Moralisierung der Märkte.

Elsa-Margareta Venzmer, MA, Wissenschaftliche Mitarbeiterin am Institut für Medienwissenschaft, Philipps-Universität Marburg; Forschungsinteressen: Digital Humanities, Audiovisuelle Medien, Film- und Fernsehwissenschaft, Feministische Theorie, Comics und Surveillance Studies.

Andre Wolf, Mimikama – Verein zur Aufklärung über Internetmissbrauch; Nach Theologiestudium und einigen Jahren Berufserfahrung als Verantwortlicher für Medien und Kommunikation ist nun die Analyse von Internetinhalten, speziell von Social Media, Wolfs Fachgebiet. Andre Wolf ist zudem beim Verein Mimikama als Blogger, Autor und Content- und Social Media Koordinator tätig.

In der Interaktion mit digitalen Systemen produzieren wir täglich eine Vielzahl an Daten, die beispielweise für wirtschaftliche, aber auch für politische Zwecke genutzt werden können. Während demokratische Systeme in Europa Wege suchen, wie mit diesen persönlichen Spuren möglichst sicher, anonym und effektiv umgegangen werden kann, zeigt sich nicht nur am Beispiel China, dass Daten auch zur politischen und gesellschaftlichen Kontrolle eingesetzt werden können.
Dieser Sammelband beinhaltet Beiträge zu aktuellen Fragen nach Chancen und Gefahren der politischen Nutzung von Daten, des Data driven Campaigning, der „Naturalisierung" personenbezogener Datenproduktion und der Demokratisierung der digitalen Kontrolle, des Datenaktivismus und Digital Citizenship sowie der digitalen Mündigkeit und der verantwortungsvollen Nutzung von Bildungsdaten.

ISBN 978-3-99106-046-8