Band 40
Heft 1-2
2018

Zeitschrift für Semiotik

Überwachung 2.0 – Zwischen Kontrolle und Komfort

Alexandra Gracev, Natalie John, Klaus Sachs-Hombach, Jörg R. J. Schirra, Anne Ulrich und Lukas R. A. Wilde
Einleitung 3

Maria Wilhelm
Who Watches the Watchmen? – Datenschutzrechtliche Anforderungen an Überwachungssysteme 9

Nils Zurawski
Der totale Unterhaltungsstaat. Überwachung im digitalen Zeitalter. Über Konsum, KI und nicht nur digitale Domestiken 23

Lena Füller, Caroline Ganzert und Marcel Lemmes
Überwachen, verführen, verkaufen – Manipulation als Schlüsselkonzept für Überwachungstheorien 45

Anne Diessner, Lisamarie Haas und Carina Konopka
„Alexa, kann ich dir vertrauen?" Sprachassistenten als Wegbereiter der gläsernen Privatsphäre 63

Interview
Nils Zurawski und Dietmar Kammerer
Was war Surveillance 1.0? Ein Gespräch über Computergeschichte, Mainframes und Zauberspiegel 83

Diskussion
Sven Jentzsch, Franziska Sieb, Frederica Tsirakidou, Martin Möller, Alexander Danner, Berit Stier und Julius Trautmann
Brauchen wir individualisierte Krankenversicherungs-Tarife in Form von Smartwatches? Protokoll einer Debatte 91

Kleinere Texte zur Praxis der Überwachung
Melanie Seifert, Ann-Christine Strupp und Anne Schneider
Social Scoring als Praxis der Überwachung. Eine Analyse der *Black Mirror*-Folge *Nosedive* 103

Yunzhi Chen, Karolina Hess, Kristie Pladson und Corina Stratmeyer
Beobachten, wie die App uns beobachtet 117

Anne Diessner, Carina Konopka, Marius Lang, Caroline Ganzert und Lena Füller
Rezensionen und Kritiken 127

Veranstaltungen 135

Vorschau auf den Thementeil der nächsten Hefte 143

Zeitschrift für
Semiotik
Band 40 • Heft 1-2 (2018)
Seite 3-8
Stauffenburg Verlag Tübingen

Einleitung

Alexandra Gracev, Natalie John, Klaus Sachs-Hombach, Jörg R. J. Schirra, Anne Ulrich und Lukas R. A. Wilde, Eberhard Karls Universität Tübingen

Überwachen wie auch Kontrollieren zählen „zu den grundlegenden gesellschaftlichen Praktiken, welche in unterschiedlicher Form ein Aspekt des Sozialen an sich sind“ (Zurawski 2007: 9). Überwachung ist demnach also nicht die Ausnahme, sondern die Regel, um soziale Verbünde zu steuern und zu erhalten. Für das kritische Nachdenken gibt es gleichwohl einen historischen Startpunkt, der mit dem Modell des Panopticons gegeben wurde und den Foucault in seinem Buch *Überwachen und Strafen* als prominentes Modell der Disziplinargesellschaft diskutiert hat. Unstrittig haben sich seitdem mit der Digitalisierung neue Formen und auch neue Akteure der Überwachung und Kontrolle herausgebildet, die in ihrer algorithmischen Gestalt, im Kontext des Konsums sowie in der bereitwilligen Nutzung neuer ‚sozialer‘ Medien und Plattformen einige Zeit unsichtbar geblieben waren, im Zusammenhang mit den verschiedenen Fällen des Datenmissbrauchs nun aber zunehmend Beachtung finden.

Das Thema des vorliegenden Hefts geht auf ein Lehrforschungsprojekt zurück, das im Wintersemester 2018/2019 im Rahmen des MA-Studiengangs Medienwissenschaft an der Eberhard Karls Universität Tübingen durchgeführt wurde. Der Titel des Lehrforschungsprojekts lautete: *Surveillance. Historische Entwicklungen und aktuelle Theorien zum Phänomen der Überwachung*. Seine Zielsetzung bestand in einem besseren Verständnis des Zusammenhangs von Medien bzw. Mediennutzung und Kontrolle bzw. Überwachung. Das Seminar sollte dabei sowohl die Darstellung von Überwachung in den Medien diskutieren als auch die Überwachung, die durch, in und mit Hilfe von Medien erfolgt. Einen interessanten aktuellen Fokus lieferte das Phänomen Facebook, da es sich hierbei um die gegenwärtig meistgenutzte Plattform weltweit handelt, über die bereits einige kritische Forschungsliteratur vorliegt.

Lehrforschungsprojekte werden am Institut für Medienwissenschaft regelmäßig durchgeführt und haben das Ziel, Forschung und Lehre stärker als üblich zu verbinden. Da Lehrforschungsprojekte vermutlich nicht die Regel in der akademischen Ausbildung sind, möchten wir dieses Format kurz

erläutern. Lehrforschungsprojekte bestehen aus mehreren Lehrveranstaltungen, nehmen in der Regel ein aktuelles Thema der Gesellschaft auf und bieten den Studierenden die Gelegenheit sowohl der wissenschaftlichen Auseinandersetzung wie auch der öffentlichen Vermittlung. Im vorliegenden Fall sollte das Projekt wichtige Positionen zur Theorie der (gegenwärtigen wie auch historischen) Überwachung vorstellen und zum Verständnis ihrer modernen Formen beitragen, wie sie etwa im Zusammenhang von Datenerfassung, Konsum und Werbung zu finden sind. Es stand damit im größeren Zusammenhang einer kritischen Gesellschafts- und Medientheorie und sollte entsprechend für moralische Probleme in diesem Bereich sensibilisieren. In praktischer Hinsicht war vorgesehen, dass die gesamte Seminargruppe die Organisation einer Tagung und die Publikation der Tagungsbeiträge verantworten sollte. Hierzu wurden Kleingruppen gebildet, die sich teilweise auf die theoretische Analyse, teilweise mehr auf die Tagungsorganisation, teilweise auf die Wissenschaftsvermittlung konzentrierten. Auf die jeweiligen Aufgaben wurden die Studierenden in spezifischen Veranstaltungen vorbereitet: den sogenannten Lehrredaktionen, in denen die gemeinsame Arbeit am Produkt im Vordergrund stand. Ergänzt wurde das Lehrforschungsprojekt in diesem Jahr durch ein zweites, kleineres Lehrforschungsprojekt, das die Tagung mit einer Debatte bereicherte. Diese hat ebenfalls mit einigen ausgewählten kleineren Arbeiten Eingang in das vorliegende Heft gefunden.

Das Lehrforschungsprojekt *Surveillance. Historische Entwicklungen und aktuelle Theorien zum Phänomen der Überwachung* umfasste insgesamt vier Lehrveranstaltungen. Während das Projektseminar (Klaus Sachs-Hombach) vor allem für die theoretischen Grundlagen zuständig war, wurden in den Lehrredaktionen einige praktische Fertigkeiten insbesondere im Bereich der Tagungsorganisation und der Wissens- bzw. Wissenschaftsvermittlung erarbeitet. Zu den theoretischen Grundlagen gehören die begrifflichen Klärungen. Für den Begriff der Überwachung gilt aber leider (analog zu vielen anderen sozialwissenschaftlichen Begriffen), dass er bisher unzureichend definiert worden ist. Als relativ unstrittig kann gelten, dass Überwachung eine Form der Beobachtung und Kontrolle von Sachverhalten und/oder Personen ist. Strittig ist aber insbesondere, ob von einem solchen unspezifischen Begriff, der im Sinne des Controllings einfach als eine Art der Steuerung verstanden werden kann, nicht ein spezifischer Begriff der Überwachung zu unterscheiden ist, der mit sehr gezielten (politischen) Zwecken verbunden ist. Im Projektseminar ging es vor allem um einen Vergleich der unterschiedlichen theoretischen Zugänge, die sich durch die Auseinandersetzung mit dem Modell des Panopticons auszeichnen. Hierbei unterscheidet die Forschung in der Regel zwischen drei Phasen (vgl. Galič u.a. 2017: 34): (1) Die mit dem Panopticon verbundene Phase, mit der insbesondere Foucaults Theorie der Disziplinargesellschaft verbunden ist, (2) die Phase der infrastrukturellen Theorien, die auf die Theorie der Kontrollgesellschaft von Deleuze zurückgehen, und schließlich (3) diverse Neukonzeptionalisierungen, in denen die Bedeu-

tung von Algorithmen im Kontext von personalisiertem Konsum hervorgehoben wird.

Ergänzt wurde das Projektseminar durch eine konzeptionelle Lehrredaktion, die Überwachung als Herausforderungen der populären Wissenschaftsvermittlung thematisierte (Anne Ulrich). Hier stand zunächst die Auseinandersetzung mit der Darstellung, Diskussion und Reflexion von Überwachung in Filmen und Fernsehserien auf dem Programm. Kameras und Bildschirme sind wichtige Instrumente von Überwachung und können in audiovisuellen Formaten besonders gut ins Bild gerückt, aber auch in ihren Grenzen reflektiert werden. Für die neueren Formen der Datenüberwachung müssen Filme und Serien erst noch eine Bildsprache entwickeln, die es erlaubt, diesen Bereich der „covert sphere" (Melley 2012) sichtbar und damit auch gesellschaftlich diskutierbar zu machen. Die Wissenschaft kann sich diese populären Darstellungen zunutze machen, um Überwachungstheorien aufzuzeigen und zu popularisieren. Die Lehrredaktion begleitete das Lehrforschungsprojekt in der zweiten Hälfte des Semesters dann aus der Perspektive der Wissenspopularisierung und untersuchte, wie diese beim Thema Datenüberwachung aussehen kann. Konkret produzierten die Seminarteilnehmer*innen eine wissenschaftlich informierte Rezension eines selbst gewählten Films oder einer Serie zum Thema Überwachung und lernten dabei, wie über potentiell verunsichernde Thematiken verständlich geschrieben werden kann. Darüber hinaus installierten sich alle Studierenden in einen zweiwöchigen Selbstversuch Selbstoptimierungs-Apps und dokumentierten ihren Alltag im Angesicht eines datenfressenden Programms. Zudem recherchierten sie, was die App mit ihren Daten anstellte. Vier Studierende haben die Ergebnisse dieser Erfahrungen in einem nachdenklichen Text für dieses Heft zusammengetragen und ausgewertet.

Eine zweite Lehrredaktion (Lukas R.A. Wilde) galt dem Bereich der Wissensvermittlung und des Wissenstransfers. Als Ergebnis wurde eine ca. zehnminütige Präsentation im TED-Talk-Format entwickelt. Diese bewusst populärwissenschaftlich angelegte Präsentation sollte eine Brücke zwischen den Seminarinhalten und deren ästhetischen Bearbeitungen durch die Filmproduktionen schlagen. Im ersten Teil der Lehrredaktion wurden die Inhalte des Seminars aufgearbeitet und auf persönliche Relevanzkriterien und außerakademische Vermittelbarkeit hin diskutiert. Daraufhin wurden verschiedene populäre Formate des Wissenstransfers gesichtet, besprochen und auf ihre Stärken und Schwächen hin geprüft (TED-Talk, Pecha Kucha, Ignite). Im Anschluss daran erstellten Teilgruppen unabhängig voneinander Entwürfe zu einer ersten Präsentation für die zweite Sitzung. Hierbei waren nicht nur konzeptuelle Fragen, sondern auch eine geeignete Vortragsweise und Aufführungslogik relevant, sowie insbesondere auch die Interaktion mit einer audiovisuellen Begleitpräsentation oder im Studio erstellte filmische Einspielungen. Aus den Materialien und Ergebnissen dieser Sitzung haben Seminarteilnehmer*innen eine finale Präsentation zusammengefügt, um diese in Eigenregie auszuarbeiten. Seminar- und fachfrem-

de Besucher*innen sollten die ästhetischen Produktionen aus zusätzlichen Perspektiven und Fragestellungen heraus wert- und einschätzen können.

Die dritte Lehrredaktion (Jörg R.J. Schirra) galt dem Projektmanagement: In dieser Lehrredaktion wurde die Planung und Durchführung der Tagung erarbeitet. In einem ersten Block hatten sich die Teams anhand vorgegebener und selbstrecherchierter ‚Checklists' mit den relevanten Planungs- und Organisationsaspekten einer Tagungsorganisation vertraut gemacht. Dabei ging es auch darum, sich Klarheit über verschiedene Tagungsformen zu verschaffen. In einer den ersten Teil abschließenden Brainstorming-Sitzung wurden die gewonnenen Erkenntnisse auf die als Abschluss zu planende Tagung angewendet, der vorgegebene thematische Rahmen zu einer Reihe von präziseren Fragestellungen ausgearbeitet und ein griffiger Tagungstitel bestimmt. Zudem wurden die Aufgaben für deren Organisation unter den Teams verteilt. Der zweite Teil der Lehrredaktion diente dem Umsetzen der Aufgaben, indem die Teams zunächst ihre bisherigen Aktivitäten und weiteren Planungen referierten und die Fortschritte diskutierten. Wichtiger Aspekt in diesem Teil war zudem das Erstellen eines genauen Fahrplans bis zur Tagung.

Die von den Studierenden organisierte wissenschaftliche Tagung fand am 13. Mai 2019 unter dem Titel *Surveillance 2.0 – Zwischen Kontrolle und Komfort* in Tübingen statt. Die Verantwortung über die Organisation übernahm eine eigene Arbeitsgruppe von Studierenden (Alexandra Gracev, Natalie John, Luna Selle) des Masterstudiengangs Medienwissenschaft. Im Rahmen eines Seminars an der Universität entwickelte die Organisationsgruppe zusammen mit ihren Kommiliton*innen einen thematischen Schwerpunkt. Dieser galt den Vor- und Nachteilen der Datenüberwachung sowie des Datensammelns und ihrem ambivalenten Spannungsverhältnis. Im Fokus standen dabei insbesondere intelligente Sprachassistenten, Suchmaschinen und soziale Medien, die aus unserem Alltag nicht mehr wegzudenken sind. Alexa, Google, Facebook & Co. vereinfachen unser Leben, indem sie uns mithilfe von Algorithmen Angebote und Werbung präsentieren, die auf unseren Interessen basieren. Sie zeigen uns das, was uns gefällt, oft sogar noch bevor wir selbst wissen, dass es uns gefällt. Doch diese Bequemlichkeit hat einen Preis: Firmen und Institutionen sammeln unsere Daten, überwachen und kontrollieren unser Nutzungs- und Konsumverhalten im Netz und verkaufen diese Informationen sogar an dritte Parteien weiter. Überwachung wird hier zu einem permanenten Zustand, der den privaten Raum immer mehr durchdringt und verändert, wodurch die Privatsphäre des Einzelnen zu verschwinden droht. Dennoch geben wir Nutzer*innen weiterhin unsere Daten freiwillig preis, präsentieren uns in sozialen Medien und nehmen die zielgerichtete Werbung der Unternehmen in Anspruch. Sind wir daher vielleicht einfach zu bequem, uns Gedanken über unsere Daten und unsere Privatsphäre zu machen und genießen die Vorteile der Datenüberwachung und -kontrolle? Oder würden wir all diese Vorzüge sofort aufgeben, wenn uns bewusst wäre, welchen Preis wir dafür zahlen?

Für die Tagung dienten die drei Unterthemen *Überwachung und Fremdsteuerung*, *Das Geschäft mit der Überwachung* sowie *Der Wandel der Privatsphäre* als Rahmenkonzept. Als Referent*innen luden die Organisatorinnen vier prominente Vertreter*innen aus Wissenschaft und Praxis ein, die sich intensiv mit dem Phänomen der Überwachung beschäftigt haben: Dietmar Kammerer von der Universität Marburg eröffnete die Tagung und warf einen historischen Blick auf das Thema Überwachung. Maria Wilhelm, Referentin der Stabsstelle Europa beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) Baden-Württemberg, stellte die rechtliche Perspektive von Überwachung vor. Wie Unternehmen Daten über (potenzielle) Kunden sammeln, Profile erstellen und damit zielgerichtete Werbung schalten, war Inhalt von Gene-Lee Englers Vortrag. Er ist als Strategy Director bei der Mediaagentur Universal McCann (UM) in Frankfurt am Main tätig, hat aber leider nicht die Zeit zur Verschriftlichung seines Beitrags gefunden. Im letzten Vortrag der Tagung sprach Nils Zurawski von der Universität Hamburg über den identitätsstiftenden Aspekt des Konsums und die Bedürfnisse der Menschen.

Ergänzt wurde das Programm durch zwei Vorträge von Studierenden des Masterstudiengangs Medienwissenschaft. So beschäftigte sich eine Gruppe von Studierenden mit der Frage, was Überwachung im 21. Jahrhundert eigentlich bedeutet und verglich dazu den Begriff *Manipulation* mit drei verschiedenen Überwachungsansätzen. Die zweite Vortragsgruppe befasste sich zentral mit der Frage, weshalb Konsument*innen endlich Verantwortung für ihre Privatsphäre übernehmen sollten. Zur Veranschaulichung der aktuellen Problematik der Datenpreisgabe verglich sie Amazons Sprachassistentin mit menschlichen Dienstboten im 19. Jahrhundert. Neben den beiden Vorträgen der Masterstudierenden im dritten Semester lockerte eine öffentliche Showdebatte die Tagung auf, die von Masterstudierenden im zweiten Semester vorbereitet worden war. In drei Durchgängen wurden dabei jeweils kurz Pro- und Contra-Argumente zu der Frage gewechselt, ob Krankenkassentarife anhand der Daten von Smartwatches bestimmt werden sollten. Insgesamt fand die Veranstaltung vor allem auch wegen des multiperspektivischen Einblicks auf das Thema Überwachung bei den Teilnehmer*innen wie auch bei den Referent*innen großen Zuspruch.

Die vorliegende Publikation wird durch einige studentische Arbeitsproben ergänzt, die aus der konzeptionellen Lehrredaktion oder aus weiteren thematisch angegliederten Seminaren stammen. Hierzu zählt auch ein Tagungsbericht, der den sonst üblichen Überblick über die Beiträge überflüssig gemacht hat. Ein Beitrag zur Serie „Black Mirror“ soll exemplarisch die eher traditionelle Form der Hausarbeit dokumentieren, während die Rezensionen und ein längerer, bereits erwähnter Bericht über einen Selbstversuch journalistischer geprägte Formen der Studienleistung darstellen.

Die Herausgeber*innen möchten sich abschließend bei allen bedanken, die mit der Durchführung der Tagung befasst waren. Besonderen Dank gilt den Referent*innen für ihre große Mühe und dem Institut für Medienwissenschaft der Universität Tübingen für die großzügige finanzielle Unterstüt-

zung. Besonderer Dank gilt Thomas Nolte, der beratend die studentischen Texte begleitet hat und in stets unermüdlicher wie zuverlässiger Weise die formale Einrichtung aller Texte besorgt hat.

Literatur

Foucault, Michel (1975). *Surveiller et punir. Naissance de la prison*. Paris: Gallimard. Deutsch von Walter Seitter: *Überwachen und Strafen. Die Geburt des Gefängnisses*. 9. Auflage Frankfurt a.M.: Suhrkamp 2008.

Galič, Maša, Timan Tjerk und Bert Jaap Koops (2017). Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation. *Philosophy & Technology* 30, 1, 9–37.

Melley, Timothy (2012). *The Covert Sphere: Secrecy, Fiction, and the National Security State*. Ithaca und London: Cornell University Press.

Zurawski, Nils (ed.) (2007). *Surveillance Studies. Perspektiven eines Forschungsfeldes.* Opladen: Budrich.

Prof. Dr. Klaus Sachs-Hombach, PD Dr. Jörg R. J. Schirra, Dr. Anne Ulrich,
Dr. Lukas R. A. Wilde, Alexandra Gracev und Natalie John
Eberhard Karls Universität Tübingen
Institut für Medienwissenschaft
Wilhelmsstr. 50
D-72074 Tübingen
E-Mail: klaus.sachs-hombach@uni-tuebingen.de

Zeitschrift für
Semiotik
Band 40 • Heft 1-2 (2018)
Seite 9-21
Stauffenburg Verlag Tübingen

Who Watches the Watchmen? – Datenschutzrechtliche Anforderungen an Überwachungssysteme

Maria Wilhelm, Leitung der Stabsstelle Europa beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg

Summary. Monitoring systems can be used by both private and public bodies. The European legislator created the legal basis and limits with the General Data Protection Regulation (GDPR; Regulation (EU) 2016/679) and the Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (Directive (EU) 2016/680). These also provide control and law enforcement possibilities for the data protection supervisory authorities. The granting of sufficient transparency is a central issue, especially in the area of video surveillance. Based on the discussion of the legal conformity of the data protection requirements themselves, the way in which information is provided is debated in this field. Here, the potential of data protection regulations remains largely unexploited.

Zusammenfassung. Überwachungssysteme können durch private und durch öffentliche Stellen eingesetzt werden. Rechtliche Grundlagen und Grenzen wurden durch den europäischen Gesetzgeber mit der Datenschutz-Grundverordnung (DS-GVO; Verordnung (EU) 2016/679) und der Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung (JI-RL; Richtlinie (EU) 2016/680) geschaffen. Diese sehen auch Kontroll- und Rechtdurchsetzungsmöglichkeiten für die Datenschutzaufsichtsbehörden vor. Die Gewährung von hinreichender Transparenz ist gerade im Bereich der Videoüberwachung eine zentrale Fragestellung. Ausgehend von der Diskussion der Rechtskonformität der datenschutzrechtlichen Vorgaben selbst wird in diesem Bereich die Art und Weise der Informationserteilung diskutiert. Hierbei bleiben Potenziale der datenschutzrechtlichen Vorgaben weitgehend ungenutzt.

1. Einleitung

Angesichts der Innovationen der letzten Jahre sieht der Mensch sich immer mehr Techniken der modernen Datenverarbeitung gegenüber, die neben anderen Verwendungszwecken auch für Überwachungsmaßnahmen eingesetzt werden können (vgl. etwa Weichert 2013: 251). Neben den Möglichkeiten der Auswertung von Kommunikationsverhalten im Online-Bereich und insbesondere innerhalb sozialer Netzwerke wurden aber auch auf eine längere historische Entwicklung zurückzuführende Beobachtungsmaßnahmen wie optische Überwachungsmittel revolutioniert. Mittels automatisierter Gesichtserkennung können Bewegungsprofile erstellt werden und sogar Gesten oder Körperbewegungen so genau abgeglichen werden, dass einzelne Personen identifiziert werden können (ausführlich Heldt 2019: 285). Die Bildung von Profilen ist Teil unseres Alltags geworden und im Bereich der interessensbasierten Werbung wie auch bei der Bildung unseres Bonitäts-Scorewertes durch Kreditauskunfteien ein zentrales Werkzeug (noch zur alten Rechtslage Arning und Moos 2014: 242; Schantz 2019b: Rn. 131). In Weiterentwicklung dieser Systeme ist China das erste Land, das ein umfangreiches staatliches Social Scoring System flächendeckend einführen will (Chinese State Council 2014: 1).

All diese Modelle bewegen sich nicht im rechtsfreien Raum, sondern tangieren Grundrechte und sehen sich den Regulierungsbemühungen des Gesetzgebers gegenüber. Dieser hat mit der Einrichtung unabhängiger Aufsichtsbehörden Kontrollorgane geschaffen, durch welche die Durchsetzung dieser Regelungen forciert und gewährleistet wird (Lewinski 2017: 1483). In materieller Hinsicht existieren Transparenzvorschriften, durch die Grundrechtseingriffe offen gelegt und Datenverarbeitungen nachvollziehbar gemacht werden. Hierdurch sollen die betroffenen Personen zu angemessenen eigenen Rechtsschutzmaßnahmen oder der Hinzuziehung der Kontrollorgane befähigt werden (Grittmann 2019: Art. 51, Rn. 9). Die Zurverfügungstellung von Informationen bedeutet aber nicht immer zugleich, dass bestimmte Vorgänge transparenter werden. Es kommt hier entscheidend darauf an, welche Informationen in welcher Art und Weise transportiert werden. Nur so kann effizient Transparenz von Datenverarbeitungsprozessen gewährleistet werden (vgl. die Kritik bei Wilhelm 2016: 903). Es bedarf also einer Rückbesinnung auf das eigentliche Schutzgut des Datenschutzes, um die gesetzlichen Vorschriften sinnvoll anwenden zu können.

2. Gesetzliche Grundlagen

Im Rahmen der letzten europäischen Datenschutzreform wurden sowohl die allgemein automatisierte Datenverarbeitungen betreffende Datenschutz-Grundverordnung (DS-GVO, ABl. L 119/1 vom 04. Mai 2016) – gemäß Artikel 2 Absatz 1 DS-GVO unterfallen ihr alle automatisierten und teilwiese

auch die nicht automatisierten Verarbeitungen personenbezogener Daten, soweit diese in einem Dateisystem gespeichert sind – als auch die JI-RL für den Bereich der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten sowie der Strafverfolgung (ABl. L 119/89 vom 04. Mai 2016) erlassen. Diese beiden sekundärrechtlichen Rechtsakte sind jeweils im Lichte des Datenschutzgrundrechts aus Artikel 8 Grundrechtecharta (GRCh) auszulegen (vgl. Sydow 2018: Rn. 7).

2.1 Datenschutzgrundrecht

Artikel 8 GRCh enthält das Datenschutzgrundrecht auf europäischer Ebene. Was genau der Inhalt dieser Rechtsposition ist, ist durch autonome Auslegung der europäischen Vorschrift zu ermitteln (vgl. Wegener 2016, Rn. 13 mit weiteren Nachweisen). Hierbei müssen die Rechtsauffassungen der europäischen Mitgliedstaaten berücksichtigt werden (Huber 2018: Rn. 14). Das herkömmliche deutsche Verständnis von einem aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 Grundgesetz (GG) hergeleiteten Grundrecht auf informationelle Selbstbestimmung muss somit durch ein autonomes Verständnis des europäischen Datenschutzgrundrechts ersetzt werden (vgl. dazu Sydow 2018: Rn. 7ff.).

2.2 DS-GVO und flankierende Gesetze

Die DS-GVO gilt von ihrem sachlichen Anwendungsbereich in Artikel 2 Absatz 1 DS-GVO Verarbeitungen für personenbezogene Daten, die vollständig oder teilweise automatisiert sind und in Bezug auf die Speicherung in Dateisystemen auch für nichtautomatisierte Verarbeitungen personenbezogener Daten. Aus dem allgemeinen Grundsatz der Rechtsmäßigkeit der Verarbeitung personenbezogener Daten aus Artikel 5 Absatz 1 Buchstabe a) DS-GVO folgen die Vorschriften der Artikel 6 bis 10 DS-GVO, in denen zulässige Rechtsgrundlagen für die von der DS-GVO erfassten Datenverarbeitungen genannt werden. An gleicher prominenter Stelle in Artikel 5 Absatz 1 Buchstabe a) DS-GVO wird auch der Grundsatz der Transparenz genannt, sodass eine Datenverarbeitung nicht nur auf einer validen Rechtsgrundlage beruhen, sondern immer auch hinreichend transparent ausgestaltet sein muss (Schantz 2019a: Rn. 5, 6 und 11). Daneben finden sich mit dem Grundsatz der Datenverarbeitung nach Treu und Glauben, den Grundsätzen der Zweckbindung der Datenminimierung, der Datenrichtigkeit, der Speicherbegrenzung und der Integrität und Vertraulichkeit in Artikel 5 Absatz 1 DS-GVO weitere Grundsätze, die bei der Auslegung der gesamten Verordnung beachtet werden müssen. Der zuvor genannte Grundsatz der Transparenz wird daneben durch zahlreiche Einzelverbürgungen der Verordnung konkretisiert (Herbst 2018: Rn. 19), wobei die prominentesten die Informationspflichten aus Artikel 13 und 14 DS-

GVO sein dürften, aufgrund derer Datenschutzhinweise erstellt werden müssen (vgl. Franck 2018: Rn. 2).

Die DS-GVO gilt nach Artikel 288 Absatz 1 des Vertrages über die Arbeitsweise in der europäischen Union (AEUV) unmittelbar in allen europäischen Mitgliedstaaten und bedarf keiner Umsetzung in nationales Recht (Vedder 2018: Rn. 18). Die Verordnung enthält zu einzelnen inhaltlichen Fragestellungen aber Öffnungsklauseln, mithilfe derer der europäische Gesetzgeber den Mitgliedstaaten wieder Regelungsspielräume überlässt (kritisch dazu Laue 2016: 463, 464 und 467). Zur Ausfüllung dieser Regelungsspielräume hat der deutsche Bundesgesetzgeber das Bundesdatenschutzgesetz (BDSG vom 30. Juni 2017 (BGBl. I S. 2097)) für Datenverarbeitungen durch private Stellen und öffentliche Stellen des Bundes und zahlreiche fachspezifische Normen erlassen (vgl. dazu den Gesetzesentwurf der Bundesregierung 1-212). Bezüglich der öffentlichen Stellen der Länder finden sich die DS-GVO flankierenden Gesetze in den Landesdatenschutzgesetzen (vgl. etwa das Landesdatenschutzgesetz Baden-Württemberg vom 12. Juni 2018 (GBl. S. 173)).

Die DS-GVO gilt auch für Straftaten und Ordnungswidrigkeiten verfolgende Behörden, soweit diese unter anderem übliche Verwaltungstätigkeiten wahrnehmen, Öffentlichkeitsarbeit leisten, Beschaffungsgeschäfte durchführen oder politisch tätig werden (vgl. Hornung und Spiecker gen. Döhmann 2019: Rn. 215). Für den verfolgenden Bereich wurden in Form der JI-Richtlinie jedoch Spezialvorschriften geschaffen.

2.3 JI-RL und Umsetzungsrechtsakte

Werden Behörden zum Zwecke der „Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung“ tätig, so finden sich spezielle europarechtliche Vorgaben in der JI-RL. Im strafverfolgenden Bereich gelten hierbei andere Maßstäbe an Transparenzvorschriften, da ansonsten die Effektivität der Strafverfolgung beeinträchtigt würde (vgl. Artikel 13 Absatz 3 JI-RL). Die JI-RL ist gemäß Artikel 288 Absatz 3 AEUV nur hinsichtlich ihrer Zielvorgaben verbindlich für die Mitgliedstaaten und muss von diesen in nationales Recht umgesetzt werden (vgl. Vedder 2018: Rn. 23 und 24). Eine hohe Anzahl an Umsetzungsmaßnahmen wird in den Polizeigesetzen des Bundes und der Länder zu finden sein, sofern sie bereits an die neue Richtlinie angepasst wurden (zum Stand der Anpassung der Bundesgesetze BfDI: 1).

2.4 Befugnisse der Aufsichtsbehörden

Artikel 8 Absatz 3 GRCh ordnet auf der höchsten Ebene der Normenhierarchie an, dass die Einhaltung der datenschutzrechtlichen Grundsätze aus Artikel 8 GRCh durch unabhängige Stellen überwacht wird. In diesem Sinne

sieht Artikel 51 Absatz 1 DS-GVO die Einrichtung von unabhängigen Datenschutzaufsichtsbehörden vor, die in Artikel 57 und 58 DS-GVO mit Aufgaben und Befugnissen ausgestattet werden (vertiefend Nguyen 2015: 265). Ähnliche Anforderungen an die Errichtung von unabhängigen Aufsichtsbehörden finden sich in Artikel 41 JI-RL, wobei Aufgaben und Befugnisse in Artikel 46 und 47 JI-RL geregelt werden.

3. Transparenz als Grundsatz des Datenschutzrechts am Beispiel der DS-GVO

Die DS-GVO beinhaltet eine Vielzahl an Transparenzvorschriften von denen neben dem Grundsatz der Transparenz aus Artikel 5 Absatz 1 Buchstabe a) DS-GVO die umfangreichste Verpflichtung in Form einer allgemeinen Rechenschaftspflicht in Artikel 5 Absatz 2 DS-GVO enthalten ist (vgl. dazu die Anforderungen bei Roßnagel 2019: Rn. 181, 182 und 183).

3.1. Der Grundsatz der Rechenschaftspflicht in Artikel 5 Absatz 2 DS-GVO

Der Grundsatz der Rechenschaftspflicht aus Artikel 5 Absatz 2 DS-GVO stellt Anforderungen an die Transparenzanforderungen von Datenverarbeitungen. Gemäß der Norm ist der Verantwortliche für die Einhaltung der oben dargestellten Grundsätze der DS-GVO verantwortlich. Hierauf bezogen stellt die Norm eine Nachweispflicht auf, die den Verantwortlichen zu hinreichenden organisatorischen Maßnahmen und Dokumentationen bringen soll, um die Rechtmäßigkeit des eigenen Handeln nachweisen zu können (Roßnagel 2019: Rn. 181, 183). Durch diese Verteilung der Nachweislast werden durch die Datenverarbeitungen betroffenen Personen entlastet und ihre Rechtsschutzmöglichkeiten vergrößert (vgl. Voigt 2019: Rn. 40). Wird eine für die Verarbeitung von personenbezogenen Daten verantwortliche Stelle von der zuständigen Aufsichtsbehörde kontrolliert, so muss die verantwortliche Stelle nachweisen können, dass sie die personenbezogenen Daten rechtskonform verarbeitet (Roßnagel 2019: Rn. 186).

In erster Linie werden aus der Grundnorm des Artikels 5 Absatz 2 DS-GVO direkt interne Dokumentationspflichten wie Mitarbeiterrichtlinien und Dokumentationen im Rahmen der internen Datenverarbeitungsprozesse abgeleitet (vgl. Pötters 2018: Rn. 33). Aber auch alle anderen Transparenzvorschriften der DS-GVO können als Konkretisierung dieser generellen Nachweispflicht gesehen werden (in Bezug auf Art. 30 DS-GVO bejahend Roßnagel 2019: Rn. 183 und 184).

3.2 Datenschutzhinweise als Transparenzmaßnahmen der DS-GVO

Artikel 13 und 14 DS-GVO sehen bestimmte Vorschriften vor, nach denen betroffene Personen über die Verarbeitung ihrer personenbezogenen Daten informiert werden müssen. Artikel 13 DS-GVO gilt für die Direkterhebung von Daten bei der betroffenen Person und Art. 14 DS-GVO für die Erhebung von anderer Stelle. Artikel 13 Absatz 1 und Artikel 14 Absatz 1 DS-GVO haben gemein, dass über Namen und Kontaktdaten der verantwortlichen Stelle, gegebenenfalls über die Kontaktdaten des Datenschutzbeauftragten, die Zwecke und die Rechtsgrundlage der Verarbeitung, Empfänger oder Kategorien von Empfängern und – falls vorhanden – die Absicht eines Drittlandtransfers informiert werden muss. Hinzu kommen die in Artikel 13 Absatz 2 und 14 Absatz 2 DS-GVO geforderten zusätzlichen Informationen, um „eine faire und transparente Verarbeitung zu gewährleisten". In der Praxis werden die beschriebenen Informationen in der Regel in der Form von Datenschutzerklärungen und Datenschutzhinweisen zur Verfügung gestellt (vgl. für Webseiten Stiemerling und Lachenmann 2014: 133).

Gemäß Artikel Absatz 12 Satz 1 DS-GVO sind diese Hinweise in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" zu übermitteln. Dies stellt für die Verarbeitung verantwortliche Stellen üblicherweise vor Herausforderungen. So nehmen die zur Verfügung zu stellenden Informationen einiges an Raum ein (vgl. auf Webseiten bezogen Stiemerling und Lachenmann 2014: 134). Auf europäischer Ebene hat der Europäische Datenschutzausschuss daher die Guidelines der Arikel-29-Datenschutzgruppe bestätigt, nach denen diese Hinweise gestuft zur Verfügung gestellt werden können (Artikel-29-Datenschutzgruppe, S. 23–24). Ausführliche Informationen können verlinkt oder mittels QR-Code eingebunden werden und nur die wesentlichen Informationen müssen auf der obersten Informationsebene enthalten sein (mit weiteren Beispielen Artikel-29-Datenschutzgruppe, S. 26).

Auch in sprachlicher Hinsicht sind die Erklärungen verständlich zu fassen. Wird beispielsweise ein konkretes Angebot vorwiegend den Einwohnern eines bestimmten Mitgliedstaates zur Verfügung gestellt, so müssen die Datenschutzhinweise auch in der Sprache dieses Staates zur Verfügung gestellt werden (Paal und Hennemann 2018: Rn. 35).

3.3 Verhaltenssteuerung durch Transparenzmaßnahmen

„Tools shape us as much as we shape them" (CNIL 2019: 6). Dieser Satz ist in einer Publikation der französischen Datenschutzaufsichtsbehörde zu lesen. Grafische Oberflächen und Transparenzwerkzeuge können uns genauso beeinflussen, wie wir sie beeinflussen (vgl. CNIL 2019: 6). Im Zuge der wachsenden Anzahl an wissenschaftlichen Arbeiten, Studien

und anderen Publikationen in diesem Feld (vgl. CNIL 2019: 45) wurden in diesem Bereich einige Hauptmethoden der Verhaltenssteuerung herausgearbeitet: So können die von der Verarbeitung personenbezogener Daten betroffenen Personen durch Nudging beeinflusst werden, wenn Ihnen durch kurzfristige Belohnungen Anreize und somit eine subjektive Tendenz für eine bestimmte Entscheidung mitgegeben werden (vgl. grundlegend Thaler und Sunstein 2008: 6; vgl. auch Forbrukerrådet 2018: 6–7). Diese Maßnahmen können von Framing und Priming durch fortgehende Betonung der positiven Aspekte der Datenverarbeitung (vgl. Forbrukerrådet 2018: 22–25) flankiert werden. Durch all diese Maßnahmen werden die Entscheidungen betroffener Personen oft in Richtung der Bejahung einer automatisierten Datenverarbeitung beeinflusst (vgl. CNIL 2019: 10).

3.4 Bildsymbole und andere Lösungen

Nach Artikel 12 Absatz 7 DS-GVO besteht die Möglichkeit, Datenschutzhinweise und -erklärungen mit standardisierten Bildsymbolen zu versehen. Gemäß Artikel 12 Absatz 8 DS-GVO ist die europäische Kommission im Zuge der Rechtssicherheit dazu berechtigt, in diesem Bereich einen delegierten Rechtsakt zu erlassen. Ein erster Entwurf derartiger Bildsymbole im Anhang der „Legislativen Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))“ des Europäischen Parlaments konnte sich innerhalb des Gesetzgebungsverfahrens zur DS-GVO leider nicht durchsetzen. Dies liegt vermutlich daran, dass die in den Datenschutzhinweisen beschriebenen Prozesse derart komplex sind, dass Grafiken sich nicht aus sich selbst heraus erklären und vom Betrachter nicht direkt gedeutet werden können. Erst wenn hier Standards gesetzt werden und allgemein geltende Symbole zentral bekannt gemacht werden, können betroffene Personen sich beim Betrachten erschließen, was die Bildsymbole bedeuten.

In der Zukunft sind besonders in diesem Bereich vereinfachende Innovationen gefragt, um die Selbstbestimmung der betroffenen Personen zu stärken (vgl. CNIL 2019: 44).

Es werden nicht mehr personenbezogene Daten erhoben, als für die spezifischen Zwecke der Verarbeitung erforderlich sind.

Es werden nicht mehr personenbezogene Daten gespeichert, als für die spezifischen Zwecke der Verarbeitung erforderlich sind.

Personenbezogene Daten werden nicht zu anderen als den Zwecken verarbeitet, für die sie erhoben werden.

Es werden keine personenbezogenen Daten an gewerbliche Dritte weitergegeben.

Es werden keine personenbezogenen Daten **verkauft oder verpachtet**.

Abb. 1: Quelle: Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)): (2017/C 378/55).

4. Transparenz und Videoüberwachung

Im Bereich der Verarbeitung personenbezogener Daten zur Videoüberwachung sieht sich die Umsetzung von Transparenzvorschriften gleich mehreren Schwierigkeiten gegenüber. Zum einen wird die Europarechtskonformität der deutschen gesetzlichen Vorschriften diskutiert (vgl. Brink und Wilhelm 2019: Rn. 18), zum anderen müssen die konkreten Transparenzmaßnahmen aber auch für alle Menschen erfassbar gestaltet werden.

4.1 Gesetzgeberische Regelungen

Neben den durch die DS-GVO vorgegebenen Vorschriften der Art. 13 und 14 DS-GVO sieht § 4 Abs. 2 BDSG vor, dass der „Umstand der Beobachtung und der Name und die Kontaktdaten des Verantwortlichen […] durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen" sind. Diese Spezialregelung für den Bereich der Videoüberwachung stellt sicher, dass bei Hinweisschildern zu Videoüberwachungsanlagen kein erheblicher Suchaufwand für betroffene Personen besteht (Brink und Wilhelm 2019: Rn. 38). Werden Daten einer bestimmten Person zugeordnet, verweist § 4 Absatz 4 BDSG auf die Artikel 13 und 14 DS-GVO. Da bei Videoüberwachungsanlagen grundsätzlich eine dahingehende Gefährdungslage anzunehmen ist, werden in der Regel daher nur die allgemeinen Artikel 13 und 14 DS-GVO anwendbar sein (Brink und Wilhelm 2019: Rn. 39).

Die Vorschrift des § 4 BDSG wird jedoch bezüglich ihres Geltungsanspruches für die Rechtmäßigkeiten der Datenverarbeitungen im nichtöffentlichen Bereich kritisiert, da der europäische Gesetzgeber gerade hier keine Öffnungsklausel für Regelungen des nationalen Gesetzgebers belassen hat (vgl. unter anderem DSK 2018: 1). Insoweit sind auch nach der Rechtsprechung des Bundesverwaltungsgerichtes die vorrangig geltenden Regelungen des Artikels 6 Absatz 1 Satz 1 Buchstabe f) DS-GVO heranzuziehen (BVerwG, Urt. v. 27.3.2019 – 6 C 2/18).

4.2 Praktische Umsetzung

Auch bezüglich der praktischen Implementierung wirft die Umsetzung der Transparenzvorschriften im Bereich der Videoüberwachung noch Fragen auf. Zwar ist die Videoüberwachung einer der wenigen Bereiche, in denen die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder ein gemeinsames Musterhinweisschild entwickelt haben. Dieses kann ausgefüllt werden und bietet insofern eine Vereinfachung im Rahmen der Handhabung der DS-GVO.

Im täglichen Gebrauch bestehen aber gerade im Bereich der Videoüberwachung erschwerende praktische Probleme. So können beispielsweise Sehgeschädigte nicht inkludiert werden, solange nur mit Hinweisschildern

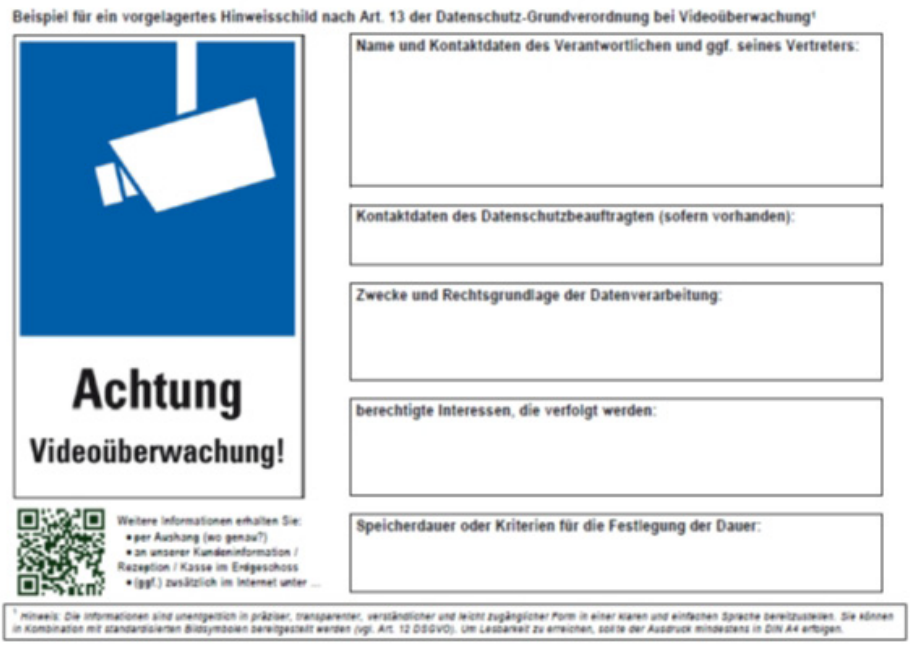

Abb. 2: Von den deutschen Datenschutzaufsichtsbehörden erarbeitete Vorlage für Datenschutzhinweise beim Betrieb einer Videoüberwachungsanlage; bereit gestellt von der LfD Niedersachsen.

gearbeitet wird. Automatisierte Lösungen führen oft zu weiteren Datenerhebungen, die theoretisch wiederum Targeting oder Profiling ermöglichen könnten und entsprechen somit oftmals nicht dem Grundsatz der Datenminimierung. Auch die Abgrenzung durch spezielle Bodenbeläge, durch die man den Beginn des videoüberwachten Bereichs mit Hilfsmitteln ertasten kann, sind aufgrund der hohen Präsenz von Videoüberwachungsanlagen im öffentlichen Raum schwer umzusetzen. Gerade in diesem Bereich sind jedoch Innovationen gefragt, da ansonsten die Verwirklichung der eigenen Rechte für im hohen Maße schutzbedürftige Personen am schwersten ist.

5. Ausblick

DS-GVO und JI-RL bilden zusammen mit den nationalen Vorschriften der Mitgliedstaaten einen neuen Rechtsrahmen für staatliche und private Überwachungsmaßnahmen, der auch eine unabhängige Kontrolle durch Aufsichtsbehörden ermöglicht. Neben dem Bestehen einer Rechtsgrundlage ist für den Schutz der betroffenen Personen aber auch die Transparenz der Maßnahmen entscheidend, da sie ansonsten keinen Rechtsschutz suchen können. Die immer komplexer und leistungsfähiger werdenden technischen Überwachungsanlagen fordern ein erhöhtes Maß an Transparenz, um die Selbstbestimmung betroffener Personen zu schützen. Hierbei gilt es, gra-

fische und technische Lösungen zu finden, die nicht anfällig für versteckte verhaltenssteuernde Maßnahmen sind. Die Entwicklung vereinfachter grafischer Darstellungen muss ebenso vorangetrieben werden und es müssen Lösungen gefunden werden, die alle Menschen inkludieren. Insoweit gilt es, Datenschutzhinweise in Zukunft nicht nur an den rechtlichen Voraussetzungen auszurichten, sondern auch die Erkenntnisse aus anderen Fachdisziplinen miteinzubinden.

Literatur

Arning, Marian und Flemming Moos (2014). Big Data bei verhaltensbezogener Online-Werbung. Programmatic Buying und Real Time Advertising. *Zeitschrift für Datenschutz* 4, 5, 242–248.

Artikel-29-Datenschutzgruppe. Leitlinien für Transparenz gemäß der Verordnung 2016/679. Angenommen am 29. November 2017. Zuletzt überarbeitet und angenommen am 11. April 2018. URL: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 [Letzter Zugriff am 04.10.2019].

Brink, Stefan und Maria Wilhelm (2019). BDSG § 4. In: Heinrich Amadeus Wolff und Stefan Brink (eds.). *BeckOK Datenschutzrecht.* München: C.H. Beck, Rn. 1–84.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI). Umsetzung der JI-Richtlinie in Deutschland. URL: https://www.bfdi.bund.de/DE/Datenschutz/Themen/Sicherheit_Polizei_Nachrichtendienste/SicherheitArtikel/JI-Richtlinie.html [Letzter Zugriff am 04.10.2019].

Bundesregierung, Entwurf eines Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU). URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2018/dsanpug.html [Letzter Zugriff am 04.10.2019].

Chinese State Council, Planning Outline for the Construction of a Social Credit System (2014–2020). 14. Juni 2014. URL: https://chinacopyrightandmedia.wordpress.com/2014/06/14/ [Letzter Zugriff am 02.10.2019].

Commission Nationale de l'Informatique et des Libertés (2019). Shaping Choices in the Digital World. From. *IP Reports* N°06. URL: https://www.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf [Letzter Zugriff am 04.10.2019].

Datenschutzkonferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK)(2018). *Kurzpapier Nr. 15.* Videoüberwachung nach der Datenschutz-Grundverordnung URL: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_15.pdf [Letzter Zugriff am 04.10.2019].

Europäisches Parlament. Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)). URL: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//DE#title2 [Letzter Zugriff am 04.10.2019].

Forbrukerrådet (2018). Deceived by Design. How tech companies use dark patterns to discourage us from exercising our rights to privacy. URL: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf [Letzter Zugriff am 04.10.2019].

Franck, Lorenz (2018). Art. 13 Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten bei der betroffenen Person. In: Peter Gola (ed.). *DS-GVO*. München: C.H. Beck, Rn. 1–59.

Grittmann, Joachim (2019). Art. 51. In: Jürgen Taeger, Detlev Gabel und Joachim Grittmann (eds.). *DS-GVO*. Frankfurt am Main: Fachmedien Recht und Wirtschaft / dfv Mediengruppe.

Heldt, Amélie P. (2019). Gesichtserkennung: Schlüssel oder Spitzel? Einsatz intelligenter Gesichtserfassungssysteme im öffentlichen Raum. *MultiMedia und Recht* 22, 5, 285–289.

Herbst, Tobias (2018). Art. 5. Grundsätze für die Verarbeitung personenbezogener Daten. In: Jürgen Kühling und Benedikt Buchner (eds.). *DS-GVO*. München: C.H. Beck, 210–232.

Hornung, Gerrit und Indra Spiecker gen. Döhmann (2019). Einleitung. In: Spiros Simitis, Gerrit Hornung und Indra Spiecker gen. Döhmann (eds.). *Datenschutzrecht.* Baden-Baden: Nomos, 158–240.

Huber, Peter M. (2018). Art. 19. In: Rudolf Streinz (ed.). *EUV/AEUV*. München: C.H. Beck.

Laue, Philip (2016). Öffnungsklauseln in der DS-GVO – Öffnung wohin? Geltungsbereich einzelstaatlicher (Sonder-)Regelungen. *Zeitschrift für Datenschutz* 6, 10, 463–467.

Lewinski, Kai von (2017). Datenschutzaufsicht in Europa als Netzwerk. *Neue Zeitschrift für Verwaltungsrecht* 36, 20, 1483–1490.

Nguyen, Alexander (2015). Die zukünftige Datenschutzaufsicht in Europa. *Zeitschrift für Datenschutz* 5, 6, 265–270.

Paal, Boris P. und Moritz Hennemann (2018). Art. 12. In: Boris P. Paal und Daniel A. Pauly (eds.). *DS-GVO*. München: C. H. Beck, Rn. 33–35.

Pötters, Stephan (2018). Art. 5. Grundsätze für die Verarbeitung personenbezogener Daten. In: Peter Gola (ed.). *DS-GVO*. München: C.H. Beck, 216–223.

Roßnagel, Alexander (2019). Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten. In: Spiros Simitis, Gerrit Hornung und Indra Spiecker gen. Döhmann (eds.). *Datenschutzrecht.* Baden-Baden: Nomos, 363–398.

Schantz, Peter (2019a). Art. 5. In: Heinrich Amadeus Wolff und Stefan Brink (eds.). *BeckOK Datenschutzrecht*. München: C.H. Beck.

Schantz, Peter (2019b). Art. 6 Abs. 1 Rechtmäßigkeit der Verarbeitung. In: Spiros Simitis, Gerrit Hornung und Indra Spiecker gen. Döhmann (eds.). *Datenschutzrecht*. Baden-Baden: Nomos, Rn. 133–139.

Stiemerling, Oliver und Matthias Lachenmann (2014). Erhebung personenbezogener Daten beim Aufruf von Webseiten – Notwendige Informationen in Datenschutzerklärungen. *Zeitschrift für Datenschutz* 4, 3, 133–136.

Sydow, Gernot (2018). Einleitung. In: Gernot Sydow (ed.). *Europäische Datenschutzgrundverordnung.* Baden-Baden: Nomos, 245–304.

Thaler, Richard H. und Cass R. Sunstein (2008). *Nudge, Improving Decisions About Health, Wealth and Happiness.* New York: Penguin.

Vedder, Christoph (2018). Art. 288. In: Christoph Vedder und Wolff Heintschel von Heinegg (eds.). *Europäisches Unionsrecht.* Baden-Baden: Nomos.

Voigt, Paul (2019). Art. 5. In: Jürgen Taeger, Detlev Gabel und Paul Voigt (eds.). *DSGVO/BDSG*. Frankfurt am Main: Fachmedien Recht und Wirtschaft / dfv Mediengruppe.

Wegener, Bernhard W. (2016). Art. 18. In: Calliess/Ruffert (eds.). *EUV/AEUV*. München: C.H. Beck.

Weichert, Thilo (2013). Big Data und Datenschutz Chancen und Risiken einer neuen Form der Datenanalyse. *Zeitschrift für Datenschutz* 3, 6, 251–259.

Wilhelm, Maria (2016). Auskunftsansprüche in der Informationsgesellschaft. *Die öffentliche Verwaltung* 21, 899–905.

Bildquellen

Abb 1: Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)): (2017/C 378/55).

Abb.2: URL: https://lfd.niedersachsen.de/startseite/themen/videouberwachung/transparenzanforderungen_bei_einer_videouberwachung_nach_der_ds_gvo/transparenzanforderungen-und-hinweisbeschilderung-bei-einer-videoueberwachung-nach-der-ds-gvo-158959.html [Letzter Zugriff am 15.09.2019]

Maria Wilhelm
Leitung der Stabsstelle Europa beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg
Königstraße 10a
D-70173 Stuttgart
E-Mail: poststelle@lfdi.bwl.de

Zeitschrift für
Semiotik
Band 40 • Heft 1-2 (2018)
Seite 23-43
Stauffenburg Verlag Tübingen

Der totale Unterhaltungsstaat. Überwachung im digitalen Zeitalter
Über Konsum, KI und nicht nur digitale Domestiken

Nils Zurawski, Universität Hamburg

Summary. Entertainment as surveillance? The Orwell'ian model of Big Brother seem no longer apt to describe the contemporary moment and its immediate future. But how should a model look like that is able to adequately grasp the dynamics and phenomena that shape societies in the 21st century? The article wants to propose such a new model and provides the necessary analysis that is needed to understand the dimensions of control and surveillance in contemporary societies. The starting point for such an analysis lies in the question why digital technologies are so widely accepted, while people often seem to ignore the problematic consequences, even when they are aware of them. The assumption is that the digital satisfies desires, which obscure a critical assessment of such new technologies, data collections and the restructuring of our everyday environments. Two hypotheses will guide the analysis. One assumes that the digital will bring back the servant, now for the masses and thus will bring initiate a re-feudalisation of societies. The second addresses the fact that digital technologies are offering ways of distinction, an important mode for the formation of identity under the conditions of consumer capitalism. With both hypothesis the article will endeavour to think about structures of power and domination in societies under the digital conditions of total entertainment.

Zusammenfassung. Unterhaltung als Überwachung? Im digitalen Zeitalter ist der Orwell'sche Big Brother nicht länger das passende Modell um die Gegenwart und Zukunft zu beschreiben. Wie müsste ein neues Modell jedoch aussehen, um den Dynamiken und Erscheinungsweisen adäquat Rechnung zu tragen, die Gesellschaften im 21. Jahrhundert kennzeichnen? Der Artikel unternimmt den Versuch, ein solches anderes Modell vorzuschlagen und stellt damit gleichzeitig die notwendige Analyse vor, die es braucht, um die Dimensionen von Kontrolle und Überwachung gegenwärtiger Gesellschaften zu verstehen. Der grundlegende Ausgangspunkt für diese Analyse ist die Frage, warum es eine so breite Akzeptanz digitaler Technologien gibt, bei gleichzeitiger Kenntnis, aber scheinbarer Ignoranz ihren Konsequenzen gegenüber. Die Vermutung ist, dass hier möglicherweise Bedürfnisse befriedigt werden, die eine Kritik an den neuen Technologien, an Datensammlungen

und der Umgestaltung von Alltagswelten obsolet erscheinen lassen. Anhand von zwei Aspekten soll diesen Fragen nachgegangen werden. Zum einen wird die These aufgestellt, dass das Digitale eine Rückkehr der Domestiken darstellt und darüber eine Re-Feudalisierung von Gesellschaft stattfindet. Zum anderen bieten viele der Technologien Möglichkeiten der Distinktion sowie der Identitätswerdung, wie sie im Konsumkapitalismus elementar sind. Diese beiden Phänomene werden genutzt um über Machtstrukturen und Herrschaftsformationen unter den digitalen Bedingungen in einer Gesellschaft der totalen Unterhaltung nachzudenken.

1. Einleitung

„Wir amüsieren uns zu Tode", stellte Neil Postman noch in den 1980er Jahren mit Blick auf das Fernsehen fest (Postman 1985). Ihm ging es damals vor allem um die Möglichkeiten von Urteilsbildung im Zeitalter der Unterhaltungsindustrie. Seine Analyse war nicht nur im Unterton kulturkritisch. Doch mit der Ausbreitung des Internet seit den 1990 Jahren und insbesondere seit den dort festzustellenden Quantensprüngen, was sowohl die Technologie, die Verbreitung als auch gesellschaftliche Bedeutung anbelangt, ist von einer solchen These nichts mehr zu hören gewesen. Ganz im Gegenteil erlebt das Fernsehen gerade durch das Internet und die Möglichkeiten des Streaming eine Art Renaissance, das Anschauen von Serien wird zum Distinktionsmerkmal der hippen, urbanen und vor allem digitalen Klasse. Nicht nur die Medien als solche haben sich gewandelt, sondern die Medientechniken haben die Bedingungen, unter denen heute viele Aspekte gesellschaftlichen und individuellen Lebens stattfinden, verändert. Dabei handelt es sich nicht um einen simplen Ursache-Wirkung-Zusammenhang, sondern um eine Geschichte wechselseitiger Beeinflussung und Nutzung aufgrund von individuellen und sozialen Bedürfnissen, die auf passende (und unpassende) Angebote und Möglichkeiten gestoßen ist. Ähnlich könnte man die von Armin Nassehi aufgestellte These zur Herkunft der digitalen Gesellschaft auch lesen. Seine Theorie der digitalen Gesellschaft basiert auf der grundlegenden Frage, für welches Problem die Digitalisierung eine Lösung sei (2019: 12). Ich kann mich dieser Grundthese sehr wohl anschließen, möchte aber in diesem Artikel vor allem einen Blick darauf werfen, welche Bedürfnisse hier möglicherweise geweckt worden sind und wie die Wechselwirkungen zwischen Gesellschaft und Technologie die Conditio Digitalis erzeugt haben, in der wir heute leben und welche mit ganz unterschiedlichen Begriffen belegt wird. Es geht mir also konkreter als Nassehi um die Wechselwirkungen, wie sie im Alltag und als soziales Phänomen nachzuzeichnen sind.

Der von mir im Titel skizzierte Unterhaltungsstaat trifft es dabei nur zum Teil, auch und gerade weil an dem Begriff Staat eine zentrale Steuerung zu hängen scheint, was selbstverständlich nicht zutreffend ist. Ganz im Gegenteil scheint es hier eher gegenläufige Entwicklungen zu geben, die

es auch einem Staat zunehmend schwierig macht, sich in einer digitalen Welt mit bisherigen politischen Steuerungsstrategien zu behaupten. Ein wichtiges, leider eher selten beachtetes Merkmal eines digitalen Zeitalters ist der Hang zu Totalitäten – auch und gerade weil dieses Zeitalter so bunt, so frei, so abwechslungsreich erscheint. Den Zusammenhang von Totalität und Freiheit, der Abwechslung bei gleichzeitigem Einschluss hat bereits 1975 und nahezu prophetisch der britische Schriftsteller J.G. Ballard in seinem Roman *High Rise* gezogen.

> Andererseits mochten Sie ihre wahren Bedürfnisse später herausstellen. Je öder und reizloser das Leben im Hochhaus wurde, desto größere Möglichkeiten bot es. Eben durch seine Effizienz übernahm das Hochhaus die Aufgabe, das soziale Gefüge, das sie alle stützte, zu bewahren. Es beseitigte erstmals die Notwendigkeit ihnen die Freiheit, von der Norm abweichende und abwegige Regungen zu erkunden. Genau in diesen Bereichen würden sich die wichtigsten und interessantesten Erscheinungen ihres Lebens zutragen. Im Gehäuse des Hochhauses geborgen und sicher wie Passagiere an Bord eines mittels Autopilot gesteuerten Verkehrsflugzeuges, hatten sie die Freiheit, sich auf jede beliebige Weise zu benehmen, die dunkelsten Ecken, die sie finden konnten, zu erkunden. In vieler Hinsicht war das Hochhaus ein Musterbeispiel für all das, was die Technologie getan hatte, um die Manifestation einer wahrhaft „freien" Psychopathologie zu ermöglichen (Ballard 2016: 48).

Die Schwierigkeit, solche literarischen Bilder auf heutige Verhältnisse anzuwenden, ist offensichtlich. Als Metapher ließe sich aber mit den evozierten Bildern eine Analogie zu den sozialen Medien und den dazugehörigen Internet-Unternehmen von Google bis Facebook ziehen. Und doch hat das von Ballard gezeichnete Bild durchaus einen Reiz, wie etwa die Thesen von Pierangelo Maset zeigen. Dieser nennt den Prozess, den er angesichts gegenwärtiger Entwicklungen zu beobachten meint, ein „Geistessterben". In dessen Mittelpunkt sieht er eine technisch-ökonomische Mentalität, die Individuen und Gesellschaft bestimmt. Die Gesellschaft scheine sich darin „zu einem komfortablen Gefängnis entwickelt zu haben, an dessen Perfektionierung wir täglich arbeiten" würden, so Maset (2010: 11).

Sowohl bei Ballard als auch bei Maset schimmert das klassische Überwachungsdispositiv von Fürsorge und Kontrolle in Variationen durch: Geborgenheit auf der einen Seite bei gleichzeitigem Abschluss auf der anderen. Freiheit hier, Überwachung dort. Den Einfluss und die Geschäftsstrategien der großen Internetunternehmen kann man skandalisieren, insbesondere ihren Umgang mit den persönlichen Daten der Nutzer. Das trifft aber nicht den entscheidenden Punkt. Auch wenn es ein ‚Aufreger' sein mag, was alles an Daten über Personen gespeichert wird, ist es nicht der eigentliche Aspekt, der im Mittelpunkt der Betrachtung stehen sollte. Vielmehr sollte es darum gehen, welche Rolle und Bedeutung diese Unternehmen, das Digitale schlechthin im Leben von Menschen, in ihrem Alltag und für eine gesellschaftliche Existenz bereits eingenommen hat. Denn die Wechselwirkungen zwischen den technischen Anwendungen sowie ihrer Akzep-

tanz und Nutzung sind in Bedürfnissen begründet. Eine Analyse muss genau jene Bedürfnisse in den Blick nehmen, die es ermöglichen, dass das Digitale einen dermaßen großen Anteil am Leben der Menschen einnehmen konnte und somit letztlich zu einer Veränderung von gesellschaftsstrukturierenden Dynamiken geführt hat. So weit, dass man über die ‚digitalen Bedingungen' von Gesellschaft nachdenken muss. Eine dieser Bedingungen, die nicht ursächlich mit dem Aufkommen digitaler Technologien in Verbindung steht, aber letztlich ihre Durchsetzung enorm befördert hat, ist die Logik des Konsums. Dazu möchte ich noch einmal auf Ballard zurückkommen, für den Konsum und die Entfremdung von der Gesellschaft prägende Themen in seinen Werken sind. Man könnte das folgende Zitat auch als eine Beschreibung der Gegenwart lesen, in der die Verbindung von digitalen Technologien als gesellschaftlicher Utopie und Heilslehre auf der einen Seite und dem Konsum als lebens- und gesellschaftsbestimmende Form auf der anderen Seite umrahmt werden von Fragen nach Macht in einer Gesellschaft. Dabei streift auch Ballard immer wieder die Frage nach Klasse und Herrschaft – welche auch gegenwärtig eher bedeutender als unwichtiger geworden sind.

> Im Kontrast dazu waren die Dienstboten, die sie im Apartmentgebäude hatte, ein unsichtbares Heer von Thermostaten und Feuchtigkeitssensoren, computergesteuerten Schalt-und Regelsystemen der Fahrstühle, die alle ihre Rolle in einer weit komplizierteren und abstrakteren Variante der Herr-Knecht-Beziehung spielten (Ballard 2016: 102f.).

Ballard thematisiert hier zwei Aspekte, die auch für die folgende Analyse wichtig sind: Macht und Herrschaft sowie die Bedeutung von Dienstboten. Bei der Diskussion der These von der Unterhaltungsgesellschaft, und somit den Bedingungen von Gesellschaft unter den Prämissen digitaler Technologien, spielen auch diese beiden Aspekte eine wichtige Rolle. Grundlegend dafür ist die Frage, warum es eine so breite Akzeptanz der Technologien und bei gleichzeitiger, scheinbarer Ignoranz ihren Konsequenzen gegenüber gibt – oder andersherum: Welche Bedürfnisse werden möglicherweise darüber befriedigt und warum spielt die Kritik an den neuen Technologien, an Datensammlungen usw. keine allzu große Rolle? Zur Beantwortung der Frage konzentriere ich mich auf den Aspekt der Distinktion einerseits und auf ein Art Wiederkehr von Domestiken andererseits. Beides hängt zusammen und bietet die Möglichkeit über Machtstrukturen und Herrschaftsformationen unter den digitalen Bedingungen von Gesellschaft nachzudenken. Die folgenden zwei Ausgangsüberlegungen sollen die Grundlage für die danach folgenden Ausführungen sein.

Die erste Überlegung ist eher eine begriffliche Einlassung zur Wahl des Begriffes ‚Unterhaltungsstaat'. Das gängige Bild um die Folgen einer sich ausbreitenden Digitalisierung besonders drastisch zu skizzieren, ist der ‚Überwachungsstaat'. Und es gibt in der Tat Grund dazu, diesen Begriff zu nutzen, um auf mögliche Gefahren neuer Technologien, ihren Einfluss auf

und ihre Verbreitung in der Gesellschaft hinzuweisen. Doch treffen die so evozierten Bilder oft nicht die Lebenswirklichkeit von Menschen, insbesondere nicht in den westlichen Demokratien, wo diese Diskurse sehr dominant sind – bei gleichzeitiger relativ großer Freiheit sowie (im globalen Vergleich) weitgehender sozialer Gerechtigkeit und Sicherheit. Vor allem aber lässt dieser Begriff einer Analyse wenig Raum, die aus dem Alltag heraus versucht zu beschreiben, wie die Digitalisierung erlebt wird. Das Bild des Unterhaltungsstaates ermöglicht mit einem Blick auf die angenehmen, praktischen, schönen und erlebten Dinge des digitalen Lebens eine neue Perspektive auf Kultur und Gesellschaft im digitalen Zeitalter. Es befreit den Diskurs von der Tristesse eines 1984, die sich in den vielen gegenwärtigen Alltagspraktiken kaum widerspiegelt – ohne die Kontrollproblematik dabei ausblenden zu wollen. Nicht zuletzt hat die Entwicklung hin zum digitalen Zeitalter auch damit zu tun, dass die Technologien den Menschen neue Möglichkeiten geben, sich selbst neu zu verorten, ihre Identität zu verhandeln, neu zu erschaffen, soziale Beziehungen anders zu knüpfen und dabei neue Formen eines Distinktionsgewinns zu kreieren als auch zu nutzen.

Daraus folgt als Konsequenz die zweite Überlegung, welche sich mit dem Erfolg der Digitalisierung im Alltag befasst. Dieser Erfolg liegt in einem ihrer zentralen Versprechen, nämlich dem der Lebenserleichterung, vermittelt über den Imperativ des Praktischen und Automatischen. Oder anders ausgedrückt, die Digitalisierung erlaubt eine Delegation von Aufgaben an Technologie, die erscheint, als würde man Domestiken und Dienerschaften befehligen – Institutionen, die einer längst vergangenen Zeit anzugehören scheinen (vgl. Bartmann 2016). Jeder kann sich nun (digitale) Dienstboten leisten, die von Ferne all die Aufgaben übernehmen, die man sonst selbst übernehmen müsste. Diese Art der digitalen Re-Feudalisierung von Gesellschaft ist enorm attraktiv, insbesondere unter den Bedingungen eines Konsumkapitalismus (vgl. Bauman 2009; Miller 2010, 2012), in dem das eigene Ich eine Marke wird, die Identität über den Konsum von Gütern, Dienstleistungen, Lebenseinstellungen, Haltungen usw. gebildet und dargestellt wird. Das ist nicht kulturpessimistisch zu verstehen, sondern der Versuch einer Beschreibung, welche Rolle diese Art kapitalistischer Wertschöpfung in der Gesellschaft spielt, nämlich die der Identitätsstiftung.

Wenn man sich aber Domestiken, wie auch immer diese aussehen, wieder leisten kann, dann wird die Beherrschung der digitalen Domestiken so zu einem Ausweis gesellschaftlicher Stellung und Bedeutung – auch wenn in einer Welt automatisierter Massenproduktion potenziell jeder diese Art der Distinktion für sich in Anspruch nehmen kann. So zeigt sich hier zumindest eine Motivation für die Nutzung digitaler Technologien, entgegen allen Warnungen vor dem Abbau von Freiheiten, der Aushöhlung des Datenschutzes oder der Entwicklung hin zu einer totalen Überwachungsgesellschaft. Will man den Gegebenheiten des digitalen Zeitalters besser Rechnung tragen und neue Möglichkeiten für die Beschreibung und Erklärung von gesellschaftlichen Prozessen haben, sollte dieser Begriff ersetzt oder zumindest modifiziert werden – die ‚totale Unterhaltungsgesellschaft' ist ein Vorschlag dafür.

2. Distinktion und Domestiken – Konsum und Überwachung

Zurück also zur Frage „Warum machen da nur so viele Leute mit?“ Warum haben so viele Menschen ein Smartphone und lassen sich freiwillig überwachen? Diese Fragen sind durchaus gerechtfertigt, helfen aber nur wenig, um die Zusammenhänge zwischen der Durchdringung des Alltags mit digitalen Technologien auf der einen sowie den Bedürfnissen der Menschen auf der anderen Seite zu verstehen. Es ist vor allem die große Variationsbreite der Digitalisierung von sehr unterschiedlichen Phänomenen, bei denen sich aber gerade in Bezug zur eingangs gestellten Frage eine Reihe von überraschenden Gemeinsamkeiten finden lassen.

So berichtet das *Wall Street Journal* am 22. Februar 2019 davon, wie Facebook die Daten von anderen Apps aus dem Smartphone auslesen kann und es auch tut. Das allein ist nicht neu und in einer Reihe von Facebook-Berichten nur eine weitere Geschichte des laxen Umganges mit den Daten anderer Menschen. Mit dabei war allerdings auch eine App (der Firma Flo Health), die von Frauen zur Kontrolle ihres Menstruationszyklus genutzt wird und von sich sagt, dass 25 Millionen Frauen aktive Nutzerinnen der App sind. Damit sammelt Facebook hochsensible Daten von 25 Millionen Frauen und ihren Angaben zu einer sehr privaten, intimen Angelegenheit. Das mag skandalös sein. Die viel interessantere Frage ist aber, warum 25 Millionen Frauen einen solchen Dienst in Anspruch nehmen, warum sie eine App benutzen, für etwas, dass zum einen eine sehr intime Angelegenheit ist, zum anderen auch ohne eine App gut funktioniert hat. Dabei sind diese spezielle Anwendung und die damit verbundenen Services nur ein Beispiel unter vielen anderen Gesundheits-Apps, mit denen man den eigenen Blutdruck, den Puls, die Fitness, Kalorien oder was auch immer messen kann. In den Stores von Google und Apple sollen 100.000 dieser kleinen Programme zur Verfügung stehen, die uns helfen können, den eigenen Körper besser zu verstehen und somit – so das Versprechen – uns selbst besser optimieren zu können, mithin bessere Menschen zu werden. Es geht bei den so verschiedenen Programmen und Plänen der digitalen Zukunft um so unterschiedliche Dinge wie Gesundheit, Mobilität, das Wohnen der Zukunft, aber auch um die Ausforschung des Menschen, um ihnen die Angebote machen zu können, die das Leben an sich vereinfachen. Angetrieben wird vieles davon selbstverständlich von kommerziellen Interessen. So sind die Unternehmen sehr interessiert daran, ihre Kunden besser zu kennen, ja zu erkennen, z.B. beim Betreten eines Geschäftes ihre Gefühle zu analysieren, um entsprechende Angebote machen zu können. Im Kern ist das Konsumpsychologie mit digitalen Mitteln. Anna Gauto beschreibt in einem Artikel die Produkte und Strategien sehr ausführlich („Sie blicken in dein Herz“, 2017) und fragt zu Recht, ob wir eine Welt akzeptieren müssen, in der alles protokolliert wird, auch gegen unseren Willen? Auch wenn diese Frage wichtig und wahrscheinlich entscheidend ist, wenn es darum geht die zukünftige digitale Ausgestaltung der Gesellschaft mitzubestimmen, so ist es nur die eine

Hälfte der Entwicklung. Die andere Hälfte muss sich mit der Frage der Lebenserleichterung und -verbesserung beschäftigen. Dem Versprechen, welches von den digitalen Anbietern, den großen Plattformen wie Google und Co gemacht wird. Ein Versprechen dessen Annahme aber nicht allein mit Zwang oder Unwissenheit erklärt werden kann, nicht hierzulande, nicht in China, wo mit dem Social Score ein umfassendes System der Alltagskontrolle geschaffen wurde. Hier wird kontrolliert, überwacht, aber eben auch belohnt und wahrscheinlich trifft, wenn man verschiedenen Berichten Glauben schenkt, die Maßnahme auf individuelle sowie gesellschaftliche Bedürfnisse.

Überhaupt lassen sich viele Entwicklungen digitaler Technologie auf den Aspekt der Lebenserleichterung zurückführen, zumindest wenn es um die Argumente ihrer Nutzung geht. Das bekannteste Beispiel dürfte hierbei Amazons Alexa sein oder ähnliche Produkte von Google oder Microsoft. Der Haushaltsassistent, der auf sprachlichen Befehl bzw. durch eine Mensch-Maschine-Kommunikation reagiert, die wie eine ‚ganz normale Interaktion' anmutet, hilft dabei, im Haushalt Dinge zu erledigen oder andere Services für die Besitzer auf den Befehl hin zu organisieren. Dazu gehört die Bedienung von so genannten Smart Homes ebenso wie eine Bestellung beim örtlichen Pizzalieferanten, die Musikauswahl in der digitalen Plattensammlung oder bei einem Streaming Dienst. Die Möglichkeiten erscheinen unerschöpflich. Dass es im Zusammenhang mit Alexa auch schon zu eher bedenklichen Entwicklungen gekommen ist, verwundert dabei nicht. Da dieser Assistent, man könnte auch sagen die technische Mitbewohnerin, alles aufzeichnet, was sich in der Wohnung so tut, wurde sie in den USA in einem Fall zur Komplizin der Strafverfolgungsbehörden (Lobe 2017; Heller 2017). Was als Spielerei erscheint, könnte tatsächlich Konsequenzen für den Bereich der Strafermittlung, der Strafprozessordnung oder auch der Rechtsprechung in diesem Bereich haben. Was die Kriminalistik angeht, so sind die Einflüsse unübersehbar, da es auch bereits jetzt so ist, dass Datenspuren Teil von Ermittlungen sein können. Die Implikationen einer freiwilligen umfänglichen Raumüberwachung sind nicht ganz absehbar. Rechtlich dürfte dann u.a. die Frage bestehen, was oder wer überhaupt ein Zeuge ist oder sein kann, wenn diese Systeme gar in der Zukunft eigene Zusammenfassungen liefern könnten, Einschätzungen oder gar Interpretationen bis hin zu Vorschlägen zu Urteilen liefern sollen (vgl. aus Berk 2012, 2017). Aus der Perspektive des Rechts, aber vor allem aus einer gesellschaftsanalytischen, besteht die Frage, inwiefern Amazon und Co Hilfskräfte der Polizei oder gar die Polizei selbst werden – sind sie dann Agenten der sozialen Kontrolle im Auftrag eines Staates oder aus eigener Motivation heraus? Was an der Oberfläche wie ein Mehr an Nutzerfreundlichkeit oder Lebenserleichterung aussieht, basiert auf algorithmischen Verfahren und wird zunehmend unter der Überschrift der Künstlichen Intelligenz verhandelt (oder angepriesen, je nachdem ob man sich davon den nächsten wirtschaftlichen Boom verspricht). Dass die Ehrfürchtigkeit, die im allgemeinen diesem Bereich digitaler Technologie entgegengebracht

wird, nicht unbedingt der richtige Umgang damit ist, zeigen kritische Betrachtungen des Themas (Pasquale 2015; Feustel 2018; Pinker 2019; zu Überwachung und Religiosität auch Taureck 2014).

Die Ausbreitung von algorithmischen Verfahren in Kombinationen durch digitale Technologien und den Bereich der Künstlichen Intelligenz stellt Gesellschaften vor viele unterschiedliche Herausforderungen, bei denen sich grundlegende Fragen aufdrängen, die sich vor allem auf die Wechselwirkungen und Abhängigkeiten von Technik und Gesellschaft beziehen. Dass dabei kaum Bereiche des täglichen Lebens ausgenommen sind, zeigen so banale Beispiel wie der tägliche Einkauf. Der Kauf mit Bargeld wird durch die Benutzung einer Bezahl-App auf dem Smartphone ersetzt, andere Karten, die Zugänge oder Rabatte ermöglichen, ebenfalls. Selbst für die Erstellung des Einkaufszettels, bisher vor allem im Alltag ein Sache von Stift und Notizblock, kann über eine App erledigt werden. Dabei ist der Zettel nicht einfach ersetzt worden. Eine solche App kann einfach mehr, merkt sich die Wünsche, das Datum, macht eventuell Vorschläge, beginnt möglicherweise den Einkauf zu regulieren. Sebastian Balzer erkennt daran nicht ganz zu Unrecht einen „Irrsinn“ (2019), wobei auch in seiner Beschreibung die Frage nach dem Warum der Benutzung von Seiten der Anwender nicht explizit gestellt wird. Es ist klar, dass die Händler den Vorgang digitalisieren wollen, denn dann können sie damit ihr eigenes Angebot verknüpfen. Initiativen im größeren Maßstab, wie das indische Programm einer ‚cashless society‘ (Ross), verfolgen andere Ziele – hier u.a. Korruptionsbekämpfung –, die Effekte der Vernetzung dürften aber auch hier ökonomisch begründet sein und den Händlern eher zum Vorteil gereichen als letztlich den Kunden. In Indien kommt dazu das Problem einer sehr ungleichen Entwicklung, einer enormen Armut bei einem substantiellen Teil der Bevölkerung, die an den Segnungen des digitalen Zeitalters nicht uneingeschränkt teilnehmen können. Daher ist ein wichtiger Grund in Indien, wie auch in den vermeintlich hoch entwickelten Staaten des Westens, der Aspekt einer ‚Modernität‘ an sich. Eine Analyse der Verbreitung digitaler Technologien im Alltag kann sich nicht nur auf die Effekte der Technik oder der soziotechnischen Wechselwirkungen im Hinblick auf Kontrolle, Überwachung oder Datenschutz allein konzentrieren, sondern muss auch den Bedürfnissen nachgehen, die möglicherweise die Akzeptanz der Technologien erleichtert und ihre Verbreitung beschleunigt. Außerdem muss sie die Hemmschwellen der Nutzung, auch in Bereichen, wo es möglicherweise wie ‚Irrsinn‘ oder schlicht abwegig erscheint, erklären. Dass vieles geht, ist ersichtlich, und technische Neuerungen werden weiterhin scheinbar alltägliche Bereiche mit neuen Möglichkeiten bereichern.

Dass es dabei um eine Kontrolle, um das Abgreifen von Daten oder schlicht Profit durch neue Geschäftsmodelle geht, kann in vielen Fällen als gegeben vorausgesetzt werden. Das erklärt aber nicht die Verbreitung selbst und die Annahme und tatsächliche Anwendung der Apps, Programme, Services und der vernetzten Lebenserleichterer insgesamt. Denn der Diskurs wird weithin kritisch geführt und auch eigene empirische Forschungen

haben gezeigt, dass das Wissen über mögliche Gefahrenpotenziale durchaus vorhanden ist (vgl. Zurawski 2011, 2014), dieses aber nicht unbedingt ein Hindernis für ihre Nutzung darstellen muss. Warum also?

Es gibt drei Punkte, die sich für eine Erklärung mit Bezug auf die möglichen Bedürfnisse auf Seiten der Nutzer anbieten. Dabei geben gerade nicht die jeweils individuellen Vorlieben der Nutzer den Ausschlag, sondern viel eher lassen sich hier soziale, kollektive Muster erkennen. Zum einen handelt es sich dabei um den bereits erwähnten Wunsch nach Modernität. Als Referenz ist hier nicht die historische Epoche der Moderne gemeint, etwa in Abgrenzung zur Postmoderne. ‚Modern sein' bezieht sich eher auf eigene Wahrnehmungen von Zeitverläufen in individuellen Biografien oder gegenwärtigen Zeithorizonten. Man braucht einfach den letzten Stand der Technik, das neueste Design und muss sich im Sinne des Konsums auf der Höhe der Zeit befinden, sonst ist man ‚von gestern'.

Des Weiteren spielt bei der Akzeptanz vieler Angebote der Aspekt der Distinktion eine wichtige Rolle. Diese ist nicht zuletzt auch mit einer Idee von Modernität verbunden, nämlich dann, wenn der Gebrauch solcher Technik eben auch ein Ausweis der eigenen Modernität ist und man sich damit möglicherweise von anderen bewusst absetzen kann.

Der dritte Punkt ist die digitale ‚Re-Feudalisierung', welche aus einem Wunsch nach Domestiken und Dienstboten entspringt, vor allem in den Mittelschichten, hier auch als Mittel der Distinktion, aber ebenso getrieben von einem Fortschrittsnarrativ, in dem auch die Idee einer Weltbeherrschung durch technische Überlegenheit, Automatisierung und allmächtiger Kontrolle der eigenen Umwelt eine maßgebliche Rolle spielt.

Mit den Begriffen von Modernität, Distinktion und Domestiken verbunden sind vor allem soziale Praktiken, in denen Menschen aufeinander bezogen in ihrem Alltag handeln, oft in Routinen, aber vor allem mit einem sozialen Sinn. Auch Überwachung ist Teil dieser Routinen und Beziehungen, häufig über Technologie vermittelt, wenn es um den Wunsch geht, ‚modern' zu sein. Das muss allerdings nicht heißen, dass Überwachung auch immer klar als solche benannt werden kann, andererseits aber auch, dass diese selbst zu einem Gut geworden ist, dass verhandelt oder konsumiert wird, eben um modern, anders, etwas Besonderes zu sein. Immer, so scheint es mir, aber ist Überwachung dabei eine Vermittlerin von Beziehungen bzw. in der Art und Weise der Beziehungen und Praktiken von Konsum und Distinktion selbst eingeschrieben.

2.1 Konsum und Distinktion

Indem Konsum auch sekundäre Bedürfnisse befriedigt, also solche, die über die primären des physischen Wohlbefindens und Überlebens hinausgehen, kommt der Distinktion dabei eine entscheidende Rolle zu (vgl. Hellmann 2005: 11ff.; anknüpfend an Bourdieu und Veblen auch Lamla 2013: 168ff.; Reith 2019). Konsum hat nicht nur ein Ziel, sondern ist das Ziel, der

Sinn und Zweck der Handlung selbst. Ähnlich unterscheidet Bauman (2009) verschiedene Abstufungen von Konsum. Vor allem unterscheidet er den Konsum vom Konsumismus, einem gesellschaftlichen Attribut, mit der eine spezifische Form menschlichen Zusammenlebens beschrieben wird. Bauman bezeichnet diese spezifische Form als Ökonomie des Überschusses und der Täuschung, in der es sichtbarer Zeichen der Zugehörigkeit bedarf, um im Prozess der Selbstidentifikation eine Identität auszubilden (vgl. Bauman 2009: 65, 108f.). Das Merkmal der Konsumgesellschaft ist die Inszenierung, nicht nur der Produkte, sondern der Menschen als Produkte in der Ausgestaltung sozialer Beziehungen. Hier soll nicht allein eine eher ‚konsumkritische' Haltung meine Ausführungen bestimmen, sondern zunächst die schlichte Tatsache, dass eine solche Logik existiert und diese strukturierend wirkt. Der britische Anthropologe Daniel Miller (2010, 2012) hat durch zahlreiche ethnografische Studien zum Konsumalltag von Menschen, ihren Beziehungen zu Dingen oder dem Sinn von Shopping gezeigt, wie eine Kultur des Konsums sich im Alltag materialisiert. Einkaufen als Erlebnis (im Deutschen eher mit dem englischen Wort „Shopping" beschrieben) ist dabei noch kein sehr altes Phänomen, dessen Ursprünge sich zu Beginn der Industrialisierung verorten lassen. Adam (2012) zeigt sehr schön am Beispiel der Entstehung von Warenhäusern, wie hier eine Kultur der Inszenierung von Massenartikeln entstanden ist, deren größter Erfolg wohl die symbolische Individualisierung eines Massenphänomens ist. Dass es dabei auch um Täuschung, Simulation, das Kopieren von adligen Lebensstilen und Symbolen ging, sollte man einfach hinnehmen, die Konsequenzen daraus für die sozialen Beziehungen sind daher nicht weniger real. Wolfgang Ullrich (2013) bezeichnet eine Kritik an dem Konsumismus als widersprüchlich, da dabei übersehen werde, dass auch eine Ablehnung innerhalb der Konsumlogik stattfände. Diese spezielle kulturpessimistische Kritik an Konsum sieht diesen als Gegenüber einer reinen Kultur, die es so allerdings nicht gegeben haben kann. Insbesondere arbeite sich eine Kulturkritik von links, so Ullrich, an den Verblendungszusammenhängen der Warenwelt ab, wobei man mittlerweile durchaus argumentieren könnte, dass auch diese Art der Kritik ein Lebensstil geworden ist und damit zu einem Teil von Konsum. Konsum ist mehr als Kaufen, Konsum beschreibt die Art und Weise, wie soziale Beziehungen gestaltet sind, nämlich über die Auswahl, die Selbstinszenierung, die symbolische Kraft von Waren, wobei eben auch die eigene Darstellung (und soziale Identität) als Form einer Ware angesehen werden kann. Meine eigene Untersuchung zu Einkaufserfahrungen und Kundenkarten (vgl. Zurawski 2011, 2014) hat hier auch gezeigt, wie soziale Beziehungen in den Alltagspraktiken des Shoppings thematisiert und verhandelt werden. Konsum ist nicht ein Extra zum ansonsten vollkommen anders verlaufenden Alltag, sondern der Alltag selbst. Interessanterweise waren bei der Benutzung von Kundenkarten die problematischen Aspekte der Datensammlung und der möglichen Überwachung von Gewohnheiten und Aktivitäten durchaus ein Thema und bekannt – das aber wurde durch andere Aspekte des Konsums überlagert. Dabei auch solche Aspek-

te, die mit und durch eine Kundenkarte geschaffen bzw. verdeutlicht worden sind, z.B. die Treue zu einem Produkt oder einem Anbieter. Kundenkarten sind, bei aller Kritik an den Datensammelpraktiken ihrer Anbieter, eben auf den Prozess des Konsums, des Shoppens ausgerichtet und werden nicht als ein Element der Überwachung wahrgenommen – anders als Kameras zur Kontrolle öffentlicher Plätze, die in Verbindung mit einer Kriminalprävention aufgestellt werden. Kundenkarten zu besitzen oder eben nicht, ist auch Teil von Distinktionspraktiken im Shopping-Kontext (vgl. Zurawski 2011a). Dabei sind auch heute Simulationen und Nachahmungen bestimmter Konsumformen und Lebensstile von besonderen Milieus Teil von Konsumpraktiken, ähnlich wie vor 200 Jahren die Nachahmung eines adligen Stils in bürgerlichen Lebensformen, wie am Beispiel der Warenhäuser ersichtlich wird. Kernaspekt einer Konsumgesellschaft ist damit ein Widerspruch: Nämlich die Individualisierung von Stilen, die Konstruktion der eigenen Identität mithilfe von Massenprodukten. Andreas Reckwitz (2017) sieht ebenfalls die von ihm als Singularitäten beschriebenen Subjektivierunspraktiken als sozial fabriziert an. Diese Singularitäten sind ein Produkt des Wunsches nach Distinktion, aber eben mit den Mitteln massenhaft produzierter Güter und massenhaft verfügbarer Symbole der Distinktion, der besonderen Lebensstile. Ökonomie und Technologie werden, so Reckwitz, in der Spätmoderne zu Singularisierungsgeneratoren (Reckwitz 2017: 15, 173ff.). Menschen suchen in dieser Spätmoderne nach dem Einzigartigen, ‚erfinden' sich quasi als Subjekte, wobei – und das wird so nicht ganz deutlich bei Reckwitz – sie dazu auf eben jene Massenprodukte zurückgreifen, die erst über eine besondere Erzählung zu dem Besonderen werden. Sonst wäre es nicht zu erklären, warum Apples iPhone einen derartigen Status erlangt hat, das Kaffeetrinken so hip geworden ist, Moden und Trends der Einzigartigkeit in Massen auftreten. Dass dabei romantische Verklärungen einer ‚guten alten Zeit' bisweilen eine dominante Rolle spielen können, zu erkennen im Retro-Design vieler Dinge, von Autos über Möbel bis hin zur Gestaltung von ganzen Stadtvierteln, Geschäften, aber auch Gewohnheiten und Trends, ist Teil solcher Erzählungen. ‚Modern-sein' bedeutet auch immer fortschrittlich zu sein, an den Fortschritt zu glauben. Obschon ein ungebrochener Fortschrittsglaube und auch eine ungebrochene Fortschrittserzählung nicht mehr so existieren wie noch in den Hochzeiten des Industriezeitalters, so schöpft der Wunsch nach Moderne auch aus dem Glauben an eine immer weitergehende Entwicklung, die teleologisch auf eine bestimmte Form der höchsten Vollendung zustrebt. Robert Feustel sieht daran eine Religiosität des Digitalen (vgl. Feustel 2018; auch Sarr 2019; zur Kritik an einer westlichen Moderne auch Latour 2008). Modern zu sein heißt auch dabei sein zu können, technologisch sowieso, aber darüber eben auch gesellschaftlich, mit einer Distinktionsleistung sich absetzen von der Masse. Die Beherrschung digitaler Technologien, die aktive Akzeptanz neuer, digital vermittelter Dienste und Angebote, die Nutzung von sozialen Medien, von Smartphones, elektronischen Bezahl-Apps, digitalen Einkaufslisten, der automatischen Steuerung des Smart Homes (oder

einzelner Funktionen in der Wohnung) sind eben jene Tätigkeiten oder Errungenschaften, über die sich diese Art der Distinktion im Sinne einer Modernität umsetzen lässt. Bei vielen der Tätigkeiten geht es nicht primär um digitale Technologien, sondern um die Umsetzung alltäglicher Praktiken mit eben jenen Apps und Technologien, gerade weil man modern sein will. Das Beispiel der Einkaufsliste zeigt sehr gut, wie sich eine nahezu banale Tätigkeit mit einem Smartphone zu einem Akt moderner Selbstvergewisserung ummünzen lässt – einfach auch, weil es geht und Teil eines Lebensstils geworden ist. Konsum und Moderne gehen in dieser Hinsicht zusammen und bedingen einander.

In dieser Analyse mag ein System wie das Sozialkreditsystem in China auf den ersten Blick nicht hinein passen. Es wirkt zu repressiv, der Staat selbst ist autoritär, teilweise willkürlich und hat nur wenig Berührungspunkte mit westlichen Demokratien (oder ihren Idealbildern). Dennoch ist China technologisch absolut auf der Höhe, wenn nicht gar vielen anderen Staaten voraus, vor allem was die Anwendung von digitalen Technologien angeht. Eine Reportage von Xifan Yang (2019; vgl. auch Dorloff 2019) in der *ZEIT* zeigt aber, dass es auch hier zum einen die kapitalistischen Strukturen sind, die eine wichtige Rolle bei der Ausbreitung und Akzeptanz der Technologien als solche spielen; zum anderen geht es beim Sozialkreditsystem um die Herstellung von Vertrauen, u.a. in Abgrenzung zu einem korrupten Staat und einer noch korrupteren Wirtschaft. Dass 80 % der Chinesen einer Untersuchung zufolge dieses System positiv bewerten, ist aus dieser Perspektive dann auch keine Überraschung. Die Überwachungstechnologie trifft auf soziale Bedürfnisse in einer autoritären Gesellschaft, in der sich manche politischen Entscheidungen sehr einfach von oben durchsetzen lassen. Auch wenn es ein Bewusstsein für die Überwachung gibt, so scheint das Bedürfnis nach Vertrauen und gesellschaftlichen Zusammenhalt stärker zu sein als die Bedenken. Das soll keine Verteidigung des Systems sein, aber ein Hinweis, dass Überwachung eben auch aus den Wechselwirkungen gesellschaftlicher und individueller Bedürfnisse, staatlicher Kontrollwünsche und technologischer Möglichkeiten entstehen kann. Das brutale System aus *1984* eignet sich nicht, um diese Wechselwirkungen zu beschreiben. Es reicht eben nicht, nur darauf zu schauen, welche Formen der Überwachung durch neue Technologien möglich sind – dank Big Data und der so genannten Künstlichen Intelligenz fast alles –, sondern es bedarf auch einer Analyse der Beweg- und Akzeptanzgründe. Modern-sein und die Dinge des Lebens mit digitaler Technologie zu erledigen, gehört dann eben auch dazu.

2.2 Domestiken und elektronische Dienstboten

Neben der Distinktion und dem Wunsch modern zu sein, ist es die Möglichkeit von Domestiken, die sich als Erklärung für den anscheinend so bedenkenlosen Umgang mit Technologien, die ein starkes Potenzial für

Überwachung und Kontrolle besitzen, anbieten. Digitale Technologien fördern eine Re-Feudalisierung von Gesellschaft, wenn auch in den überwiegenden Fällen nur als Simulation und des sowie-als-ob. Die damit verbundenen Praktiken schließen an die durch einen Konsumkapitalismus geprägten Formen der Identitätsbildung und Alltagspraktiken nahtlos an. Und es sind nicht von ungefähr die Mittelklassen die hauptsächlichen Träger dieser Kultur, eben die kulturellen Klassen wie sie bei Reckwitz heißen (ähnlich sieht auch Lamla das Bürgertum als einen Hauptakteur und beschreibt dabei den Consumer Citizen, 2013: 182ff.) oder ein neues Bürgertum, wie es von Christoph Bartmann (2016) als neue Feudalherren (meine Begrifflichkeit) ausgemacht wird. Bartmann seinerseits beschreibt sehr anschaulich, wie sich digital vermittelt ein Heer an Servicepersonal organisieren lässt – vom bekannten Pizzaboten, dem Hausmeister, der Putzfrau, Handwerkern, Babysittern bis hin zu Fahrdiensten oder den viel beschriebenen Paketlieferanten. Er schöpft seine vielfältigen Beispiele aus seinen Erfahrungen aus New York, wo er das Goethe-Institut geleitet hat. Deutlich wird dabei vor allem, wie hier eine neue Unterklasse entsteht, ein Heer an Dienstboten und Haushaltspersonal, welches die oft unsichtbare Seite eines digital befeuerten Kapitalismus ausmacht – schlecht bezahlt, kaum organisiert, nicht selten illegal, auf sich selbst zurückgeworfen ohne große Absicherung. Shoshana Zuboffs (2015, 2018) Analyse des Überwachungskapitalismus findet hier eine sehr passende Entsprechung. Bartmann beschreibt die vielfältigen Verflechtungen und konzentriert sich nicht zu Unrecht auf die so genannten Plattformen (Google, Amazon, AirBnB, Uber usw.), um sein Argument deutlich zu machen. Der Vorteil an dieser Art von Service-Personal im Gegensatz zu echtem Hauspersonal à la Downton Abbey ist, dass es wenig bis gar nichts kostet, immer verfügbar ist und als billige Angestellte oder Selbstständige den Unterboden eines modernen Kapitalismus darstellt. Diese Art der Domestiken sind nicht neu, sondern Teil einer Dienstleistungsökonomie, die allerdings durch digitale Technologien und Plattformen dynamisiert wurde. Die Ausbeutungsverhältnisse treten noch stärker zutage, die Aspekte der Überwachung vielfältiger Lebensbereiche wird enger und gravierender – Plattformen und ihre Angebote sind zusehends mit dem Alltag verwoben und beeinflussen ihn (vgl. dazu auch Murakami Wood und Monahan 2019; Lobe 2019). Die Plattformen haben immer mehr Einfluss und Kontrolle im und über den Alltag von Menschen. Nun sind die Konsumenten der Plattformen nicht ihre Arbeiter, dennoch erwirtschaften die Unternehmen mit ihnen einen Gewinn, sei es durch die angebotenen Dienstleistungen oder die weitere Verwendung ihrer Daten. Da die Plattformen anstreben, allumfassend zu sein, also möglichst viele Aspekte des Lebens einschließen wollen, ist dieser Vergleich durchaus berechtigt. Noch allerdings gibt es keine Plattform für alles, sondern sie decken nur ganz spezielle Bereiche (Mobilität, Ferienwohnungen, Spiele) oder größere Ausschnitte ab (Google, Amazon usw.). Mehr und mehr aber verschmelzen auch hier die verschiedenen Aspekte des täglichen Lebens, so dass man von einer Totalisierung sprechen kann, was die Angebote, die Kontrolle und

den über diese Plattformen organisierten Alltag angeht. Darin wird Ballards Beschreibung mehr und mehr zur Realität der Gegenwart, wenn er schreibt, dass

> genau in diesen Bereichen […] sich die wichtigsten und interessantesten Erscheinungen ihres Lebens zutragen [würden]. Im Gehäuse des Hochhauses geborgen und sicher wie Passagiere an Bord eines mittels Autopilot gesteuerten Verkehrsflugzeuges, hatten sie die Freiheit, sich auf jede beliebige Weise zu benehmen, die dunkelsten Ecken, die sie finden konnten, zu erkunden (Ballard 2016: 48).

Darüber hinaus bieten die digitale Welt und ihre Technologien aber noch mehr als nur eine elektronische Kommunikation mit echten Menschen (auch wenn man diese im besten Fall nicht sieht oder wahrnimmt bzw. per Plattform über diese verfügt wird), nämlich die automatischen Helfer im Internet der Dinge. Und das beinhaltet mehr als nur die vielen Hilfe-Apps, wie die zitierten Smartphone-Einkaufszettel oder die App fürs Menstruationsmanagement. Hier geht es konkret um die Steuerung von Dingen, Geräten, Maschinen, ganzer Häuser (als „smart homes“), dem Alltag ganz allgemein bis hin zum autonomen Fahren und einem umfassenden Mobiliätsmanagement. Über das Internet der Dinge scheint sich der Traum von der automatisierten Umwelt, in einigen Fällen auch den automatisierten Menschen, endgültig umsetzen zu lassen. Der Traum ist dabei nicht so neu, aber gerade die aufkommende Moderne, gekennzeichnet u.a. durch eine Rationalisierung von Welt, hat immer wieder, zumindest fiktional, diese Verbindungen gezogen. Von E.T.A. Hoffmanns Sandmann, Goethes Zauberlehrling, Shelleys Frankenstein, H.G. Wells oder anderen Fantastik- und später den Science Fiction-Autoren bietet der automatisierte Helfer oder der helfende, aber durch den Menschen kontrollierte Automat, der Roboter, immer wieder ein willkommenes Sujet, über die eigene Unvollkommenheit, aber eben auch die eigenen Machtfantasien oder die menschliche Hybris selbst nachzudenken – vor allem wenn die Kontrolle dem Menschen entgleitet. Und mit der digitalen Vernetzung kann sich nun fast jeder Diener dieser Art wieder leisten. Die Beherrschung der digitalen Domestiken wird so zu einem Ausweis gesellschaftlicher Stellung und Bedeutung – auch wenn in einer Welt automatisierter Massenproduktion potenziell jeder diese Art der Distinktion für sich in Anspruch nehmen kann. Damit würde sich der Kreis auch wieder schließen. Neben den Aspekten der Bequemlichkeit und der eigenen Lebenserleichterung wird so die Verfügbarkeit über Domestiken wieder schick, zu einem Teil des eigenen Lifestyles, einem Aspekt absoluter Modernität und Praktikabilität, der eigenen Effizienzsteigerung, die sich scheinbar logisch ergibt, aber eben auch nicht mehr ist als Teil eines ökonomischen Narratives der totalen Verfügbarkeit und der eigenen Optimierung. Das Mängelwesen Mensch (Arnold Gehlen) schafft sich Abhilfe durch eine digitale Vermehrungsmeute (Canetti 2006), eingebettet in einen Konsumkapitalismus und die digitalen Technologien. Dass der Weg zu Überhöhungen der Technologie ins Religiöse nicht weit und quasi angelegt ist

in der Wahrnehmung von digitaler Technologie, zeigt Robert Feustel (2018) in seiner Analyse des Informationsbegriffes und daran hängender Menschenbilder. Und auch das Silicon Valley benutzt immer wieder Bilder quasi religiöser Anmutung, wenn z.B. der (mittlerweile verstorbene) Steve Jobs einem evangelikalen Prediger gleich die neueste Entwicklung von Apple vorgestellt hat. Eine Fetischisierung von Technologie lässt sich hier sehr anschaulich zeigen. Die Verbindungen des Silicon Valley zu New Age-Esoterik, den Hippies bis hin zu evangelikalen Erweckungsbewegungen wurde u.a. von Turner (2008) nachgezeichnet. Als hoch rationale, aber dennoch techno-religiöse Variante davon erscheint die sogenannte Bewegung der Transhumanisten (vgl. u.a. Spreen u.a. 2018). Ihre Ideen, mit Technik den Menschen überwinden zu wollen, bilden mehr als nur eine technische Neugier ab. Man kann sich allerdings fragen, warum und für wen, wenn es denn dann keine Menschen mehr gibt, die diesen Zustand genießen oder ausnutzen können. Steven Pinker (2019) hält diese Versprechungen der Künstlichen Intelligenz und ihrer Übernahme der Macht ohnehin für überzogen und die Technik eher für eine Projektionsfläche von Wünschen, Träumen und Vorstellungen denn greifbare Realität, vor allem aber ein falsch verstandenes Konzept von Intelligenz. Dennoch gibt es eine wachsende Bereitschaft bei Forschern und Vordenkern des Digitalen, den Menschen vom Computer her zu denken, also zu fragen, ob die Menschen nicht den Computern ähnlicher werden (Siemons 2019).

In die Niederungen des Alltages spielen diese Ideen zwar hinein, ihre Erscheinungsweisen sind hier allerdings viel banaler, auch wenn die Ideen oft hochfliegend sind und die Rettung der Welt, die Zukunft der Menschheit versprochen wird. Wenn es um die elektronischen, digitalen Dienstboten geht, dann kommt man nicht an den Smart Home-Ideen vorbei, in denen die bauliche Infrastruktur und die Funktionalität von Wohnungen oder Eigenheimen digital vernetzt ist. Florian Rötzer spricht hier sehr passend von der „neuen Unheimlichkeit“ (2019). Bezüglich einer Re-Feudalisierung des Alltages als Teil von Disktinktionspraktiken des digital modernen Bürgers bietet sich das Smart Home geradezu als Beispiel an, auch wenn die Handreichungen mitunter banal sind – automatisch Licht anmachen, Kameras per Smartphone kontrollieren, die Heizung steuern oder den Herd anmachen. Gerade das Wohnen ist nicht nur ein elementarer Teil des Alltages, sondern ein Feld der Selbstfindung, der Selbstdarstellung und Identitätskonstruktion, in dem Distinktion zum Prozess der Subjektivierung fest dazu gehört (vgl. Miller 2010). Hinsichtlich der Auswirkungen ist aber hier nicht zu unterschätzen, dass die Vernetzung eben einen ehemals absolut privaten Raum, das eigene Heim, wenn nicht öffentlich, so doch transparent und von außen kontrollierbar macht. Ein Smart Home scheint den Bewohnern die Wünsche vorwegzunehmen, das Management abzunehmen, so Rötzer (2019), auch wenn es tatsächlich von der Ferne aus kontrollierbar wird, und eben nicht allein durch die Bewohner, sondern durch die Unternehmen, die entsprechende Infrastrukturen, technische Einheiten und Netzwerke anbieten sowie, wie so häufig im digitalen Zeitalter, durch den Zugriff unbefugter Dritter von außen.

Beim Wohnen lässt sich insofern die eigene Modernität und die dazugehörige technologische Kompetenz besonders gut darstellen und ausleben. Über die Automatisierung des Alltages u.a. mit der digitalen Verfügbarkeit eines selbst programmierten Hauses, lässt sich somit besonders gut zeigen, dass ‚man es sich leisten kann' und entsprechend nichts mehr selbst machen muss, sondern eben ‚machen lässt'. Die Kontrolle wird zu einem Teil des Konsumangebots, sowohl die Kontrolle über das Haus als auch die Kontrolle der Technik über das eigene Leben. Sich überwachen zu lassen – was im Alltag als digitale Verfügbarkeit und Beherrschung der Umwelt durch Technik erlebt wird – ist Teil einer Distinktionspraxis, weshalb hier von einem ‚Konsum der Überwachung' gesprochen werden sollte und eben nicht nur von der Überwachung von Konsumgewohnheiten. Dass diese Art der Überwachung möglicherweise auch ein Privileg für manche Gruppen von Menschen darstellt, während es für andere eine Unvermeidlichkeit oder gar ein Zwang sein kann, verweist auf den Ungleichheitscharakter des Überwachungskapitalismus, in deren Rahmen die Ausbreitung der digitalen Technologien mit ihren Versprechen stattfindet. Auch wenn die Allverfügbarkeit der Smartphones und der Digitalisierung eine Demokratisierung der Möglichkeiten verspricht, so ist nicht anzunehmen, dass bestehende Ungleichheiten beseitigt werden. Im Gegenteil, es werden neue geschaffen.

3. Fazit: Optionalmaschinen und die totale Unterhaltung

Wenn ich dem Konzept der Singularitäten von Reckwitz (2017) folge, worin er das Merkmal des Sozialen in der Spätmoderne sieht, wären das dazu passende technische Gerät das Smartphone, welches wie eine individualisierte Optionalmaschine die Verlängerung der Welt für jedes Individuum ist. Alles, von den Dienstboten bis hin zur Steuerung eines Smart Homes, vom Management der eigenen sozialen Beziehungen und seiner Kontakte bis hin zu den Informationen über die Welt, lässt sich bequem davon aus steuern. Das Globale erreicht jeden einzelnen unvermittelt, das Smartphone als Fenster zur Welt, ein Interface der Wirklichkeitserfahrung und -erkundung. Was allerdings aussieht wie eine Technologie der Emanzipation, ist in den meisten Fällen nur ein Gerät um Optionen auszuwählen, deren Zusammenstellungen von den Plattformen selbst vorgenommen wurden. Was am Ende erscheint, ist dann nur noch eine eingeschränkte, oft passgenaue Auswahl, zugeschnitten auf den oder die jeweilige Nutzerin. Es ist lediglich nur noch die Simulation einer grenzenlosen Auswahl. Der Kulturwissenschaftler Cohn als auch der Philosoph und Kognitionswissenschaftler Dennett sehen das Problem in der Art und Weise, wie Welt präsentiert wird und welche Möglichkeiten bestimmte Formen der Technologie bieten bzw. nicht mehr bieten. Dennett betont vor allem die Abhängigkeit durch die Technologie, wenn er feststellt, dass „[…] pretty soon we become so dependent on our new tools that we lose the ability to thrive without them.

Options become obligatory“ (Dennett 2019: 44). Cohn beschäftigt sich in seinem Buch *The Burden of Choice* (2019) intensiv mit eben diesen Optionen. Die ‚Auswahl haben‘ ist das Kernelement einer Konsumgesellschaft, um die eigene Individualität auszudrücken. Cohn sieht darin allerdings unter den Bedingung digitaler Technologien eine Sackgasse und befürchtet, dass „the act of making choices ceases to be a performance of individuality and instead becomes an operation of conformity“ (Cohn 2019: 35). Auf analytischer Ebene stimme ich ihm zum, würde aber behaupten wollen, dass dieser Identitäts- und Individualisierungsprozess dennoch als Erzählung weiter funktioniert, weswegen die Strategie auch bestehen bleibt. Der Trick ist es, auch diese Konformität weiterhin als Ausdruck der Individualität zu verschleiern. Ebenso wie eine Singularität, wie sie Reckwitz beschreibt, die mit den Produkten aus einer Massenproduktion umgesetzt wird, die als besonders individuell vermarktet oder als solche angesehen werden. In beiden Fällen werden die Zusammenhänge so verschleiert, dass auch eine Kontrolle und die Überwachung der Konsumenten genau dort ansetzen kann – in ihrem Konsumalltag, zu dem eben auch gehört, erreich- und verortbar zu sein, mithin also überwachbar (vgl. Zurawski 2014; Marx 2016).

Was Cohn für den gesamten Bereich der Auswahl- und Empfehlungsalgorithmen ausführt und sehr anschaulich und kritisch darlegt, kann man konzentriert auf das Smartphone anwenden. Letztlich ist es das Gerät, die Technologie, welches die Ströme bündelt und quasi immer dabei ist. Smartphones sind Optionsmaschinen, in dem dort über standardisierte Möglichkeiten der Auswahl die Illusion einer vielfältigen und sehr persönlichen Auswahl erzeugt wird (vgl. auch Cohn 2019: 187). Die Optionsmaschinen schränken die Auswahlen ein, um die Qual der Wahl zu minimieren und bieten aber dennoch ein Interface, dass das beständige Auswählen wie einen Akt persönlicher Autonomie aussehen lässt. Das hat in mehrerlei Hinsicht mit dem Smartphone als Technologie, als Kulturgut und Symbol als auch als Produkt von Unternehmen zu tun, die mehr als nur Telefongeräte bzw. hochleistungsfähige, tragbare Computer herstellen. Und es hat mit den Algorithmen zu tun, die diesen Prozessen Struktur geben. Dass sich Smartphones wenig eignen, die benutzten Apps auch zu programmieren, die aktive und emanzipatorische Teilhabe an den digitalen Technologien auf das eher passive Auswählen beschränkt, verstärkt den Eindruck ihrer rein auf Konsum ausgelegten Beschränkung noch zusätzlich (vgl. u.a. Sambuli 2017). Für das Argument, dass Überwachung unter den Bedingungen der Digitalisierung vor allem konsumiert wird (auch wenn das im Alltag weder so genannt wird, noch so erscheint), ist eine Betrachtung der Technologie wichtig und darüber hinaus ihre Bedeutung innerhalb der Strukturen eines Überwachungskapitalismus, wie ihn Shoshana Zuboff skizziert hat. Cohns Beobachtungen und Thesen sind vor allem deshalb wichtig, da die Strukturen des digitalen Überwachungskapitalismus weitreichend sind. Sie sind nicht unbedingt neu, aber in ihrer Reich- und Tragweite bedeutsam hinsichtlich der Frage, wie sich heute Macht vor allem über die Beherrschung des Marktes auch politisch auswirken kann. Amazon, Google, Apple und

Co sind als Plattformen sowohl die Anbieter von Inhalten, sie stellen die Zugangsgeräte, ermöglichen den Zugang zum Netz und lenken den Diskurs. Sie sind Hersteller der Technologie, Produzent und Kaufhaus in einem. Mehr Kontrolle über Form, Inhalt und dank digitaler Technologien auch der Nutzer selbst geht fast nicht. Es lässt sich angesichts der Kontrolle von Inhalt, Form und Auswahl sowie den dargebotenen Optionen von den Möglichkeiten einer Formatierung der Wirklichkeit sprechen, die eng mit den kulturellen Gegebenheiten und der technischen Ausgestaltung der Geräte zusammenhängen.

Im Sinne Pierangelo Masets wäre es jenes von ihm diagnostizierte Geistessterben. Um eine eher positiv konnotierte Dimension in die Analyse zu bringen, würde ich den Aspekt der Unterhaltung hervorheben wollen. Damit wäre es möglich, digitale Technologie als kulturelles Phänomen zu benennen, welche untrennbar von ihren Inhalten und den Produzenten geworden ist. Die Überwachung ist möglich, weil sie in den Produkten und der Art und ihrer Nutzung angelegt ist und von ihnen scheinbar nicht trennbar ist. Digitale Technologien sind eben nicht mehr nur Ergänzungen zum sonstigen Leben, sondern Kern des Sozialen geworden und über sie damit auch die Kontrolle von Gesellschaft und Individuen. In diesem Sinne kann man das von Ballard evozierte Bild des Hochhauses als Totalität auch auf eine Unterhaltungsgesellschaft anwenden, die durch und über digitale Technologie kontrolliert wird, wobei die Bedürfnisse ihrer Mitglieder nach Distinktion und Modernität die Erklärungen für ihre Akzeptanz liefern würden.

> In vieler Hinsicht war das Hochhaus ein Musterbeispiel für all das, was die Technologie getan hatte, um die Manifestation einer wahrhaft „freien" Psychopathologie zu ermöglichen (Ballard 2016: 48).

Die Gesellschaft der Singularitäten als freie Psychopathologie in einer digital erzeugten, vermittelten und beherrschten Überwachungsgesellschaft, deren innere Logik Unterhaltung, Distinktion und der widersprüchliche Wunsch einer Zugehörigkeit zu einem individualisierten Kollektiv ausmacht? Darüber gilt es in Zukunft nachzudenken. Diese Gesellschaft ist möglich, weil ihre Verlockungen und Versprechungen auf die individuellen und kollektiven Bedürfnisse innerhalb der Gesellschaft treffen. Gewissermaßen ko-evolutionär entwickeln sich beide aufeinander bezogen. Die Digitalisierung ist nicht der Ausgangspunkt einer solchen Gesellschaft, sondern die willkommene Konsequenz ohnehin bestehender Bedürfnisse.

Literatur

Adam, Birgit (2012). *Alles, was das Herz begehrt. Von Wunderkammern und Konsumtempeln*. Hildesheim: Gerstenberg.

Ballard, J.G. (1975). *High Rise*. London: Jonathan Cape. Deutsch von Michael Koseler: *High-Rise*. Berlin: diaphanes 2016.

Balzer, Sebastian (2019). App zum Einkaufen. *Frankfurter Allgemeine Sonntagszeitung* 24.03.2019, 26.

Bartmann, Christoph (2016). *Die Rückkehr der Diener. Das neue Bürgertum und sein Personal.* München: Hanser.

Bauman, Zygmunt (2007). *Consuming Life.* Oxford: Polity Press. Deutsch von Richard Barth: *Leben als Konsum.* Hamburg: Hamburger Edition 2009.

Berk, Richard (2012). *Criminal Justice forecasts of Risk: A Machine Learning Approach.* New York: Springer.

Berk, Richard (2017). An impact assessment of machine learning risk forecasts on parole board decisions and recidivism. *Journal of Experimental Criminology* 13, 2, 193–216.

Bourdieu, Pierre (1979). *La distinction. Critique sociale du jugement. Paris: Les éditions de minuit.* Deutsch von Bernd Schwibs und Achim Russer: *Die feinen Unterschiede. Kritik der gesellschaftlichen Urteilskraft.* Frankfurt a.M.: Suhrkamp 1987.

Canetti, Elias (2006). *Masse und Macht.* Frankfurt a.M.: Fischer.

Cohn, Jonathan (2019). *The Burden of Choice. Recommendations, Subversion, and Algorithmic Culture.* New Brunswick: Rutgers Univ. Press.

Dennet, Daniel (2019). What can we do. In: John Brockman (ed.). *Possible minds. 25 ways of looking at AI.* New York: Penguin.

Dorloff, Axel (2019). Chinas intelligenter Schule entgeht nichts. URL: https://www.deutschlandfunk.de/alles-unter-kontrolle-chinas-intelligenter-schule-entgeht.680.de.html?dram:article_id=438868 [Letzter Zugriff am 30.08.2019].

Feustel, Robert (2018). *„Am Anfang war die Information". Digitalisierung als Religion.* Berlin: Verbrecher Verlag.

Gauto, Anna (2017). Sie blicken in dein Herz. *Die Zeit* 16.02.2017, 26.

Heller, Piotr (2017). Alexa, war es Mord? *Frankfurter Allgemeine Sonntagszeitung* 07.05.2017, 59.

Hellmann, Kai-Uwe (2005). Soziologie des Shopping: Zur Einführung. In: Kai-Uwe Hellmann und Dominik Schrage (eds.). *Das Management des Kunden: Studien zur Soziologie des Shopping.* Wiesbaden: Verlag für Sozialwissenschaften, 7–36.

Lamla, Jörn (2013). *Verbraucherdemokratie. Politische Soziologie der Konsumgesellschaft.* Frankfurt a.M.: Suhrkamp.

Latour, Bruno (1991). *Nous n'avons jamais été modernes. Essai d'anthropologie symétrique.* Paris: Éditions La Découverte. Deutsch von Gustav Roßler: *Wir sind nie modern gewesen. Versuch einer symmetrischen Anthropologie.* Frankfurt a.M.: Suhrkamp 2008.

Lobe, Adrian (2017). Kommissar Kühlschrank – Wenn die Technik zum Zeugen wird. *Spektrum der Wissenschaft* 24.01.2017. URL: https://www.spektrum.de/kolumne/kommissar-kuehlschrank-wenn-die-technik-zum-zeugen-wird/1436201 [Letzter Zugriff am 30.08.2019].

Lobe, Adrian (2019). Die Plattformen haben das partizipative Web gekapert. *Telepolis* 08.04.2019. URL: https://www.heise.de/tp/features/Die-Plattformen-haben-das-partizipative-Web-gekapert-4365432.html [Letzter Zugriff am 30.08.2019].

Marx, Gary T. (2016). *Windows into the Soul. Surveillance and Society in an Age of High Technology.* Chicago: Chicago University Press.

Maset, Pierangelo (2010). *Geistessterben. Eine Diagnose.* Stuttgart: Radius.

Miller, Daniel (2010). *Stuff.* Cambridge: Polity Press.
Miller, Daniel (2012). *Consumption and its Consequences.* Cambridge: Polity Press.
Murakami Wood, David und Torin Monahan (2019). Editorial: Platform Surveillance. *Surveillance and Society* 17, 1–2, 1–6.
Nassehi, Armin (2019). *Muster. Theorie der digitalen Gesellschaft*. München: C.H.Beck.
Pasquale, Frank (2015). *The Black Box Society. The Secret Algorithms That Control Money and Information.* Cambridge: Harvard University Press.
Pinker, Steven (2019). Tech Prophecy and the Underappreciated Causal Power of Ideas. In: John Brockman (ed.). *Possible minds. 25 ways of looking at AI.* New York: Penguin, 100–112.
Postman, Neil (1985). *Amusing Ourselves to Death. Public Discourse in the Age of Show Business*. New York: Penguin. Deutsch von Reinhard Kaiser: *Wir amüsieren uns zu Tode. Urteilsbildung im Zeitalter der Unterhaltungsindustrie*. Frankfurt a.M.: Fischer 1985.
Reckwitz, Andreas (2017). *Die Gesellschaft der Singularitäten.* Frankfurt a.M.: Suhrkamp.
Reith, Gerda (2019). *Addictive Consumption. Capitalism, Modernity and Excess*. Milton Park: Routledge.
Rötzer, Florian (2019). Die neue Un-Heimlichkeit. *Fabrikzeitung.ch* 01.04.2019. URL: https://www.fabrikzeitung.ch/die-neue-un-heimlichkeit/#/ [Letzter Zugriff am 30.08.2019].
Sambuli, Nanjira (2017). Africans need to grow technology, but on their own terms. *Daily Nation* 20.07.2017. URL: https://www.nation.co.ke/oped/blogs/dot9/nanjira/3225972-4024894-5g89wl/index.html [Letzter Zugriff am 30.08.2019].
Sarr, Felwine (2019). *Afrotopia*. Berlin: Matthes & Seitz.
Siemons, Mark (2019). Wir Cyborgs. *Frankfurter Allgemeine Sonntagszeitung* 04.08.2019, 33.
Spreen, Dirk, Bernd Flessner, Herbert M. Hurka und Johannes Rüster (2018). *Kritik des Transhumanismus. Über eine Ideologie der Optimierungsgesellschaft.* Bielefeld: transcript.
Taureck, Bernhard (2014). *Überwachungsdemokratie. Die NSA als Religion.* Paderborn: Wilhelm Fink.
Turner, Fred (2008). *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism.* Chicago: Univ. Chicago Press.
Ullrich, Wolfgang (2013). *Alles nur Konsum. Kritik der warenästhetischen Erziehung*. Berlin: Wagenbach.
Veblen, Thorstein (1899). *The Theory of the Leisure Class.* New York: Macmillan. Deutsch von Suzanne Heintz und Peter von Haselberg: *Theorie der feinen Leute. Eine ökonomische Untersuchung der Institutionen.* Frankfurt a.M.: Fischer 2007.
Yang, Xifan (2019). Wir sehen Dich. *Die Zeit* 10.01.2019, 13–15.
Zuboff, Shoshana (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology* 30, 1, 75–89.
Zuboff, Shoshana (2018). *Das Zeitalter des Überwachungskapitalismus.* Frankfurt a.M.: Campus.
Zurawski, Nils (2011). Local practice and global data. Loyalty cards, social practices and consumer surveillance. *Sociological Quarterly* 52, 4, 509–527.

Zurawski, Nils (2011a). ‚Budni, ist doch Ehrensache!' – Kundenkarten als Kontrollinstrument und die Alltäglichkeit des Einkaufens. In: Nils Zurawski (ed.). *Überwachungspraxen – Praktiken der Überwachung. Analysen zum Verhältnis von Alltag, Technik und Kontrolle.* Opladen: Budrich UniPress, 65–86.

Zurawski, Nils (2014). Consuming Surveillance: Mediating Control Practices Through Consumer Culture and Everyday Life. In: André Jansson und Miyase Christensen (eds.). *Media, Surveillance and Identity*. New York u.a.: Peter Lang, 32–48.

Dr. habil. Nils Zurawski
Universität Hamburg
Inst. für kriminologische Sozialforschung
Allende-Platz 1
D-20146 Hamburg
E-Mail: nils.zurawski@uni-hamburg.de
Webseite: http://www.surveillance-studies.org

Zeitschrift für
Semiotik
Band 40 • Heft 1-2 (2018)
Seite 45-62
Stauffenburg Verlag Tübingen

Überwachen, verführen, verkaufen – Manipulation als Schlüsselkonzept für Überwachungstheorien

Lena Füller, Caroline Ganzert und Marcel Lemmes, Eberhard Karls
Universität Tübingen

Summary. Many classical as well as modern theories on surveillance connect mechanisms of surveillance directly with a transformation of our way of living. The goal of this article is to examine this connection between surveillance and influence in the works of Michel Foucault, Gilles Deleuze, Zygmunt Bauman, and David Lyon. By employing the concise term "Manipulation" in the sense defined by Alexander Fischer, we gain new perspectives on the hierarchy between the watcher and the watched in their theories, and can derive implications on why surveillance technology is increasingly adopted and accepted in our everyday life.

Zusammenfassung. In vielen klassischen wie auch modernen Überwachungstheorien lässt sich auf den ersten Blick eine Verbindung zwischen Überwachungsmechanismen und der Veränderung unserer Lebensführung erkennen. Dieser Beitrag untersucht diesen Zusammenhang zwischen Überwachung und Beeinflussung in den Arbeiten von Michel Foucault, Gilles Deleuze, Zygmunt Bauman und David Lyon. Mithilfe des klar umrissenen Manipulationsbegriffs nach Alexander Fischer können hier neue Perspektiven auf die Hierarchie zwischen Überwacher und Überwachtem aufgezeigt werden und es ergeben sich Implikationen für Antworten auf die Frage nach dem zunehmenden Einsatz und der zunehmenden Akzeptanz von Überwachungstechnologien in unserem Alltag.

1. Einleitung

Das Feld Überwachung bietet für die verschiedensten wissenschaftlichen Zugänge ein breites Spektrum an Forschungsgegenständen und Analyseinstrumenten. Eine eindeutige Definition des Begriffs liegt allerdings nicht vor. Wohl aber lassen sich verschiedene relevante Aspekte dieses breiten Themenfeldes bestimmen, welche in verschiedenen Forschungstraditio-

nen untersucht werden. So rücken im Zuge der Überwachungsforschung einerseits Fragen nach der allgemeinen, abstrakten Funktionsweise von Überwachung (Zweck- und Zielgerichtetheit, Routine und Systematik) sowie konkreter technischer Spezifika (zum Beispiel Datensammlung, -auswertung und -speicherung) in den Blick, andererseits eröffnen sich Fragen nach den Folgen von Überwachung und ihrer tatsächlichen Wirkung auf Alltag und Gesellschaft (Einfluss auf Prozesse, Regelung von Zugängen) und die Beschaffenheit von Akteursbeziehungen (Machtinstanzen, Hierarchien, Verhältnis zwischen Überwacher und Überwachtem) (vgl. zum Beispiel den Definitionsversuch von Zurawski (2007: 9–11), der all diese Facetten abbildet). Ein konkretes zeitgenössisches Phänomen, welches sich auf all diese Facetten hin untersuchen lässt, ist die computergestützte Klassifikation von Daten, die heute in vielen Bereichen zur Strukturierung und Ordnung unserer Gesellschaft zum Einsatz kommt. Dabei werden etwa personenbezogene Daten, wie GPS-Daten oder biometrische Daten gesammelt. Die systematische Erfassung, Aufzeichnung und Weiterverarbeitung von Daten ermöglicht ein detailliertes Profiling, woraus eine kontinuierliche Überwachung resultiert (vgl. Bächle 2016: 157). In Form von Fingerabdrücken, Einkaufsdaten oder Passwörtern werden Menschen zu „vermessbaren Identitäten, deren Wert oder deren G e f ä h r d u n g s p o t e n z i a l für die Gesellschaft quantifizierbar scheint“ (Bächle 2016: 157; Hervorhebung von den Autoren vorgenommen). Aus diesem Zitat werden zwei grundlegende Bereiche unseres Alltags ablesbar, in denen die datengestützte Überwachung zum Tragen kommt: der Bereich der Ökonomie und des Konsums einerseits und der Bereich Sicherheit und Kriminalität andererseits. Dieser Aufsatz wird sich mit einem Phänomen befassen, welches eindeutig dem ersten Bereich zuzuordnen ist: der Beeinflussung unseres Konsums und der Ökonomisierung unserer Leben durch Überwachung. Denn in Zeiten von Facebook, Google und Instagram werden die aus Daten gewonnenen Profile großflächig zur Stimulierung unseres Konsumverhaltens eingesetzt; schließlich erlauben sie es, passgenaue Werbeanzeigen zu erstellen – sogenanntes *Target Advertising* – und auf uns zugeschnittene Suchergebnisse und Inhalte zu präsentieren.

In diesem Zusammenhang soll im vorliegenden Beitrag der Manipulationsbegriff nach Fischer im Überwachungskontext untersucht werden, denn Fischer wirft in seinem Werk eine drängende These auf, die vor dem Hintergrund von Target Advertising und nutzerspezifischer Werbung erneut an Brisanz gewinnt: „Früher wurde [die Manipulation] gefürchtet, heute gilt sie fast schon als normal. Doch sollten wir weiter fürchten oder mit den Schultern zucken?“ (Fischer 2017: 21). In ihren Überlegungen zu Überwachung und Gesellschaft verhandeln schon Foucault und Deleuze Formen von Einflussnahme, aber auch die jüngeren Denker Lyon und Bauman setzen sich bewusst mit diesem Phänomen auseinander. Keiner der hier genannten Forscher verwendet dabei jedoch explizit den Begriff der Manipulation. Der Beitrag wird deswegen einerseits analysieren, welche Rolle dem Manipulationsbegriff, basierend auf Fischers Verständnis, in den Ausführung von

Foucault und Deleuze und in den Theorien von Bauman und Lyon zur modernen Überwachung im Konsumbereich zukommen kann, andererseits soll herausgearbeitet werden, inwiefern die spezifische Perspektive des Manipulationsbegriffs zu einem besseren Verständnis der theoretischen Ansätze beitragen kann. Folgende Fragen sollen beantwortet werden: Wodurch definiert sich Manipulation und welche Wirkungsmechanismen liegen ihr zugrunde? Welche Rolle kommt dem Manipulationsbegriff in Michel Foucaults Disziplinargesellschaft und der darauf basierenden Kontrollgesellschaft nach Gilles Deleuze zu? Wie können Baumans und Lyons Ansätze zu Konsum im Überwachungskontext vor dem Hintergrund dieses Manipulationsbegriffs verstanden werden? Und wie kann Manipulation als Schlüsselkonzept innerhalb von Überwachungstheorien verortet werden?

2. Grundlegende Begriffsklärung: Was ist Manipulation?

„Manipulation finden wir in vielen Bereichen – in der Werbung, in der Politik und in Partnerschaften oder sonstigen Beziehungen“ (Fischer 2017: 14). Der Manipulationsbegriff ist jedoch äußerst vielschichtig, wird disziplinübergreifend verwendet und oft nur unzureichend spezifiziert. „Der Begriff Manipulation wird (historisch und bis heute) in einer solch vielfältigen Weise genutzt, dass die Grenzen des Konzepts verschwimmen (bzw. verschiedene Konzepte ineinanderfließen)“ (Fischer 2017: 29). Die Diskussion der Manipulation vor dem Hintergrund der Überwachung unseres Kaufverhaltens erfordert deswegen eine vorangehende Definition und Eingrenzung von Manipulation. Diese sollen eine Kontextualisierung und Überführung des Manipulationsbegriffs in den aktuellen Diskurs der Überwachung durch Target Advertising und nutzerspezifischer Werbung erlauben.

Folgend soll zunächst eine Abgrenzung der Manipulation zu Nötigung und Zwang einerseits und rationaler Überzeugung andererseits vorgenommen werden. Anschließend soll geklärt werden, welche Mechanismen bei Manipulation wirken, um am Ende dieses Kapitels ein Verständnis des Manipulationsbegriffs herauszuarbeiten, das eine Verhandlung zeitgenössischer Überwachungsphänomene erlaubt.

2.1 Formen der Manipulation und begriffliche Abgrenzung

Allgemein werden unter Manipulation verschiedene Formen der Beeinflussung verstanden. Eine dieser Formen besteht laut Fischer darin, uns gewaltsam zu etwas zu bringen, letztlich zu etwas zu zwingen, wobei die Problematik darin besteht, dass wir in unserer Freiheit eingeschränkt werden (Fischer 2017: 13). Für diese Form der Manipulation gilt Benesch und Schmandt zufolge, dass sie zurecht gefürchtet wird, da ihr eine verdeckte, verheimlichte, indirekte Zielsetzung zugrunde liegt, die den Betroffenen hin-

tergeht, um ihn so in die Fänge zu bekommen (vgl. Benesch und Schmandt 1979: 7–13). Die Autoren Benesch und Schmandt gehen soweit, Manipulation als psychische Fesselung zu beschreiben, welche sich auf verheerende Weise nachteilig auswirkt (vgl. Benesch und Schmandt 1979: 7–13). „Im Hinblick auf bestimmte […] Komponenten wie die nachteilige Behandlung des Manipulierten, die Undurchsichtigkeit der Manipulation und die rational unterdeteminierende Art dieser Beeinflussungsform" (Fischer 2017: 28) kommen jedoch Zweifel an der Allgemeingültigkeit dieser Definition auf, die in erster Linie eine gewaltfokussierte, zwanghafte Form der Manipulation beschreibt. Diese Form überschneidet sich inhaltlich stark mit dem Konzept der Nötigung und des Zwangs und lässt sich damit abgrenzen von jenen Mechanismen, die bei der Überwachung durch Target Advertising und nutzerspezifischer Werbung vorkommen, da physische wie psychische Gewalt hier ausgeschlossen werden können und auch eine nachteilige Behandlung sowie eine generelle Undurchsichtigkeit der Beeinflussung nicht zwingend gegeben sind.

Wie Fischer weiter erkennt, gibt es neben diesen offenkundigen Formen, die mit Target Advertising und nutzerspezifischen Werbevorschlägen wenig gemein haben, auf welchen jedoch historisch gesehen in zahlreichen Untersuchungen der Fokus lag, Arten der Manipulation, die häufig unter dem Begriff der Beeinflussung verhandelt werden (vgl. Fischer 2017: 28). Diese subtileren Arten von Einflussnahmen, die vielleicht gerade wegen ihrer Subtilität besonders durchdringend und allgegenwärtig sein mögen, erfuhren hingegen weniger Aufmerksamkeit, obwohl sie viel unmittelbarer in uns wirken können als ein rationales Argument (vgl. Fischer 2017: 26).

> Verschiedene Techniken und, damit verbunden, verschiedene Theorien werden als unterschwellige Manipulation bezeichnet. […] Im psychologischen Sinn meint unterschwellige Beeinflussung die unbewusste Stimulation von handlungsauslösenden Impulsen oder Motiven, also von Bedürfnissen, Wünschen, Trieben, Strebungen (Heller 1984: 20).

Die Beeinflussung und Erzeugung von Bedürfnissen, Wünschen, Trieben und Strebungen spielt eine entscheidende Rolle für unser Konsumverhalten, da wir aus ihnen die Entscheidung für oder gegen ein Produkt ableiten. Worin bei dieser subtilen Art der Manipulation durch Einflussnahme der Unterschied zur rationalen Entscheidung besteht, geht aus einer weiterführenden, spezifischen Untersuchung der Einflussnahme hervor:

> Die Einflussnahme geschieht durch die aktive Veränderung der affektiven Anziehungskraft von bestimmten Zwecken oder die Modifikation eines Handlungskontextes, der so Zwecke in einem affektiven Sinne angenehmer/unangenehmer erscheinen lässt und damit die nahegelegte Wahl attraktiver/unattraktiver macht und ihre Wahrscheinlichkeit erhöht/verringert (Fischer 2017: 31).

Diese Definition verdeutlicht, dass eine aktive Veränderung vorgenommen wird, welche nicht intrinsisch durch den Manipulierten, sondern extrinsisch durch den Manipulator geschieht. Somit entsteht zwar beim Manipulierten zunächst der Eindruck einer freien Wahl, die theoretisch auch möglich ist, jedoch liegt der wahrscheinlicheren Wahl keine rationale Entscheidung, sondern eine affektive Beeinflussung zugrunde. So lässt sich die Manipulation vor dem Hintergrund der Überwachung unseres Kaufverhaltens also nicht nur von Nötigung und Zwang, sondern auch von einer rationalen Entscheidung abgrenzen.

2.2 Mechanismen der Manipulation

Die Mechanismen, die bei Manipulation wirken, können sich in zwei verschiedene Arten einteilen lassen: kurzfristig-situative Beeinflussung und langfristig-dispositionale Beeinflussung (vgl. Fischer 2017: 135). Dabei ist es wichtig zu verstehen, dass beide Konzepte nicht als diametral gedacht werden dürfen, sondern lediglich als Kategorien zur näheren Definition dienen, da es selbstverständlich Phänomene gibt, in denen wiederholte kurzfristig-situative Beeinflussung zu langfristig-dispositionaler Beeinflussung wird und so die Grenzen zwischen beiden verschwimmen (vgl. Fischer 2017: 135). Fischer definiert sechs Mechanismen, welche diesen beiden Kategorien zugrunde liegen. Diese lauten „Knappheit", „Neigungen", „Soziale Bewährtheit", „Reziprozität", „Verpflichtungen" und „Autorität" (vgl. Fischer 2017: 141–143).

Beim Manipulations-Mechanismus K n a p p h e i t geht es darum, dem Rezipienten zu vermitteln, den negativen Effekt, etwas zu verpassen, zu vermeiden und deswegen den positiven Effekt, etwas Seltenes zu erstehen, zu aktivieren (vgl. Fischer 2017: 141). Dies führt beispielsweise dazu, dass Rezipienten solcher Botschaften geneigt sind, ein Produkt zu kaufen oder in eine Dienstleistung einzuwilligen, um sich nichts entgehen zu lassen. Ein typisches Beispiel hierfür wäre ein Produkt aus einer sogenannten ‚limited Edition'.

Der Mechanismus N e i g u n g e n macht sich das Bedürfnis des Menschen zu gefallen zu Nutze, indem konkrete Situationen geschaffen werden, in denen konstruierte Gemeinsamkeiten eine Gelegenheit zur Manipulation bieten, unter anderem, wenn Sympathien oder Antipathien genutzt werden, um ein Zugehörigkeitsgefühl entstehen zu lassen (vgl. Fischer 2017: 142). Dies tritt zum Beispiel auf, wenn beliebte Influencer für ein Produkt werben, das sie selbst vorgeben zu nutzen, und so eine spezifische Zielgruppe dazu bringen, sich ebenfalls für dieses zu entscheiden.

Beide beschriebenen Mechanismen erzielen meist Erfolge, wenn es um kurzfristig-situative Beeinflussung geht, im Gegensatz zum Manipulations-Mechanismus der S o z i a l e n B e w ä h r t h e i t, der oft zu langfristigen Manipulationen führt (vgl. Fischer 2017: 142) „Hier sind wirkmächtige Affekte, die mit der Zugehörigkeit und Selbstbestärkung in dem, wer man ist,

verbunden sind. Dies wird auch relevant, wenn es um die Beeinflussung von Gruppen geht" (Fischer 2017: 142). Ein Beispiel hierfür wäre die Nutzung beziehungsweise der Erwerb eines spezifischen Produktes auf Basis positiver Erfahrungen anderer Personen im eigenen sozialen Umfeld im Umgang mit diesem Produkt.

Ein Mechanismus, der sowohl kurzfristig-situativ wie auch langfristig-dispositional greift, ist die Reziprozität: Dieser Mechanismus beruht darauf, dass Individuen sich anderen gegenüber zu etwas verpflichtet fühlen, wenn sie selbst etwas von ihnen erhalten haben (vgl. Fischer 2017: 142–143). Dieser Mechanismus tritt beispielsweise ein, wenn Firmen Werbegeschenke kostenlos ausgeben, um im Gegenzug potentielle Kunden dazu zu bringen, nun auch etwas bei ihnen zu kaufen.

Bei Mechanismen zur Beeinflussung, die auf Verpflichtungen basieren, geht es auch um kurzfristige, vor allem aber um langfristig angelegte Muster: „Individuen ziehen sich ungern aus vertraglichen Bindungen zurück, sie fühlen sich verpflichtet […] Dinge zu tun, sie wollen vorhandenen Wertvorstellungen und Handlungsmustern folgen […]" (Fischer 2017: 143).

Dieses Konsistenzstreben, welches ebenfalls beim Mechanismus der Autorität zum Tragen kommt, kann sich ein Manipulator zunutze machen (vgl. Fischer 2017: 143). Die Wirkung einer Autorität zu gehorchen ist sowohl kurzfristig als auch langfristig und als Disposition des Individuums wirksam (vgl. Fischer 2017: 143). Ein Werbegestalter, der einen echten Zahnarzt mit Namen und Doktortitel einsetzt, um eine Zahnpasta zu bewerben, weiß um diesen Autoritäts-Mechanismus.

Es wird dadurch ersichtlich, dass Manipulation als Stimulus betrachtet werden kann, mit dem Ziel, in einer bestimmten Situation eine veränderte Handlungsleitung herbeizuführen (vgl. Fischer 2017: 137). Diese Beeinflussung der Handlung erfolgt extrinsisch durch den sogenannten Manipulator und beruht auf verschiedenen Mechanismen, welche sich Bedürfnisse und Affekte des Manipulierten zunutze machen. Im Folgenden soll nun der Manipulationsbegriff nach Fischer im Überwachungskontext untersucht werden. Dazu werden die folgenden drei Analysekategorien herangezogen: Manipulation liegt dann vor, wenn (1) in einer Wahlsituation bei einem Akteur eine aktive Veränderung extrinsisch durch einen anderen Akteur vorgenommen wird. (2) Diese Akteure lassen sich als Manipulierter und Manipulator bestimmen und unterscheiden. (3) Die Wahlsituation erscheint dem Manipulierten als frei, jedoch liegt aufgrund der affektiven Beeinflussung eine Verzerrung vor.

3. Disziplin, Kontrolle, Manipulation?

Im zweiten Teil dieses Aufsatzes soll zunächst eine historische Reflexion über die Relevanz von Einflussnahme im Allgemeinen und Manipulation im Besonderen in klassischen Überwachungstheorien erfolgen. Dafür werden

die Disziplinargesellschaft bei Michel Foucault und die darauf basierende Kontrollgesellschaft nach Gilles Deleuze auf ihren Bezug zu durch Überwachung ermöglichter Einflussnahme hin analysiert und es soll herausgestellt werden, welche Bedeutung der Beeinflussung der überwachten Subjekte in den jeweiligen Modellen zukommt. Wie sich in der folgenden Analyse außerdem zeigen wird, lässt sich die jeweils prädominante Form der Einflussnahme auch als Abgrenzungskriterium zwischen beiden Ansätzen anwenden. Denn obwohl die beiden Konzepte oft als sich ausschließende, klar voneinander abzugrenzende Modelle verhandelt werden (vgl. zum Beispiel Zurawski 2011: 7; Galič u.a. 2017) – Deleuze selbst zufolge können beide Überwachungsregime sogar historisiert auf einer Zeitachse angeordnet werden: die Kontrolle ersetze die Disziplin (vgl. Deleuze 2017: 254–255) –, ist eine Zuordnung spezifischer Phänomene zu einem der beiden Modelle und eine genaue Markierung des Übergangs von der Disziplinar- zur Kontrollgesellschaft mitunter schwierig. Zunächst folgt jeweils ein kurzer Überblick über die beiden Konzepte, auf den sich dann die jeweilige Analyse stützt.

3.1 Michel Foucault: Die Disziplinargesellschaft

Den inhaltlichen Löwenanteil über sein Konzept der Disziplinargesellschaft formulierte Foucault in seinem Werk *Überwachen und Strafen*, das im französischen Original erstmals 1975 veröffentlicht wurde – obgleich, wie sich im Folgenden herausstellen wird, eine Einordnung seiner hier formulierten Überlegungen in den Kontext seiner anderen Arbeiten die einzelnen Elemente dieses Konzeptes noch einmal präzisieren kann. Insbesondere das Kapitel über den von Foucault so benannten ‚Panoptismus' gibt Aufschluss über Wirkungsweise und Zielsetzung eines omnipräsent und omnipotent auftretenden Überwachungsregimes. Basierend auf Benthams architektonischem Modell des Panopticons konstruiert Foucault in seinem Werk die Idee einer Sichtbarkeitsmaschinerie, die durch das Machtinstrument der Disziplinierung eine Ökonomisierung verschiedener Lebensbereiche ermöglicht (vgl. Foucault 2014: 253, 256, 258–259, 265, 267). Das Panopticon „programmiert […] das elementare Funktionieren einer von Disziplinarmechanismen vollständig durchsetzten Gesellschaft" (Foucault 2014: 268), und diese Mechanismen wiederum seien „das einheitliche technische Verfahren […], durch welches die Kraft des Körpers zu den geringsten Kosten als ‚politische Kraft' zurückgeschraubt und als nutzbare Kraft gesteigert wird" (Foucault 2014: 284).

Im Kern setzt die panoptisch organisierte Disziplinargesellschaft nach Foucault drei Dinge voraus: Erstens muss es in ihr eine normierte Vorstellung der individuellen Lebensführung geben, die zweitens durch den panoptischen Betrieb permanent überprüft wird und drittens durch die Disziplinierung, also durch Bestrafung bei Abweichungen, durchgesetzt wird. Gerade der dritte Aspekt soll hier noch einmal betont werden, denn obwohl

Foucault selbst den Schluss zieht, dass irgendwann die Durchsetzung der Norm allein durch den panoptischen Betrieb gelingen mag – nämlich wenn das überwachte Individuum die Machtverhältnisse und die Norm völlig internalisiert (vgl. etwa Foucault 2014: 260) – so darf nicht außer Acht gelassen werden, dass es gar nicht zu dieser Internalisierung kommen kann, wenn Abweichungen von der Norm nie korrigiert werden. Gleichsam ist es aber gerade diese Internalisierung, die das Modell der panoptischen Disziplinargesellschaft aus der Perspektive des Manipulationsbegriffs interessant macht. Denn ganz intuitiv lässt sich hinter dem Begriff der Internalisierung zunächst eine Form der Einflussnahme vermuten: die durch die extrinsische Disziplinarmacht konstituierte Hierarchie und Lebensnorm (re-) formiert das Subjekt. Aber ist der bestimmende Modus dieser Einflussnahme das, was nach Fischer Manipulation genannt werden kann? Um diese Frage zu klären, sollen die im Vorfeld herausgearbeiteten Analysekategorien des Manipulationsbegriffs genutzt werden.

Zunächst gilt es, die relevanten Akteure zu bestimmen, also denjenigen, der Einfluss ausübt und denjenigen, der beeinflusst wird. In Foucaults Modell lassen sich auf den ersten Blick viele unterschiedliche panoptische Institutionen und somit auch diverse Akteursgruppen finden: die von Foucault aufgezählten Beispiele reichen von psychiatrischen Asylen, Gefängnissen und Erziehungsheimen bis hin zu Fabriken (Foucault 2014: 256). Es sind allerdings nicht die jeweiligen Institutionen für sich, sondern ihre Gesamtheit, die die von Foucault beschriebene Disziplinargesellschaft konstituiert; die Machtform der Disziplin ist nicht an die Institutionen gebunden (Foucault 2014: 276–277). Deswegen kann die Betrachtung von Akteurspaaren wie Patient und Pfleger, Gefangener und Wärter, Schüler und Lehrer oder Arbeiter und Aufseher zwar beispielhafte Einblicke in die Funktionsweise der Disziplinargesellschaft geben (wie es Foucault selbst mit seiner Analyse des panoptisch organisierten Gefängnisses vorführt), allerdings sind sie nur bedingt verallgemeinerungsfähig. Und laut Foucault selbst ist das panoptische Prinzip, also der Kern der Disziplinargesellschaft, das Ergebnis einer Verallgemeinerung der in den Institutionen vorzufindenden Disziplinen (vgl. Foucault 2014: 277). Im panoptischen Betrieb geht es nicht um einzelne Individuen, sondern um eine „Sammlung von getrennten Individuen“ (Foucault 2014: 258) – was in einem für eine Gesellschaft verallgemeinerten Modell letztlich die gesamte Bevölkerung impliziert.

Ein Blick auf andere relevante Begriffe und Konzepte aus Foucaults Gesamtwerk schafft hier noch einmal Klarheit. Mit dem Begriff der ‚Gouvernementalität‘ etwa wird deutlich, dass in Foucaults Gesellschaftsverständnis Macht auf Kollektive wirkt und ein zentrales Herrschaftsinstrument darstellt (vgl. Foucault 2004: 521). So ergibt sich der Staat aus den Beziehungen und Verbindungen zwischen Subjekten, die wiederum grundlegend von Macht- und Wissensverhältnissen beeinflusst werden (vgl. Lenke 2014: 262). Die Beziehungen zwischen den Subjekten und ihr Verhältnis zueinander kann durch Normierung beeinflusst werden, wie etwa Foucaults Konzept der ‚Bio-Politik‘ verdeutlicht. Als Bio-Politik lassen sich Machttechni-

ken zusammenfassen, die „die sorgfältige Verwaltung der Körper und die rechnerische Planung des Lebens“ (Foucault zitiert nach Gehring 2014: 231) – also eine dramatische und vollumfängliche Beeinflussung der Bevölkerung – ermöglichen. Für eine panoptisch organisierte Disziplinargesellschaft bedeutet das letztlich, dass man die Machthabenden, den Staat, und die Machtlosen, die Bevölkerung, als relevante, verallgemeinerte Akteure benennen kann. Der Staat übt Einfluss auf die Bevölkerung aus.

Nun gilt es zu klären, ob es sich bei dem Einfluss des Staates auf die Bevölkerung tatsächlich um Manipulation handelt. Zur Erinnerung: um eine Beeinflussungssituation als Manipulation bezeichnen zu können, muss es sich um eine Situation der Wahl handeln, in der sich der Manipulierte in putativer Freiheit tendenziell für die vom Manipulator präferierte Option entscheidet. Da der Staat in der von Foucault beschriebenen Disziplinargesellschaft seinen Einfluss durch die Etablierung von Normen ausübt, muss zunächst geklärt werden, in welchem Maße diese Normen bindend sind. Denn die Sanktionierung von Normen kann, allgemein gesprochen, „von ausdrücklichem Lob bis zu drakonischer Bestrafung, von der stummen Bestätigung durch Nichtreaktion bis zur deutlichen Verurteilung nach Recht und Gesetz“ (Abels 2009: 53) reichen.

Als erstes soll ein genauerer Blick auf die Internalisierung der Lebensnorm in der Disziplinargesellschaft geworfen werden. Allgemein gesprochen ist Internalisierung – besonders während der Sozialisation – ein gängiges Mittel zur Durchsetzung von Normen, trägt sie doch zu deren Normalisierung bei (Abels 2009: 53). Neben harmlosen Verhaltensregeln wie „du sollst beim Essen nicht schmatzen“ erlernen wir in unseren jungen Jahren auch komplexere Gebote über das Zusammenleben in einer Gesellschaft, wie etwa das Gebot von Gewaltfreiheit und Hilfsbereitschaft. Die durch den panoptischen Betrieb und die Disziplinen verinnerlichte Lebensnorm sieht Foucault wohl in jedem Fall kritischer als die gerade angeführten Beispiele. Denn mit dieser Lebensnorm geht ein klares hierarchisches Machtverhältnis einher; dadurch, dass das beobachtete Individuum dieses Machtverhältnis internalisiert, wird es „zum Prinzip seiner eigenen Unterwerfung“ (Foucault 2014: 260). Besonders deutlich wird dies, wenn man einen genaueren Blick auf Foucaults Verständnis des Individualkörpers wirft:

> [D]ie Machtverhältnisse legen ihre Hand auf ihn [den Körper]; sie umkleiden ihn, sie markieren ihn, dressieren ihn, martern ihn, zwingen ihn zu Arbeiten, verpflichten ihn zu Zeremonien, verlangen von ihm Zeichen. […] [Z]u einer ausnutzbaren Kraft wird der Körper nur, wenn er sowohl produktiver wie unterworfener Körper ist (Foucault 2014: 37).

In diesem Sinne ist der Körper in einer modernen Gesellschaft nicht das Ziel von Disziplinierungsmaßnahmen, sondern dient nur als Vermittler. So dient etwa der körperliche Freiheitsentzug in Form einer Haftstrafe nicht etwa der ‚peinlichen‘ Strafe des Leibes, sondern der Beraubung von Frei-

heit in Geist und Seele (Foucault 2014: 18–19). Der panoptische Zugriff auf den Körper macht „eine Unterscheidung von Selbst- und Fremdkontrolle, von eigenem und fremdem Begehren, von Herrscher und Beherrschtem, von Macht und Ohnmacht nicht länger möglich“ (Siebenpfeiffer 2014: 219). Von einer Freiheit der Wahl kann man hier nicht wirklich sprechen.

Viel mehr wird mit Blick auf Fischers Abgrenzung des Begriffs ‚Manipulation‘ zu artverwandten Konzepten deutlich, dass die in der Disziplinargesellschaft vorzufindende Form der Einflussnahme eher dem Zwang gleicht. Dies wird auch noch einmal durch die in den Disziplinarinstitutionen verankerten Überprüfungsmechanismen deutlich, die Foucault herausarbeitet. Prüfungen in Form von „Tests, Gespräche[n], Befragungen oder Konsultationen“ (Foucault 2014: 288) etwa im juristischen wie auch im schulischen Bereich oder innerhalb eines Betriebes zeichnen sich in der Regel nur bedingt durch eine Freiwilligkeit des jeweils Untersuchten aus. Darüber hinaus verwendet Foucault in seinem Kapitel zum Panoptismus auch selbst mehrfach den Begriff des „Zwangs“ (vgl. zum Beispiel Foucault 2014: 256, 269, 285). Abschließend lässt sich also festhalten, dass der prädominante Modus der Einflussnahme in Foucaults panoptischer Disziplinargesellschaft nicht die Manipulation, sondern der Zwang ist. Gleichsam muss man allerdings notieren, dass das dominante extrinsische Zwangsmittel, nämlich die Internalisierung der Machtverhältnisse und der Lebensnorm, auf eine ähnlich subtile Weise wirkt und zum Einsatz kommt wie es bei einer Manipulation zu erwarten wäre.

3.2 Gilles Deleuze: Die Kontrollgesellschaft

In vielerlei Hinsicht kann das von Gilles Deleuze in seinem *Postskriptum über die Kontrollgesellschaft* ausbuchstabierte Modell als eine auf Foucaults Überlegungen aufbauende Aktualisierung der Disziplinargesellschaft verstanden werden. So nimmt Deleuze etwa diverse begriffliche Veränderungen an Foucaults Modell vor. Anstelle der Disziplin als „Gußform“ tritt die Kontrolle als modulierendes „Sieb“ mit veränderlicher Körnung; die „Fabrik“ weicht dem „Unternehmen“; das „Examen“ der permanenten Kontrolle (Deleuze 2017: 256–257). Was an Deleuzes Überlegungen einen besonders frappierenden Unterschied zu Foucaults Modell markiert, ist die Modulierbarkeit der Einflussnahme auf das Individuum, das bei Deleuze in Form des „Dividuums“, als zweigeteilte Entität aus körperlich-fleischlicher Präsenz und digitalisierbarer Datenstruktur wiedergeboren wird (Deleuze 2017: 257–258).

Zu Recht benennt Deleuze den Wirkmechanismus der Disziplinargesellschaft als langfristig und diskontinuierlich (Deleuze 2017: 260). Die bei Foucault beschriebene Internalisierung einer Lebensnorm, die, wie im vorigen Kapitel herausgearbeitet wurde, einer bindenden, zwanghaften Einflussnahme gleichkommt, zielt auf eine endgültige, prinzipiell abschließbare Veränderung der Individuen ab. Wenn Foucault davon ausgeht, dass der pan-

optische Betrieb durch die Internalisierung der Lebensnorm irgendwann ohne einen tatsächlichen Überwacher und die Ausübung von Strafe auskommen kann, so muss es zwangsläufig einen Zeitpunkt geben können, zu dem die Lebensnorm von allen Individuen völlig internalisiert wurde, sodass diese nicht mehr diszipliniert werden müssen. Wenn nun an die Stelle der langfristigen, diskontinuierlichen Disziplin die kurzfristige aber kontinuierliche Kontrolle tritt (vgl. Deleuze 2017: 260), welche Implikationen hat das für den Modus der Einflussnahme? Folgt Deleuzes Kontrollgesellschaft ebenfalls dem Muster erzwungener Beeinflussung oder kann in diesem Fall von Manipulation die Rede sein?

Genau wie bei der vorigen Analyse sollen zunächst die relevanten Akteure bestimmt werden. Wo bei Foucault das verallgemeinerbare Prinzip des panoptischen Betriebs letztlich in der Beziehung von Staat und Bevölkerung verortet werden konnte, so scheint bei Deleuze eine Verschiebung des Blicks von der staatlich-politischen zur wirtschaftlich-kapitalistischen Sphäre angemessen. Deleuze sieht nämlich die Einschließungsmilieus in der Krise, die sich in Foucaults Modell unter staatlichen Vorgaben entwickelten (vgl. Deleuze 2017: 255). Disziplinarinstitutionen wie die Familie, die Schule oder das Gefängnis, aber auch die oberste Disziplinarmacht in Form des Staates, erfahren eine radikale Ökonomisierung und lassen sich nach Deleuze jeweils als Abwandlungen eines bestimmten Archetypen verstehen, nämlich dem des Unternehmens, dass die Fabrik als Formierungsinstitution der Körper ersetzt (vgl. Deleuze 2017: 60). Zwar hat Foucault die Ökonomisierung aller Leben, „die Bindung unnützer oder unruhiger Bevölkerungen“ um die „Nützlichkeit von Individuen [zu] vergrößern“ (Foucault 2014: 269–270), schon für seine Disziplinargesellschaft als wichtiges Ziel der Disziplinierung ausgemacht, so treibt Deleuze diese Überlegungen in seiner Kontrollgesellschaft allerdings auf die Spitze. Das prägende wirtschaftliche Prinzip, der Kapitalismus, ist nämlich „nicht mehr für die Produktion da, sondern für das Produkt, das heißt für Verkauf oder Markt“ (Deleuze 2017: 259–260). Diese Mutation des Kapitalismus ersetzt den Staat als beeinflussenden Akteur. Wo der staatlich geregelte Zugriff auf die Leben und Körper in Foucaults Disziplinargesellschaft nötig war, um die Individuen von Geburt an durch die Einbindung in Institutionen für eine ökonomische Produktion nutzbar zu machen, wird diese Rolle in Deleuzes Kontrollgesellschaft vom Markt selbst übernommen: „Marketing heißt jetzt das Instrument der sozialen Kontrolle“ (Deleuze 2017: 260).

Mit einem Verweis auf die Literatur könnte hier die Argumentationsführung bereits beendet werden und der Modus der Einflussnahme in der Kontrollgesellschaft als Manipulation benannt werden. Im Eingangszitat zum Kapitel zum Manipulationsbegriff erklärt Fischer bereits, dass Manipulation unter anderem im Bereich der Werbung anzutreffen ist. Mit dieser Einschätzung ist er nicht alleine. So befindet etwa auch der Philosoph Allen Wood, der in einem sehr ähnlichen Tenor wie Fischer eine Neu-Definition des Manipulationsbegriffs vornimmt, mit Blick auf Werbung und Marketing, dass diese „manipulation in its purest […] possible form“ (Wood 2014: 39)

seien. Allerdings soll der Zusammenhang zwischen Marketing und dem Manipulationsbegriff hier noch einmal um der Vollständigkeit willen detaillierter herausgearbeitet werden. Dem weiter oben vorgelegten Analyseschema für Manipulationssituationen gemäß soll nach der Bestimmung der relevanten Akteure, dem Markt als Beeinflussender und der Bevölkerung als Beeinflusste, das Vorhandensein einer als frei wahrgenommenen Wahlsituation überprüft werden. In der Kaufen-Verkaufen-Struktur des kapitalistisch durchstrukturierten Marktes treffen unterschiedliche Produkte von unterschiedlichen Unternehmen aufeinander und buhlen um die Aufmerksamkeit – oder präziser formuliert: das Geld – der Käufer. Wenn in der Vorstellung eines ‚homo oeconomicus' davon ausgegangen wird, dass der Kunde rationale Kaufentscheidungen trifft (vgl. Nicosia 1966), so muss zwangsläufig sowohl von der Möglichkeit zur Wahl als auch einer Freiheit der Wahl ausgegangen werden, denn eine rationale Entscheidung bedeutet schließlich, dass das Individuum auf Basis eines individuellen Abwägens verschiedener Argumente eine Entscheidung fällt. Die Irrationalität von Kaufentscheidungen kommt allerdings immer wieder in Analysen zutage (siehe zum Beispiel Heller (1984: 46–48) für ein Resümee einer Analyse aus dem Jahr 1940 über den Kauf von Autos). Es sind nicht nur rationale Argumente, die die Auswahl von Produkten bestimmen; so mischen auch Emotionen und Affekte, festgesetzte Stereotypen und Denkmuster sowie situative Faktoren bei der Entscheidung für oder wider einen Kauf mit. Das bietet eine breite Angriffsfläche für Manipulation. Die von Fischer ausgemachten Wirkmechanismen von Manipulation lassen sich alle in den Bereichen der Werbung und des Konsums festmachen, wie in den Beispielen in Kapitel 2.2 bereits geschehen. Wenn Marketing also das Instrument der sozialen Kontrolle in Deleuzes Kontrollgesellschaft ist, so ist die Manipulation folgerichtig ihr prädominanter Modus der Einflussnahme.

4. Überwachter Konsum – manipulierter Konsum

Eine Veränderung im Überwachungsapparat, wie sie Deleuze im Übergang von der Disziplinar- zur Kontrollgesellschaft beschreibt, attestieren auch Zygmunt Bauman und David Lyon. In ihren Schriften zum Thema Überwachung spielt der Begriff ‚Konsum' eine zentrale Rolle. Zwar stehe er für viele für ein „Reich des Vergnügens, des Flanierens und der Freiheit" (Bauman und Lyon 2013: 150), tatsächlich werden vor und nach jedem Kauf, ob online oder offline, eine Vielzahl an personenbezogenen Daten erfasst, gespeichert und ausgewertet, was das Phänomen aus einer Überwachungsperspektive interessant macht. Die zentrale Bedeutung des Marktes als dominanter Akteur im alltäglichen Überwachungsgeschehen wurde bereits anhand der Überlegungen von Deleuze im vorangegangenen Kapitel deutlich. In seiner Kontrollgesellschaft stellt Marketing das Instrument der Wahl zur sozialen Kontrolle dar, welches nach der Logik der Manipulation operiert, wie die vorangegangene Analyse gezeigt hat. Folglich liegt es auf der Hand, auch die

Überlegungen von Bauman und Lyon zum Thema Konsum – eine Thematik, die logischerweise den Bereich Marketing mitumfasst, gleichsam aber darüber hinaus geht – auf sein Verhältnis zu Manipulation zu untersuchen. Wo Deleuzes Überlegungen zu Marketing sich eher auf den Bereich des Verkaufs und somit auf die Kaufentscheidung des Konsumenten konzentrieren, gehen Bauman und Lyon, mitunter auch aufgrund ihrer größeren zeitlichen Nähe zu aktuellen technischen Entwicklungen, einen Schritt weiter. Wenn David Lyon etwa von einem „data double" (z.B. Lyon 2007: 88) spricht, so nimmt er etliche Datenströme in den Blick, die mal enger, mal weniger eng mit dem tatsächlichen Kauf von Produkten in Verbindung stehen. Basierend auf diesen Datenströmen werden kundenspezifische Profile angelegt, die miteinander verknüpft werden (vgl. Bauman und Lyon 2013: 151). Bauman und Lyon zufolge beruht diese Klassifizierung von Kunden auf einer minutiösen Verwaltung von Daten, die im Hintergrund abläuft, initiiert von großen Konzernen wie Amazon, Facebook, Google & Co. (vgl. Bauman und Lyon 2013: 150). Das Resultat sind – um hier einen Rückbezug zum Thema Marketing zu nennen – unter anderem personenbezogene Werbeanzeigen, etwa Vorschläge für den nächsten Einkauf, die Amazon-Kunden direkt nach dem Kauf präsentiert werden, speziell für den jeweiligen Kunden zusammengestellt. Viele Konsumenten empfinden die für sie passgenauen Vorschläge als angenehm, Kunden nehmen diese Art von Verführung also oft als vorteilhaft wahr (vgl. Bauman und Lyon 2013: 150). Die Wahrscheinlichkeit, dass die vorgeschlagenen Produkte den Konsumenten gefallen, ist verhältnismäßig hoch, da die Vorschläge auf umfangreichen Einkaufsdaten und ausgeklügelter Statistik basieren. Die Unternehmen kennen die Wünsche, Bedürfnisse und Interessen ihrer Kunden bis ins kleinste Detail.

Diese Form von kontinuierlicher (Daten-)Überwachung ist allgegenwärtig. Bauman und Lyon zufolge ist „die Praxis des Überwachens" (Bauman und Lyon 2013: 7) in viele Bereiche unseres Lebens eingedrungen. „Überwachung ist ein Grundzug der modernen Welt" (Bauman und Lyon 2013: 7), was wiederum, sofern Überwachung und Manipulation als zunehmend miteinander vernetzt betrachtet werden, Fischers These, Manipulation sei zu etwas A k z e p t i e r t e m geworden, bestätigen würde. Besonders paradox ist dabei, dass Kunden auf eine für sie angenehme Weise zum Konsum motiviert werden, parallel aber „systematischen und umfassenden Überwachungsmaßnahmen unterworfen werden" (Bauman und Lyon 2013: 29). Für den Konsumbereich verwenden Bauman und Lyon den Begriff der „flüchtigen Überwachung" (Bauman und Lyon 2013: 12) oder „liquid surveillance" (Lyon 2010). Während früher Daten nur für einen bestimmten Zweck erhoben wurden, sind diese nun immer leichter auch auf andere Zwecke übertragbar, die Grenzen werden unsichtbar. Die Praktiken der Überwachung breiten sich folglich zunehmend aus, Überwachung wird „flexibler und mobiler" (Bauman und Lyon 2013: 14) und sie greift in neue Bereiche über – wie auch in den Konsumbereich.

Basierend auf den Datenmengen und den Nutzer-Klassifikationen werden um Konsumenten herum sogenannte Filter Bubbles errichtet. So erhalten beispielsweise zwei Nutzer, die denselben Begriff in die Google-Suchmaske eingeben, unterschiedliche Suchergebnisse, denn ihnen wird eine individualisierte Vorauswahl an Ergebnissen präsentiert. Die Auswahl trifft Google für sie basierend auf Wohnort, älteren Sucheingaben und anderen nutzerspezifischen Kriterien. Bauman und Lyon sehen diese technische Möglichkeit mit Blick auf den Konsum vor allem insofern problematisch, als „man mit der Überwachung der Verbraucher insbesondere im Internet nicht nur ‚gute Kunden' aufspüren und mit Vergünstigungen und weiteren Angeboten binden, sondern auch alle jene abwehren will, die nicht das gewünschte Verhalten an den Tag legen" (Bauman und Lyon 2013: 152). Die Filterblasen führen folglich auch dazu, dass „faule" Kunden oder Konsumenten „mit Mängeln" durch sogenannte „Bannoptiken" (Bauman und Lyon 2013: 156) aufgespürt und künftig von Marketingaktionen ausgeschlossen werden. Bauman formuliert diesen Zusammenhang aus Konsumentensortierung und Überwachung wie folgt:

> Today's Big Brother is not about keeping people in and making them stick to the line, but about kicking people out and making sure that when they are kicked out that they will duly go and won't come back (Bauman 2006: 25).

Im Bereich der Überwachung von Konsumenten werden „pan- und synoptische Vorrichtungen erst dann eingesetzt, wenn das Überwachungsgebiet mit Hilfe des Bannoptikums ‚gesäubert' worden ist" (Bauman und Lyon 2013: 156). Das sogenannte Demarketing grenzt unrentable Kunden aus.

Einen entscheidenden Wandel, der das Konsumverhalten beeinflusst, sieht Bauman in der „Verlagerung von der Bedürfnisbefriedigung (die Warenproduktion folgt der bestehenden Nachfrage) auf die Bedürfnis*erzeugung* (die Nachfrage folgt der Warenproduktion)" (Bauman und Lyon 2013: 154). So entstehen auf Seiten der Konsumenten Bedürfnisse, die zuvor gar nicht existierten. Das Resultat dieser Wandlung: Unternehmen nutzten ab sofort jegliche Mittel, um in Konsumenten neue Wünsche und Bedürfnisse zu wecken. Der Konsument von heute wiederum ist davon überzeugt, dass das Glück im Konsum und in neuwertigen Waren läge. So lassen sich Werbeangebote gezielt an die Personen richten, die bereits konsumorientiertes und kaufwilliges Verhalten zeigen. Kleine Anreize reichen schon aus, um diese Art von Zielgruppe zum Kauf zu bewegen. Dank heutiger Technologien und Algorithmen lässt sich exakt berechnen, „wann und wofür die Kaufbereitschaft am größten und bereit ist" (Bauman und Lyon 2013: 154).

Mit Blick auf den Manipulationsbegriff lassen sich aus diesem kurzen Aufriss bereits zentrale Charakteristika der von Bauman und Lyon beschriebenen Konsumentenüberwachung festhalten. So lassen sich als beeinflussende Akteure klar benannte Tech- und Internet-Konzerne wie Amazon, Facebook und Google ausmachen, die Entscheidungen ihrer jeweiligen Nutzer beeinflussen und gar manipulieren. Damit sind die Akteure bei Bau-

man und Lyon von allen hier verhandelten Überwachungskonzepten am genauesten bestimmt. Gemäß Fischer liegt Manipulation dann vor, wenn der Beeinflusste, in diesem Fall der Nutzer oder Konsument, eine scheinbar freie Wahl hat, aber dann basierend auf einer affektiven Beeinflussung keine rationale Entscheidung treffen kann. Dass diese Bedingungen im Bereich der „liquid surveillance" erfüllt sind, markiert etwa Bauman in seinen Überlegungen zu Konformität zu flexiblen, sich immer wieder wandelnden Vorgaben in modernen Gesellschaften:

> Obedience to standards […] tends to be achieved nowadays through enticement and seduction rather than by coercion – and it appears in the disguise of the exercise of free will, rather than revealing itself as an external force (Bauman 2015: 86).[1]

Um diesen Gedanken noch einmal im Bereich des Konsums zu verorten, so erscheint dem Nutzer beziehungsweise Konsumenten etwa ein getätigter Kauf als eine freie Entscheidung, eine freie Wahl aus eigenem Antrieb und unbeeinflusst getroffen. Doch eine „external force", die sich dem Konsumenten nicht als solche zu erkennen gibt, hat ihn in seiner Entscheidung beeinflusst: das Marketing. Wo dieses früher dem Zweck gedient hat, den bereits vage interessierten Kunden auf das eigene Produkt aufmerksam zu machen und ihn dann zum Kauf zu animieren, so erfüllt es heute den Zweck, eine Begehrlichkeit bei möglichst jedem potentiellen Kunden zu erwecken – auch solchen, die zunächst überhaupt kein Interesse am eigenen Produkt hatten – und im Zuge dessen unrentable Konsumenten zu finden und herauszufiltern. Wie oben beschrieben, bezeichnen Bauman und Lyon diese Entwicklung einerseits als einen entscheidenden Wandel von der Bedürfnisbefriedigung zur Bedürfniserzeugung, andererseits als eine synoptische Abwandlung des Panoptismus als „Bannoptikum". Die Kunden bemerken gar nicht, dass sie das Bedürfnis nach dem Produkt vor den ständigen Werbeanzeigen gar nicht verspürt haben. Diese aktive Veränderung wurde extrinsisch von einem Manipulator, wie Amazon, Facebook oder Google, erzeugt. Somit kann der Konsument keine rationale Entscheidung treffen. Diese Form von subtiler Beeinflussung kann folglich, gemäß Fischer, als Manipulation bezeichnet werden.

5. Fazit: Überwachung und Manipulation

Es war mitunter Ziel dieser Arbeit, den Begriff Manipulation als relevanten und fruchtbaren Ausgangspunkt für die Beschreibung von modernen Überwachungsphänomenen aufzuzeigen. Wie in den hier vorgenommenen Analysen deutlich gemacht wurde, ermöglicht es der Manipulationsbegriff verschiedene Facetten und Folgen von Überwachungsverhältnissen zu verdeutlichen und zeitgenössische Überwachung aus einer neuen Blickrichtung zu verstehen. Vor allem erlaubt er für Analysen eine Schärfung der Perspektive, indem er die Zielgerichtetheit der Überwachung mit

dem hierarchischen Verhältnis zwischen Überwacher und Überwachtem verknüpft.

Bei der Betrachtung der historischen Ansätze von Foucault und Deleuze etwa wurde deutlich gemacht, dass eine Zielgerichtetheit der jeweils beschriebenen Überwachungspraxen vorliegt, nämlich die Beeinflussung der allgemeinen Lebensführung bei Foucault einerseits und die Kontrolle unseres Konsumverhaltens bei Deleuze andererseits. Auch hat sich der Begriff hier als nützliches Kriterium erwiesen, um eine Unterscheidung zwischen beiden Modellen zu vereinfachen. Denn wie sich gezeigt hat, lässt sich der Wandel der prädominanten Überwachungsmaxime im Übergang von der Disziplinargesellschaft zur Kontrollgesellschaft auch anhand der jeweils prädominanten Form der Einflussnahme bestimmen, die an den jeweiligen Überwachungsapparat gebunden ist: die Foucault'sche Disziplin gleicht dem Zwang, die Deleuze'sche Kontrolle lässt sich dagegen durch und durch als Manipulation im Überwachungskontext begreifen, die in der Etablierung des Marketings und der Werbung als Mittel zur sozialen Kontrolle kulminiert. Wo bei Foucault die Überwachung als Mittel zur Durchsetzung der Disziplin durch Zwang fungiert, ist sie bei Deleuze eine notwendige Bedingung, um eine effektive soziale (und vor allem auch wirtschaftliche) Kontrolle durch Manipulation zu ermöglichen.

Die Untersuchung der gegenwärtigen Theorien von Bauman und Lyon anhand des Manipulationsbegriffs nach Fischer ergab, dass es sich gemäß der im Vorfeld herausgearbeiteten Analysekategorien bei den von ihnen beschriebenen Überwachungsphänomenen im Konsumbereich um Wahlsituationen mit Manipulationspotenzial handelt. Die Akteure in diesem Manipulationsprozess sind bei Bauman und Lyon eindeutig bestimmbar: Tech- und Internet-Konzerne wie Amazon, Facebook und Google beeinflussen unsere Kaufentscheidungen und erzeugen durch Marketingmaßnahmen wie Target Advertising Bedürfnisse bei Konsumenten, die zuvor so nicht existierten. Gleichsam sind es diese Konzerne, die sowohl über die Hard- und Software verfügen, um eine umfassende Überwachung unserer Daten zu betreiben. Das Ziel der Überwachung unserer digitalen Fußspuren ist aber nicht mehr bloß die Manipulation unserer Kaufentscheidungen. Da sich der Konsumismus zunehmend als die gängige Lebensweise etabliert, impliziert eine Manipulation unseres Konsumverhaltens auch eine Manipulation eines Bereichs unserer Lebensführung – nicht zuletzt sind in den letzten Jahren vermehrt etwa Diskussionen um die Beeinflussung unserer politischen Landschaft durch die neuen Möglichkeiten des Target Advertising entbrannt.

Wie sich anhand der hier vorgeführten Analysen zeigt, nimmt die Bedeutung von Beeinflussung für Überwachungstheorien zu. Insbesondere die Manipulation als eine allzu leicht von den in den jeweiligen Modellen Überwachten Subjekten übersehene Form gewinnt mit Blick auf die zunehmende Computerisierung von Überwachungstechniken einerseits und deren zunehmendem ökonomischen Einsatz andererseits an Relevanz. Es lässt sich also als abschließendes Plädoyer festhalten, dass eine bewusste Refle-

xion von potentiellen Manipulationsfällen bei der Betrachtung von neuen Überwachungsphänomenen und der Entwicklung neuer Überwachungstheorien gewinnbringend ist. Drei Aspekte haben sich hier bei den Untersuchungen besonders deutlich gezeigt: der Manipualtionsbegriff ermöglicht (a) eine Schärfung der Akteursverhältnisse und ihrer Beziehungen zueinander für konkrete Überwachungsphänomene, lässt (b) mögliche Antworten auf Fragen nach der Akzeptanz von Überwachungstechniken sichtbar werden und erlaubt (c), die Folgen von Überwachung für die individuelle Lebensführung prägnanter und eindrücklicher darzustellen. Letzteres wird auch dem Ziel vieler Arbeiten innerhalb der Surveillance Studies gerecht, sowohl ein Problembewusstsein zu schaffen als auch einen konkreten gesellschaftlichen Wandel anzustoßen. Wie die vorliegende Arbeit aufzeigen konnte, ermöglicht das Verhandeln von Manipulation als Schlüsselkonzept moderner Überwachungstheorien einen relevanten Zugang für den Diskurs vorangegangener, gegenwärtiger und auch zukünftiger Überwachungsphänomene.

Anmerkungen

1 Der Vergleichspol, den Bauman in diesem Zitat anspricht, ist die panoptische Disziplinargesellschaft nach Michel Foucault. Bauman bestätigt insofern also auch den in Kapitel 3.1 herausgearbeiteten Befund, dass der prädominante Modus der Einflussnahme bei Foucault der des Zwangs ist.

Literatur

Abels, Heinz (2009). Werte und Normen. In: Heinz Abels (ed.). *Einführung in die Soziologie.* Band 2: *Die Individuen in ihrer Gesellschaft.* Wiesbaden: VS Verlag für Sozialwissenschaften, 15–56.

Bächle, Thomas Christian (2016). *Digitales Wissen, Daten und Überwachung zur Einführung.* Hamburg: Junius.

Bauman, Zygmunt (2006). *Liquid fear.* Cambridge: Polity Press.

Bauman, Zygmunt (2015). *Liquid modernity.* Cambridge, Malden: Polity Press; Blackwell.

Bauman, Zygmunt und David Lyon (2013). *Liquid Surveillance. A Conversation.* Cambridge: Polity Press. Deutsch von Frank Jakubzik. *Daten, Drohnen, Disziplin: Ein Gespräch über flüchtige Überwachung.* Berlin: Suhrkamp 2013.

Benesch, Hellmuth und Walther Schmandt (1979). *Manipulation und wie man ihr entkommt.* Stuttgart: Deutsche Verlagsanstalt.

Deleuze, Gilles (1990). Post-scriptum sur les sociétés de contrôle. *L'autre journal* 1. Deutsch von Gustav Roßler: Postskriptum über die Kontrollgesellschaften. In: Gilles Deleuze. *Unterhandlungen. 1972–1990.* 6. Auflage. Frankfurt a.M.: Suhrkamp 2017, 254–262.

Fischer, Alexander (2017). *Manipulation: Zur Theorie und Ethik einer Form der Beeinflussung.* Berlin: Suhrkamp.

Foucault, Michel (1975). *Surveiller et punir. Naissance de la prison.* Paris: Gallimard. Deutsch von Walter Seitter: *Überwachen und Strafen: Die Geburt des Gefängnisses.* 19. Auflage. Frankfurt a.M.: Suhrkamp 2014.

Foucault, Michel (2004). *Sécurité, territoire, population. Cours au Collège de France, 1977–1978.* Paris: Seuil. Deutsch von Claude Brede-Konersmann: *Sicherheit, Territorium, Bevölkerung: Die Geschichte der Gouvernementalität I.* Frankfurt a.M.: Suhrkamp 2006.

Galič, Maša, Tjerk Timan und Bert-Jaap Koops (2017). Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation. *Philosophy & Technology* 30, 1, 9–37.

Gehring, Petra (2014). Bio-Politik/Bio-Macht. In: Clemens Kammler, Rolf Parr, Ulrich Johannes Schneider und Elke Reinhardt-Becker (eds.). *Foucault-Handbuch. Leben – Werk – Wirkung.* Stuttgart: J.B. Metzler, 230–232.

Heller, Eva (1984). *Wie Werbung wirkt: Theorien und Tatsachen.* Frankfurt a.M.: Fischer.

Lenke, Thomas (2014). Gouvernementalität. In: Clemens Kammler, Rolf Parr, Ulrich Johannes Schneider und Elke Reinhardt-Becker (eds.). *Foucault-Handbuch. Leben – Werk – Wirkung.* Stuttgart: J.B. Metzler, 260–263.

Lyon, David (2007). *Surveillance studies: An overview.* Malden: Polity Press.

Lyon, David (2010). Liquid surveillance: The contribution of Zygmunt Bauman to Surveillance Studies. *International Political Sociology* 4, 4, 325–338.

Nicosia, Francesco M. (1966). *Consumer decision process: Marketing and advertising implications.* Englewood Cliffs: Prentice-Hall.

Siebenpfeiffer, Hania (2014). Körper. In: Clemens Kammler, Rolf Parr, Ulrich Johannes Schneider und Elke Reinhardt-Becker (eds.). *Foucault-Handbuch. Leben – Werk – Wirkung.* Stuttgart: J.B. Metzler, 266–272.

Wood, Allen W. (2014). Coercion, manipulation, exploitation. In: Christian Coons und Michael Weber (eds.). *Manipulation. Theory and practice.* Oxford: Oxford University Press, 17–50.

Zurawski, Nils (2007). Einleitung: Surveillance Studies: Perspektiven eines Forschungsfeldes. In: Nils Zurawski (ed.). *Surveillance Studies. Perspektiven eines Forschungsfeldes.* Opladen, Farmington Hills: Barbara Budrich, 7–24.

Zurawski, Nils (2011). Die praktischen Dimensionen von Überwachung, Kontrolle und Überprüfung. In: Nils Zurawski (ed.). *Überwachungspraxen – Praktiken der Überwachung. Analysen zum Verhältnis von Alltag, Technik und Kontrolle.* Opladen, Farmington Hills: Budrich University Press, 7–19.

Lena Füller, Caroline Ganzert und Marcel Lemmes
Eberhard Karls Universität Tübingen
Institut für Medienwissenschaft
Wilhelmsstr. 50
D-72074 Tübingen
E-Mail: klaus.sachs-hombach@uni-tuebingen.de

Zeitschrift für
Semiotik
Band 40 • Heft 1-2 (2018)
Seite 63-82
Stauffenburg Verlag Tübingen

„Alexa, kann ich dir vertrauen?“ Sprachassistenten als Wegbereiter der gläsernen Privatsphäre

Anne Diessner, Lisamarie Haas und Carina Konopka, Eberhard Karls
Universität Tübingen

Summary. For some years now, language assistants have been making their way into everyday lives of many people. The intelligent personal assistants integrated in smartphones and special speakers seem to make the life of those who use them easier. At the same time, however, they open up possibilities for interfering with the privacy of users. Companies collect large amounts of sometimes sensitive personal data for improved functionality and marketing. This calls into question the traditional understanding of privacy. This article discusses the technical functioning of language assistants, elaborates on the transformation of privacy, and problematizes the new helpers concerning their relationship to the users' privacy, using Amazon's Alexa as an example.

Zusammenfassung. Seit einigen Jahren halten Sprachassistenten Einzug in den Alltag zahlreicher Menschen. Die intelligenten persönlichen Assistenten, die in Smartphones und speziellen Lautsprechern integriert sind, scheinen vorrangig das Leben ihrer Nutzer zu erleichtern. Gleichzeitig eröffnen sie jedoch Möglichkeiten des Eingriffs in die Privatsphäre der Nutzer. Unternehmen sammeln große Mengen teils sensibler persönlicher Daten für eine verbesserte Funktionalität und Marketing. Damit wird das traditionelle Verständnis von Privatheit infrage gestellt. Der vorliegende Artikel erörtert die technische Funktionsweise von Sprachassistenten, arbeitet die Transformation der Privatsphäre heraus und problematisiert die neuen Helfer am Beispiel von Amazons Alexa im Hinblick auf ihr Verhältnis zur Privatsphäre der Nutzer.

1. Einführung

Amazons Alexa, Apples Siri, Microsofts Cortana und Google Assistant – das Gespräch mit einem Sprachassistenten gehört für Millionen von Konsumenten zur täglichen Routine. Die sprachgesteuerten Systeme sind in Smartphones und bestimmten Lautsprechern integriert und sollen als soge-

nannte intelligente persönliche Assistenten eine Erleichterung in vielen Lebensbereichen darstellen (vgl. Lenz-Kesekamp und Weber 2018: 18; López u.a. 2018: 241). Der vorliegende Artikel möchte Sprachassistenten im Rahmen der ‚Surveillance Studies' untersuchen (vgl. z.B. Lyon 2007). Dabei soll ihre Auswirkung auf die Privatsphäre beleuchtet und Amazons Sprachassistent Alexa beispielhaft in den Fokus gestellt werden. Es soll aufgezeigt werden, inwiefern Sprachassistenten ein weiterer Schritt in Richtung einer gläsernen Privatsphäre sind und weshalb diese einen nachhaltigen Schutz benötigt.

Der erste Teil bietet zunächst eine Einführung in die grundlegenden Funktionsweisen digitaler Sprachassistenten. Amazons Alexa wird hierbei als Beispiel dienen. Auf Grundlage des theoretischen Hintergrunds werden Sprachassistenten metaphorisch als Dienstboten des 21. Jahrhunderts bezeichnet. Die Metapher wird im Weiteren ausgeführt, um das heuristische Potenzial des Vergleichs für die weitere Argumentation der Arbeit nutzen zu können. Bereits in früheren Epochen zeigte sich der Wunsch der Menschen nach einem bequemen Leben, indem unliebsame Aufgaben anderen übertragen wurden. Mit der Nutzung heutiger Sprachassistenten verhält es sich ähnlich. Dennoch unterscheiden sich diese digitalen Dienstboten in einigen Aspekten fundamental von ihren analogen Vorfahren. Ziel der Dienstbotenmetapher ist es also, das Problembewusstsein für die neuen, digitalen Dimensionen von Dienstboten zu schärfen, da diese gravierende Auswirkungen auf die Privatsphäre der Nutzer haben können. Der zweite Teil widmet sich sodann der Problematisierung von Risiken der neuen Technologien für die Privatsphäre. Zunächst werden die theoretischen Grundlagen und der Wert der Privatsphäre beleuchtet, um anschließend den Einfluss von Amazons Alexa auf die Privatsphäre der Nutzer stellvertretend für Sprachassistenten zu diskutieren: Besteht die Gefahr, dass Alexa einen Beitrag zum vollständigen Verlust jeder Privatheit leistet und zur Transformation in eine Überwachungsgesellschaft beiträgt? Der dritte Teil stellt die Ergebnisse der Arbeit resümierend nebeneinander und bietet einen Ausblick auf das zukünftige Verhältnis von Sprachassistenten zur Privatsphäre.

2. Digitale Sprachassistenten als Dienstboten des 21. Jahrhunderts

Zu Beginn werden die Grundlagen eines theoretischen Verständnisses digitaler Sprachassistenten gelegt, auf welchen die weiteren Ausführungen aufbauen. Hierzu bietet dieser Abschnitt zunächst einen allgemeinen Überblick über die Funktionsweise von Sprachassistenten, um anschließend Amazons Alexa als konkretes Beispiel einzuführen. Außerdem parallelisiert dieser Abschnitt Sprachassistenten mit Dienstboten. Der Vergleich soll zu einem tieferen Verständnis der Privatsphärenproblematik führen, die den Schwerpunkt dieses Aufsatzes bildet. Bereits vorab sei angemerkt, dass Sprachassistenten als Teil einer weitreichenden technisch-digitalen Ent-

wicklung zu verstehen sind und die Machtverhältnisse zwischen den Großkonzernen und ihren Kunden eine andere Dimension einnehmen, als zwischen dem Adel und den analogen Dienstboten. Dennoch bringt der Vergleich einen Mehrwert hinsichtlich der Fragestellung dieser Arbeit.

2.1 Theoretischer Hintergrund digitaler Sprachassistenten

Im Jahr 2011 wurde der erste Sprachassistent unter dem Namen *Siri* im Rahmen der Vorstellung des iPhone 4S lanciert. Handelte es sich in der Anfangszeit noch um einen amüsanten Zeitvertreib, kann heute aufgrund der enormen technischen Fortschritte tatsächlich von einem intelligenten Assistenten im Alltag die Rede sein (vgl. Lenz-Kesekamp und Weber 2018: 19; Hoy 2018: 81). Derzeit gehören neben Apples Siri außerdem Google Assistant, Microsofts Cortana und Amazons Alexa zu den bekannten Produkten. Sprachassistenten sind definiert als „eine Software, die die menschliche Sprache interpretieren und über synthetisierte Stimmen interagieren kann" (Lenz-Kesekamp und Weber 2018: 18; vgl. auch Hoy 2018: 81). Diese Software ist in Smartphones und speziellen Lautsprechern (sogenannte ‚Smart Speaker') integriert.

Sprachassistenten liegt die Technologie des ‚Natural Language Processing' (NLP) zugrunde. NLP befasst sich mit der Verarbeitung der natürlichen Sprache, dem „Verstehen sowie der Semantik von Wörtern und Sätzen, der Klassifizierung von Texten, der korrekten Aussprache und Betonung sowie der Syntaxanalyse und der Beantwortung von Fragen" (Lenz-Kesekamp und Weber 2018: 19). Die Sprache ist der einzige Mediator zwischen dem Menschen und der Maschine. Es fehlen Nutzerschnittstellen wie Touchpads und Computermäuse. Deswegen ist auch von ‚Voice-First'-Geräten die Rede, die den intelligenten Assistenten über Hardware verfügbar und ansprechbar machen. Solche Geräte setzen die sogenannte ‚Zero-User-Interface'-Strategie um. Die grundlegende Idee hierbei ist, dass eine Interaktion, Kommunikation bzw. Transmission nicht offensichtlich durch das Gerät vermittelt wird. Das Gerät tritt vielmehr in den Hintergrund, um eine möglichst natürlich wirkende Benutzerschnittstelle zu gewährleisten. Der Dienst soll sich also bestmöglich in den Kontext der Nutzer einfügen (vgl. Bedford-Strohm 2017: 486–487; siehe auch López u.a. 2018: 241). Lenz-Kesekamp und Weber (2018: 19) nennen deshalb als Ziel digitaler Sprachassistenten, „eine möglichst weitreichende Kommunikation auf Augenhöhe zwischen Mensch und Computer per Sprache zu schaffen". Den Untersuchungen von López u.a. (2018) zufolge variiert das Gefühl von Natürlichkeit bei der Nutzung verschiedener Sprachassistenten. Im Test schnitt der Google Assistant am besten hinsichtlich des Natürlichkeitsgefühls bei der Interaktion mit Nutzern ab (vgl. ausführlich López u.a. 2018: 241–242).

Zur Konkretisierung der Funktionsweise von Sprachassistenten wird im Folgenden ein genauerer Blick auf Amazons Alexa geworfen. Der US-ame-

rikanische Online-Versandhändler Amazon ist ein Vorreiter im Gebiet der Sprachassistenten. Mit dem Namen Alexa wird seit 2014 das ‚Gehirn' der Gerätelinie Echo bezeichnet. Es handelt sich dabei um intelligente Smart Speaker mit integrierter Sprachsteuerung, die schätzungsweise 5,9 % der deutschen Internetnutzer verwenden. In den USA lag der Durchschnittswert 2018 bei etwa 15,4 % (vgl. Lenz-Kesekamp und Weber 2018: 19). Mittlerweile gibt es mehrere Produktvarianten des Smart Speakers, die sich im Grunde lediglich in der Lautsprechergröße unterscheiden: Amazon Echo, Echo Dot, Echo Plus, Echo Spot, Echo Show und andere Alexa-Geräte. Im Falle von Echo Spot und Echo Show weisen die Geräte zusätzlich ein Display auf.[1]

Die Funktionsweise der Smart Speaker beruht auf der soeben beschriebenen Technologie des NLP. Alle Echo-Geräte sind mit einer intelligenten Spracherkennungssoftware über ein Microphone-Array ausgestattet, das permanent aktiv eingeschaltet sein muss. Ein integriertes technisches Modul ermöglicht die Verbindung zum Internet und somit auch die Übermittlung der Sprachdaten an die Amazon Cloud. Das festgelegte Aktivierungswort lautet ‚Alexa'. Wird dieses sogenannte ‚wake word' vernommen, wird der Sprachbefehl oder die Frage des Nutzers aus den Umgebungsgeräuschen herausgefiltert und aufgenommen (z.B. ‚Alexa, schalte das Licht ein'). Die Audiodatei wird an die Amazon Cloud geschickt und in einen Text umgewandelt. Dieser Text wird entsprechend interpretiert und je nach Anfrage mit einem bestimmten ‚Skill' verknüpft. Der Lautsprecher gibt die Sprachausgabe des Assistenten aus und ermöglicht damit den Dialog mit den Nutzern (vgl. Bedford-Strohm 2017: 487; Lenz-Kesekamp und Weber 2018: 19; Hoy 2018: 82). Aufgrund der fortschreitenden Entwicklungen im Bereich der natürlichen Spracherkennung ‚versteht' der Sprachassistent auch diverse Formulierungen ein- und desselben Sprachbefehls, um zum gewünschten Ergebnis zu gelangen (vgl. Hoy 2018: 82–83). Es entsteht somit eine hybride Kommunikationsgemeinschaft zwischen Mensch und Maschine, die sich zunehmend in Richtung einer symmetrischen Verständigung entwickelt (vgl. Roser 2018: 250–251). Lenz-Kesekamp und Weber (2018: 21) nehmen eine Einteilung der Alexa Skills in folgende Kategorien vor:

- ‚Built In Skills': Auf dem Gerät bereits vorinstallierte Skills (z.B. die Ausgabe von Zeit);
- ‚Customs Skills': Externe Skills, die via Aktivierungswort den Dialog mit Usern ermöglichen;
- ‚Smart Home Skills': Skills zum Bedienen entsprechender automatisierter Anwendungen im Haushalt;
- ‚Flash Briefing Skills': Skills, die dem Nutzer schnelle vordefinierte Informationen bieten.

Diese Einteilung passt zu der Beobachtung, dass sich die Sprachassistenten verschiedener Entwickler einige Basisfunktionen teilen, sich jedoch in

weiteren Funktionalitäten (oder eben Skills) unterscheiden (vgl. López u.a. 2018: 241). Hoy (2018: 81, 93) nennt folgende Basisfunktionen, die via Sprachbefehl von allen digitalen persönlichen Assistenten ausgeführt werden können:

- Das Versenden und Vorlesen von Textnachrichten und E-Mails, das Tätigen von Anrufen;
- Die Beantwortung einfacher Informationsfragen (z.B. ‚Wie spät ist es?', ‚Wie wird das Wetter heute?');
- Das Einstellen von Timern und Weckern, Kalendereinträge tätigen;
- Erinnerungen setzen, Listen anlegen, einfache mathematische Berechnungen ausführen;
- Die Medienwiedergabe von verbundenen Diensten wie iTunes, Netflix, Spotify steuern;
- Die Bedienung von ‚Internet-of-Things'-Geräten wie Thermostate, Lichter, Alarmanlagen;
- Witze und Geschichten erzählen.

Weitere Funktionen können je nach Anbieter hinzugefügt werden. Die besagten Skills sind offen für Drittentwickler. Viele Medienhäuser, Unternehmen oder private Entwickler bieten sie an. Im Falle von Amazon werden die Skills nach einem Zertifizierungsprozess im Skill-Store veröffentlicht und für die Nutzer von Amazons Alexa verfügbar gemacht. Das Prinzip des Skill-Stores ähnelt dabei vom Prinzip dem App-Store für Smartphone-Anwendungen (Bedford-Strohm 2017: 487; Lenz-Kesekamp und Weber 2018: 20–21; vgl. auch Hoy 2018: 83). Wirtschaftlich betrachtet entwickeln sich Sprachassistenten damit zu einem neuen, vielversprechenden Touchpoint für die Kundenkommunikation von Unternehmen (dazu ausführlich Lenz-Kesekamp und Weber 2018: 18–19, 21). Amazons Alexa ist derzeit mit den meisten Drittentwickler-Erweiterungen auf dem Markt präsent (vgl. Bedford-Strohm 2017: 487; Hoy 2018: 84).

Alexa soll, wie alle Sprachassistenten, vorrangig der Erleichterung des Alltags der Nutzer dienen. Sprachassistenten gehören also wie die meisten Digitalisierungsstrategien zum neuzeitlichen Effizienzdenken und zum Dogma einer immer zeit- und kosteneffizienteren Bedürfnisbefriedigung (vgl. Bedford-Strohm 2017: 489–490, 492; zu zukünftigen Nutzungsweisen vgl. Hoy 2018: 85–86).

2.2 Die metaphorische Rückkehr der Dienstboten

Alexa als ein Helfer im Alltag legt einen Vergleich mit traditionellen Dienstboten nahe (vgl. zur Idee auch Zurawski 2014; Bartmann 2016; Krajewski 2010 zum Zusammenhang zwischen Medien und Dienern). Ein solcher Vergleich bietet das heuristische Potenzial, das Verhältnis von Sprachassistenten zu Privatsphäre und Überwachung aus einer anderen Perspektive

zu ergründen. Um das Verständnis und die Problematisierung des Themas zu veranschaulichen, sollen im Folgenden einige Parallelen von Sprachassistenten und Dienstboten aufgezeigt werden.

Als Blütezeit des analogen Dienstbotenwesens gilt in Westeuropa das 19. und beginnende 20. Jahrhundert. Dienstboten waren im Haushalt wohnende angestellte Dienstkräfte, die verschiedene Arbeiten in der Haus- und Landwirtschaft übernahmen. Es handelte sich um eine äußerst inhomogene Berufsgruppe mit einer steilen innerberuflichen Hierarchie. Dienstboten waren rechtlich eingebunden in den Haushalt ihrer Arbeitgeber und hatten ihren Anordnungen in stiller Unterwürfigkeit Folge zu leisten. Genügsamkeit, Anpassungsfähigkeit und die Bereitschaft zur Unterordnung waren daher gern gesehene Fähigkeiten von Dienstboten (vgl. Budde 1999: 149–175; Maurer 1995: 162). Die Eingebundenheit in den Haushalt und die idealtypischen Charaktereigenschaften der Dienstboten spiegeln sich in heutigen Sprachassistenten wider. Durch die Umsetzung der oben beschriebenen ‚Zero-User-Interface'-Strategie werden Sprachassistenten möglichst natürlich und unauffällig wirkend in den Kontext der Nutzer integriert. Die Geräte sind so programmiert, dass sie willenlos die Befehle der Nutzer ausführen und rund um die Uhr verfügbar sind. Ein Blick auf die Geschichte des Dienstbotenwesens zeigt, dass auch bei ihnen lange Arbeitszeiten bis zu 16 Stunden täglich nicht unüblich waren. Die Willkür der Dienstherrschaft entschied über den Arbeitsbeginn und das -ende. Bedienstete sollten lediglich die ihnen aufgetragenen Aufgaben möglichst unbemerkt erledigen (vgl. Budde 1999: 160–161; Maurer 1995: 177).

Eine weitere Parallele von Sprachassistenten und analogen Dienstboten besteht in der heutigen Ansprache. Die Ansprache digitaler Sprachassistenten erfolgt stets mit weiblichen Vornamen, im Falle von Amazon handelt es sich um den Frauennamen Alexa (vgl. Roser 2018: 250). Ab Ende des 19. Jahrhunderts kann eine zunehmende Feminisierung des Dienstbotenwesens ausgemacht werden, die sich heute fortzusetzen scheint (vgl. Budde 1999: 153–156). Bedford-Strohm (2018: 492) führt für die Nutzung weiblicher Figuren als Profilierung des Produktcharakters von Sprachassistenten ebenso historische Gründe an. Laut der klassischen Rollenverteilung wurden Frauen oftmals als Helferinnen angesehen. Darüber hinaus sollten jedoch auch technisch-pragmatische Gründe berücksichtigt werden: Frauenstimmen weisen oftmals eine bessere akustische Verständlichkeit auf und werden als freundlicher wahrgenommen (vgl. Bedford-Strohm 2018: 492). Das Anstellen von Dienstboten zeugte bereits früher von Reichtum und einem höheren Sozialprestige und hatte mithin eine Art Repräsentationscharakter in der Gesellschaft (vgl. Maurer 1995: 169, 174–175). Heutzutage kann in einigen Sprachassistenten z.B. in Form teurerer Smart Speaker durchaus weiterhin ein soziales Abgrenzungsmerkmal ausgemacht werden. Dennoch handelt es sich bei heutigen Dienstboten eher um eine Art Massenware, zumal in nahezu jedem Smartphone ein Sprachassistent integriert ist und Smart Speaker in einigen Ausführungen bereits relativ kostengünstig zu erhalten sind (vgl. Hoy 2018: 81).

Ein letzter Aspekt deutet ein möglicherweise problematisches Verhältnis von Dienstboten zur Privatsphäre an: Die früheren Dienstboten lebten im Haushalt ihrer Herrschaft. Aufgrund des engen Zusammenlebens lernten sie ihre Arbeitgeber genau kennen, denn sie bekamen von morgens bis abends die Geschehnisse und Gespräche im Haushalt mit. So waren Herrschaften auf die Loyalität ihrer Dienstboten angewiesen. Es sind Fälle des sozial gemischten Umgangs oder gar Freundschaften zwischen Dienstboten und Herrschaften überliefert. Doch nicht selten entwickelte sich eine Atmosphäre des Misstrauens und des Unverständnisses. Dies zeigt sich auch daran, dass das neugierige Dienstmädchen, das beispielsweise durch das Schlüsselloch äugt oder an der Tür lauscht, ein beliebtes zeitgenössisches Motiv in der Malerei darstellte (vgl. Budde 1999: 170–171; Maurer 1995: 168–169, 185). Schon in früheren Zeiten bemerkte man neben all den Vorzügen durchaus auch die Schattenseite von Dienstboten hinsichtlich der Privatsphäre. Bei Amazons Alexa und weiteren Sprachassistenten nehmen diese Bedenken allerdings ganz neue Dimensionen an, wie im nächsten Kapitel erläutert wird. Dabei gilt es nämlich trotz aller Parallelen und ähnlichen Mustern zu früheren Zeiten vor allem eins im Hinterkopf zu behalten: Amazons Alexa kann zwar stellvertretend als digitaler Nachkomme der Dienstboten im 21. Jahrhundert bezeichnet werden, doch Alexa ist kein Mensch, wie es die früheren Dienstboten waren. Alexa ist eine Maschine, die sich weder durch ein Gewissen noch durch ein Gefühl für Loyalität auszeichnet. Hinter den Anwendungen stehen in erster Linie wirtschaftliche Interessen großer Konzerne wie Amazon.

An dieser Stelle lässt sich festhalten, dass Sprachassistenten wie Amazons Alexa durch ihre vielfältigen Funktionen durchaus in der Lage sind, den Alltag ihrer Nutzer bequemer zu gestalten. Sprachassistenten spiegeln den stetigen technischen Fortschritt in der natürlichen Sprachverarbeitung wider. Es hat sich gezeigt, dass die Dienstbotenmetapher das Verhältnis der heutigen Nutzer von Sprachassistenten zu ihren Geräten passend beschreiben kann. Die digitale Dimension hat jedoch tiefgreifende Auswirkungen auf die Privatsphäre. Den vielen Erleichterungen im Alltag, die Sprachassistenten ihren Nutzern auf der einen Seite bieten, steht auf der anderen Seite ein Eindringen Dritter in die Privatsphäre gegenüber. Die Dienstbotenmetapher verdeutlicht diese Ambivalenz auf eine prägnante Weise – früher wie heute ist Komfort an die Preisgabe der Privatsphäre gebunden. Das folgende Kapitel widmet sich genauer den Veränderungen im Hinblick auf die Privatsphäre, die durch die Nutzung von Sprachassistenten entstehen.

3. Transformationen der Privatsphäre

In Zeiten der Digitalisierung lässt sich im Spannungsfeld von Sicherheit, Freiheit, Persönlichkeitsrecht, technischen Möglichkeiten und wirtschaftlichen Interessen eine kontroverse Debatte über die Privatsphäre beobach-

ten. Ziel dieses Kapitels ist es, das Problemfeld zu umreißen und die Nutzung von Sprachassistenten darin einzuordnen. Essentiell erscheint darüber hinaus die Frage, welchen Wert Privatheit hat und warum sie überhaupt als schützenswert angesehen wird.

3.1 Privatsphäre und Big Data

Die Debatte um die Privatsphäre ist seit Jahren präsent und wurde dabei sehr kontrovers geführt. Dabei finden sich zahlreiche Subdiskurse, weshalb zunächst eine Eingrenzung vorgenommen werden muss. In der Diskussion geht es häufig um das Verschwimmen der Grenze zwischen Privatsphäre und Öffentlichkeit durch die sogenannten sozialen Netzwerke. Dabei zeigt sich eine paradoxe Haltung: Einerseits äußern Nutzer Wertschätzung für Privatsphäre, geben jedoch andererseits freiwillig private Informationen preis (vgl. Steinbicker 2019: 88). Dieses Missverhältnis sei nicht in der Verantwortung von Nutzern, sondern in den Verhältnissen zu sehen, stellt Steinbicker fest: „Sie werden vor die Wahl gestellt zwischen der unbedingten Wahrung ihrer Privatsphäre und der – mit Preisgabe privater Informationen, also Offenheit verbundenen – Entfaltung ihrer Subjektivität“ (Steinbicker 2019: 88–89).

Einen Schritt weiter geht es nun in der Entwicklung zum ‚Internet of Things‘, das verschiedene Geräte und Dienste mit dem Internet verknüpft. Die Preisgabe privater Informationen dient dabei nicht mehr der Entfaltung von Subjektivität, sondern Komfort und Konsum. Denn für digitale Dienstboten wie Alexa sind Informationen über den Nutzer die Grundlage ihrer Funktionsweise. Steinbicker betont, „je personalisierter die Geräte und Systeme in ihren Hilfestellungen für die Lebensführung werden sollen, je mehr Informationen von und über uns benötigen sie“ (Steinbicker 2019: 84–85). Dabei sei die Spracheingabe nicht nur wichtig, um uns zu verstehen, sondern ebenso zur stetigen Verbesserung der Interpretation.

Darüber hinaus sind die individuellen Nutzerdaten für Konzerne wie Google, Facebook und Amazon wirtschaftlich höchst bedeutsam. Die Unternehmen sammeln diese im Hintergrund, um ein immer differenzierteres Profil anlegen zu können, das in der Folge personalisierte Werbung ermöglicht. Umschrieben wird dieses Sammeln und Verknüpfen von Nutzerdaten häufig als ‚Big Data‘. Obgleich der Internetnutzer in der Regel weiß, dass Daten von ihm gesammelt werden, kann er das Ausmaß meist nicht absehen oder kontrollieren, wie Baumann ausführt: „Unsere digitalen Existenzen weiten sich im virtuellen Raum ungeheuerlich aus, denn bei jeder digital mediatisierten Aktivität werden personenbezogene Daten gesammelt und gespeichert, oft in fremden Staaten“ (Baumann 2015: 7). In dieser Entwicklung hin zu einer immer umfassenderen Beobachtung der Internetnutzung sieht Baumann daher die eigentliche Bedrohung der Privatheit. Denn diese Beobachtung könne Individuen nun auch in Zusammenhängen entblößen, in denen Privatsphäre bislang nicht zur Disposition

gestanden habe: Bezog sich die Debatte über Privatsphäreverletzungen bislang auf individuelles Verhalten, z.B. in Online-Netzwerken oder TV-Shows wie *Big Brother*, müssten mittlerweile technologische und ökonomische Interessen berücksichtigt werden, da gesammelte Metadaten gänzlich neue Rückschlüsse auf den Nutzer zuließen (vgl. Baumann 2015: 17). Auch Stempfhuber und Wagner sehen in der unübersichtlichen Rekombination von Daten, dem ‚Profiling', die größte Herausforderung:

> Dabei stellen die User diese Daten schlichtweg durch ihren Gebrauch des Internets zur Verfügung, die dann ohne konkrete Fragestellung aufgezeichnet und weiter verwertet werden – sei es für Zwecke staatlicher Kontrolle, sei es für Marketingaspekte (Stempfhuber und Wagner 2019: 7).

Genau in diesem Spannungsfeld der Interessen verortet Baumann (2015: 7) die Gefahr für die Privatsphäre: Dem Internet folgten Markt und Staat gemeinsam mit ihren Gewinn- und Herrschaftsinteressen. Die Privatsphäre sei dabei nur hinderlich und werde daher unterlaufen, obgleich sie bislang eine wesentliche Rolle für die Machtbalance zwischen Individuum, Staat und Wirtschaft gespielt habe.

In der Folge stehen sich zwei konträre und wenig zielführende Perspektiven gegenüber, wie Stalder (2019) beschreibt. Auf der einen Seite finden sich die sogenannten ‚Post-Privacy'-Befürworter. Diese sehen als Folge des Verschwindens der Privatsphäre neue Toleranz und Offenheit. Radikale Transparenz schafft demnach die illusionäre Art der Selbstdarstellung ab, garantiert Meinungsfreiheit, deckt Ungerechtigkeiten auf und führt zu einem besseren Miteinander. Stalder zufolge verkenne ‚Post-Privacy' allerdings neue Formen der Diskriminierung. Auf der anderen Seite stehen Skeptiker, die das Ende des freien Denkens postulieren. Doch auch diese düstere Prognose „ist steril, denn in der Verkennung der neuen Möglichkeiten der Autonomie, verkommt sie zur reaktionären Nostalgie, die sich nach den klaren Verhältnissen von Autorität und Unterwerfung sehnt" (Stalder 2019: 108). Im Bemühen um eine objektivere Betrachtungsweise der Thematik scheint es sinnvoll, sich auf die Kernthemen zu besinnen und zunächst deutlich zu machen, welchen Wert Privatheit überhaupt beanspruchen kann.

3.2 Privatsphäre als schützenswertes Gut

Bevor ein Blick auf die Debatte um Privatsphäre in Zeiten der Digitalisierung möglich ist, sollte Privatheit definiert werden und ihre Einordnung als schützenswertes Gut begründet werden.

Eine historische Annäherung zeigt, dass die private und die öffentliche Sphäre schon seit vielen Jahrhunderten untrennbar miteinander verbunden sind. Der Begriff „Privatheit" stammt aus dem Lateinischen. Abgeleitet vom Verb „privare", was ‚berauben' bedeutet, bezeichnete „privatus"

den Bürger, der sich nicht politisch betätigte. Er war der öffentlichen Beobachtung entzogen bzw. beraubt (vgl. Schaar 2007: 15–16). Privatsphäre in der heutigen Bedeutung und ihr Gegenstück, die moderne Öffentlichkeit, haben sich vor allem in der bürgerlichen Gesellschaft herausgebildet. Das Bürgertum hegte den Wunsch, die individuellen Verhältnisse und Vorlieben den Einblicken Dritter zu entziehen, um so ein öffentliches Handeln überhaupt erst möglich zu machen (vgl. Schaar 2007: 16). Ohne Privatheit kann es also keine freie Öffentlichkeit geben, zumal die Privatsphäre als Raum des individuellen Rückzugs als eine Voraussetzung der freien Meinungsbildung gilt (vgl. Schaar 2007: 15–16). Im Laufe der Geschichte zeigt sich: „Je ‚öffentlicher' die Öffentlichkeit wurde, je größer also der Radius der veröffentlichten Informationen wurde, desto dringender wurde der Schutz der Privatheit" (Schaar 2007: 17).

Doch Privatheit ist nicht allein als Gegenstück zu Öffentlichkeit bedeutsam. Verletzungen der Privatsphäre betreffen in erster Linie das Individuum, das erscheint auf den ersten Blick logisch. Allerdings ist es für eine wissenschaftliche Auseinandersetzung mit dem Thema notwendig, rationale Gründe für die individuelle Bedeutsamkeit von Privatsphäre zu erkennen. Baumann (2015) untermauert seine Forderung nach Privatheit als Menschenrecht daher mit drei grundlegenden Interessen: Würde, Freiheit bzw. Autonomie und Gleichheit. Beobachtung im weitesten Sinne kann je nach Kontext eine Verletzung der Würde bedeuten, die nicht nur von der subjektiven Bewertung des Beobachteten abhängt, sondern genauso auch durch Außenstehende erkennbar sein kann. Ein viel diskutiertes Beispiel ist hier die TV-Sendung *Big Brother*: Zwar entscheiden sich die Kandidaten bewusst für die konstante Kameraüberwachung, als Zuschauer empfindet man jedoch etwa Aufnahmen unter der Dusche als entwürdigend für die gefilmte Person. Beobachtung stellt weiterhin eine Einschränkung der menschlichen Freiheit und Autonomie dar, da bei Entscheidungen unter Beobachtung Fremdbestimmung immer eine Rolle spielt. Schließlich schützt Privatsphäre vor Diskriminierung, da sie gesellschaftliche Ungleichheiten verdeckt, die nicht für das Gemeinwohl notwendig sind (vgl. Baumann 2015: 14–15).

Beate Rössler setzt sich in ihrer Monographie *Der Wert des Privaten* intensiv mit der Frage auseinander, welche Bedeutung Privatheit für das Individuum hat. Um definitorisch nicht von Begriffen wie „Öffentlichkeit" abhängig zu sein, schlägt sie einen anderen Ansatz zum Verständnis von Privatheit vor: „[A]ls privat gilt etwas dann, wenn man selbst den Zugang zu diesem ‚etwas' kontrollieren kann. Umgekehrt bedeutet der Schutz von Privatheit dann einen Schutz vor unerwünschtem Zutritt anderer" (Rössler 2001: 23). Legt man diese Definition zugrunde, zeigt sich deutlich, dass zwischen Privatsphäre und ‚Big Data' ein unübersehbarer Zusammenhang besteht: Der Nutzer hat keine Kontrolle darüber, wer welche Daten sammelt und damit Zugang dazu hat – ‚Big Data' stellt somit per se eine Verletzung der Privatsphäre dar. Damit ist jedoch weiterhin nicht geklärt, warum Privatsphäre schützenswert sein sollte. Rössler begründet dies in erster

Linie mit der Autonomie des Menschen. Privatheit in drei Differenzierungen ist dabei Teil des Rechts auf Selbstbestimmung: die Privatheit der Daten (informationell), private Entscheidungen und Handlungen (dezisional) und die Privatheit der Wohnung (lokal) (vgl. Rössler 2001: 25). Dass kein Fremder ohne Einladung die eigene Wohnung betreten darf oder dass Entscheidungen persönlicher Natur nicht mit jedem geteilt werden, leuchtet schnell ein. Der Wert informationeller Privatheit, um die es vorrangig bei der Diskussion um ‚Big Data' geht, ist dagegen weniger offensichtlich. Rössler meint mit dem Begriff die Kontrolle über die Informationen der eigenen Person gegenüber anderen. Im Grunde bedeutet dies, dass eine Person einschätzen kann, wie andere über sie denken bzw. was sie über sie wissen:

> [D]er Schutz informationeller Privatheit ist deshalb so wichtig für Personen, weil es für ihr Selbstverständnis als autonome Personen konstitutiv ist, (in ihren bekannten Grenzen) *Kontrolle über ihre Selbstdarstellung* zu haben, also Kontrolle darüber, wie sie sich wem gegenüber in welchen Kontexten präsentieren, inszenieren, geben wollen, als welche sie sich in welchen Kontexten verstehen und wie sie verstanden werden wollen (Rössler 2001: 209; Hervorhebung im Original).

Wird jemand heimlich abgehört oder beobachtet, herrscht sowohl eine kognitive als auch eine voluntative Asymmetrie zwischen Beobachtern und Beobachteten, was bedeutet, dass die Personen nichts von der Beobachtung wissen und diese auch nicht wollen. Diese Asymmetrie ist ebenfalls bei ‚Big Data' gegeben. Zwar wissen die meisten Nutzer über die Datensammlung Bescheid, können das Ausmaß und die Weiterverbreitung jedoch nicht erfassen. In der Regel wollen Nutzer das Vorgehen nicht explizit, sie nehmen es lediglich aufgrund der gebotenen Gratifikation hin (vgl. Rössler 2001: 204).

Informationelle Privatheit ist dabei nicht nur ein intrinsisches Bedürfnis, sondern bildet die Voraussetzung für das Ausüben von Autonomie (vgl. Rössler 2001: 203). Ganz grundsätzlich stellen die neuen Informationstechnologien aus zwei Gründen ein Problem dar: Einerseits, weil sie gegen den Willen von Personen ‚entprivatisieren' und andererseits, weil sie zu einer Bereitschaft der Reduktion des Privaten führen können. In der Konsequenz verliert die Privatsphäre an Bedeutung:

> Dies trifft dann jedoch nicht nur die Idee eines gelungenen – selbstbestimmten – Lebens, sondern auch die Idee der liberalen Demokratie: die nämlich auf autonome und sich ihrer Autonomie bewusste und diese schätzende Subjekte angewiesen ist (Rössler 2001: 218).

Neben der Autonomie des Individuums sieht Matzner (2017) die Dimension sozialer Beziehungen als relevant für Privatsphäre an. Er möchte daher mit dem Begriff der relativen Privatheit Rösslers Ansatz weiterführen und auf die Beziehungsebene ausweiten (vgl. Matzner 2017: 79). Relevant sind

hier besonders die sozialen Rollen, die Personen in alltäglichen Kontexten einnehmen. Privatheit wird in diesem Zusammenhang verstanden als Moderator für die Ausgestaltung dieser Rollen:

> Privatheitsnormen moderieren, welche Erscheinungsweisen eine Rolle beim Kuratieren dieser Erscheinung und deren Wahrnehmung durch andere spielen können. Sie moderieren die Art und Weise, wie wir werden können, wer wir sind, indem sie verschiedene Erscheinungen in verschiedenen Situationen auseinanderhalten (Matzner 2017: 88).

Der Wert von Privatheit besteht folglich nicht nur in einer individuellen autonomen Entscheidung. Vielmehr geht es darum „die Freiheit zu schützen, bestimmte Personen sein oder werden zu können" (Matzner 2017: 90). Im sozialen Gefüge wird diese Entscheidung nicht unabhängig getroffen, sondern im Zusammenspiel mit anderen als Aushandlungsprozess. Insgesamt „schützt Privatheit grundsätzlich die Freiheit zur Veränderung, die Freiheit eine andere Person werden zu können und damit auch die Pluralität menschlichen Lebens" (Matzner 2017: 92).

3.3 Sprachassistenten als Bedrohung für die Privatsphäre

Wie genau haben Sprachassistenten nun einen Einfluss auf die Privatsphäre ihrer Nutzer? Alexa hat viele Funktionen, die eine positive Auswirkung auf den Alltag haben. Die Kommunikation mit verschiedenen Diensten muss nicht mehr manuell ausgeführt werden, sondern kann durch gesprochene Sprache stattfinden. Der Nutzer muss sich nicht mehr bewegen, denn der Sprachbefehl reicht aus, selbst für kleine Aufgaben wie die Regelung der Lautstärke. Die Nutzung von Sprachassistenten ist bequem und vereinfacht einige Handlungen im Alltag. Begeisterte Nutzer würden sagen, dass die positiven Aspekte der Nutzung überwiegen und negative Aspekte weniger stark ins Gewicht fallen. Negative Auswirkungen der Nutzung sprachbasierter Assistenten existieren jedoch ebenso und sollen in diesem Kapitel genauer betrachtet werden.

3.3.1 Technische Angreifbarkeit von Alexa durch Dritte

Ein zentraler Aspekt, der die Nutzung von Amazons Alexa problematisch macht, ist die Angreifbarkeit der Sprache. Studien, wie die der Michigan State University und der Chiao Tung University in Taiwan (2018) zeigen, dass Angriffe auf die Sicherheit von Alexa möglich sind und welches Ausmaß diese annehmen können. Alexa reagiert, sobald sie ihr Aktivierungswort erkennt. Es gibt jedoch keine Einstellung, dass nur der Besitzer des Geräts einen Befehl senden kann. Jede Person, die das Aktivierungswort ausspricht und einen validen Sprachbefehl äußert, kann eine Funktion von

Alexa starten. Die Spracheingabe ist nicht personalisiert. Da das Gerät im Normalfall innerhalb geschlossener, privater Räume steht, ist ein Eingriff durch fremde Personen eher unwahrscheinlich. Trotzdem kann beispielsweise ein Gast ebenfalls Befehle an Alexa richten. Da Alexa fast ausschließlich durch menschliche Sprache gesteuert wird, jedoch keine physische Person anwesend sein muss, ist die Sprachsteuerung angreifbar (vgl. Ali u.a. 2018: 1). Es ist also auch möglich, dass eine Person außerhalb der Wohnung einen Sprachbefehl an Alexa richten kann. Alexa nimmt laut der Studie von Ali u.a. nur Sprachbefehle innerhalb von acht Metern auf (vgl. Ali u.a. 2018: 4). Dies bedeutet, dass sich eine Person innerhalb dieses Radius' befinden muss. Ein geöffnetes Fenster ist jedoch eine Möglichkeit, wie der Sprachbefehl an Alexa gerichtet werden kann, auch von außerhalb des Raumes, in dem sie sich befindet. Eine weitere Möglichkeit dafür sind Geräte mit Lautsprechern, die Sprachbefehle äußern können. Über einen laufenden Fernseher oder das Radio können so ebenfalls Sprachbefehle an Alexa gerichtet werden. Außerdem könnten die Geräte durch Hacker gesteuert werden. Ali u.a. (2017) schlagen vor, eine sensorische Technologie einzuführen, die misst, ob sich eine physische Person innerhalb des Raumes befindet. So könnte man sicherstellen, dass andere Geräte oder Personen außerhalb des Raumes nicht unbeaufsichtigt mit Alexa kommunizieren können.

Alexa und die verknüpften Skills an sich können also durch dritte Personen angegriffen werden. Zusätzlich können aber noch weitere Anwendungen durch Dritte attackiert werden, wenn der Sprachassistent beispielsweise mit ‚Smart-Home-Devices' verknüpft ist. Wenn jemand durch das Fenster Alexa auffordert, das ‚Smart-Lock' der Haustüre zu öffnen, kann die dritte Person sich Zugang zum Haus verschaffen. Dieses Beispiel zeigt, welches Ausmaß die Angreifbarkeit des Kommunikationsweges mit dem Sprachassistenten annehmen kann.

Eine Studie der Firma Syss (2017) zeigt ebenfalls, dass Anwendungen, die auf dem ‚Internet of Things' basieren, leicht angegriffen werden können. Das ‚Internet of Things' kann als „Kommunikation zwischen intelligenten Geräten ohne aktives Zutun des Menschen" (Schreiber und Straßheim 2017: 623) bezeichnet werden. Mit der Vision von allgegenwärtigen ‚intelligenten' Umgebungen geht die Angst vor einer umfassenden Überwachung des Einzelnen durch den Staat und die Wirtschaft sowie vor Missbrauch durch Kriminelle einher (vgl. Langheinrich 2007: 233). Wie bereits beschrieben, können so verknüpfte intelligente Systeme durch Dritte gesteuert werden:

> Befindet sich nun das Smartphone […] im Haus und ist ein Sprachassistent aktiv, reicht ein gekipptes Fenster aus, um sich die Haustüre öffnen zu lassen. […] Hierbei ist allein der Befehl ausschlaggebend, der Sprachassistent ist nicht fähig, Menschen anhand ihrer Stimme zu unterscheiden (Schreiber und Straßheim 2017: 625).

Außerdem kann ein Angreifer durch Manipulation des Datenverkehrs die Software kontrollieren. Da Sprachassistenten nur mithilfe des Internets und einer Verknüpfung mit der Cloud funktionieren, können sich Angreifer über die gespeicherten Daten Zugang zum System verschaffen, zum Beispiel über veraltete Software (vgl. Schreiber und Straßheim 2017: 624). Weil sie keinen internen Speicher besitzen, werden alle Anfragen, Befehle oder Informationen allgemein direkt in der Cloud gespeichert. Daraus entsteht ein „erhöhtes Sicherheitsrisiko, weil Angreifer nur einen zentralen Punkt, nämlich den in der Cloud angesiedelten Server des Anbieters, attackieren müssen, um zu einer Vielzahl von Systemen Zugang zu erhalten" (Schnurer 2015: 24). Die Angreifbarkeit der Technik hinter Alexa ist also definitiv gegeben. Welche Motive oder welchen Nutzen ein Angreifer hat, den Sprachassistenten über Sprache oder die Software zu manipulieren, kann unterschiedlicher Natur sein.

Warum ist es nun aber problematisch, wenn ein Sprachassistent wie Alexa attackiert wird? Einerseits gibt es die Möglichkeit, dass eine fremde Person Zugang zu den privaten Räumen des Nutzers erlangt. Wie in Kapitel 3.2 beschrieben, ist aber auch die informationelle Privatheit der Personen eingeschränkt, wenn solche Sicherheitslücken bestehen. Andererseits kann eine fremde Person in die Kommunikation mit dem Gerät eingreifen und möglicherweise Anwendungen starten, die nachteilig für den Nutzer sind.

3.3.2 Preisgabe privater Daten aus Bequemlichkeit und die Folgen

Daten, die Alexa von ihren Nutzern speichert, können ebenfalls durch solche externen Angriffe missbraucht werden. Gleichzeitig haben die Anbieter der Sprachassistenten jederzeit Zugriff auf diese Daten und nutzen sie für Werbezwecke und die Verbesserung ihrer Dienste. Schnurer thematisiert ‚Big Data' als Nebenprodukt der Bequemlichkeit, die Anwendungen wie Sprachassistenten ermöglichen: „Auch hier erkaufe ich mir also Bequemlichkeit in Form von Spracheingabe und immer besser auf mich zugeschnittene Ergebnisse mit Daten und Informationen, die ich dem jeweiligen Anbieter zur Nutzung überlasse" (Schnurer 2015: 24). Die digitalen Dienstboten ermöglichen es, viele Aktionen und Kommunikationen stark zu erleichtern. Durch die Nutzung dieser Geräte im privaten Raum lässt man aber auch die jeweiligen Anbieter mit hinein in die eigene Privatsphäre:

> Der Preis für diese Bequemlichkeit ist ganz eindeutig die Aufgabe unserer Privatheit im klassischen Sinne. Unser Leben wird von privaten Unternehmen in einem Maße durchleuchtet und erfasst, von dem Geheimdienste nur träumen können – und das mit unserer fleißigen Mithilfe (Schnurer 2015: 28).

In ihren Privatsphärebestimmungen sind die Nutzungsvereinbarungen streng geregelt und auch gesetzlich vorgeschrieben. Da die Standardein-

stellung die Speicherung aller Daten zulässt, muss der Nutzer selbst aktiv werden. Auch die Aufzeichnung aller Vorgänge, die über Alexa getätigt werden, wird erst auf Initiative des Nutzers gelöscht.

Unternehmen wie Amazon, Google oder Facebook brauchen große Mengen an Daten, um ihren Service zu verbessern und um Werbung so anzubieten, dass sie auf den einzelnen Nutzer zugeschnitten ist. Bei dem Sprachassistenten Alexa handelt es sich um ein Gerät, das sich in der privaten Wohnung befindet und dort immer in Bereitschaft ist, Sprachbefehle entgegenzunehmen. Aufgrund ihrer Technik müssen Sprachassistenten die ganze Zeit mithören. Die Unternehmen versichern zwar, dass die Sprachaufnahme erst nach Nennung des Aktivierungswortes startet, doch hier besteht ein großes Potenzial für Datendiebstahl und andere Angriffe (vgl. Hoy 2018: 85). Alexa kann also spätestens sobald das Aktivierungswort ausgesprochen wird, private Gespräche mithören und intime Themen, Vorlieben oder Gewohnheiten erfahren. Darin zeigt sich eine große Parallele zu den analogen Dienstboten. Dienstboten hatten, wie in Abschnitt 2 beschrieben, einen direkten Zugang zum privaten Raum ihrer Geschäftsgeber und konnten dort an intime und private Informationen gelangen. Der Nutzen war – wie bei den digitalen Dienstboten auch – trotzdem groß und schien zu überwiegen. Die Loyalität der Dienstboten wurde vorausgesetzt. Die Loyalität eines technischen Gerätes, in diesem Falle Alexa, wird von den Nutzern ebenfalls vorausgesetzt. Dies beinhaltet ebenfalls die Loyalität eines wirtschaftlichen Unternehmens mit finanziellen Interessen an der Nutzung des Produkts. Prinzipiell ist diese Loyalität in den Privatsphäre-Einstellungen von Amazon abgesichert und es ist für das Unternehmen nicht nützlich, dieses Vertrauen der Kunden zu verletzen. Dies würde dem wirtschaftlichen Interesse ebenfalls schaden. Viel wichtiger ist diese Thematik aus der Perspektive des Nutzers. Welchen Einfluss hat die freiwillige Preisgabe solcher privaten und intimen Informationen auf die Privatsphäre? Die Nutzer von Sprachassistenten[2] geben nebenbei persönliche Daten her, um diese Geräte nutzen zu können. Datenpreisgabe ist also die Zugangsschwelle, die überschritten werden muss, um teilhaben zu können.

Das Vertrauen, das die Nutzer Firmen wie Amazon entgegenbringen, ist hierbei ähnlich groß wie das Vertrauen, das man engen Freunden oder Familienmitgliedern entgegenbringt. Intimste Themen können von Alexa erfasst, gespeichert und mit anderen Daten verknüpft werden. Durch die Skills, die Alexa nutzt, können ebenfalls Dritte auf diese Daten zugreifen. Sie müssen es sogar, um überhaupt Anfragen verarbeiten zu können. Mithilfe von Suchanfragen und Sprachbefehlen an Alexa können Amazon oder Google von privaten Informationen erfahren, wie beispielsweise einer Schwangerschaft oder auch von bestimmten Vorlieben. Die Daten sind also preisgegeben und können hinterher zwar wieder gelöscht werden, verarbeitet wurden die Daten dann jedoch bereits. Schnurer fordert daher einen bewussteren Umgang mit den persönlichen Daten: „Wir müssen lernen, wirklich Privates privater zu halten als bisher. Wir müssen ein Bewusstsein dafür entwickeln, wie schnell wir wo Datenspuren hinterlassen“ (Schnurer 2015: 28).

Dienstboten, die einen Zugang zu den privaten Räumen ihrer Arbeitgeber hatten, erlangten das Vertrauen durch ihre Loyalität. Sie waren außerdem Ansprechpartner bei persönlichen Fragen ihrer Arbeitgeber. Bei technischen Geräten wie Alexa fällt der menschliche Charakter, der Dienstboten auszeichnet, weg. Dadurch, dass das Gerät aber mit einer menschenähnlichen Stimme spricht, wird wiederum Intimität erzeugt. In einer Studie der Universität Hohenheim, durchgeführt von Trepte und Masur (2015), wurden 2.824 Personen befragt, worüber sie besonders besorgt sind, wenn es um ihre Privatheit im Internet geht. 75 Prozent der Befragten sind sehr besorgt, dass sie keinen Einblick haben, was mit ihren Daten geschieht. In derselben Studie wurde aber auch gefragt, ob die Nutzer wissen, dass sie ihre personenbezogenen Daten einsehen können. Nur 44 Prozent der Befragten wussten davon. In der Studie geht es um das Internet im Allgemeinen und die Privatheit im Wandel.

Eine Studie des Marktforschungsinstituts Rheingold (Buggert 2017) befragte Nutzer von Alexa speziell zu ihrer Einstellung gegenüber der Technologie. Die Studie ist mit qualitativen Interviews durchgeführt worden und deshalb nicht repräsentativ, kann aber trotzdem ein Stimmungsbild wiedergeben. In der Studie wurden 20 Personen im Alter zwischen 20 und 75 Jahren befragt und parallel Erfahrungsberichte in sozialen Medien ausgewertet. Die Befragten werten Alexa als ihren persönlichen Zugang zur Technik der Zukunft und der Besitz eines sprachgesteuerten Assistenten wird als Statussymbol betrachtet. Gleichzeitig hat Alexa Auswirkungen auf das Machtgefühl ihrer Nutzer: „Bei den Nutzern ist die Hoffnung groß, dass sich mit Alexa eine neue Ära der Allmacht eröffnet“ (Buggert 2017: o. S.). Diese Macht zeichnet sich besonders dadurch aus, dass die Nutzer ohne viel Aufwand auf alle möglichen Anwendungen zugreifen können. Sie können Befehle geben und sich so ohne Widerspruch Wünsche erfüllen oder Aufgaben abnehmen lassen. Außerdem ruft Alexa durch die Kommunikation über Sprache ein Gefühl der Geborgenheit hervor (vgl. Buggert 2017). Hier zeigt sich, dass die sprachliche Ebene der Kommunikation und die Personalisierung des Geräts Auswirkungen auf die Emotionen der Nutzer haben können. Die Nutzer sind es gewohnt, dass ihre Kommunikationspartner menschlich sind und fühlen sich deshalb bei Sprachassistenten eher geborgen, wenn sie menschliche Züge haben. Paradoxerweise gaben die Befragten jedoch auch an, dass Alexas Funktionen in ihnen Angst vor dem Kontrollverlust in Bezug auf Abhängigkeit und Fremdbestimmung hervorrufen. Dies wird besonders auf den Verlust der Kontrolle über die persönlichen Daten und freien Entscheidungen bezogen:

> Sie fürchten mit Alexa buchstäblich in einen Zustand der Hörigkeit zu geraten. Vordergründig machen sich diese Befürchtungen oft daran fest, dass Alexa und damit Amazon einen rund um die Uhr abhören. Nichts ist mehr privat. ‚Amazon wird zur Datenkrake, die mich kategorisiert und alles von mir weiß.‘ Hintergründig ist mit der Hörigkeit aber auch die Furcht vor dem völligen persönlichen Kontrollverlust verbunden (Buggert 2017: o. S.).

Die Verbraucherzentrale (2017) warnt ebenfalls vor den Gefahren, die potenziell durch die Nutzung eines Sprachassistenten wie Alexa für die persönliche Privatsphäre entstehen können. Darüber hinaus können auch die Persönlichkeitsrechte von Gästen oder Familienmitgliedern verletzt werden, wenn diese sich im Raum befinden und Alexa aktiv ist.

Zusammengefasst lässt sich also sagen, dass besonders die leichtfertige Hergabe von privaten Informationen an ein Wirtschaftsunternehmen problematisch ist. Die aufgezeigten Sicherheitslücken müssen bei der Nutzung von digitalen Assistenten mitbedacht werden, genau wie die Interessen, die Unternehmen an den gewonnenen Daten haben. Der ehemalige Datenschutzbeauftragte (2003 bis 2013) der Bundesregierung Peter Schaar betont die Rolle des Nutzers in dieser Thematik:

> So darf nicht vergessen werden, dass durch die stetige Erhebung, Speicherung, Übermittlung und Auswertung persönlicher Daten den Betroffenen zunehmend die Kontrolle darüber entgleitet, wer was über sie weiß. Wenn der Einzelne die Verfügungsmacht über die von ihm preisgegebenen Informationen verliert, ist sein Recht auf informationelle Selbstbestimmung im Kern bedroht (Schaar 2007: 50).

Damit spricht Schaar konkret die Bedrohung der Privatsphäre und die darin enthaltenen Werte an. Informationelle Selbstbestimmung und die Kontrolle über persönliche und private Daten werden aufgegeben. Die Zerstreuung von Daten führt dazu, dass der Einzelne diese nicht mehr überblicken kann und so die Kontrolle darüber verliert, wer welche Daten über ihn gespeichert hat. Außerdem wird die Datenhergabe in unterschiedlichen Kontexten (Sprachassistenten, Soziale Netzwerke, Online Shopping, usw.) zu einer Notwendigkeit, die nur durch Verzicht vermieden werden kann. Je öfter persönliche Daten angegeben werden, desto mehr verlieren sie an Bedeutung. Psychologisch gesehen wird mit ihrer Degradierung zur Nebensächlichkeit die Schwelle des Widerstands bei den Nutzern geringer.

4. Konklusion

Sprachassistenten können als Wegbereiter der gläsernen Privatsphäre angesehen werden, wie dieser Artikel exemplarisch anhand von Amazons Alexa erörterte. Durch ihre vielfältigen Funktionen stellen die intelligenten persönlichen Assistenten einerseits eine Erleichterung in vielen Lebenssituationen dar. Dabei lassen sie sich in vielerlei Hinsicht mit Dienstboten des 18. bzw. 19. Jahrhunderts parallelisieren. Die heutige digitale Dimension der Dienstboten hat jedoch andererseits tiefgreifende Auswirkungen auf die Privatsphäre: Sprachassistenten haben durch ihre Funktionsweise technische Sicherheitslücken, die von Angreifern genutzt werden können, um sich Zugang zu den privaten Räumen der Nutzer zu verschaffen. Damit wird die lokale Privatheit gefährdet. Der größere Einfluss digitaler Dienstboten wie Alexa liegt jedoch bei der informationellen Privatheit der Nutzer.

Durch die großen Datenmengen, die ein Sprachassistent speichern und weitervermitteln muss, sind auch viele persönliche und intime Daten im Umlauf. In der Cloud werden sie vom Anbieter zwar geschützt, befinden sich trotzdem außerhalb der Kontrolle der Nutzer selbst. Den Firmen, die Sprachassistenten anbieten, wird also großes Vertrauen entgegengebracht. Dieses Vertrauen bezieht sich einerseits darauf, dass mit den Daten vertrauensvoll umgegangen wird und keine Überwachung des privaten Raums der Nutzer stattfindet. Andererseits vertrauen die Nutzer darauf, dass die Anbieter ihre Daten nicht verlieren oder verkaufen. Obwohl dieses Vertrauensverhältnis durch die Privatsphärebestimmungen geregelt ist, gibt der Nutzer die Kontrolle über seine persönlichen Daten und Informationen ab.

Obgleich einige Post-Privacy-Anhänger in einer gläsernen Privatsphäre die Chance für mehr Toleranz und Transparenz sehen, hat sich gezeigt, dass Privatheit als schützenswertes Gut anzusehen ist. Denn Privatheit ist erstens für die individuelle Autonomie des Menschen konstitutiv, da ein selbstbestimmtes Leben nur möglich ist, wenn jede Person frei entscheiden kann, was andere über sie wissen. Dabei handelt es sich zweitens um einen Aushandlungsprozess, dessen Ergebnis die Repräsentation einer Person in einem sozialen Kontext ist. Privatheitsnormen fungieren hier als Moderator. Schließlich ist drittens Privatheit unerlässlich, um eine funktionierende gesellschaftliche Öffentlichkeit zu schaffen. Privatheit kann somit als essentiell für eine demokratische und freiheitliche Gesellschaft gesehen werden.

Daraus ergibt sich die Notwendigkeit, die Privatsphäre nachhaltig zu schützen (vgl. Schaar 2007: 237). Einerseits liegt die Verantwortung für die persönlichen Daten der Nutzer zwar bei den Firmen, die sie verwenden. Insgesamt sollten Politik, Wirtschaft und Wissenschaft mit technischen Möglichkeiten verantwortungsvoll umgehen (vgl. Schaar 2007: 221). Doch das Verantwortungsbewusstsein für die eigenen Daten muss andererseits beim Nutzer der Sprachassistenten selbst beginnen: „[Die Privatsphäre] wird mehr denn je davon abhängen, welchen Wert unsere Gesellschaft diesem Gut beim Abwägen gegenüber Bequemlichkeit, Effizienz und Sicherheit zuweisen wird“ (Langheinrich 2007: 233).

Anmerkungen

1 Laut Amazons Produktseite, abgerufen von https://www.amazon.de/b?ie=UTF8&node=12775495031 [Letzter Zugriff am 24.02.2019].

2 Nicht nur die Nutzer von Sprachassistenten geben ihre Daten preis, auch Nutzer des Internets im Allgemeinen oder Besitzer von Kundenkarten tun dies. Hier soll aber der Fokus auf die Nutzer von Sprachassistenten gelegt werden.

Literatur

Ali, Kamran, Xinyu Lei, Chi-Yu Li, Alex X. Liu, Guan-Hua Tu und Tian Xie (2017). The Insecurity of Home Digital Voice Assistants – Amazon Alexa as a Case Study. URL: https://arxiv.org/pdf/1712.03327.pdf [Letzter Zugriff am 07.03.2019].

Bartmann, Christoph (2016). *Die Rückkehr der Diener. Das neue Bürgertum und sein Personal.* München: Carl Hanser.

Baumann, Max-Otto (2015). *Privatsphäre als neues digitales Menschenrecht?: Ethische Prinzipien und aktuelle Diskussionen.* Hamburg: Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI).

Bedford-Strohm, Jonas (2017). Voice First? Eine Analyse des Potentials von intelligenten Sprachassistenten am Beispiel Amazon Alexa. *Communicatio Socials* 4, 485–494.

Budde, Gunilla-Friederike (1999). Das Dienstmädchen. In: Ute Frevert und Heinz-Gerhard Haupt (eds). *Der Mensch des 19. Jahrhunderts.* Frankfurt a.M. und New York: Campus, 148–175.

Buggert, Sebastian (2017). Pilotstudie. Wie Alexa die geheimen Wünsche ihrer Nutzer erfüllt. URL: http://www.rheingold-marktforschung.de/pilotstudie-alexa/ [Letzter Zugriff am 06.03.2019].

Hoy, Matthew B. (2018). Alexa, Siri, Cortana, and More. An Introduction to Voice Assistants. *Medical Reference Service Quarterly* 37, 1, 81–88.

Krajewski, Markus (2010). *Der Diener. Mediengeschichte einer Figur zwischen König und Klient*. Frankfurt a.M.: Fischer.

Langheinrich, Marc (2007). Gibt es in einer total informatisierten Welt noch eine Privatsphäre? In: Friedemann Mattern (ed.). *Die Informatisierung des Alltags. Leben in smarten Umgebungen.* Berlin und Heidelberg: Springer, 207–264.

Lenz-Kesekamp, Vera und Tony Weber (2018). Alexa Skills. Welche Chancen und Risiken sind damit verbunden? *Wirtschaftsinformatik & Management* 6, 18–25.

López, Gustavo, Luis Quesada und Luis A. Guerrero (2018). Alexa vs. Siri vs. Cortana vs. Google Assistant. A Comparison of Speech-Based Natural User Interfaces. In: Isabel L. Nunes (ed.). *Advances in Human Factors and System Interactions.* Cham: Springer, 241–250.

Lyon, David (2007). *Surveillance Studies. An Overview.* Malden: Polity Press.

Matzner, Tobias (2017). Der Wert informationeller Privatheit jenseits von Autonomie. In: Steffen Burk, Martin Hennig, Benjamin Heurich, Tatiana Klepikova, Miriam Piegsa, Manuela Sixt und Kai Erik Trost (eds.). *Internetrecht und Digitale Gesellschaft: Band 10. Privatheit in der digitalen Gesellschaft.* Berlin: Duncker & Humblot, 75–93.

Maurer, Michael (1995). Dienstmädchen in adeligen und bürgerlichen Haushalten. In: Gotthard Frühsorge, Rainer Gruenter und Beatrix Freifrau Wolff Metternich (eds.). *Gesinde im 18. Jahrhundert.* Hamburg: Felix Meiner, 161–187.

Roser, Andreas (2018). Warum sprechen Menschen mit Maschinen? *Wissenschaft & Praxis* 69, 5–6, 249–256.

Rössler, Beate (2001). *Der Wert des Privaten.* Frankfurt a.M.: Suhrkamp.

Schaar, Peter (2007). *Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft.* München: Bertelsmann.

Schnurer, Georg (2015). Selbst vermessen – fremd gesteuert? Konsequenzen der totalen Vernetzung. *Information – Wissenschaft & Praxis*, 67, 1, 22–28.

Schreiber, Sebastian und Alexander Straßheim (2017). IoT-Penetrationstest. *Datenschutz und Datensicherheit* 41, 10, 623–627.

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

Steinbicker, Jochen (2019). Überwachung und die Digitalisierung der Lebensführung. In: Martin Stempfhuber und Elke Wagner (eds.). *Praktiken der Überwachten: Öffentlichkeit und Privatheit im Web 2.0.* Wiesbaden: Springer Fachmedien, 79–96.

Stempfhuber, Martin und Elke Wagner (2019). Einleitung. In: Martin Stempfhuber und Elke Wagner (eds.). *Praktiken der Überwachten: Öffentlichkeit und Privatheit im Web 2.0.* Wiesbaden: Springer Fachmedien, 1–13.

Trepte, Sabine und Philipp K. Masur (2015). Privatheit im Wandel. Eine repräsentative Umfrage zur Wahrnehmung und Beurteilung von Privatheit (Bericht vom 18. Juni 2015). Stuttgart: Universität Hohenheim. URL: https://www.uni-hohenheim.de/fileadmin/einrichtungen/psych/Team_MP/Berichte/Bericht_-_Privatheit_im_Wandel_2014-06-18.pdf [Letzter Zugriff am 06.03.2019].

Verbraucherzentrale (2017). Amazon hört zu: „Echo“ jetzt auch in hiesigen Wohnzimmern. URL: https://www.verbraucherzentrale.de/aktuelle-meldungen/digitale-welt/amazon-hoert-zu-echo-jetzt-auch-in-hiesigen-wohnzimmern-13149 [Letzter Zugriff am 06.03.2019].

Zurawski, Nils (2014). Geheimdienste und Konsum der Überwachung. In: *APuZ* 64, 14–19.

Anne Diessner, Lisamarie Haas und Carina Konopka
Eberhard Karls Universität Tübingen
Institut für Medienwissenschaft
Wilhelmsstr. 50
D-72074 Tübingen
E-Mail: klaus.sachs-hombach@uni-tuebingen.de

Interview

Zeitschrift für
Semiotik
Band 40 • Heft 1-2 (2018)
Seite 83-90
Stauffenburg Verlag Tübingen

Was war Surveillance 1.0? Ein Gespräch über Computergeschichte, Mainframes und Zauberspiegel

Nils Zurawski, Universität Hamburg
Dietmar Kammerer, Philipps Universität Marburg

Summary. Media scholar Dietmar Kammerer and Nils Zurawski, sociologist and editor of the blog surveillance-studies.org. met on the occasion of the 2019 Tübingen conference Surveillance 2.0. Motivated by Kammerer's lecture the two talk about notions of the "electronic brain", which has been part of many historic science fiction narratives. Kammerer explains how the metaphors and visual imaginations of then envisioned futures have changed in light of technological evolutions and hence the surveillance of society at large. And they explore why we witness yet a different contemporary situation then these imaginations have thought of.

Zusammenfassung. Der Medienwissenschaftler Dietmar Kammerer und Nils Zurawski, Soziologe und Herausgeber des Blogs Surveillance-Studies, trafen sich anlässlich der Tübinger Konferenz Surveillance 2.0 über die Geschichte von Technologie und Überwachung. Angeregt durch den Vortrag Kammerers sprechen sie über historische Vorstellungen vom Elektronenhirn, wie sie in alten Science Fiction-Narrativen immer wieder vorkamen. Kammerer erläutert, inwiefern sich die Metaphern und visuellen Bilder der Zukunft und somit auch der Überwachung der Gesellschaft im Zuge technologischer Entwicklungen verändert haben und warum wir heute dennoch eine andere technologische Umgebung haben, als sich diese in den Vorstellungen ausgemalt wurde.

Das folgende Gespräch zwischen Dietmar Kammerer und Nils Zurawski ist während der Tagung Surveillance 2.0 entstanden, die im Mai 2019 in Tübingen stattgefunden hat. Beide Wissenschaftler haben auf dieser Tagung einen Vortrag gehalten. Dietmar Kammerer sprach dabei zum Thema ‚Was war Surveillance 1.0? Ein Blick in die Geschichte von Mainframes und Zauberspiegeln'. Im Gespräch mit Nils Zurawski (siehe Beitrag in diesem Heft) spricht Kammerer über die Geschichte der Überwachung, wie sich die Computer-Technologien seit den Anfängen des 20. Jahrhunderts verändert haben und mit ihnen auch die Blicke in die jeweilige Zukunft immer wieder neu angepasst wurden.

Das Gespräch ist auch in dem Podcast „Berichte aus Panoptopia“[1] nachzuhören.

NZ: In deinem Vortrag hast du über die Widersprüche und auch Absurditäten der technischen Entwicklung Surveillance 1.0 gesprochen. Du hast berichtet, was man sich damals hinsichtlich der Bedeutung von Computern in der Gesellschaft so vorgestellt hat und wie es sich dann tatsächlich entwickelte. Wo stehen wir denn heute? Inwieweit haben sich die Visionen von damals in der Wirklichkeit von heute erfüllt oder wurden gar übertroffen? Was ist aus den Robotergehirnen geworden?

DK: Vieles, was in den 1950er und 1960er Jahren über den Computer – das „Elektronenhirn“, wie es damals hieß – gesagt und gedacht wurde, ist nicht eingetreten. Weder die optimistischen Prognosen, nach denen Roboter uns unsere mühseligsten Arbeiten abnehmen werden, noch die pessimistischen, die Angst vor dem einen, alles kontrollierenden und überwachen den Zentral-Computer, der die Herrschaft übernimmt. Das war ein großes Thema in der Popkultur, etwa im Spielfilm. Man denke nur an Stanley Kubricks *2001 – A Space Odyssey* oder, weniger bekannt, an *Alphaville* von Jean-Luc Godard oder *Colossus: The Forbin Project* von Joseph Sargent, wo am Ende die gesamte Menschheit von einem Computer kontrolliert und versklavt wird.

Diese Paranoia richtetet sich auf den einen großen Zentralrechner. Das ist offensichtlich nicht eingetreten und spielt heute kaum noch eine Rolle, weder in Filmen noch in der Diskussion. Und einer der der Gründe dafür ist der Paradigmenwechsel um 1968 vom Zentralcomputer hin zum „Personal Computer“, also zu der Idee, dass jede Frau, jeder Mann bei sich zu Hause einen Computer auf den Schreibtisch stellen kann und diesen ebenso benutzen kann für die Arbeit wie für die Freizeit. Ein Computer für schnelle Merkzettel, um Briefe zu schreiben, Zeichnungen zu machen, Fotografien zu verwalten, das Privatleben zu organisieren. Das war ein Bruch in der Geschichte des Computers Ende der 1960er Jahre, der vielen die Hoffnung gegeben hat: Wir werden uns befreien, dieser Alptraum von der Herrschaft eines zentralen Computers kann abgewendet werden, der Computer ist gezähmt und persönlich geworden, nutzerfreundlich.

Die Firma, die das am erfolgreichsten und am gewinnträchtigsten propagiert hat, war Apple. Der Durchbruch für Apple kam mit dem legendären Werbespot von Anfang 1984, der das Thema *1984* und Orwell aufgreift. Der zeigt ein ‚Big Brother‘-Szenario, in der die Menschen wie Insassen kahlrasiert sind, graue Kleidung tragen, vor einem riesigen Telescreen sitzen und sich Hassparolen des großen Bruders anhören. Bis eine Frau auftritt, die den Screen mit einem Hammerwurf zerstört. Der Spot endet mit der Botschaft: „Wir, die Firma Apple, werden in diesem Jahr den Macintosh einführen und deswegen wird 1984 nicht wie das Buch *1984*“, d.h., der benutzerorientierte, ‚persönliche‘ Computer wird den Zentralcomputer, den großen Bruder, verhindern.

Und wie wir eine Generation später wissen, ist dieses Versprechen auf komplizierte Weise sowohl erfüllt worden als auch pervertiert, ins Gegenteil gekehrt. Das war spätestens klar, als durch Edward Snowden Präsentationen der NSA öffentlich wurden, in denen Angestellte der Agency ganz gezielt den Werbespot zitieren und sich über Apple-Kunden lustig machen – sie als „Zombies" bezeichnen, die ihre eigene Überwachung wünschen. Es war also genau dieser Trend zum „persönlichen" Computer, der mir hilft, meinen Alltag zu organisieren, der mich bei alltäglichen Erledigungen unterstützt und der genau deshalb all meine persönlichen Daten kennt, alles über mich weiß, eben weil es mein persönlicher Computer ist. Genau der ermöglicht es der NSA, Google, Facebook und all den weniger bekannten Datenhändlern heute, Dinge über uns zu erfahren, die sie sonst nicht erfahren würden.

NZ: Die Entwicklung ist also ein zweischneidiges Schwert. Ich denke z.B. an die Handy-Durchdringung von infrastrukturell armen Regionen wie Afrika, in denen Mobilfunk blendend funktioniert. Das Persönliche funktioniert, die große Infrastruktur ist jedoch weitgehend eher problematisch und anfällig. Und andererseits ist der persönliche Computer aber der persönliche Überwacher, der ja auch bei mir in der Hosentasche sitzt.

DK: Ich bin kein Experte, was die Nutzung von Mobilfunkgeräten in Afrika angeht. Ich weiß aber, dass das ein großes Thema ist, dass das Smartphone dort einen großen Teil der fehlenden Infrastruktur ersetzt, was ja erst mal eine gute Sache ist. Aber man müsste genau hinsehen: Welche Apps werden in welcher Weise genutzt? Wer hat auf diese Daten Zugriff? Das müsste man genauer untersuchen. Meine ungeprüfte Vermutung ist, dass für die großen Internet-Unternehmen der ökonomische Gewinn in Afrika erstmal nicht so spannend ist, sondern dass hier neue Modelle getestet werden und in großem Maßstab Abhängigkeiten geschaffen werden, die sich in Zukunft auszahlen könnten.

NZ: Siehst du es als ein großes Problem an, dass sich alles so auf ein Gerät zuspitzt, welches ich als Optionsmaschine bezeichnen würde? Unser ganzes Leben findet ja in bzw. über das eine Gerät vermittelt statt. Auch wenn man jetzt keine Nägel damit einschlagen kann, so bündeln sich dennoch unsere verschiedensten Lebensbereiche darin: das Private, das Geschäftliche, wir kaufen ein, wir verwalten unsere Häuser, wir bedienen die uns umgebende Infrastruktur darüber. Das wäre doch so eine Plattform, wie du sie ansprichst, oder?

DK: Im Augenblick bündelt das Smartphone sehr viele Aktivitäten: Kommunikation auf vielerlei Weisen, Navigation, Informationsbeschaffung, Entertainment, Einkauf, Organisation des Alltags, Fitness, Selbstoptimierung und vieles mehr. Ich weiß, dass du „Optionsmaschine" als Einschränkung verstehst – man bekommt genau diese Optionen vorgeschrieben und keine

anderen –, aber ich würde die lenkenden oder auffordernden Aspekte stärker betonen. Mittlerweile gibt es ja sogar Apps, die einen daran erinnern, das Smartphone auch mal aus der Hand zu legen, Stichwort „Digital Wellbeing". Nur, dass die nächste Generation von Geräten nicht einmal mehr in unserer Hand sein wird. Geräte wie Alexa werden ja über die Sprache gesteuert, die muss und soll man gar nicht mehr anfassen. Das sind Sensoren, die in unsere Umwelt eingelassen sind. Die Möglichkeit von Eingriffen oder Veränderungen am Gerät durch uns entfällt, weil die Software nicht im Gerät, sondern auf weit entfernten Servern läuft. Und das wird noch zunehmen im „Internet der Dinge".

NZ: … sozusagen jeder Kühlschrank und jeder Herd hat dann eine Erkennung, wir brauchen dann nicht mal mehr Alexa als eine zentrale Steuerung …

DK: Mit einem Fitness-Armband müssen wir nicht mehr interagieren, das zeichnet von alleine auf, wieviel wir uns bewegen, wann wir uns bewegen, wohin wir uns bewegen. Alles, was der Mensch – der User – noch tun muss, ist, das Gerät ab und zu mal aufzuladen und anzuziehen. Das ist der Weg vom Bediener zum Diener. Wir füttern die Geräte mit Daten und mit Elektrizität, mehr müssen wir nicht leisten. Wir müssen nur noch sehr niederschwellig mit Technik interagieren, nur noch Inputs geben.

Das wird noch zunehmen, bloß ist das dann nicht mehr das Smartphone. Auch das Smartphone ist historisch wie alle Medientechnik. Es werden neue Gadgets kommen, andere Ein- und Ausgabegeräte werden sich an die Endpunkte einer riesigen Daten-Infrastruktur setzen, die allerdings das Zeug dazu hat, ziemlich dauerhaft monopolisiert zu sein, wenn die Politik nicht eingreift. Wo läuft das alles zusammen, auf welchen Datenbanken, wer hat darauf Zugriff, wie viele Leute, wie wenige Leute? Das Smartphone ist nur das Ende einer viel größeren Maschine und wie die aussieht, das muss man analysieren.

NZ: Wenn das aktuelle Stichwort die „künstliche Intelligenz" ist, erkennst du da irgendwas aus der Geschichte wieder? Werden hier die gleichen Versprechungen gemacht, nur mit einem neuen Begriff? Werden da gewissermaßen alte Träume neu aufgewärmt oder befinden wir uns tatsächlich jetzt an der Schwelle zum Superhirn, dem mechanischen, digitalen, quantencomputergesteuerten Großhirn?

DK: Auch die KI ist ein alter Traum, oder Alptraum, je nachdem. Schon in den 1950er Jahren gab es diese Versprechungen oder Drohungen vor einer Zukunft, in der ein Roboterhirn, das unendlich intelligent, aber eben nicht menschlich ist, die Herrschaft übernimmt und unsere freiheitliche Gesellschaft zerstört. Oder, im Gegenteil, der Menschen wird dank Technik seine Freiheit und Menschlichkeit voll ausleben: Dann können wir uns zurücklehnen und uns ganz der Kunst und der Kreativität und der Muße hingeben. Eine Art digitales Schlaraffenland der ewigen Erfüllung.

Das ist beides nicht eingetreten und ich glaube, zumindest die Forschung hat sich von der KI im starken Sinne verabschiedet. Ich glaube, Experten verwenden diesen Begriff nur noch nostalgisch oder mit einem Grinsen. Was es heute gibt, ist „machine learning", das ist freilich etwas ganz anderes, als was sich die populäre Vorstellung heute oder die Forschung vor fünfzig Jahren unter „Künstlicher Intelligenz" vorstellt bzw. vorgestellt hat. Heute entwickelt und erforscht man keine intelligenten Maschinen, sondern automatisierte Entscheidungssysteme, die durch massiv viele Daten und durch menschliche Hilfe lernen, Entscheidungen zu treffen: Ist das auf dem Bild ein Hund oder eine Katze? Was macht dieser Mensch, wo kommt der her, was hat der vor? Solche Art von Entscheidungen oder Klassifizierungen überlassen wir der Maschine. Das ist keine Intelligenz, das ist im Gegenteil extreme Spezialisierung.

Es ist ein Fehler zu denken, dass eine Maschine, die eine Sache sehr gut kann, im Grunde alles andere auch sehr gut kann. Nein, die kann ganz genau und nur das, wofür sie trainiert wurde. Der Vorteil von Computern ist ja gerade, dass sie so enorm dumm sind, also gleichgültig gegenüber ihrem Programm und ihrem Input, den sie stur abarbeiten, das aber praktisch mit Lichtgeschwindigkeit. Und ja, auf diese Weise gibt es eine Menge Aufgaben die ein Computer besser, schneller, zuverlässiger erledigen kann als ein Mensch. Aber auch hier muss man nicht alles glauben. Vor kurzem machte eine Meldung die Runde über eine Studie zur Erkennung von Hautkrebs. Hautärzte und ein Computer bekamen dieselben Bilder von Hautauffälligkeiten vorgelegt und siehe da: Der Rechner hat Hautkrebs im Schnitt zuverlässiger erkannt als die Ärzte. Die Überschrift dazu: „Künstliche Intelligenz schlägt Hautärzte", als wäre es ein Fußballspiel oder ein Boxkampf. Liest man sich die Artikel durch, wird es differenzierter: Den Ärzten wurden Bilder vorgelegt, aber in Wirklichkeit entscheidet kein Arzt anhand eines Bildes: Er spricht mit den Patienten, sieht ihn sich ganz an, fühlt und tastet die Haut und trifft dann erst eine Entscheidung. Der Computer war zudem nur auf eine sehr spezifische Form von Hautkrebs trainiert worden. Ein Arzt hingegen muss sehr viele Varianten abwägen. Das war auch das eigentliche Ergebnis der Studie: Der Computer kann Ärzte in ihrer Diagnose in bestimmten Fällen unterstützen, nicht mehr und nicht weniger. Es hieß nicht: Er kann sie ersetzen. Aber dennoch lautet die Überschrift: Computer vs. Mensch: Eins zu Null. „Wir legen der Maschine Bilder vor, wir legen den Menschen Bilder vor", das ist kein fairer Vergleich.

Wie gesagt, das ist eigentlich eine gute Meldung: Wir entwickeln Methoden, um Leben zu retten. Aber in der Wahrnehmung dampft das zusammen auf: Der Mensch hat mal wieder verloren. Dabei war das nur ein Laborversuch, der unter sehr spezifischen Bedingungen ausgeführt wurde.

NZ: Du hast gerade von den Dienern gesprochen. Und es gibt ja einen Traum von den vielen Dienern, die wir für uns arbeiten lassen können und die alles für uns erledigen. Ich habe manchmal das Gefühl, wenn es irgendwo „Bing" macht in meinem Haushalt, sei es mein Handy oder eine Maschi-

ne oder irgendwas, dass ich dann laufe und dass ich mich sozusagen scheuchen lasse von meinen elektronischen Domestiken.

DK: Ja, aber das gilt für Technik und Werkzeuge überhaupt, nicht nur bei elektronischen Geräten. Jeder, der einen Hammer, eine Schaufel oder eine Axt benutzt, muss wissen, wie man diese benutzt, muss seine Bewegungen anpassen. Selbst wenn es nur ganz kleine muskuläre Anpassungen sind, muss sich der Körper den Artefakten, die er benutzt, anpassen. Die Frage ist nur, in welchem Maße, wie groß ist unser Freiheitsgrad. Der Mensch musste sich ans Auto anpassen, und ich rede jetzt nicht von ‚intelligenten' Smart Cars, sondern von knatternden Kisten um 1900. Da mussten Straßen gebaut werden, man musste Regeln lernen, da musste man sich auf seinen Bürgersteig beschränken, auf einmal war man Fußgänger und nicht mehr Stadtbewohner.

Ja, wir müssen ans Telefon rennen, aber das war auch schon 1880 so. Ein Telefonanruf ist ein ‚Anruf' oder ein Befehl an mich. Aber ich kann aufstehen und rangehen oder ich kann sitzenbleiben und es ignorieren. Das Bürgertum um 1900 hatte sich entschieden, erst einmal die Diener, die Haushälterin rangehen zu lassen, man öffnete ja auch nicht selbst die Tür, wenn jemand klingelte.

Also, wir müssen uns an unsere Artefakte und Werkzeuge anpassen. Das hat aber nicht so sehr etwas mit Überwachung oder mit Medien zu tun, sondern mit Technik überhaupt. Wann sagen wir: Nee, ich kann noch Treppe laufen. Und wann nehme ich den Aufzug?

NZ: Wir machen uns so möglicherweise auch abhängig von der Technik, die uns eigentlich eher helfen sollte? Der Traum besteht dann in einem digitalen Schlaraffenland, wo man nichts mehr tun muss. Das scheint mir die Vision zu sein. Aber wenn wir Gefahr laufen, machen wir uns abhängig und haben dann keine andere Option mehr, können nicht mehr entscheiden?

DK: Ich scheue mich immer davor, Risikoszenarien zu entwerfen, in dem Sinne: So und so wird es kommen. Einerseits findet eine Art Deskilling statt und vieles wird uns abgenommen. Im Bereich des Computers ist das offensichtlich, früher musste man Assemblersprachen lernen, um einen Computer erst einmal zu programmieren, denn jeder Computer war tatsächlich einzigartig und hatte seine eigene Sprache. Jetzt ist alles universal geworden und benutzerfreundlich und ist (wörtlich) kinderleicht.

Allerdings ist unglaublich viel Zeit, Aufwand und Forschung genau darauf verwendet worden, die Computer so zu gestalten, dass sie scheinbar mühelos zu bedienen sind, dass sie genau zu wissen scheinen, was wir gerade wollen – dass sie persönlich werden, wie schon beschrieben. Und all diese Arbeit hat den Zweck, dass wir den Computer, diese hoch spezialisierte und teure Maschine, in unserer Freizeit nutzen können, dass sich sogar Arbeit wie Freizeit, wie Muße anfühlt: Heute dürfen und müssen ja

die meisten an ihrem Arbeitsplatz kreativ sein und sich frei fühlen und der Personal Computer unterstützt das.

Das erinnert mich an die Vision des jungen Marx vom „totalen Menschen", für den dank Fortschritt und Technik die gesellschaftliche Arbeit durch „freie Tätigkeit" ersetzt wird, vormittags fischen und jagen, abends Gedichte schreiben. Daraus ist bekanntlich im ersten Anlauf nichts geworden, aber ausgerechnet Silicon Valley will es uns nun ermöglichen. Was nun das digitale Schlaraffenland angeht, in dem wir uns zurücklehnen und zu gar nichts mehr verpflichtet sind, das ist in genau dieser Formulierung natürlich eine Horrorvorstellung. Der völlige Alptraum. Wie kann ich mich verwirklichen, wenn ich nichts mehr zu tun habe? Wieso sollte der Kühlschrank entscheiden, ob und wann ich Milch brauche? Wieso sollte mein Einkauf per Drohne zu mir geliefert werden? Weshalb sollte ein Algorithmus für mich meine Lieblingsmusik finden? Wer kann sich das ernsthaft wünschen? Absolut irre.

NZ: Sind das dann eher etwas naive technische Ingenieursträume, wir machen uns die Welt Untertan?

DK: Schaut Euch Wall-E an, ein ganz großartiger Film. Die ganze Menschheit ist der Vermüllung der Erde im Raumschiff entflohen, jetzt sitzen sie alle in fliegenden Sesseln und drücken nur noch auf Knöpfe. Alles kommt und geht auf Knopfdruck und alle wiegen 200 kg und können sich nicht mehr von alleine bewegen: Das ist das Versprechen. Und dann kommt ein Roboter mit großen Augen und einer Liebe zu Pflanzen und befreit uns daraus.

NZ: Sehr schönes Schlusswort, Dietmar, ich danke Dir!

DK: Ich danke für das Gespräch!

Anmerkungen

1 Der komplette Podcast kann unter https://www.surveillance-studies.org/2019/06/bap5-tuebinale-2019-surveillance-2-0/ abgerufen werden. In diesem Beitrag wurde nur das Interview mit Dietmar Kammerer abgedruckt.

Dr. habil. Nils Zurawski
Universität Hamburg
Inst. für kriminologische Sozialforschung
Allende-Platz 1
D-20146 Hamburg
E-Mail: nils.zurawski@uni-hamburg.de
Webseite: http://www.surveillance-studies.org

Dr. Dietmar Kammerer
Philipps Universität Marburg
Inst. Für Medienwissenschaft (DFG-Projekt mediarep.org)
Deutschhausstr. 9
D-35037 Marburg
E-Mail: dietmar.kammerer@staff.uni-marburg.de

Diskussion

Zeitschrift für
Semiotik
Band 40 • Heft 1-2 (2018)
Seite 91-102
Stauffenburg Verlag Tübingen

Brauchen wir individualisierte Krankenversicherungs-Tarife in Form von Smartwatches? Protokoll einer Debatte

Sven Jentzsch, Franziska Sieb, Frederica Tsirakidou, Martin Möller, Alexander Danner, Berit Stier und Julius Trautmann, Eberhard Karls Universität Tübingen

Summary. As part of the conference "Surveillance 2.0 – Zwischen Kontrolle und Komfort" at the Eberhard Karls University of Tübingen, six Masters students of Media Science participated in a public debate. They discussed the issues of individualised health insurance rates which are linked to behaviour data measured by smartwatches. Pros and cons were presented in three turns on each side. The arguments dealt with this specific form of surveillance and its potential effects on collective benefits and individual freedom. The government emphasises the encouragement of healthy living, social fairness and prevention of diseases, while the opposition counters particularly with privacy concerns, relentless health pressure as well as ethical and moral risks of that kind of surveillance. The debate's protocol and a preface about debating culture will be provided below.

Zusammenfassung. Im Rahmen der Tagung „Surveillance 2.0 – Zwischen Kontrolle und Komfort" der Eberhard Karls Universität Tübingen fand eine öffentliche Debatte zwischen sechs Masterstudierenden der Medienwissenschaft statt. Gegenstand dieser Debatte war die Frage nach einer Einführung von individualisierten Krankenversicherungstarifen, die sich an von Smartwatches gemessenem Verhalten orientieren. In drei Durchgängen wurden abwechselnd Pro- und Contra-Argumente debattiert, wie diese Form von Überwachung zwischen kollektivem Nutzen und persönlicher Freiheit eingeordnet werden kann. Während die Regierung die Förderung von Gesundheit, soziale Gerechtigkeit und Prävention von Krankheiten als zentrale Punkte anführt, kontert die Opposition mit Datenschutzbedenken, permanentem Gesundheitszwang und ethischen wie moralischen Problematiken dieser Überwachung. Das Protokoll der Debatte wird hier mit einem Vorwort zur Debattenkultur wiedergegeben.

Vorwort

Wer kritische Stimmen zum aktuellen Zustand politischer Debatten sucht, muss nicht lange suchen: Im August beklagte ein Leitartikel der Augsburger Allgemeinen: „Unsere Debattenkultur ist überdreht" (Schmitz 2019). In den Augen von Kathrin Werner in der SZ ist sie hingegen „verkümmert" (Werner 2019). Peter Maxwill im *SPIEGEL* sekundierte, immer mehr Menschen würden sich aus dem öffentlichen Meinungsaustausch zurückziehen (vgl. Maxwill 2019). Die aufgeworfenen Schlagworte lauten Filterblasen, Internethetze, Fake News, Donald Trump. Die Kommentatoren sind in ihren Befunden nicht kohärent, und es wäre auch zu fragen, ob es sich um ein genuin neues Phänomen handelt – beides soll hier aber nicht weiter vertieft werden. Zusammenfassend lässt sich folgende Beschädigung unserer Streitkultur konstatieren: Fehlende Toleranzbereitschaft für andere politische Haltungen erzeugt vermiedene oder nur scheinbare, von persönlichen Attacken geprägte Debatten und umgekehrt.

Dies gefährdet unsere Demokratie, denn für diese ist die öffentliche Debatte – verstanden als kontroverse, aufeinander bezogene Bearbeitung von Entscheidungsfragen (vgl. Kemmann 2006: 56) – konstitutiv. Ihre Aufgabe ist „den Bürgern Entscheidungsoptionen an[zu]bieten, die dann durch Wahlen ihren Willen kundtun können" (Kramer 2006: 71). Bleibt die Debatte also aus oder wird unter verkehrten Bedingungen geführt, behindert dies die demokratische Willensbildung. Das ist zum Beispiel im Bereich Überwachung fatal, wenn die Grenzen zwischen kollektiver Sicherheit und persönlicher Freiheit ausgelotet werden sollen.

Einen Versuch, eine geregelte Debattenkultur wieder in die Gesellschaft zu tragen, unternimmt der Debattiersport, der sich in den vergangenen Jahrzehnten von Großbritannien auch nach Deutschland ausgebreitet hat (vgl. Kemmann 2006: 62–65).

Er beruht auf den folgenden Prinzipien:

1. Die dortige Debatte steht jedem offen, unabhängig von politischer Erfahrung. Die dahinterstehende Grundannahme ist, dass jeder Bürger – eine Auseinandersetzung mit dem Thema vorausgesetzt – in der Lage ist, sich argumentativ dazu zu äußern.
2. Die Debattenteilnehmer werden einer Position zugelost, die sie vertreten sollen. Sie sollen so herausgefordert werden, sich bisweilen über „perspective taking" (Batson 2009: 267–279) in andere Meinungen hineindenken zu müssen und so ihre politische Empathiefähigkeit zu erhöhen.
3. Die daran anschließende Debatte folgt klaren Regeln: Beide Seiten haben aufeinander folgende, gleiche Redezeit; Fehlverhalten wie persönliche Angriffe werden sanktioniert.[1]
4. Am wichtigsten ist der Schritt danach: Man könnte einwenden, dass das agonale, wettkampfbasierte Setting eher eine Verhärtung der Positionen mit sich ziehe. Tatsächlich führt die Debatte aber nicht obwohl, son-

> dern gerade weil sie „den jeweiligen Konflikt pointiert herausstell[t]“ (Kramer 2006: 71) dazu, dass die Zuhörer und Teilnehmer „das verhandelte Problem sowohl rational wie emotional bewerten können“ (Kramer 2006: 75) und so Verständigung möglich wird (für eine genauere Auseinandersetzung zum Verhältnis zwischen Debatte und Verständigung vgl. Kramer 2006): Je mehr sich beide Seiten bemüht haben, ihre Position glaubhaft und überzeugend zu vertreten, desto eher wird es möglich, beide Positionen nachzuvollziehen, selbst wenn man seine Meinung nicht ändern sollte.

Eine Annäherung an eine solche Form des Debattierens wurde in vergangenen Semestern von Studierenden der Medienwissenschaft in Tübingen vorgenommen. Sechs Studierende ohne Debattier-Vorerfahrung wurden je zur Hälfte der Pro- und der Contra-Seite (‚Regierung‘ und ‚Opposition‘) zugeteilt. Der Gegenstand ihrer Debatte: Ein in den letzten Jahren zu beobachtender Trend, dass Krankenversicherer gezielt den Kauf von Smartwatches und Fitnessarmbändern fördern und gesundes Verhalten ihrer Versicherten belohnen (vgl. Austin 2019; Anonym 2016). Dieses Themenfeld berührt gleichzeitig viele Bereiche – Gesundheit, Datenschutz und sozioökonomische Erwägungen. Die Streitfrage lautete: Wäre eine Zukunft wünschenswert, in der individualisierte Krankenversicherungstarife existieren, die sich nach dem von Smartwatches protokollierten Verhalten bemessen? Nach Vorbereitung im Team veranstalteten die Studierenden dazu eine halbstündige Live-Debatte vor Publikum.

Diese Debatte finden Sie im Folgenden in verschriftlichter Form. Sie hat nicht den Anspruch, eine politische oder juristische Expertendiskussion zu ersetzen, sondern soll vielmehr Argumente zu diesem Thema zugänglich machen und zur weiteren Auseinandersetzung mit demselben anregen.[2]

Anfangsrede der Regierung (Franziska Sieb)

Immer mehr Menschen tragen auch in Deutschland Smartwatches – und das ganz freiwillig. Sie sind nützlich, denn sie zeigen uns, ob wir uns genügend bewegen oder nicht. Wir von der Regierung plädieren dafür, die Krankenkassenbeiträge mit Hilfe der Daten von Smartwatches individuell an den Versicherten anzupassen. In Deutschland ist die Krankenversicherung gesetzlich geregelt. Diese gesetzlichen Krankenkassen werden durch das sogenannte Solidaritätsprinzip und eben nicht nach Krankheitsbild finanziert. Diese Art der Finanzierung hat zum Ziel, Krankheitskosten für alle bezahlbar zu machen. An diesem Prinzip wollen auch wir nichts ändern – aber Krankenkassen bieten Zusatzleistungen und seit 2015 ist es ihnen ebenfalls erlaubt, Zusatzbeiträge zu erheben. Hierdurch erhofft man sich, das Kostenbewusstsein der Versicherten anzusprechen. Genau diese Zusatzleistungen und Zusatzbeiträge sollten in unseren Augen individuell angepasst werden: Denn warum sollten gesund lebende Menschen genau-

so viel zahlen wie Menschen, die einen schlechten Lebenswandel haben? Und würde eine individuelle Anpassung der Beiträge nicht vielleicht sogar viele Menschen dazu motivieren, gesünder und mit mehr Bewegung zu leben?

Schon heute zahlen viele Krankenkassen Prämien für gesundheitsfördernde Maßnahmen. Sie geben bereits Geld zu Fitnessarmbändern usw. dazu. Dies würden die Krankenkassen nicht tun, wenn sie sich dadurch nicht weniger Ausgaben bei den Krankheitskosten der Versicherten versprechen würden. Wenn Krankenkassen bereits solche gesundheitsfördernden Fitnesstracker finanzieren, warum sollten sie dann nicht auch von den Daten profitieren?

Smartwatches motivieren durch die Visualisierung der Bewegung zu einem gesünderen Lebensstil. Wenn ich den ganzen Tag am Schreibtisch saß oder auf der Couch lag und abends sehe, dass ich mich heute kaum bewegt habe, bin ich durch die Visualisierung der fehlenden Bewegung vermutlich eher motiviert, abends nochmal eine Runde um den Block zu laufen. Ohne die Visualisierung der Smartwatch ist mir aber häufig gar nicht oder zumindest weniger bewusst, wie wenig ich mich bewegt habe. Doch bereits wenig Bewegung kann Krankheiten im Vergleich zu gar keiner Bewegung vorbeugen. Übergewicht, welches häufig durch zu wenig Bewegung verursacht ist, ist in vielen westlichen Ländern eines der größten Gesundheitsprobleme, aus welchem viele weitere Erkrankungen resultieren können. Würde die Krankenkasse Fitnessbänder an jeden ihrer Versicherten herausgeben, könnten auch einkommensschwache Menschen von den Vorteilen dieser Tracker profitieren. Durch das kostenfreie Armband würde auch ihnen die Möglichkeit gegeben, ihre Bewegung zu visualisieren.

Durch gesündere Menschen sparen Krankenkassen viel Geld. Dies würde wiederum geringere Beiträge für alle Versicherten bedeuten. Die Versicherungen müssten weniger Geld für die Behandlung ihrer Kunden ausgeben, da diese seltener krank werden. Zudem müssen Krankenkassen seltener Lohnausgleichszahlungen tätigen, und auch die Wirtschaft insgesamt würde durch die selteneren Krankheitsfälle dank der Fitnessarmbänder profitieren: Weniger Arbeitnehmer fallen wegen Krankheit aus, wodurch die deutsche Wirtschaft jährlich mehrere Millionen sparen würde.

Ein weiterer positiver Nebeneffekt: die gesammelten Daten der Krankenkasse können Ärzten und Versicherten zur Verfügung gestellt werden, wodurch Krankheiten frühzeitiger und besser erkannt werden könnten. So würden nicht nur die Krankenkassen, sondern auch der Versicherte selbst von den Daten der Smartwatch profitieren. Sie hätten bessere Behandlungschancen. Schließlich ist es meistens leichter, Krankheiten in einem frühen Stadium zu behandeln als in einem späteren. Wenn die Daten ständig aufgezeichnet und geprüft werden, fallen bereits leichte Unregelmäßigkeiten auf, die ein Indiz für eine schwere Krankheit sein könnten. Diese Früherkennung würde erneut zu geringen Ausgaben der Krankenkasse führen, da Behandlungen von früh erkannten Krankheiten häufig viel preiswerter sind als Behandlungen in einem späteren Krankheitsstadium. Wie

Smartwatches Leben retten können, soll an Hand eines Beispiels, über welches Huffpost.com am 22. September 2015 berichtete, verdeutlicht werden: Im Jahr 2015 spielte der damals 18-jährige Paul Houl im Football-Team seiner Schule. An einem heißen Sommertag absolvierte er zwei Trainings und fühlte sich im Anschluss nicht gut. Er dachte, er sei lediglich ein bisschen aus der Übung – ging duschen und legte sich kurz schlafen, als er später aufwachte checkte er seine Apple Watch. Diese zeigte ihm, dass seine Herzschlagrate viel zu hoch war. Nach Rücksprache mit seinem Trainer und der Schulkrankenschwester fuhr er in die Notaufnahme, wo eine Rhabdomyolyse festgestellt wurde. Mit Rhabdomyolyse wird in der Medizin die Auflösung quer gestreifter Muskelfasern bezeichnet, zu welchen u.a. die Herzmuskulatur zählt. Wäre Houle nicht durch seine Apple Watch auf die Unregelmäßigkeit so frühzeitig aufmerksam gemacht worden, wäre er vermutlich gestorben. Man sieht also, Smartwatches können Leben retten!

Neben den lebensrettenden Funktionen so einer Smartwatch, zeigt das Beispiel von Houle auch, dass bereits viele Menschen sowieso schon eine Smartwatch tragen. Ungefähr ein Drittel der Menschen wären dazu bereit, die gesammelten Daten des Fitnesstrackers an ihre Krankenkasse zu übertragen, wenn sie davon profitieren könnten. Dies zeigt eine Studie des Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (bitkom) aus dem Jahr 2016.

Es bleibt also festzustellen, dass das Gesundheitssystem durch individualisierte Versicherungsbeiträge gerechter werden würde. Durch die Individualisierung der Beiträge müsste jeder Versicherte für sich selbst und seine Handlungen Verantwortung übernehmen.

Anfangsrede der Opposition (Frederica Tsirakidou)

„Brauchen wir individualisierte Krankenversicherungs-Tarife?"– Die Frage, die wir von der Opposition uns stellen, ist, wann Überwachung problematisch wird. Wann gehen wir einen Schritt zu weit? Wann befinden wir uns mitten in der Dystopie, die Werke wie *1984* vorausgesagt haben? Denn ja, ‚Big Brother is watching you'. Noch werden wir nicht wie im Orwell Klassiker 24/7 über den Teleschirm überwacht: aber Armbänder, die die Gesundheit messen, sind schon ein grundlegender Schritt in die falsche Richtung. Ich wertschätze die Argumente der Regierung, aber es tut mir leid, der Zweck heiligt nicht die Mittel. Gesundheit sollte nicht zum Preis von Überwachung zu haben sein. Wenn wir heute Armbänder unsere Gesundheit messen lassen, wo werden wir dann morgen sein? – Werden wir Kameras einsetzen, die Kranke zuhause überwachen, wie in einem anderen dystopischen Roman: *The Circle*? Nun sind aber diese Romane bald keine Fiktion mehr, sondern ein Abbild der grausamen Realität.

Denken wir über die Konsequenzen nach, die entstehen, wenn wir die individualisierten Krankenversicherungs-Tarife einführen: Ja, wir erhalten individuelle Pflege, aber wir geben unsere Daten ab, machen uns zum frei-

willigen Versuchskaninchen. Man stelle sich hierbei die Frage, wer die Daten bekommt. Unsere Daten gehören nun der Forschung und Medizin. Verdammt krank, oder? Einzelne Daten können miteinander verknüpft werden, demographische Bilder können kreiert werden – vielleicht ein Fortschritt in der Medizin, aber definitiv ein Schritt Richtung *1984*. Dieses Prinzip sieht man mittlerweile häufig, frei nach dem Motto ‚gib mir deine Daten und ich helfe dir', bequeme Dienstleistungen gegen Daten auszutauschen. Firmen wie MyHeritage oder 23andme versprechen beispielsweise eine detaillierte Analyse der DNA, man erfährt wo seine ethnischen Wurzeln liegen und ob man Erbkrankheiten hat. Ein verlockendes Angebot, aber zum Preis der eigenen DNA, die jetzt in den Händen der Firma liegt! Maschinen vergessen nicht: Stellen Sie sich ein Gespräch beim Arzt in der Zukunft vor, der plötzlich alles über ihre Jugendsünden weiß. Wenn Sie von den Krankentarifen profitieren wollen, müssten Sie also eigentlich Ihr ganzes Leben gesund leben!

Die Armbänder zwingen die Versicherten also zur Gesundheit. Und dieser Gesundheitszwang geht weit über den bereits existierenden sozialen Zwang auf Social Media hinaus – denn es ist ein Zwang, der durch Überwachung geschieht! Wenn Sie sich gesund ernähren und gesund leben, dann zahlen Sie weniger. Gut für die Armen? Na, dann messen Sie doch mal die Werte eines Fabrikarbeiters, der lange arbeitet, wenig schläft und sich von billigem Essen ernährt. Die Arbeit der Armen fordert den Körper, ergo schlechtere Werte auf dem Armband, ergo mehr bezahlen. Wer arm ist, wird hier eher noch ärmer und für Detox-Kuren, um die Werte aufzubessern, ist hier einfach das Geld nicht drin. Und die Schere zwischen Arm und Reich? Sie geht noch weiter auseinander! Willkommen in der Dystopie. Von behinderten, chronisch kranken und depressiven Menschen muss ich gar nicht erst anfangen, sie werden für etwas bestraft, wofür sie nichts können. Die neue digitale Gesellschaft zielt auf den Außenseiter, statt ihn zu schützen!

Ein weiterer Nachteil ist die Umsetzbarkeit: Wir behaupten, Geld kann besser eingesetzt werden als in die Verbreitung von Überwachungsarmbändern. Davon abgesehen, das Armband ersetzt keinen Arzt, es kann nicht alles messen und es kann vor allem nicht so genau messen, wie ein Arzt messen könnte, ebenso kann es kein menschliches Urteil ersetzen. Die Armbänder sind aber da, immer und überall. Sie folgen Ihnen zur Arbeit, sind an Ihrem Handgelenk, wenn Sie schlafen.

Abschließend kann ich sagen, dass vermeintliche Vorteile digitaler Dienstleistungen oft an Zwang und Überwachung gekoppelt sind. Urplötzlich hat man sich die Online Banking App oder das ein oder andere ach so praktische Feature aufschwatzen lassen. Warum? Es geht nicht anders! Der Zugriff auf analoge Alternativen wird immer komplizierter, oft heißt es dann ‚mit dem Strom schwimmen oder sterben'. Aber Gesundheit sollte in keinem Fall nur zum Preis von Überwachung verfügbar sein!

In der digitalen Gesellschaft wird uns oft eine Art ‚Detachment', eine Ablösung von der materiellen Sache vorgeworfen. Aber unsere Gesund-

heit sollte beim besten Willen nicht nur aus Zahlen bestehen; nicht von einer Smartwatch gemessen werden, denn die Würde des Menschen ist ja bekanntlich unantastbar.

Antwort der Regierung (Martin Möller)

Meine sehr verehrten Damen und Herren; in ihrer Anfangsrede hat unsere geschätzte Opposition behauptet, Fitnesstracker würden es einfacher machen, Leute auszuspionieren. Tatsächlich ist auch die Regierung der Meinung, dass Fitnesstracker im schlimmsten Fall ein Risiko für die Privatsphäre ihrer Nutzer sein können. Allerdings möchten wir von der Regierung die Opposition daran erinnern, dass es in unserem Alltag seit Jahren bereits ein anderes Gerät gibt, das ein wesentlich größeres Sicherheitsrisiko darstellt und das so gut wie jeder von uns täglich benutzt. Sie alle tragen es mit großer Wahrscheinlichkeit gerade in ihrer Tasche, meine Damen und Herren: Das Smartphone.

Denn auch das für unsere moderne Gesellschaft so wichtig gewordene Smartphone birgt in der Realität eine Vielzahl an Risiken im Hinblick auf den Datenschutz. Tatsächlich sind unsere Smartphones sogar noch um ein Vielfaches unsicherer als ein Fitnesstracker, da sie von Hackern wesentlich einfacher ausspioniert werden können als besagter Fitnesstracker, und zudem auch noch wesentlich mehr persönliche Daten, wie Anschrift, E-Mail-Adresse und diverse wichtige Passwörter, gespeichert haben. Wenn Smartphones datenschutztechnisch nun aber sogar noch gefährlicher als Fitnesstracker und zudem auch noch weitaus verbreiteter sind, warum würde dann niemand von uns auch nur im Traum daran denken, sie ebenfalls zu verbieten?

Die Antwort auf diese Frage ist einfach, meine Damen und Herren. Smartphones sind für unsere Gesellschaft so unglaublich wichtig geworden, dass sie für unser Leben weitgehend überlebensnotwendig geworden sind. Und genau diese Bedeutung messen wir von der Regierung auch der neuen Technologie der Fitnesstracker zu. Denn wie wir bereits gehört haben, retten Fitnesstracker nachweisbar Leben. Und auch wenn wir von der Regierung die Befürchtungen der Opposition in Sachen Datenschutz teilen, so sind wir gleichzeitig auch der Ansicht, dass das Retten von Menschenleben um ein Vielfaches wichtiger als datenschutzrechtliche Bedenken ist – die, wie ich Sie erinnern möchte, zu diesem Zeitpunkt lediglich Bedenken sind.

Darüber hinaus möchten wir die Opposition an dieser Stelle darauf aufmerksam machen, dass ein Drittel aller Erwachsenen auch ohne unseren Vorschlag bereits mit Hilfe diverser Fitnessapps eine Art Fitnesstracking betreibt. Die gesundheitlichen Daten dieser Leute sind also schon in Umlauf. Wenn all diese Daten also bereits in Umlauf sind, warum sollten die Leute dann nicht wenigstens von ihren Daten profitieren dürfen? Zusätzlich wären die Daten jener Leute, die bereits Fitnesstracking betreiben, auf den Fit-

nessarmbändern, die unser Vorschlag anbietet, wesentlich sicherer, als auf ihrem Smartphone, weshalb unser Vorschlag auch in Bezug auf Datenschutz von Vorteil ist.

In ihrer Anfangsrede sprach die Opposition zudem davon, Smartwatches würden kranke oder unsportliche Patienten benachteiligen. Die Opposition scheint dabei leider vergessen zu haben, dass sich bei den von uns geforderten Krankenkassentarifen, wie schon zuvor erwähnt, der Versicherungsbeitrag nur verbessern, jedoch nicht verschlechtern kann. Dass Kranke aufgrund ihres schlechten Gesundheitszustandes mehr Geld bezahlen müssen, ist also vollkommen unmöglich. Tatsächlich würde unser Vorschlag eine Anpassung der Krankenkassentarife jenen Kranken und Unsportlichen, welche die Opposition durch unseren Vorschlag benachteiligt sieht, sogar helfen. Denn dadurch, dass sich dank der Smartwatches mehr Versicherte für einen gesünderen Lebensstil entscheiden werden, müssten die Krankenkassen auch weniger Geld für deren Behandlung ausgeben, wodurch wiederum mehr Geld für die Behandlung von ebenjenen Kranken und Unsportlichen zu Verfügung stünde.

Antwort der Opposition (Alexander Danner)

Der Büroarbeiter ist also in der Argumentation der Regierung mehr wert als der Handwerker oder Industriearbeiter. Nicht nur, dass der Handwerker oder Industriearbeiter einen niedrigeren Bildungsabschluss hat, sondern auch durch die höhere Gesundheitsbelastung am Arbeitsplatz wird der Industriearbeiter oder Handwerker diskriminiert. In der Schweiz sind bis zu 6000 mg Feinstaub am Arbeitsplatz erlaubt. Handwerker und Industriearbeiter sind höheren körperlichen Belastungen und auch gesundheitlichen Risiken wie etwa dem Feinstaub ausgesetzt. Die Lebenserwartung ist bei dieser Berufsgruppe deutlich geringer. Die Regierung diskriminiert damit vorsätzlich alle Handwerker und Industriearbeiter und deren Arbeit, die durch gesundheitliche Einschränkungen in ihrem Job ein schlechteres Gesundheitsbild abgeben werden – und dadurch mehr bezahlen müssen.

Ich möchte keine Gesellschaft haben, in der wir am Ortseingang Schilder aufhängen müssen und die Städte nur für Büromitarbeiter frei sind, weil deren Arbeit ja viel gesünder ist. Es wird ein Gesundheitspass kommen, der dann Privilegien vergibt. Gesundheit darf kein Gut sein, das gewisse Berufe diskriminiert. Ein Mensch ist kein Diesel-Fahrverbot.

An dieser Stelle möchte ich die fiktive Geschichte von Tom erzählen. Tom ist ein aufstrebender junger Mann. Sportlich aktiv, lebt gesund und will sich diesen Monat auf eine Stelle bei der Staatsanwaltschaft bewerben. Tom freut sich schon auf die Arbeit. Als einer der Besten hat er sein Jurastudium abgeschlossen, auch sonst ist er sehr gewissenhaft. Er hat sein Studium mit diversen Auszeichnungen beendet. Die Chancen stehen also sehr gut. Also bewirbt er sich. Er bekommt am selben Tag noch eine Absage, mit der Begründung, dass seine gesundheitlichen Voraussetzungen zu

schlecht seien, er würde nicht die Lebenserwartung eines durchschnittlichen Arbeiters erfüllen und hätte ein hohes Risiko, frühzeitig an Leukämie zu erkranken. Tom bekommt diesen und viele weitere Jobs nicht.

Unsere geschätzte Regierung wird jetzt sagen, das ist ja eine fiktive Geschichte, die unvorstellbar ist. An diesem Punkt würde ich gerne auf das Punktesystem in China verweisen. Bürger in China müssen sich bald ein Führungszeugnis zur ‚sozialen Vertrauenswürdigkeit' ausstellen lassen, basierend auf einem Punkte- und Benotungssystem zum Verhalten, das dem Arbeitgeber vorgelegt werden muss. Glauben Sie bloß nicht, dass die Fitnessüberwacher am Handgelenk nicht zu einem ‚Gesundheitszeugnis' führen! Aber ich möchte hier die Frage aufwerfen: Wird es den Menschen mit diesem Druck besser gehen? Beantworten Sie Sich diese Frage selbst.

Schlussrede der Regierung (Berit Stier)

Mit den individuell angepassten Krankenkassentarifen haben wir endlich eine wirksame Lösung gefunden, wie viele Menschen dazu motiviert werden können, gesünder zu leben, und das auf freiwilliger Basis. Sie kennen alle diese furchtbaren Bilder auf den Zigarettenpackungen, die Menschen vom Rauchen abschrecken sollen. Dank des angepassten Krankenkassentarifs kann der gesunde Lebenswandel aus einer rein positiven Motivation heraus entstehen – nämlich einfach um Geld zu sparen –, um dafür belohnt zu werden, dass man sich um sich selber und seine Gesundheit kümmert. Drei der häufigsten Krankheiten unserer Gesellschaft sind Diabetes, Fettleibigkeit, die oft zu Herzkrankheiten führt, sowie Rückenleiden. Und wie Sie eben schon gehört haben, ist die Unterstützung im Kampf gegen diese Krankheiten auch enorm wichtig. Dass durch dieses System höchstwahrscheinlich mehr Menschen eine gesunde Lebensweise, sprich mehr Bewegung, gesünderes Essen usw., verfolgen werden, sollte daher an sich schon Argument genug sein.

Aber dieses System birgt weitere enorme Vorteile: Einmal wäre da die soziale Fairness: Warum sollten Menschen, die gesund leben, genau so viel zahlen wie Menschen, die sich ungesund ernähren, rauchen und ihrer Gesundheit offensichtlich durch ihren Lebensstil schaden? Es ist durch eine Wristly-Studie erwiesen, dass Leute, die eine Fitnesswatch tragen, dadurch sowieso schon gesünder leben, warum also darf das nicht begünstigt werden?

Durch mehr gesunde Menschen spart die Krankenkasse wie gesagt auf Dauer außerdem auch Geld – und das kann sie dann anderswo sinnvoll anlegen, wie beispielsweise die Krankenkassenbeiträge generell senken. Und dadurch profitieren dann auch einkommensschwächere Menschen davon.

Und ja, wie bei allen Daten, die wir preisgeben, müssen auch hier die Daten geschützt und die Anonymität gewahrt werden. Aber Gesundheit und Fairness sind genauso wichtig wie gesicherte Daten. Und mit den

Daten, die die Krankenkasse hat, können nicht nur Tarife angepasst werden, sondern sie könnten auch Ärzten zur Verfügung gestellt werden. Stellen Sie sich vor, Sie kommen ins Krankenhaus, müssen schnell behandelt werden, aber der Arzt muss erstmal herausfinden was Sie überhaupt haben. Hätte er aber Zugriff auf diese technisch sehr genauen Daten, die die Krankenkasse dank des Tarifs von Ihnen hat, könnte er viel schneller handeln und Sie behandeln. Ärztliche Besuche werden dank des höheren Datenvolumens allgemein also viel effizienter.

Durch individuell angepasste Krankenkassentarife, die sich nach den übertragenen Daten der Fitnesswatches richten, haben wir also größere soziale Fairness: Jeder ist für sich selbst verantwortlich. Außerdem haben wir durch die finanziellen Einsparungen einen enormen Motivationsaspekt, gesünder zu leben und wir haben Möglichkeiten, die Daten positiv einzusetzen, wie sie z.B. dem Arzt zur Verfügung zu stellen. Ob mit oder ohne Tarif, unsere Daten werden ohnehin gesammelt. Wieso sollte man dann von seinen Daten nicht wenigstens finanziell profitieren?

Schlussrede der Opposition (Julius Trautmann)

Unser Ausgangspunkt in dieser Debatte ist die These, dass eine derartige Überwachung von Gesundheit ein zu hoher Preis für individuelle Tarife bei Krankenkassen ist.

Natürlich führt die Regierung die Motivation und Förderung von Gesundheit in der Bevölkerung und positive Effekte für die Wirtschaft wie Ersparnisse im Gesundheitssystem als Argumente auf. Unsere Argumente hingegen sind moralischer und prinzipieller Natur. Denn Gesundheit und Überwachung dürfen nicht in denselben Topf geworfen werden. Auch das mit der Freiwilligkeit ist so eine Sache. Denn die Folge dieser Entwicklung wäre ein sozialer Zwang, ein Mechanismus, der sich zunehmend auf alle auswirkt. Wer will schon sehen wie andere auf einmal weniger zahlen als man selbst, nur wegen einer Uhr am Handgelenk? Und wem soll hier überhaupt geholfen werden? Der nächste Automatismus, der in Gang gesetzt werden würde, ist noch größere soziale Ungleichheit. Wohlhabendere können es sich leisten, gesund zu leben, während arme oder weniger gut situierte Menschen die vergleichsweise überteuerten Tarife zahlen müssen. Selbst wenn sie eine Smartwatch tragen würden, müssten sie vermutlich immer noch mehr zahlen, aufgrund des schlechteren Gesundheitszustandes.

Unser zweites Hauptargument ist die digitale Überwachung durch Daten und die Gefahr des Missbrauchs dieser Daten. Wer ist denn tatsächlich dazu bereit, alles über sich und seinen Körper preiszugeben? Die totale Transparenz? Als wäre der digitale Fußabdruck eines jeden von uns im Internet nicht schon groß genug. Das Ende vom Lied ist ein vollkommenes demographisches Profil, das der Kontrolle und Überwachung durch den Staat, aber auch durch Unternehmen und Wissenschaft dient. So können die intimsten Eigenschaften schnell in die falschen Hände geraten. Und da

braucht auch niemand mit dem Stichwort der sogenannten Datensicherheit um die Ecke kommen. Schon heute jagt ein Datenskandal und Leak den nächsten, wenn jeder 15-jährige Schüler aus dem Haus der Eltern die Daten von Politikern und Prominenten hacken kann, wie sollen dann unsere Gesundheitsdaten ausreichend geschützt sein? Die Auswirkungen des Gesundheitszustandes gehen also weit über die Krankenkassen hinaus. Wie zuvor mit dem Beispiel an Tom illustriert, leben wir in einer Leistungsgesellschaft, die durch einen derartigen Konkurrenzdruck durch Gesundheit noch weiter vorangetrieben werden würde.

Abschließend gilt also zu sagen, der Zweck heiligt hier nicht die Mittel. Natürlich gibt es in der Theorie gewisse Vorteile, die in der Praxis jedoch nur für einen verschwindend geringen Teil der Bevölkerung positiv ausfallen und somit nur Einzelfälle darstellen würden. Im direkten Vergleich zu den von uns geschilderten vorhersehbaren, aber auch vielen unvorhersehbaren negativen Konsequenzen wäre es schlichtweg unverantwortlich, an Smartwatches gekoppelte Krankenkassentarife einzuführen. Die Dystopie eines panoptischen Gesundheitssystems würde Realität werden und wir müssten mit der Gewissheit leben, zu jeder Zeit einsehbar zu sein und kontrolliert werden zu können. Diese Vorstellung ist eine völlige Fehlorientierung unseres Gesundheitssystems und tritt den ursprünglichen Sinn des Sozialwesens mit Füßen. Es geht schließlich immer noch um Solidarität und nicht um Fitness-Fairness. Der Staat muss positivere Anreize für einen gesunden Lebenswandel schaffen, die ohne eine völlige Überwachung seiner Bürger möglich sind.

Anmerkungen

1 Exemplarische Regelwerke finden sich z.B. unter: URL: https://www.streitkultur.net/debatte/#regeln [Letzter Zugriff am 20.08.2019].

2 Weitere Debatten zum Themenfeld Überwachung von nationalen bzw. internationalen Spitzenteams im Debattiersport findet man in Videoform beispielsweise zur digitalen Klarnamenpflicht (Finale Campus-Debatte Tübingen 2018, URL: https://www.youtube.com/watch?v=Mxww9ZdhfBw [Letzter Zugriff am 20.08.2019]) und zur Metadaten-Verstaatlichung (Finale Europameisterschaft 2016, URL: https://www.youtube.com/watch?v=9Y6WKhKcFkg [Letzter Zugriff am 20.08.2019]).

Literatur

Anonym (2016). Wenn die Krankenkasse Ihre Fitness-App mitliest. *Die Welt* 05.04.2016. URL: https://www.welt.de/gesundheit/article154004816/Wenn-die-Krankenkasse-Ihre-Fitness-App-mitliest.html [Letzter Zugriff am 06.08.2019].

Austin, Patrick Lucas (2019). This Health Insurance Giant Wants to Pay for Your Apple Watch. *Time Magazine* 29.01.2019. URL: https://time.com/5515510/apple-aetna-watch-insurance/ [Letzter Zugriff am 06.08.2019].

Batson, C. Daniel (2009). Two Forms of Perspective Taking. Imagine How Another Feels and Imagining How You Would Feel. In: Keith D. Markman, William Martin Klein und Julie A. Suhr (eds.). *Handbook of Imagination and Mental Simulation.* New York: Psychology Press, 267–279.

Kemmann, Ansgar (2006). Debatte als didaktischen Instrument. In: Olaf Kramer (ed.): *Rhetorik der Debatte.* Tübingen: Max Niemeyer, 55–67.

Kramer, Olaf (2006). Konflikt statt Konsens? Die Debatte als Medium politischer Kommunikation und das universalpragmatische Ideal der rationalen Verständigung. In: Olaf Kramer (ed.). *Rhetorik der Debatte.* Tübingen: Niemeyer, 68–82.

Maxwill, Peter (2019). Wir schweigen die Demokratie zugrunde. *Spiegel Online* 21.07.2019. URL: https://www.spiegel.de/panorama/gesellschaft/streitkultur-und-demokratie-wie-wir-sie-zugrunde-schweigen-a-1261127.html [Letzter Zugriff am: 05.08.2019].

Schmitz, Gregor Peter (2019). Unsere Debattenkultur ist überdreht. *Augsburger Allgemeine* 02.08.2019. URL: https://www.augsburger-allgemeine.de/politik/Unsere-Debattenkultur-ist-ueberdreht-id55079276.html [Letzter Zugriff am: 05.08.2019].

Werner, Kathrin (2019). Streit tut gut! *Süddeutsche Zeitung* 18.05.2019. URL: https://www.sueddeutsche.de/wirtschaft/debatten-kuehnert-thunberg-1.4451063 [Letzter Zugriff am 05.08.2019].

Sven Jentzsch, Franziska Sieb, Frederica Tsirakidou, Martin Möller,
Alexander Danner, Berit Stier und Julius Trautmann
Eberhard Karls Universität Tübingen
Institut für Medienwissenschaft
Wilhelmsstr. 50
D-72074 Tübingen
E-Mail: klaus.sachs-hombach@uni-tuebingen.de

Kleinere Texte zur Praxis der Überwachung

Zeitschrift für
Semiotik
Band 40 • Heft 1-2 (2018)
Seite 103-115
Stauffenburg Verlag Tübingen

Social Scoring als Praxis der Überwachung. Eine Analyse der *Black Mirror*-Folge *Nosedive*

Melanie Seifert, Ann-Christine Strupp und Anne Schneider, Eberhard Karls Universität Tübingen

Summary. The Social Credit System, which is currently being tested in China, is viewed very critically by some sides, although the principle of scoring, i.e. the assignment of a certain point value to a person, has spread in many other industrial countries long since. Digitalisation and Big Data technologies accelerate and intensify these developments even further and thus favour the monitoring and behaviour control of people. This principle of scoring and surveillance is taken up in numerous fictional narratives as a dystopic scenario, e.g. by the Netflix series *Black Mirror*. The episode *Nosedive* deals with these issues of surveillance and Social Credit Systems. In addition to a film analytical examination of *Nosedive*, this essay also deals with a comparison of the socio-critical representation of scoring within the episode and the real existing system in China.

Zusammenfassung. Das Social Credit System, das derzeit in China getestet wird, wird von einigen Seiten sehr kritisch betrachtet, obwohl sich das Prinzip des Scoring, also die Zuordnung eines bestimmten Punktewertes zu einem Menschen, auch in vielen anderen industriellen Ländern schon längst ausgebreitet hat. Digitalisierung und Big Data-Technologien beschleunigen und intensivieren diese Entwicklungen noch zusätzlich und begünstigen so die Überwachung und Verhaltenssteuerung der Menschen. Dieses dystopisch wirkende Szenario wird in zahlreichen fiktiven Narrativen aufgegriffen. So auch von den Machern der Netflix-Serie *Black Mirror*, welche in der Episode *Nosedive* die Themen Überwachung und Social Credit System behandeln. Dieser Essay beschäftigt sich neben einer filmanalytischen Auseinandersetzung mit *Nosedive* zudem mit einem Vergleich der gesellschaftskritischen Darstellung des Scorings innerhalb der Episode und des real existierenden Systems in China.

1. Einleitung

In der Schule und Universität werden unsere Noten von allen Seminaren und Kursen zu einer Durchschnittsnote zusammengerechnet. Man spricht hier auch von einem ‚Score'. Die Punkte in Flensburg, die man für sein Verhalten im Straßenverkehr erhält, oder der SCHUFA-Wert, der die Kreditwürdigkeit eines Menschen abbilden soll, bilden ebenfalls einen solchen Score. Doch nicht nur in der analogen Welt gibt es das Prinzip des ‚Scoring'. In unserer digitalisierten Welt breitet sich die Praxis immer weiter aus, da sie durch Big Data-Technologien immer schneller und intensiver betrieben werden kann. Eine Definition für den Begriff des Scoring hat der Sachverständigenrat für Verbraucherfragen in seinem Gutachten „Verbrauchergerechtes Scoring" geliefert: „Scoring ist die Zuordnung eines Zahlenwertes (des Scores) zu einem Menschen zum Zweck der Verhaltensprognose oder Verhaltenssteuerung. Die Bestimmung dieses Zahlenwertes erfolgt in der Regel auf der Grundlage einer breiten Datenbasis durch ein algorithmisches Verfahren" (Gigerenzer u.a. 2018: 860). Das Problem beim digitalen Scoring: Oft ist es schwierig nachzuvollziehen, wie der jeweilige Score zustande kommt – es mangelt also an der nötigen Transparenz.

Die vorliegende Arbeit beschäftigt sich mit dem Prinzip des Social Scoring, wie es derzeit in China getestet und betrieben wird. Stichwort: Social Credit System (SCS). Auch im Film wird das Prinzip des Social Scoring immer wieder bildlich und narrativ dargestellt. In diesem Zusammenhang wird im Speziellen die Folge *Nosedive* der Netflix-Serie *Black Mirror* abgehandelt und analysiert. Die Arbeit gliedert sich demnach wie folgt: Zuerst wird allgemein auf die Serie *Black Mirror* eingegangen, die in der Regel dystopische Welten zeigt, welche durch neue Technologien entstehen können, und diese kritisch hinterfragt. Anschließend wird näher auf die Folge *Nosedive* in Hinblick auf Überwachung und die Praxis des Scoring eingegangen und einer filmischen Analyse unterzogen. Im Anschluss daran soll dann der Vergleich mit dem chinesischen Social Credit System gezogen werden, indem die Kernpunkte und Ziele dieses Systems genauer erläutert werden.

2. Überwachungsgesellschaften und Dystopien in *Black Mirror*

2.1 Die Serie Black Mirror

Eine dystopische Welt, in der das Social Credit System eine große und wichtige Rolle spielt, entwirft die britische Science-Fiction-Serie *Black Mirror* in der Folge *Nosedive*, zu Deutsch ‚Abgestürzt'. Ideengeber und Hauptproduzent ist Charlie Brooker, der mit der Serie verschiedene Auswirkungen der Verwendung von Technik und Medien auf die Gesellschaft überspitzt thematisiert. Laut Brooker handele sie von der Art, wie wir alle leben und innerhalb von zehn Minuten leben könnten, wenn wir ungeschickt wären

(Brooker 2011). Der Titel stehe demnach für „den kalten, glänzenden Bildschirm eines Fernsehers, eines Computerbildschirms, eines Smartphones“, in dem sich das moderne Individuum selbstverliebt, narzisstisch, manipulierbar und meinungsfrei spiegele (Brooker, zitiert nach Ströbele 2016).

Die einzelnen Folgen nehmen zwar im Rahmen kleiner Hinweise zum Teil Bezug aufeinander, sind aber in sich abgeschlossen und erzählen eigenständige Geschichten. Deshalb gehört *Black Mirror* zur Kategorie der Anthologie-Serien. Da jede Episode eine andere Besetzung hat und an anderen Schauplätzen, teils sogar in verschiedenen Realitäten spielt, lässt sie sich als Gesamtkonzept nur schwer in ein Genre einordnen – von Thriller über Horror bis zu Drama und Satire ist alles dabei. Nachdem es die Serie 2011 und von 2013 bis 2014 schon einmal gab, wurde sie 2016 wieder aufgegriffen und feiert seither international hohe Erfolgszahlen. Inzwischen erstreckt sich *Black Mirror* über fünf Staffeln. Zudem veröffentlichten die Produzenten zwischen der vierten und fünften Staffel den interaktiven Film *Black Mirror: Bandersnatch*, in dem man als Zuschauer die Möglichkeit hat, an verschiedenen Stellen durch eigene Entscheidungen den Verlauf der Geschichte zu verändern. Das Besondere an *Black Mirror* ist, dass sie unseren aktuellen Umgang mit alltäglichen, digitalen Medien weiterdenkt und so überspitzt, dass daraus unüberschaubare, meist erschreckende Szenarien entstehen. Doch so abwegig die jeweils erschaffenen Welten zunächst erscheinen, bleibt der Zuschauer doch am Ende einer jeden Episode mit einem unwohlen Gefühl zurück. Denn wenn man genauer darüber nachdenkt, sind die Szenarien meist gar nicht so weit entfernt von dem, was schon jetzt Realität ist.

2.2 Foucault lässt grüßen

In ihrer Analyse zu *Black Mirror* befassen sich die Autoren Özge Bayraktar Özer und Aslı Özlem Tarakçioğlu mit der Intertextualität der Serie und deren Bezug zum Panoptizismus nach Foucault. Obwohl das Hauptthema auf den möglichen negativen Auswirkungen aktueller und zukünftiger Technologien basiere, bieten die meisten Episoden der Serie vielfältige Perspektiven auf dystopische Welten, um verschiedene Formen der Überwachungsgesellschaft abzubilden. Die Autoren nehmen an, dass der Panoptizismus nach Foucault die Grundlage dafür bilde, wie das Schlüsselthema der Überwachung in der gesamten Reihe kritisiert werde. Die Verweise auf eine panoptische Überwachung seien zwar nicht vollständig explizit, aber als intertextuelles Element ein subtiles Thema innerhalb der Serie.

Die meisten *Black Mirror*-Episoden behandeln also verschiedene Unterthemen der Überwachung wie Sicherheit, Datenschutz, Bestrafung oder Autorität. Die in der Serie dargestellten, dystopischen Welten können als Spuren eines panoptischen Systems interpretiert werden, das entweder von einem Individuum oder vom Staat ausgeht (vgl. Bayraktar Özer und Tarakçioğlu 2019: 73). Um ihre These zu untermauern, haben die beiden Autoren acht

verschiedene Episoden aus den ersten vier Staffeln im Hinblick auf Intertextualität untersucht, die sich ihrer Meinung nach auf die Überwachungsgesellschaft als Hauptthema fokussieren (vgl. Bayraktar Özer und Tarakçioğlu 2019: 74).

Darunter befindet sich zum Beispiel die zweite Folge der ersten Staffel: *Das Leben als Spiel* (*15 Million Merits*). Ein wichtiges Bindeglied zwischen der Episode und dem Panoptizismus sei die physische Struktur der Lebensräume der Menschen, denn jeder Mensch lebt in einem einzelnen, kleinen und zellenartigen Raum, dessen Wände keinerlei Fenster besitzen, sondern quasi aus Bildschirmen bestehen. Auch die Arbeitsabschnitte der Individuen sind als Zellen konzipiert:

> These divided cells aim to physically individualize people and separate them from others in line with the invisibility function of Bentham's panoptic prison design which prevents any possible collective attempt of those under surveillance against the order […]. The closed environment where people work and live makes it easier to observe every act of individuals and to create a surveillance society (Bayraktar Özer und Tarakçioğlu 2019: 74).

Indem Menschen in bestimmten Bereichen eingeschlossen bleiben, könne man ihre Handlungen aufzeichnen und Maßnahmen ergreifen, um diese Handlungen zu disziplinieren und zu manipulieren. Versuche eine Person, sich dem zu widersetzen, erinnere sie das Überwachungssystem daran, dass sie vollständig sichtbar ist. Ein weiterer wichtiger Punkt sei, dass der eigentliche Überwacher nie zu sehen ist: „The unknown/unseen identity and presence of the observer ensures the continuity of surveillance" (Bayraktar Özer und Tarakçioğlu 2019: 74).

Ein weiteres Beispiel der beiden Autoren ist die Folge *Das transparente ich* (*Entire History of You*). Innerhalb dieser Realität haben die meisten Menschen einen Chip hinter dem Ohr implantiert, mit dem sie jederzeit ihre Erinnerungen wieder abspielen und sogar mit anderen teilen können. Während dies zu Beginn der Folge noch recht harmlos wirkt, erkennen wir im weiteren Verlauf die eher unschönen Seiten dieses Gadgets: Der Mensch ist komplett durchleuchtbar und quasi zur Transparenz verpflichtet. Das Äquivalent zum Wächter im Panoptikon-Turm sei in *Das transparente Ich* der Mikrochip (vgl. Bayraktar Özer und Tarakçioğlu 2019: 74). Entsprechend der Theorie des Panoptizismus sind sich die Einzelpersonen der Tatsache bewusst, dass sie ständig überwacht werden und die überwachende Instanz jederzeit über das Implantat auf ihr Gedächtnis zugreifen könne.

Diese und andere Beispiele zeigen den Autoren zufolge, dass sich die Produzenten von *Black Mirror* in der Serie auf die nachteiligen Auswirkungen der Spitzentechnologien als Hauptthema fokussieren. Eines der am häufigsten besprochenen Themen in den Episoden sei die panoptische Überwachung der Gesellschaft und des Einzelnen. Foucaults Panopticon werde von der Serie also nicht explizit thematisiert, liefere aber die Idee für die Serie und forme ihren Inhalt, indem sie wichtige Motive wie ständige

Sichtbarkeit, die unbekannte Identität des Überwachenden und die Verletzung der Privatsphäre in den Blick nehme (vgl. Bayraktar Özer und Tarakçioğlu 2019: 77f.).

2.3 Verlust der Individualität

Auch der Autor Tony McKenna hat sich mit den dystopischen Dimensionen der Serie beschäftigt – allerdings eher mit Blick auf George Orwell. Innerhalb von *Black Mirror* werde ein Aspekt der modernen Kultur einer Kritik durch die düstere, satirische Vorstellungskraft des Schöpfers Brooker unterzogen. Seine Analyse widmet er im Wesentlichen der Episode *Das Leben als Spiel* (*15 Million Merits*), die bereits angesprochen wurde. Die sozialen Bindungen, die einen Menschen mit einem anderen verbinden und die Grundlage der politischen Solidarität bilden, seien in der dargestellten Welt völlig verschwunden. Ein solcher Ansatz, der das Individuum von seiner sozialen Basis trenne, impliziere, dass diejenigen, die unten sind, ihr eigenes Gespür für Individualität verlieren und sich in eine amorphe Masse verwandeln. Sie werden ausgenutzt und von den scheinbaren Geschenken der Menschen an der Spitze betört. „Because the illusion has such potency, the people who cast it, those who orchestrate it, are transformed into a mysterious, enigmatic and almost transcendental entity – to couch it in Orwellian terms, they become the all-seeing, all-knowing Big Brother" (McKenna 2019: 369).

Sie herrschen McKenna zufolge nicht nur über die physischen Körper der Massen, sondern auch über deren Verstand (vgl. McKenna 2019: 369). *Black Mirror* spielt also ganz bewusst mit diversen Theorien und Diskursen um Überwachung, neue Technologien und Digitalisierung und baut diese thematisch, auf dystopische Weise in die fiktiven Welten der einzelnen Episoden ein.

3. Filmische Darstellung der Überwachung in *Nosedive*

3.1 Schöne neue Welt?

In diesem Teil wird auf die filmische Darstellung der Überwachung in Nosedive eingegangen. Die permanente Überwachung erfolgt durch die Mitmenschen, die gegenseitig ihre Interaktionen anhand einer Fünf-Sterne-Skala bewerten. Durch einen hohen Score erhält man bessere Dienstleistungen, Discounts oder Zutritt zu bestimmten Gebäuden, wodurch die Pflege des eigenen Images besonders attraktiv wird. Die Protagonistin Lacie versucht, in dieser Welt ihren Weg zu finden und stößt an ihre Grenzen, bis sie erkennt, worauf es wirklich ankommt.

Die Folge beginnt unmittelbar in der durch SCS geprägten Welt: Inmitten einer Vorstadt, bestehend aus weißen, sauberen und glatten Häusern

mit perfekt gepflegten Vorgärten, lebt die Protagonistin Lacie Pound. Musikalisch untermalt wird die Szenerie durch melancholische Klaviermusik von Max Richter, was bereits darauf hindeutet, dass nicht alles so perfekt zu sein scheint. Perfekt geschminkt und in Pastellfarben gekleidet, joggt Lacie durch die Nachbarschaft, während sie über ihr Smartphone ihren Social Media Kanal checkt, um die Interaktionen mit ihren Mitmenschen zu bewerten. Als sie nach Hause kommt, trifft sie auf ihren Bruder Ryan, der so gar nicht in die perfekte suburbane Welt passen will: Seine graue Kleidung differenziert ihn ebenfalls von dieser Welt, in welcher der Beliebtheitsgrad der Menschen anhand einer Fünf-Sterne-Skala dargestellt wird. Hier scheint nicht das Kapital, sondern der soziale Status zu zählen. Alles ist friedlich, ruhig und alle Menschen lächeln sich an, sind zuvorkommend und freundlich. Die Kameraeinstellung ist dabei im Head and Shoulder Close-up, wodurch die gekünstelte Mimik betont wird.

Lacie will aus der Wohngemeinschaft mit ihrem Bruder ausziehen und trifft sich daher zu einer Wohnungsbesichtigung. Ebenfalls in einer Nachbarschaft, die schon fast unreal perfekt erscheint. In der Wohnung wird Lacie mit einer holographischen Projektion ihrer Selbst überrascht, welche ein glückliches Leben mit einem imaginären Partner in dieser Wohnung führt. Das Bild springt in die Totale – der Zuschauer sieht, wie Lacie mit personalisierter Werbung manipuliert wird. Die Farbe des Lichts, dem die Hologramme entspringen, setzt ebenfalls pastellfarbene Akzente in türkis. Allerdings muss sie feststellen, dass die Wohnung über ihrem finanziellen Budget liegt. Ein Discount ist nur möglich, wenn sie ihr aktuell auf 4.2 liegendes Social Media Rating auf 4.5 bringt. Mit Gedanken, wie sie ihr Rating am schnellsten erhöhen kann, verlässt sie die Wohnung, nicht ohne eine riesige Leinwand mit animiertem Inhalt gegenüber der Wohnung zu bemerken. Es sind wieder sie und ihr imaginärer Partner, die sich glücklich zeigen – personalisierte Werbung im Großformat.

3.2 Mehr Erfolg durch Authentizität

Der Plan, ihr Social Media Ranking zu erhöhen, führt sie zu einem Unternehmen namens *Reputelligent*. Auch hier sind wieder Sauberkeit und minimalistische Einrichtung in den Farben rosa, türkis und weiß zu beobachten. Der Berater empfiehlt ihr mehr Authentizität. 18 Monate würde es dauern, wenn sie auf normalem Wege ihr Ansehen derart steigern möchte. Bis dahin wäre die begehrte Wohnung wohl bereits anderweitig vergeben. Die Zeit arbeitet also gegen sie.

Wieder verbringt Lacie viel Zeit in sozialen Medien. Lacie beschließt, hier ein Foto der im Gegensatz zur Welt recht unordentlichen und zusammengeflickten Stoffpuppe Mr. Rags zu posten. Diese scheint eine Verbindung zwischen ihr und einer alten Schulfreundin Naomi herzustellen. Naomi gehört zu den sogenannten ‚hohen Vieren', also einer Person, die Lacies Ranking bei einer Bewertung steigern könnte. Letztendlich führt dies dazu,

dass Naomi – eine Frau, die in äußerst hohen Kreisen verkehrt – Lacie zu ihrer Hochzeit als Trauzeugin einlädt. Durch die Aufnahmen von Naomi in der Halbnahen wird klar, was das SCS mit den Menschen gemacht hat: Jede Handlung und jeder Schritt dienen dazu, den anderen zu gefallen. Durch ihre übertriebene Mimik, Gestik und Ausdrucksweise wird das Gefühl vermittelt, Naomi hätte sich bereits sehr stark an die Gegebenheiten des SCS angepasst.

3.3 Die unaufhaltsame Abwärtsspirale

Die Freude über die Einladung wird von einem Streit mit ihrem Bruder überschattet. Seine in der Rolle des Bruders gut gemeinten Ratschläge und Fragen zu ihrem Vorhaben weist sie von sich. All das nur, um an ihre „falschlächelnde Gefängniszelle" zu kommen, wie er ihre Traumwohnung bezeichnet. Im Streit verlässt sie die Wohnung, während die Nacht hereinbricht. Noch ahnt sie nicht, welche Abwärtsspirale sie mit der ersten negativen Bewertung durch ihren Bruder noch erwartet. Angekommen am Flughafen, der weiterhin die Welt von Ordentlichkeit und Pastell darstellt, muss sie feststellen, dass ihr gebuchter Flug ausfällt. Die in einem hellen Blau gekleidete Dame am Terminal kann direkt alle ihre Daten einsehen und anhand dessen bewerten, welche Alternativen für sie in Frage kommen. Da ihr aktuelles Ranking keine Optionen zulässt, verliert sie die Fassung. Ein in schlichtem Grau gehaltener Sicherheitsbeamter sühnt das Verhalten mit einem drastischen temporären Ranking-Abzug für 24 Stunden. Sie gerät dadurch in eine Abwärtsspirale, da sie durch ihr schlechteres Ranking in immer ungünstigere Situationen gerät.

Schließlich sieht sie sich gezwungen, auf ein Auto umzusteigen. Die Veränderungen, als sie ihre schöne geschützte Welt verlässt, werden sofort sichtbar. Sie muss ein veraltetes Elektroauto fahren. Den Pastelltönen weicht jetzt Neonlicht in der Dunkelheit. Falsches Lächeln und heuchlerisches Zuvorkommen lösen sich in Ehrlichkeit und Gleichgültigkeit auf. Das Ranking sinkt, die Abwärtsspirale ist unaufhaltsam. Ihre Kleidung in türkis und rosa verschmilzt nicht mehr mit der Umgebung, sondern bildet einen Kontrast. Die Welt sieht immer mehr aus, wie wir sie kennen.

Die Situation wird immer aussichtsloser, bis eine ältere Frau mit einem heruntergekommenen Truck anhält und ihr eine Mitfahrgelegenheit anbietet. Sie hat mit der Welt abgeschlossen. Alles ist nun in gedeckten Farben gehalten, viel Grau und Beige. Die Einstellung wechselt von der Totalen in die Halbtotale. Der Unterschied zur zuvor dargestellten Welt wird dadurch auch visuell unterstrichen. Die ältere Dame erzählt Lacie, warum sie der vom SCS geprägten Gesellschaft entsagt hat. Als sie feststellen musste, dass ein Ranking bei Leben und Tod wertlos ist, hat sie sich von dem System gelöst. Sie ist nun nicht mehr der permanenten Überwachung durch ihre Mitmenschen ausgesetzt und kann das Leben führen, das sie für richtig hält. Eine 1.4 ist sie jetzt, aber sie scheint glücklich zu sein.

Nach einer gewissen Zeit muss Lacie die Mitfahrgelegenheit wechseln. Währenddessen bekommt sie einen Anruf von Naomi. Da diese mitbekommen hat, wie niedrig Lacies Ranking mittlerweile ist, möchte sie sie nicht mehr auf der Hochzeit dabei haben und macht Lacie klar, dass die Einladung zur Hochzeit nur den Zweck eines Prestige-Boosts für Naomi hatte. Alles auf Naomis Seite des Gesprächs entspricht noch dem anfangs ordentlichen und pastellfarbenen Weltbild.

Lacie gibt trotzdem nicht auf und muss – nachdem sie es sich mit ihrer bunten Mitfahrgelegenheit verscherzt hatte – nun den Rest des Weges mit einem Quad zurücklegen. Um die finale Absperrung zu umgehen, muss sie mitten durch den Wald fahren – wobei sie kopfüber im Schlamm landet. Sie ist ihrem Ziel so nahe; die Hochzeit ist in vollem Gange. Alles ordentlich, viel rosa, viel weiß, viel künstliches Lachen und jede Menge gegenseitige (Ego-) Ranking-Boosts. Doch dann richten sich die Blicke auf Lacie, die schlammüberzogen, mit roten, verdreckten und chaotischen Haaren und einem schief sitzenden, rosafarbenem Kleid die Hochzeitsfeier stürmt. Lacie hat es endlich geschafft und greift sofort zum Mikrofon, um ihre Rede als Trauzeugin zu halten. Doch währenddessen verliert sie endgültig die Fassung: Das ist der erste Moment, in dem sie Naomi ihre Meinung sagen kann, nach all den Jahren der Anpassung und der unehrlichen Bewertungen.

3.4 Entkoppelt vom System

Letztendlich wird sie abgeführt. In einem sterilen und grauen Raum wird sie fotografiert, ihre Kontaktlinsen werden entfernt und sie kommt – immer noch völlig verdreckt und verwahrlost – in eine Zelle. Tränen lachend sieht sie den Staub von der Decke rieseln. In der gegenüberliegenden Zelle befindet sich ein Mann – völlig sauber und ordentlich angezogen. Sie beginnen sich gegenseitig an den Kopf zu werfen, was ihnen gerade in den Sinn kommt. Lacies Lächeln wird ehrlicher, während ihr Mund weiterhin vulgäre Beleidigungen formt. Ihren Wunsch hat sie vielleicht nicht erreicht – aber vielleicht war diese Form der Reinigung viel wichtiger; und in dem Moment, in dem sie lauthals in die Kamera schreit, realisiert sie ihre neugewonnene Freiheit und Erlösung.

4. Deutung der Episode

Die Welt, in der die Protagonistin Lacie lebt, weist viele Parallelen zu unserem Alltag auf und scheint nicht allzu weit von unserer Realität entfernt zu sein. Durch die gespielte Authentizität der Personen wird deutlich, welche Auswirkungen das dargestellte Social Credit System auf die Gesellschaft hat, wo jeder Schritt von den Mitmenschen überwacht und bewertet wird. Es lässt sich ebenfalls als ein panoptisches System deuten, das rhizomatisch in der Gesellschaft verwurzelt ist. Es ist zwar möglich, sich nicht der

ständigen Beobachtung auszusetzen – allerdings führt dies zu Einschränkungen im alltäglichen Leben. Es handelt sich um ein an soziale Medien gebundenes System, das auf Wertungen der Mitmenschen gegründet ist. Die fiktive, in der Zukunft spielende Erzählung ist ein dystopisches Narrativ, das die negativen Konsequenzen eines SCS beschreibt. In den Medien wird die *Black Mirror*-Folge oft mit dem Social Credit System in China verglichen und mit diesem in Zusammenhang gebracht. Die Gemeinsamkeit beider Systeme: Jedes Individuum wird mit einem einzigen Score bewertet, der zudem eine soziale Funktion innehat und eine Vielzahl an Konsequenzen, negativ wie positiv, mit sich bringen kann. In der Serie machen sich diese Konsequenzen bzw. die jeweilige Höhe des Scores im Alltag bemerkbar. Je niedriger der Score, desto stärker sind die Rechte und Möglichkeiten der Menschen in der Serie eingeschränkt (vgl. Mac Síthigh und Siems 2019: 29). So hat die Protagonistin Lacie beispielsweise mit Einschränkungen bei kommerziellen Entscheidungen und dem Zugang zu öffentlichen Diensten zu kämpfen. Worum es sich beim Social Credit System in China handelt und wie es genau funktioniert, soll im folgenden Abschnitt erläutert werden.

5. Praxisbeispiel: Chinas Social Credit System

5.1 Das Konzept und die Idee des Social Credit Systems

Das SCS, das China im Jahr 2020 einheitlich im ganzen Land einführen will, hat aufgrund der internationalen Berichterstattung weltweit für Aufsehen und Diskussionen gesorgt. Das Ziel der chinesischen Regierung: die gesamte Gesellschaft – Individuen, Organisationen, Regierungsbehörden sowie Unternehmen – zu überwachen, um anschließend deren Vertrauens- bzw. Kreditwürdigkeit individuell bewerten zu können. Im Planungsentwurf, der 2014 erschienen ist, wurde Folgendes zur Idee des SCS geschrieben:

> [The SCS's] inherent requirements are establishing the idea of a sincerity culture, and promoting honesty and traditional virtues, it uses encouragement for trustworthiness and constraints against untrustworthiness as incentive mechanisms, and its objective is raising the sincerity consciousness and credit levels of the entire society (übersetzt aus dem Chinesischen von Creemers 2018: 2).

Der jeweilige, von Algorithmen errechnete Social Credit Score ergibt sich aus einer Vielzahl von Faktoren wie Gesetzeskonformität, Einhaltung des von der Regierung festgelegten ideologischen Rahmens, aus sozialen und wirtschaftlichen Aktivitäten usw. (vgl. Liang u.a. 2018: 416). Hierbei werden diverse öffentliche und private Daten miteinander verknüpft, die aus verschiedenen Quellen wie CCTV-Kameras, Aufzeichnungen, Polizeiakten, Social Media und mehr erhoben werden, um ein einzelnes Rating zu generieren und je nach Punktestand eine Note zu vergeben (vgl. Diab 2017: 11).

Beim SCS handelt es sich also nicht primär um ein finanzielles Kredit-Rating wie wir es in Deutschland als SCHUFA kennen. So erklären Liang u.a.: „China's SCS goes beyond a financial credit rating, since it incorporates not only the evaluation of financial and commercial activities but also the assessment of social behaviors" (Liang u.a. 2018: 425). Das System basiert außerdem auf einem Straf- und Belohnungssystem, das heißt, der Score bestimmt anschließend, ob der jeweilige Akteur Leistungen oder Sanktionen erhält, und bewertet, ob man einerseits Zugriff auf Privilegien wie Bildung, Märkte, gesundheitsbezogene Leistungen oder Ähnliches bekommt oder andererseits mit Einschränkungen rechnen muss, z.B. keine Beförderung im Job oder keinen Kredit erhält.

5.2 Das Social Credit System – ein ‚orwellscher' Albtraum?

Vor allem in den Medien wurde umfassend über das Konzept des SCS diskutiert. Nach Genia Kostka hätte das SCS das Potenzial, die staatliche Steuerung von Wirtschaft und Gesellschaft radikal zu verändern (Kostka 2019: 1). In der Presse wird das SCS oft als ‚Großdatenüberwachungssystem' dargestellt, welches auf Big Data und Kommunikations-Technologien basiert, und dessen Ziel es ist, das komplette soziale, politische und wirtschaftliche Leben der Bürger zu überwachen, zu bewerten und die Menschen somit zu disziplinieren. So sprach die *TAZ* in einem Artikel vom „größten Volkserziehungsprogramm, das die Menschheit je erlebt hat" (Lee 2018). Außerdem werden immer wieder Bezüge zu Orwells dystopischen Roman *1984* erstellt – man spricht vom ‚Orwellian Nightmare' – und auch Begriffe und Konzepte aus den Surveillance Studies wie die ‚Disziplinargesellschaft' von Foucault oder Lyons ‚Social Sorting' werden im Zusammenhang mit dem SCS gennant.

5.3 Startschuss für Pilotprojekte

Obwohl erst in den letzten Jahren vermehrt über das SCS berichtet wurde – 2014 wurde der Bau des nationalen SCS vom Staatsrat publik gemacht – ist anzumerken, dass der erste Plan des SCS bereits im Jahr 1991 entwickelt wurde, ursprünglich um Probleme im Handels- und Finanzsektor lösen zu können und um größere Transparenz zu schaffen (vgl. Kostka 2019: 3). Noch ist das chinaweite SCS jedoch nicht umgesetzt worden, da in Zusammenarbeit mit IT-Unternehmen zuallererst eine einheitliche Informationsstruktur in Form von Datenaustauschplattformen geschaffen werden müsse (vgl. Kostka 2019: 2). Um dem nationalen SCS ein Stück näher zu kommen, sind jedoch bereits mehrere Pilotprojekte gestartet, die sowohl von lokalen Regierungen wie auch kommerziellen Unternehmen wie *Alibaba*, das als das chinesische Amazon bezeichnet wird, eingeführt wurden, um mithilfe von Leistungs- und Sanktionssystemen das Verhalten der chinesi-

schen Nutzer zu steuern (vgl. Kostka 2019: 1). Die kommerziellen Initiativen (zu den bekanntesten zählen *Sesame Credit* und *Tencent Credit*) beruhen hierbei auf Freiwilligkeit und fungieren eher als Loyalitätsprogramme:

> Commercial SCSs offer users a wide range of benefits including qualification for personal credit loans, easier access to sharing economy services (e.g., renting of bikes or cars), fast-tracked visa applications, preferential treatment at hospitals, and free health check-ups (Kostka 2019: 4).

So wird bei *Sesame Credit* ein Score zwischen 350 und 950 Punkten pro User errechnet, der sich aus Informationen wie Finanzkreditaufzeichnungen, verfügbaren Vermögenswerten, persönlichen Informationen, Verhalten und Präferenzen sowie sozialen Beziehungen ergibt (vgl. Síthigh und Siems 2019: 15). Die staatlichen Pilotprojekte, die in mehreren chinesischen Städten bereits eingesetzt werden, sind hingegen obligatorisch und werden als Mechanismus des Sozialmanagements eingesetzt. Außerdem gibt es Black Lists, die von den Regierungen veröffentlicht werden, um besonders ‚unvertrauenswürdige' Personen und Organisationen zu listen, die anschließend Sanktionen und Einschränkungen wie ein Verbot der Nutzung von Hochgeschwindigkeitszügen oder eingeschränkte Finanzdienste erhalten (vgl. Kostka 2019: 3).

6. Ausblick und Fazit

Auch wenn die *Black Mirror*-Folge *Nosedive* auf den ersten Blick Gemeinsamkeiten zum SCS aufweist, gibt es doch einige bedeutende Unterschiede zwischen der fiktionalen, dystopischen Erzählung und der Realität in China: So wird man beim SCS nicht von anderen Mitbürgern subjektiv bewertet bzw. bewertet selbst jede soziale Interaktion mit anderen. Stattdessen wird mit Algorithmen und Big Data gearbeitet. Auch weisen Síthigh und Siems darauf hin, dass die Bedrohung nicht wie in der Serie in der Tyrannei der Menge, sondern in der Macht des Staates liegt, der womöglich ab 2020 ähnlich Big Brother alles und jeden überwacht und als moralische Instanz auftritt (vgl. Mac Síthigh und Siems 2019: 29). Durch die filmische Darstellung der Überwachung wird die dystopische Erzählweise verstärkt: Die durch Pastellfarben geprägte Vorstadt, die an die Ästhetik vieler Instagram-Accounts erinnert, vermittelt ein Bild einer reinen, sauberen und perfekten Welt, abseits von Kriminalität, Unfreundlichkeit und sozialer Isolation. Durch die Nahaufnahmen wird dem Zuschauer klar, welchen Preis die Menschen für diese Welt bezahlen müssen: Sie wirken gekünstelt und aufgesetzt, die scheinbare Authentizität lässt die Protagonisten zu Karikaturen werden, die nur auf Oberflächlichkeiten Wert legen. Die Überwachung durch die Mitmenschen hat alle Bevölkerungsschichten durchdrungen.

Trotzdem zeigt uns die Episode *Nosedive* mit einem Verweis auf das SCS, wie unsere Zukunft vielleicht einmal aussehen könnte – und dass wir

in manchen Aspekten gar nicht so weit davon entfernt sind. Die Einzelheiten der Systeme mögen zwar noch sehr verschieden sein, doch die Aspekte, die damit zusammenhängen, betreffen unsere Gesellschaft in vielfacher Hinsicht schon jetzt: Die gegenseitige Bewertung anderer Menschen in den (sozialen) Medien, falsche Authentizität, die enorme Bedeutung des sozialen Status und vieles mehr. Auf zunächst subtile und dann sich immer mehr steigernde Weise vermittelt uns Charlie Brooker, wie schnell man in dieser pastellfarbenen, scheinbar ‚perfekten' Welt in einem rasend schnellen Strudel abstürzen kann, wenn man zu viel auf den eigenen Status gibt. Dabei hält er uns wie so oft den schwarzen Spiegel vors Gesicht und lässt uns erkennen, dass auch wir in dieser falschen, unperfekten Welt voller sozialem Druck gefangen sind.

Literatur

Bayraktar Özer, Özge und Aslı Özlem Tarakçioğlu (2019). An intertextual analysis of Black Mirror. Panopticism reflections. *The Journal of International Social Research* 12, 62, 71–78.

Brooker, Charlie (2011). The dark side of our gadget addiction. *The Guardian* 01.12.2011. URL: https://www.theguardian.com/technology/2011/dec/01/charlie-brooker-dark-side-gadget-addiction-black-mirror [Letzter Zugriff am 16.08.2019].

Creemers, Rogier (2018). China's Social Credit System. An Evolving Practice of Control. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175792 [Letzter Zugriff am 30.09.2019].

Diab, Ramon Salim (2017). Becoming-Infrastructure. Datafication, Deactivation, and the Social Credit System. *Journal of Critical Library and Information Studies* 1, 1, 1–23.

Gigerenzer, Gerd, Felix Rebitschek und Gert Wagner (2018). Eine vermessene Gesellschaft braucht Transparenz. *Wirtschaftsdienst* 98, 12, 860–866.

Kostka, Genia (2019). China's social credit system and public opinion. Explaining high levels of approval. *New Media & Society* 27, 7, 1–29.

Lee, Felix (2018). Social Scoring in China. Im Reich der überwachten Schritte. *taz* 10.02.2018. URL: https://taz.de/Social-Scoring-in-China/!5480926/ [Letzter Zugriff am 31.07.2019].

Liang, Fan, Vishnupriya Das, Nadiya Kostyuk und Muzammil Hussain (2018). Constructing a Data-Driven Society. China's Social Credit System as a State Surveillance Infrastructure. *Policy & Internet* 10, 4, 414–453.

Mac Síthigh, Daithí und Mathias Siems (2019). The Chinese Social Credit System. A model for other countries? *EUI Department of Law Research Paper*. Nr. 2019/1.

McKenna, Tony (2019). Behind the Black Mirror. The Limits of Orwellian Dystopia. *Critique* 47, 2, 365–376.

Ströbele, Caroline (2016). Black Mirror. Die Serie, die Trump voraussah. *Die Zeit* 23.11.2016. URL: https://www.zeit.de/kultur/film/2016-11/black-mirror-netflix-serie-rezension [Letzter Zugriff am 30.09.2019].

Melanie Seifert, Ann-Christine Strupp und Anne Schneider
Eberhard Karls Universität Tübingen
Institut für Medienwissenschaft
Wilhelmsstr. 50
D-72074 Tübingen
E-Mail: klaus.sachs-hombach@uni-tuebingen.de

Kleinere Texte zur Praxis der Überwachung

Zeitschrift für
Semiotik
Band 40 • Heft 1-2 (2018)
Seite 117-127
Stauffenburg Verlag Tübingen

Beobachten, wie die App uns beobachtet

Yunzhi Chen, Karolina Hess, Kristie Pladson und Corina Stratmeyer, Eberhard Karls Universität Tübingen

Unsere Welt gerät aus den Fugen – oder zumindest kann man leicht diesen Eindruck gewinnen. Wir alle stecken fest in einem Medienstrudel von Nachrichten über Klimaveränderung und Staatskrisen, in einer Arbeitswelt, die immer mehr für immer weniger verlangt. Das Gefühl des Kontrollverlustes greift um sich. Viele versuchen darum ein Stück Kontrolle zurückzugewinnen, wenigstens über sich selbst. Sie streben an, mehr Sport zu machen, weniger Zeit vor Bildschirmen zu verbringen und produktiver zu arbeiten.

So ist in den letzten Jahren ein Trend zur Selbstverbesserung entstanden. Parallel dazu bietet der Markt eine Menge kleine digitale Helfer auf, die das Wunschdenken zur Wirklichkeit werden lassen. Online finden sich unzählige kostenlose Apps, die den Nutzern bei der Selbstverbesserung zur Seite stehen. Klingt ganz uneigennützig, oder? Aber App-Entwickler müssen auch ihre Miete zahlen, und bekanntlich heißt es: „Wenn du etwas kostenlos bekommst, bist du das Produkt". Irgendetwas stimmt also nicht ganz.

Im Rahmen eines Seminars zum Thema Überwachung hat sich ein Kurs von Medienwissenschaftsstudierenden aufgemacht, die Welt dieser Apps zu erkunden. Eine Woche lang haben sie beobachtet und dokumentiert, wie eine bestimmte App ihr Leben beobachtet und dokumentiert. Sie haben nachgefragt, was dabei mit ihren Daten passiert, und überlegt, was das für unsere Gesellschaft bedeutet. Im Mittelpunkt stand die Frage, wer es ist, der am Ende die Kontrolle gewinnt. Hier sind drei ihrer Geschichten.

Neues Ziel: Konzentration!

Ein kleiner Setzling sprießt auf dem Bildschirm. Das erste Zeichen von Leben in einer neuen Welt der Konzentration und Produktivität. „Forest – Stay focused. Be productive on work & study", steht im Google Play Store geschrieben. Carina ist dabei, eine App zu testen, die ihr eine schlechte Angewohnheit abgewöhnen soll: das Handy immer in der Hand zu haben.

Bis zu vier Stunden am Tag schauen wir durchschnittlich auf unsere Smartphones. Mehr und mehr Menschen spüren eine Sucht nach dem kleinen Taschenhelfer. Manche Smartphone-Hersteller haben bereits Apps entwickelt, die ihren Kunden dabei helfen, ihre Bildschirmzeit zu erfassen und ihnen ein Stück Kontrolle über die Versuchung

zu geben. Es gibt Dutzende ähnliche Apps, wie *Brain Focus – Productivity Timer* oder *Productivity Challenge Timer*, die zum Download bereitstehen und Handysüchtigen beim ‚Clean-Werden' helfen sollen.

Bei *Forest* öffnet der Nutzer die App, um eine handyfreie Sitzung mit selbst festgelegter Länge zu starten. *Forest* pflanzt dann einen virtuellen Baum auf dem Handy. Die nächsten 10 bis 120 Minuten kann Carina dem Baum zusehen, wie er heranwächst. Warnung: Sollte sie die App schließen – egal ob um durch Instagram zu surfen oder eine dringende E-Mail zu beantworten –, stirbt der Baum. *Forest* fordert seine Nutzer heraus, das Handy auch mal wegzulegen. Die App will dich vor dir selbst schützen in den Momenten, in denen du ungebrochene Konzentration brauchst.

Wenn Carina durchhält, bekommt sie als Lohn einen voll ausgewachsenen digitalen Baum. Die Sitzungen und Bäume häufen sich mit der Zeit und führen zu einem wachsenden virtuellen Wald der Produktivität auf der Homepage der App. „Je härter du arbeitest, desto grüner wird dein Wald".

Die ersten Tage verlaufen perfekt. Carina ist motiviert und konzentriert. Sie verzichtet immer öfter auf ihr Smartphone und lässt einen Baum nach dem anderen sprießen. Die Sitzungen werden immer länger und kommen schon bald an die Zwei-Stunden-Grenze. Doch irgendwann kommt mitten in der Sitzung der dringende Wunsch zum Googlen auf. Sie zögert. Ihrem Sprössling zuliebe hält sie sich zurück und wartet. Die App hat über ihren Impuls gesiegt und Carina triumphiert. Doch am nächsten Tag bekommt sie eine dringende Nachricht und gibt nach. Während sie die App wechselt, bekommt sie eine transparente Mitteilung, die ihren Sprössling verdeckt. „Bist du sicher, dass du die App schließen willst? Das wird deinen kleinen Baum töten." Sie bestätigt. Ein kleiner, welker Zweig taucht auf dem Bildschirm auf. „Dein Baum ist aufgrund von Telegram gestorben, beim nächsten Mal wird es einfacher."

Wenn es nur ein nächstes Mal geben würde… Am Ende hat Carina alles aus der App herausgeholt. Langsam verliert *Forest* seinen Reiz. Sie hat alle Zeitziele erreicht. Sie hat den Tod eines Baumes überlebt, auch wenn ihr Baum es nicht tat. Und die Bonuspunkte, die *Forest* für jeden neuen Baum gewährt und die sie gegen neue Baumarten und Hintergrundmusik eintauschen kann, sind nicht weiter motivierend. Mehr kann und will die App offensichtlich nicht bieten. Carina fragt sich: Hätte die App ihr Verhalten auch ohne die ‚Geiselnahme' des Baumes ändern können?

Was denkt Foucault zu dem Thema?

Carinas Kommilitoninnen und Kommilitonen aus der Philosophie würden vermutlich auf Michel Foucault verweisen. Der französische Philosoph beschäftigte sich in seinem Buch *Überwachen und Strafen* intensiv mit der Welt der Selbstkontrolle. In diesem sagt er, dass die Kontrolle über die Menschen – ihr Denken und ihren Körper – einer der Hauptpfeiler der sozialen Ordnung ist. Am effektivsten funktioniert die Kontrolle, wenn der Mensch die Regeln verinnerlicht hat.

Nach Foucault gelingt dieses Verinnerlichen am besten mit Hilfe von Disziplinarmaßnahmen. In seiner Beschreibung des Panoptikums sieht das folgendermaßen aus: Der Kontrollierende, hier ein Wächter in einem Gefängnis, kann den zu Kontrollierenden immer beobachten und mögliches Fehlverhalten sofort bestrafen. Derjenige, der

kontrolliert wird, beispielsweise ein Gefangener, sieht den Wächter jedoch nicht. Er kann nicht nachvollziehen, wann und was genau beobachtet wird. Da er befürchten muss, unter ständiger Überwachung zu stehen, verhält er sich regelkonform, bis dieses Verhalten irgendwann zur Gewohnheit wird. Er kontrolliert sich nach einiger Zeit also selbst und von sich heraus.

Die App *Forest* übernimmt im Grunde die gleiche Funktion wie der Wächter. Sie überwacht Carina unaufhörlich und bestraft sie – mit dem Tod des Baumes – für ihr Fehlverhalten. Der einzige Unterschied besteht darin, dass Carina sich ihren Wächter selbst ins Haus gelassen hat und dass sie weiß, dass sie überwacht wird. Dennoch soll das gleiche Ziel erreicht werden: Die Regel, die Carina sich selbst aufgestellt hat, nämlich nicht mehr die ganze Zeit am Handy zu sein, wird durch die App umgesetzt.

Während man nun virtuell Holzfäller spielt, gibt man gleichzeitig persönliche Informationen wie Email-Adresse, Ort und Informationen über genutzte Apps ab. Diese Informationen nutzt der Wächter *Forest*, um sie an seine Kunden weiterzugeben. Nach einer Woche hat Carina einen Wald mit 54 Bäumen wachsen lassen, welchen sie schließlich ermüdend fand, während das Datenbiest wieder eine neue Mahlzeit gefunden hat auf seiner Jagd nach mehr Informationen. Diese Art der Informationen kann in den richtigen (oder falschen) Händen dazu genutzt werden, um Nutzer zu beeinflussen, so wie Foucault es beschreibt.

Der besorgte Überwacher

Eine tanzende Frau im Club. Ein Junge, der Videospiele spielt. Freunde, die beim Abendessen miteinander lachen. Ein junger, in Bücher versunkener Mann stellt uns die Frage: „Was würdest du mit einer Stunde extra am Tag tun?“

Die App *Smarter Time* verspricht Lisamarie eine Stunde mehr am Tag, um all das zu tun, was sie gerne tun möchte.

Es erinnert ein wenig an Goethes Faust. Lisamarie erlaubt *Smarter Time*, Informationen über alle ihre täglichen Aktivitäten zu sammeln. Im Ausgleich zeigt *Smarter Time* Lisamarie eine Übersicht, wie und mit was sie ihre Zeit verbringt. Von da aus kann sie Zeitfresser finden, eliminieren und ihre Zeit sinnvoller nutzen.

„Smarter Time lernt von allem“, erklärt die Webseite, „deinen Endgeräten, deinem Aufenthaltsort, deiner Eingabe, Sensoren, Apps“.

Nur mit ihrem Namen und einer E-Mail-Adresse lässt sich die App starten und das Lernen beginnt. *Smarter Time* folgt ihr überall hin, es zeichnet nicht nur ihr digitales Verhalten auf, sondern auch den Ort und die Zeit. Es sucht nach Daten, die Muster aufzeigen, um Lisamaries Routinen herauszufinden.

Dabei kommt es natürlich auch zu Fehlern. *Smarter Time* kann zwar sagen, dass sie sich an der Universität befindet, aber es kennt den Unterschied zwischen Unterricht und einem Kaffeeplausch nicht – zumindest nicht ohne Hilfe. Also fragt es wie ein eifersüchtiger verliebter Teenager, was Lisamarie gerade so macht. „Eigentlich muss ich also auch ein bisschen auf die App aufpassen, so wie sie auch auf mich aufpasst“, berichtet Lisamarie in ihrem Logbuch.

Langsam wird die App immer schlauer und bald schon kennt das Programm jede ihrer Bewegungen und Verhaltensweisen, welche es auch genau verzeichnet. Die Stunden,

die sie an Instagram verschwendet, lassen sie zusammenschrecken. Aber wie es so schön heißt: Die Wahrheit tut weh. Oder, um ein anderes Sprichwort zu zitieren: Wissen ist Macht, denn es gibt ihr die Chance, die verlorenen Stunden für sich zurückzufordern.

Doch im Gegensatz dazu ertappt sich Lisamarie dabei, wie sie zu ihrem PC schielt. Weil dieser von der App nicht erfasst ist, würde das die Statistik verbessern. Außerdem verursacht die dauerhafte Überwachung bei ihr ein Gefühl der Paranoia, umso mehr als sie herausfindet, dass *Smarter Time* nicht nur ihre Adresse kennt, sondern auch weiß, in welchem Raum sie sich befindet. Schlafzimmer? Es überwacht ihren Schlaf. Küche? Sie ist wohl am Kochen. Badezimmer? – Nun, das System ist klar.

Aber sie ist nicht die einzige, die sich über ihre Privatsphäre Sorgen macht. Auch *Smarter Time* ist besorgt. In bestimmten Momenten fragt *Smarter Time* nach, ob sie diese Aktivität wirklich aufzeichnen möchte. Die Erklärung der allgemeinen Geschäftsbedingungen sichern dem Hersteller die „Verarbeitung" der gesammelten Daten. Die Ausnahme sind dabei nur solche Aktivitäten, die als „secret" oder „sensitiv" deklariert wurden. Anders als der Rest ihrer Daten, welche in die Smarter Time-Cloud wandern, bleiben diese Informationen auf dem Smartphone.

Diese Sicherheitsmaßnahme aber hat einen gegenteiligen Effekt im Vergleich dazu, was damit vermutlich angestrebt war. Lisamarie schreibt: „Das macht mich stutzig. Es gibt also doch Momente, in denen man der App nicht vertrauen kann? Dabei werden die Daten ja nur zu meinem persönlichen Self-Improvement aufgezeichnet, oder? Sensible Daten muss ich selbst beschützen. Wenn ich beschließe, sie mit Smarter Time zu teilen, dann speichern sie sie auch ab."

Die Geschäftsbedingungen von *Smarter Time* brauchen 138 Wörter, um die Frage nach den persönlichen Daten und ihren unterschiedlichen Speicherorten zu klären. Um Daten nur auf dem Smartphone und nicht in der Cloud zu speichern, müssen die Aktivitäten von Lisamarie selbst als ‚geheim' gekennzeichnet werden. Sie kann sich dann entscheiden, ob sie ihre Daten mit *Smarter Time* teilt, sie als „geheim" deklariert oder ob sie die App überhaupt weiter nutzt. Was mit den „verarbeiteten" Daten passiert, ist nicht klar.

Das Programm nimmt sich das Recht heraus, die Informationen, die der Nutzer zur Verfügung stellt, für „statistische Zwecke" zu nutzen. Aber da der Anbieter um die Privatsphäre seiner Nutzer besorgt ist, verspricht er, dass jegliche Daten, die für kommerzielle Zwecke von Drittanbietern, also seinen Businesspartnern, verwendet werden, anonymisiert werden.

Statistische Zwecke? Drittanbieter und Businesspartner? Das kann ja nur heißen, dass die Daten weitergegeben und kommerziell genutzt werden. Wenn nicht, warum sollte man sich dann die Mühe machen es aufzuschreiben? Was das alles für Lisamarie und ihre Daten am Ende bedeutet, ist weniger offensichtlich.

„Was ich nicht weiß, macht mich nicht heiß."

Diese fehlende Klarheit zeigt: Die Welt der Selbstverbesserungs-Apps hat ein Problem mit der Transparenz. Eine Studie der Universität des Saarlandes aus dem Jahr 2016 zeigt gleich mehrere Probleme auf.

Den Nutzern zufolge fühlen sich 75 % unwohl dabei, ihre Gesundheitsdaten auf einer App zu speichern. Sehr hoch ist auch die Sorge bezüglich der Standortinforma-

tionen und finanziellen Angaben. Trotz dieser Sorgen gaben nur 47 % an, dass sie die Geschäftsbedingungen lesen. Forschern zufolge ist die Dunkelziffer, die einfach nur auf Zustimmen klickt, vermutlich viel größer, da viele diese Frage gar nicht beantworteten.

Das würde bedeuten, dass viele Nutzer nach dem Motto handeln: „Was ich nicht weiß, macht mich nicht heiß". Der Nutzen der App scheint also größer zu sein als das Sicherheitsbedürfnis – oder die Bereitschaft, sich mit dem Kleingedruckten auseinanderzusetzen.

Die Forscher haben sich für die Nutzer die Hände schmutzig gemacht und die Geschäftsbedingungen der acht Apps analysiert: Auch wenn man die Gefahr von Hackern immer im Hinterkopf hat (*MyFitnessPal* wurde beispielsweise im Jahr 2018 gehackt und musste rund 150 Millionen betroffene Nutzer darüber informieren), zeigte die Untersuchung vor allem, dass es unzählige legale Wege für Apps gibt, um Daten an andere Anbieter zu verkaufen – für Werbung oder möglicherweise an Krankenversicherungen oder Vorgesetzte, die ein Auge auf ihre Untergebenen haben wollen.

Die Apps werden zusätzlich vielleicht noch von anderen Firmen aufgekauft, ohne dass der Nutzer viel davon erfährt. Adidas kaufte 2015 beispielsweise die App *Runtastic* und erwarb so auch gleich alle Nutzerdaten. Für gesetzliche Maßnahmen müssen manche Apps ihre Daten auch abgeben.

Viele Teilnehmer der Studie glaubten nicht, dass die Apps, denen sie so viel anvertrauten, ihre Daten in dieser Weise weiterreichen würden, obwohl die Apps in ihren Angaben recht transparent sind. Hätte man nur die Geschäftsbedingungen gelesen, anstatt sie einfach wegzuklicken. Die Analyse förderte zutage, dass sich die Betreiber in der Regel verpflichten, ihre Nutzer über mögliche Änderungen zu informieren, manche hatten sich dafür allerdings eine kleine Hintertür eingebaut und sich das Recht im Voraus einräumen lassen. Diese Praxis ist beunruhigend, da es die Betreiber theoretisch dazu befähigt, die Daten an unterschiedlichste Geschäftspartner zu verkaufen, bevor der Nutzer überhaupt die Chance hatte seinen Account zu löschen.

Die Anonymisierung der Daten, welche eine App wie *Smarter Time* seinen Nutzern verspricht, imponiert den Forschern dabei wenig. Wenn man sich die Daten anschaut, die im Allgemeinen tagtäglich von uns erhoben werden, ist es keine große Schwierigkeit, die Puzzlestücke zusammenzusetzen. Um ein Datenprofil zu erstellen, braucht man keinen Namen, und wenn doch, ist es anhand des Datenhaufens einfach, die Person doch noch zuzuordnen. *Smarter Time* kann sogar die Anzahl der Räume in einem Haus und den genauen Aufenthaltsort weitergeben.

Als letztes warnen die Autoren auch davor – wie eingangs schon erwähnt –, dass Firmen diese Daten auch für die Beeinflussung von Nutzern verwenden könnten. Dieses Vorgehen gibt es bereits. 2017 berichtete die *New York Times,* wie das Beförderungsunternehmen Uber eine Kombination aus Daten und Kognitionswissenschaft nutzte, um seine Fahrer länger arbeiten zu lassen. Alle Uber-Fahrer sind eigentlich selbstständig und bestimmen somit auch ihre eigene Arbeitszeit. Um die Fahrer auf der Straße zu behalten, installierte die Firma eine Software in der App ihrer Fahrer, welche sie an ihr Lohnziel erinnerte und automatisch die nächste Fahrtanfrage annahm, während die aktuelle Fahrt noch im Gange war.

Ryan Calo, Rechtsprofessor an der Universität in Washington, beschäftigt sich damit, wie Firmen Daten nutzen, um Menschen zu beeinflussen. In der *New York Times* erklär-

te er, wie das Uber-System dieses Wissen nutzt: „Ihre Kontrolle über das Interface und die Bedingungen der Transaktion werden dafür genutzt, das Verhalten ihrer Fahrer so zu beeinflussen, dass sie das tun, was man von ihnen erwartet."

Smarter Time versprach Lisamarie eine Stunde mehr am Tag. Was sie bekam, hatte nur einen kleinen Effekt auf ihre Angewohnheiten, aber einen großen auf ihre Emotionen, mit wachsenden Schuldgefühlen und Angst vor Überwachung. Auch verbrachte sie ihre Zeit zunehmend damit, die App über jeden ihrer Schritte auf dem Laufenden zu halten und gewann so nie die versprochene Extrastunde. Währenddessen fand *Smarter Time* eine neue Seele, welche es auf dem Altar der Drittanbieter und Businesspartner darbringen konnte.

Die Gesundheits-App, nach der es dir schlechter geht

Seit vielen Jahren liebt Caroline schon das Joggen, da war es eine logische Wahl, eine Running-App zu installieren, die sich leicht in ihre Routine integrieren lässt.

„Endo ist eine Kurzform für Endorphine, die sich während des Sports bilden", erklärt die Webseite. „Mondo bedeutet ‚Welt' in Italienisch und Esperanto. Endomondo ist eine Welt der Endorphine!"

Endorphine sind körpereigene Opioidpeptide, sie wirken schmerzstillend und sind auch dafür verantwortlich, dass man nach körperlichen Betätigungen ein gutes Gefühl bekommt. Nicht die schlimmste Welt, in der man leben könnte.

Endomondo begleitet Caroline während ihrer Läufe auf ihrem Smartphone. Wie auch *Smarter Time* will die App sie erstmal kennen lernen. Sie greift auf die Standortinformationen zu, um ihre Rennstrecke aufzuzeichnen, ihre Geschwindigkeit, ihren Herzschlag und die verbrannten Kalorien auszurechnen. Sie speichert ihre Läufe und benachrichtigt sie, wenn sie ihren derzeitigen Rekord geschlagen hat. Genauso wie *Forest* stellt sie ihr eine Aufgabe. Sie kann sich Ziele setzen, spezielle Workouts abschließen, sogar in den Wettstreit mit anderen *Endomondo*-Nutzern treten oder ihre eigene Bestzeit herausfordern – ein großer Haufen neuer Dienste für die Hobbyläuferin.

Eines Montagnachmittags wird der Lauf, der eigentlich dabei helfen sollte, den Kopf wieder frei zu kriegen, zu einem verzweifelten Versuch, den Rekord vom Vortag zu brechen. Caroline treibt ihren Körper immer weiter, aber umsonst. Die Caroline vom Montag verliert gegen die Caroline vom Sonntag. Geschlagen kehrt sie von ihrem Lauf zurück. Das ist nicht das Hobby, das sie kennt und liebt. Die Freude, die Caroline am Sonntag durch den Bericht von *Endomondo* über einen persönlichen Rekord gespürt hat, führt schließlich dazu, dass sie den Spaß an ihrem Hobby verliert. Psychologen nennen das den „Korrumpierungseffekt".

Er lässt sich wie folgt beschreiben: Wenn jemand eine externe Belohnung, wie Geld oder Lob, für eine Leistung bekommt, die man ohnehin gerne macht, findet man die Handlung weniger erfreulich. Die Belohnung misst der Handlung nur von außen einen Wert zu. Die intrinsische Motivation nimmt ab und koppelt sich gewissermaßen an die Belohnung eines Anderen. Am Ende ist die Belohnung kein nettes Extra, sondern eine Notwendigkeit, um sich überhaupt für die Handlung zu motivieren.

Genau das passiert Caroline mit *Endomondo*. Den Spaß am Laufen ersetzt die App durch ein Gieren nach der Belohnung – in diesem Fall nach einer neuen Bestzeit. Das Laufen wird etwas, das nur aus Erfolgswillen weiter betrieben wird und nicht für das gute Gefühl.

Wenn sie mal nicht joggen geht, wird sie von der App erinnert. Sie sollte doch gerade laufen. Auf dem Bildschirm ihres Handys liest sie: „Du willst doch nicht, dass der ganze Zucker auf deiner Hüfte bleibt!" Wie ein erhobener Zeigefinger in Form von Body-Shaming weist die Push-Nachricht sie darauf hin, wieder zu den Sportschuhen zu greifen. Verärgert wischt sie über das Display, um die Nachricht loszuwerden.

Diese tonlose Kommunikation lässt die kalte Neutralität dieser datengenerierenden App für einen kurzen Moment erkennen – und den sonst verborgenen Anbieter, der dahintersteckt. In diesem Fall sammelt die App für einen amerikanischen Sportmode-Giganten Under Armour, einen Konkurrenten von Nike und Adidas, Daten über das Laufverhalten ihrer Nutzer. *Endomondo* bietet, zusätzlich zu der Ernährungs-App *MyFitnessPal*, nützliche Dienste für ihre Zielgruppe an, die auch für das Unternehmen hilfreich sind.

Jetzt schaut Caroline ständig auf ihren Bildschirm und passt die Geschwindigkeit ihrer Schritte an die Grafik an, die sie auf dem Bildschirm in den blauen und grünen Liniendiagrammen sieht. Die Grafik verdeutlicht aber auch all jene Daten, die über das Fitnessleben dieser potenziellen Kundin gesammelt und direkt an Under Armour übermittelt werden.

Der Lauf der Gesundheitsdaten

Ein wenig Recherche zeigt zudem, dass Under Armour die Kundendaten aus der App an Facebook verkauft. Auch wenn ein solches Verhalten zu erwarten ist, sollte der Handel mit persönlichen Gesundheitsinformationen eine rote Linie darstellen, insbesondere wenn Krankenkassen in die Welt der Gesundheits-Apps einsteigen.

Diese Bedenken werden von Anne geäußert, einer Kommilitonin, die eine solche App getestet hat. Die Techniker Krankenkasse (TK) hat vor kurzem eine App eingeführt, die bürokratische Prozesse rationalisieren und ihren Kunden neue Dienste anbieten soll. Das Unternehmen präsentiert sich dabei zunächst als besonders datenschutzbewusst, wie dies von einer Krankenkasse auch erwartet werden kann. Nutzer können sich sogar per Post für die App registrieren (dass Annes ursprünglicher Registrierungsbrief in der Post verloren gegangen ist, ist eine andere Geschichte).

Einmal registriert, bietet die App eine Handvoll nützlicher Dienste, etwa die Übermittlung von Krankmeldungen und die Einreichung von Kosten für Impfungen und Osteopathie. Außerdem bietet sie ein neues Bonusprogramm. So kann Anne gesunde Gewohnheiten wie die Verwendung eines Schritt- oder Kalorienmessgeräts per App aufzeichnen und erhält dafür Punkte von der Versicherungsgesellschaft, die gegen Ermäßigungen für Fitnesskurse, Zahnreinigungen und andere Gesundheitsleistungen eingelöst werden können.

Seltsamerweise ist die *TK-App* jedoch nicht mit der Technologie ausgestattet, um Dienste wie Schritt- oder Kalorienzähler selbst bereitzustellen. Kunden, die dieses Prämiensystem nutzen möchten, werden stattdessen auf Apps von Drittanbietern wie *Endomondo* verwiesen, was den Datenschutz für ihre Gesundheitsdaten wesentlich beeinträchtigt.

Gesundheitsdaten von Dritten fernzuhalten ist nicht das einzige Problem, das an der Schnittstelle von Fitness-Apps und Gesundheitsvorsorge zu finden ist. Schriftstellerin und Datenschutzaktivistin Juli Zeh bringt diesen Gedanken in ihrem 2009 veröffentlichten Roman *Corpus Delicti: Ein Prozess* auf den Punkt. Die Geschichte spielt in einer Zukunft, in der es verboten ist, ungesund zu leben. Rauchen und Trinken sind untersagt, Sport ist Pflicht und der Staat nutzt ein kompliziertes Netz an Überwachungstechnologien, um dies alles nachzuverfolgen. Die zentrale Frage des Romans ist: Was passiert, wenn eine Gesellschaft, die frei von Gebrechen sein will, sich zu einer transformiert, in der Gebrechlichkeit verboten ist? Die Frage trifft den Nerv der Zeit in einer Gesellschaft, die körperliche Fitness und Selbstverbesserung beständig einfordert. Zehs dystopische Fantasie will nicht nur unterhalten, sondern auch die Gefahren eines blinden Bejahens derjenigen Technologien aufzeigen.

Die Techniker Krankenkasse ist eine gesetzliche Krankenkasse. In den Händen einer privaten Krankenversicherung jedoch könnten die intimen Gesundheitsdaten, die von dieser und ähnlichen Apps erhoben werden, zur Verweigerung des Versicherungsschutzes genutzt werden. Es ist fraglich, welche Rolle es überhaupt spielt, wie sorgsam Krankenversicherer mit den selbsterhobenen Gesundheitsdaten ihrer Kunden umgehen, wenn sie doch bereits diejenigen sind, in deren Händen sie den größten Schaden anrichten können? Und was, wenn Apps wie *Endomondo* sie an den Meistbietenden versteigern?

Zurück zu unserer Joggerin: Was Caroline betrifft, so ist sie froh, als die Testwoche vorbei ist und sie ihr Hobby wieder wie früher ausüben kann. Ihre Gefühle werden nicht länger von ihrer Geschwindigkeitsstatistik gefangen gehalten. Die Welt der Endorphine hatte sich als eine Welt des Stresses herausgestellt; eine, die – wie auch die beiden ersten Apps – weit mehr von ihr einforderte, als sie ihr gab.

Die Ironie des Selbstversuchs (und der Selbstoptimierungs-Apps)

Die Erfahrungen der Studierenden waren durchweg eher negativ. Wie ist dies – die zufällige Einschätzung einer Gruppe von Studierenden, die sich im Rahmen eines Seminars über digitale Überwachung verpflichteten, die Apps zu testen – mit den Reaktionen der Millionen Nutzer zu vergleichen, die diese Apps heruntergeladen, genutzt und begeistert bewertet haben?

> „Simple to use, extremely versatile. Loved having the extra motivation in my ear." *Endomondo*-User

> „I love this app. I always know who when and where. Very healthy to see for yourself how you spend your time." *Smarter Time*-User

> „Guilt is a powerful motivator. I feel extremely guilty if I do anything else except study when a tree is growing. Five stars." *Forest*-User

Vielleicht ist die Ironie der Geschichte nicht, dass die Apps scheinbar das Gegenteil dessen leisten, was sie versprechen. Vielmehr ist es die Art und Weise, wie sich Apps

und Tester im Rahmen der Selbstversuche in einem Kreislauf des Testens und Überwachens gegenseitig beobachtet und dokumentiert haben, mit dem Ziel, die Schwächen des Anderen aufzudecken.

Die Natur des Selbstversuchs versetzt den Forscher und seinen Gegenstand in die seltsame Position, ein- und derselbe zu sein. Dass das Beobachten seiner selbst im Zustand der Beobachtung durch eine App anders ist als die Wahrnehmung eines Nutzers, der schlicht ein Optimierungsziel hat und zu seiner Erreichung ein Werkzeug verlangt, ist wohl wenig überraschend.

Ganz unabhängig von dieser Frage des persönlichen Wahrnehmens und Erlebens bleibt aber die Tatsache bestehen, dass Selbstverbesserungs-Apps eine nie dagewesene Menge an Daten über die intimsten Lebenssphären produzieren. Mobile Apps sind Programme und als solche nur fähig, die für sie vorgesehene Aufgabe zu erfüllen – einen digitalen Wald zu pflanzen oder zu messen, wie schnell man von A nach B gelangt. Dennoch haben die persönlichen Daten, die in diesem Prozess abfallen, endlose Verwertungspotenziale, wie Uber schon zeigt.

Die Frage (und Antwort darauf) ist also komplexer, als nur die nach einem schlichten Daumen-hoch oder -runter für Selbstverbesserungs-Apps. Vielmehr gilt es zu fragen, was sie mit der Menschheit machen, mit der Demokratie, mit unserer Freiheit. Bleibt noch genügend Zeit, über diese Entwicklung zu reflektieren? Oder befinden wir uns unbewusst bereits auf dem Weg in ein Kontroll-Regime? Wie können wir dies verhindern?

Und wo ist die App, die uns d a b e i hilft?

Yunzhi Chen, Karolina Hess, Kristie Pladson und Corina Stratmeyer
Eberhard Karls Universität Tübingen
Institut für Medienwissenschaft
Wilhelmsstr. 50
D-72074 Tübingen
E-Mail: klaus.sachs-hombach@uni-tuebingen.de

Zeitschrift für
Semiotik
Band 40 • Heft 1-2 (2018)
Seite 127-134
Stauffenburg Verlag Tübingen

Rezensionen und Kritiken

Die geheimdienstähnlichen Methoden der Unterhaltungsindustrie

Anne Diessner

Die erste Staffel der US-amerikanischen Serie *UnREAL* blickt hinter die Kulissen von Reality-TV und offenbart ein System aus Manipulation, Intrigen und Grenzüberschreitungen.

Dass Dating-Sendungen wenig mit der tatsächlichen Suche nach der großen Liebe zu tun haben, ist dem Fernsehpublikum meist bewusst. Zu welch fragwürdigen Methoden der Manipulation und Überwachung mitunter bei der Produktion gegriffen wird, dürfte dagegen schockieren. In *UnREAL* kehrt die Produzentin Rachel Goldberg (Shiri Appleby) nach einem Nervenzusammenbruch zurück ans Set von *Everlasting*, einer fiktiven Dating-Show nach dem Prinzip des *Bachelor*. Das Produktionsteam um die ausführende Produzentin Quinn King (Constance Zimmer) sorgt hier mit allen Mitteln dafür, dass die Einschaltquoten stimmen. Rachel mit ihrem Gespür für gute O-Töne und einem ausgesprochenen Manipulationstalent ist dabei Gold wert. Der Rest des Teams ist allerdings nicht gerade begeistert von der Rückkehr der labilen Rachel – Konflikte sind vorprogrammiert. Außerdem hat Rachel immer wieder Gewissensbisse angesichts ihrer schamlosen Manipulationen…

In der Drama-Serie von Marti Noxon und Sarah Gertrude Shapiro, die mittlerweile vier Staffeln umfasst und in Deutschland seit 2016 bei Amazon Prime Video zu sehen ist, manifestiert sich in verblüffender Weise ein Foucault'sches Machtgefüge. Im *Everlasting*-Filmset werden die beiden zentralen Merkmale der Disziplinargesellschaft aus der Theorie des französischen Philosophen sichtbar: produktive Disziplinierung und panoptische Überwachung. Disziplin funktioniert dabei durch die Kombination von drei Voraussetzungen: Zum einen werden die Individuen nach Wertigkeiten klassifiziert – gut zu erkennen, wenn die Kandidatinnen auf stereotype Rollen wie ‚Jungfrau' oder ‚Intrigantin' reduziert werden. Zum anderen ist die Zeit strikt eingeteilt, und schließlich gibt es eine streng hierarchische Befehlskette, die nicht hinterfragt wird. Das Filmset bildet so einen abgeschlossenen Kosmos mit allgegenwärtiger Überwachung. Jeder Schritt wird von sichtbaren und unsichtbaren Kameras eingefangen, Mikrofone zeichnen jedes Wort auf, über Funkgeräte sind jederzeit Anweisungen möglich. Nicht einmal die Vergangenheit ist sicher vor der Filmcrew: Die Kandidatinnen sind so gründlich durchleuchtet worden, dass psychische Erkrankungen, Traumata und andere Geheimnisse ans Licht kommen – und früher oder später gegen sie verwendet werden.

Der schonungslose Blick auf die geheimdienstähnlichen Methoden der Unterhaltungsindustrie wirkt dabei selten überzeichnet, sondern eher schockierend realistisch. Dies rührt sicherlich daher, dass die Serie auf wahren Begebenheiten beruht. In *Sequin Race*, einem Kurzfilm von Sarah Gertrude Shapiro, verarbeitet die Produzentin ihre

Erfahrungen am Set von *Der Bachelor*. Es kommt daher wohl nicht von ungefähr, dass in *UnREAL* die Unterscheidung von Überwachern und Überwachten nicht so leicht fällt. Denn gerade das Produktionsteam ist geprägt von hierarchischen Machtstrukturen, Konflikten, Manipulationen und ständiger Beobachtung.

Ging es bei Foucault noch um die Herstellung von Konformität, ist im Unterhaltungsfernsehen das Gegenteil erwünscht: Je skandalöser, intimer, nicht-konformer das Verhalten, desto besser. So wird aus dem überwachenden Blick ein voyeuristischer. Charakteristisch dafür ist die letzte Szene der ersten Folge: Rachel sitzt vor mehreren Monitoren, auf die die Bilder von Überwachungskameras übertragen werden. Zu sehen sind die Zimmer der Kandidatinnen: Eine meditiert, eine andere erbricht sich, eine dritte hat Sex – Situationen, die normalerweise privat sind und bleiben sollten. Die Kamera nimmt Rachels Perspektive ein, sodass der Zuschauer selbst zum Voyeur wird – eine präzise Metapher für die Funktionsweise von Reality-TV.

UnREAL wirft einen zynischen Blick hinter die dunklen Kulissen des Reality-TV. Trotz ernsthafter Thematisierung der fragwürdigen Methoden am Set gelingt es den Machern, einen satirischen Ton anzuschlagen und so gute Unterhaltung zu bieten. Der Zuschauer bleibt schließlich mit der Hoffnung zurück, dass die Realität der Fernsehindustrie nicht ganz so abgründig ist.

Marti Noxon und Sarah Gertrude Shapiro (USA, Lifetime, seit 2015): UnREAL. Staffel 1. In Deutschland verfügbar auf Amazon Prime Video.

Überwachung ist kein Allheilmittel

Carina Konopka

Die US-amerikanische Fernsehserie *The Wire* ist meisterhaft authentisch. Eine geschickte Überwachungstaktik soll den Drogenkönig Baltimores mattsetzen und den ‚War on Drugs' vorantreiben.

D'Angelo Barksdale (Larry Gilliard Jr.) erklärt zwei jungen Männern die Regeln des Schachs. Die Bedeutung der Szene reicht tiefer, als es auf den ersten Blick erscheinen mag: D'Angelo ist der Neffe des berühmt-berüchtigten Drogenbosses Avon Barksdale (Wood Harris), die jungen Männer sind Dealer seiner Bande. Die Schachfiguren symbolisieren in ihren Funktionen die innere Struktur des mächtigsten Drogenrings von Baltimore. Auf der gegnerischen Seite kämpft die Anti-Drogen-Spezialeinheit der Polizei rund um James „Jimmy" McNulty (Dominic West) für ihren ‚König': die Justiz beziehungsweise die Rechtsstaatlichkeit.

Die HBO-Serie, die 2002 erstausgestrahlt wurde, verbindet die Drogenproblematik mit dem Thema Überwachung auf höchst realistische und reflektierte Weise. Sie stellt Überwachung als notwendiges Mittel der Polizeiarbeit dar und hinterfragt gleichzeitig deren Wirksamkeit. Die Überwachungsmaßnahmen der Polizei involvieren Operationsketten aus technischen und menschlichen Akteuren. Ihr Einsatz intensiviert sich über die Episoden hinweg. Die Ermittler versprechen sich mittels Beschattungen, Fotografien, Überwachungsvideos und Spitzeln hilfreiche Informationen über den Drogenring zu gewinnen. Sorgfältig sammeln sie die Puzzleteile ihrer Ermittlungen auf einer Pinnwand im Revier.

Die Deutung der verschiedenen Hinweise stellt sich jedoch als schwierig heraus. *The Wire* idealisiert den Einsatz von Überwachungstechnik also nicht. Auch das Scheitern und die zahlreichen hilflosen Versuche der Polizei trotz der Überwachung werden ausführlich thematisiert. Wirkt das ermüdend auf die Zuschauer oder macht das eben den Reiz der Serie aus? Fakt ist, dass die Polizisten eben nicht die erwarteten Superhelden sind und technische Methoden mit dem Menschen als Anwender und Zeichendeuter an ihre Grenzen stoßen. Passend dazu sind die Handlungsstränge der Polizisten auf komplexe Weise mit denjenigen der Drogengangster verwoben.

Diese sind sich der ständigen Überwachung bewusst. Nach dem foucaultschen Panopticon führt das Bewusstsein einer potenziell permanenten Überwachung zur Internalisierung des Machtverhältnisses. Um Sanktionen zu vermeiden, passen die Überwachten ihr Verhalten den vorgegebenen Normen an. In *The Wire* versuchen die Gangster, sich dem Zugriff der Polizei auf kreative Weise zu entziehen. Einer dieser Wege ist der Einsatz von codierten Pagern und Münztelefonen als Kommunikationsmittel. Die erwünschte Regelkonformität der Gangster im Sinne eines Unterlassens des Drogenhandels bleibt damit aus, und das Konzept des Panopticon ist nicht vollständig anwendbar. Es verdeutlicht jedoch die herrschenden Machtbeziehungen in der Serie. Dass das Schachspiel gegen den Drogenring keine einfache Partie ist, zeigt sich auch daran, dass die Polizei viele bürokratische und technische Hürden überwinden muss, um die Überwachungsarbeit auch auf die besagten Kommunikationsmittel der Barksdale-Bande ausweiten zu dürfen: Damit sie das Material vor Gericht verwenden können, müssen die Polizisten jedes angezapfte Telefon zusätzlich vor Ort mit dem Fernglas beobachten.

The Wire-Schöpfer David Simon und Ed Burns beschönigen die Realität in ihrer Serie also nicht, sondern stellen sie so dar, wie sie ist – brutal, bürokratisch und unberechenbar. Ihr Wissen schöpfen sie aus ihren persönlichen Berufserfahrungen in Baltimore. Die Zuschauer dürfen mit *The Wire* von diesem Erfahrungsschatz profitieren und sich auf eine Serie von Qualität und Tiefe freuen, die nicht dem Gut-gegen-Böse-Schema typischer Polizeiserien folgt. Vielmehr macht die Serie den Zuschauern klar, was polizeiliche Überwachungsarbeit tatsächlich bedeutet. Überwachung ist kein Allheilmittel, das zwangsläufig schnell zu einem ‚guten' Ende führt. Wie in einem Schachspiel ist jeder Zug vom Gegenzug abhängig – und eine Partie kann sich lange hinziehen. Die Zukunft der ‚Könige' bleibt in der von Armut, Drogenkriminalität und Zerfall geprägten postindustriellen amerikanischen Großstadt jedenfalls bis zum Schluss spannend.

David Simon, Robert F. Colesberry und Nina Kostroff Noble (USA, HBO, 2002): The Wire. Staffel 1. In Deutschland auf DVD oder online erwerbbar.

Das Problem mit dem perfekten System

Marius Lang

Eine Welt ohne Mord und Totschlag: Das klingt zu schön, um wahr zu sein. Mit *Minority Report* liefert Steven Spielberg seine effektgeladene Vision einer solchen Welt, in der dann doch nicht alles so perfekt ist, wie es scheint.

Wie würde sich die Gesellschaft ändern, wenn wir Verbrechen verhindern könnten, bevor sie passieren? Wenn wir in die Zukunft sehen könnten, wäre die Welt dann eine bessere? In Steven Spielbergs Film *Minority Report* von 2002 ist dies mehr als nur eine Fantasie. Die Polizeiabteilung Precrime im Washington D.C. des Jahres 2054 macht es möglich. Ihre Geheimwaffe: Drei hellseherische Menschen, die katatonisch in einem Wasserbad vor sich hinvegetieren. Sie sind die sogenannten Precogs, Agatha, Arthur und Dashiel. Nicht umsonst sind sie nach berühmten Kriminalautoren benannt. In ihren Wachkomas sehen sie die Zukunft. Erst wenn sie alle gleichzeitig eine Vision haben, wird ein Mord geschehen. Precrime-Chef John Anderton (Tom Cruise) und sein Team haben somit die Mordrate in Washington auf Null heruntergebracht.

Nun soll Precrime landesweit ausgedehnt werden. Doch zunächst muss das System natürlich geprüft werden, durch Agent Witwer vom Justizministerium (Colin Farrell). Für ihn ist klar, ein System kann noch so perfekt sein, der Mensch ist es nicht. Da kann Anderton noch so viele Morde verhindern.

John Anderton ist schließlich auch eine schwierige Persönlichkeit. Dass ein derartig gebrochener Mann Leiter einer so wichtigen Spezialeinheit ist, wirkt beinahe unglaubwürdig. Nachdem sein Sohn Jahre zuvor umgebracht wurde, ging Andertons Ehe in die Brüche, er selbst ist drogenabhängig. Witwer traut ihm nicht, und dass er dazu allen Grund hat, liegt auf der Hand. Als die neueste Vision der Precogs dann auch noch voraussagt, dass John selbst in den nächsten 36 Stunden zum Mörder wird, wird Anderton selbst vom Jäger zum Gejagten. John entführt Agatha, eine der Precogs, und versucht mit ihrer Hilfe, seine zukünftige Unschuld zu beweisen.

Minority Report basiert auf einer Geschichte von Science-Fiction-Autor Philip K. Dick. Das Thema des Filmes ist dabei ein überraschend zeitgemäßes, vor allem in einer Welt nach 9/11. Spielberg stellt die Frage, was totale Überwachung bringt, wie weit Überwachung gehen darf und wie perfekt ein Überwachungssystem sein kann. Das Ergebnis ist ein effektreicher, optisch beeindruckender und thematisch hochinteressanter Actionthriller.

Die Ethik des Filmes lässt sich dabei in zwei Ebenen unterteilen. Zum einen ist da die Kritik am scheinbar perfekten Überwachungssystem. Einem System, das eben doch keine absolute Sicherheit garantiert und in dem Menschen für schlimmste Verbrechen bestraft werden, ohne diese je begangen zu haben. Precrime ist ein riesiges Panopticon, in dem alle Bewohner Washingtons rund um die Uhr überwacht werden. Auf den Bildschirmen in der Zentrale der Spezialeinheit sind einzelne Eindrücke der Precogs zu sehen, die die intimsten Momente im Leben namenloser Bürger zeigen. Diese Bürger können ihre Wächter selbst nicht sehen, nein, sie wissen nicht einmal, dass sie überwacht werden. Dies wird durch eine Szene am Anfang des Films deutlich gemacht, in der ein werdender Mörder festgenommen wird und daraufhin überrascht und entgeistert reagiert.

Die Bewohner Washingtons sind auf den Bildschirmen und in den Köpfen ihrer Wächter ebenso entmenschlicht wie die Precogs selbst, die geistesabwesend in ihren Wasserbädern herumdämmern und nicht mehr sind als ein Teil der Überwachungsmaschinerie. Ihr Dilemma verdeutlicht die andere Ebene, auf der sich die Ethik des Filmes bewegt. Wie kann man die Nutzung menschlichen Lebens für derartige Zwecke rechtfertigen? Eine Antwort liefert der Film leider nicht.

Eine klarere Antwort findet man hingegen auf die Frage, ob wir unseren Überwachern wirklich trauen können. „Quis custodiet ipsos custodes“, wie schon in Juvenals Satiren gefragt wurde, wer überwacht die Wächter? Und was ist, wenn wir dieser Instanz auch nicht trauen können? Andertons Situation, in der er sich selbst als Opfer einer Verschwörung wiederfindet, zeigt diese Problematik sehr deutlich. Ebenso wenig können wir aber unseren Augen trauen. Dies ist ein weiterer Aspekt, der in dem Film eine große Rolle spielt, nämlich wenn der Unterschied zwischen realen Bildern und optischen Täuschungen und Illusionen zum Tragen kommt.

Wo Spielbergs Film gegenüber seiner Vorlage leider etwas schwächer abschneidet, ist in den emotionalen Aspekten der Geschichte. Spielbergs Stärken sind bekanntlich die großen Emotionen und sprichwörtlichen Happy Ends. *Minority Report* jedoch hätte durchaus mehr von Dicks düsterer, zynischer Weltsicht vertragen können. Doch zumindest ist alles gut anzusehen. Cruise spielt gewohnt solide, sein Anderton ist ein glaubwürdiger, gebrochener Mann auf der Flucht vor einem Monster, das er selbst erschaffen hat. Über einige Schwächen im Drehbuch kann man da getrost hinwegsehen und mit diesem Film einen spannenden Abend erleben, wenn auch mit einigen Längen.

Steven Spielberg (USA, 20th Century Fox u.a., 2002): Minority Report, 145 min.

Menschwerden im totalitären Überwachungsstaat

Caroline Ganzert

Der Nachwende-Film *Das Leben der Anderen* ist ein wahres Glanzstück deutscher Filmgeschichte. Eine kulturpolitische Erzählung vom linientreuen Stasi-Hauptmann Wiesler, der während eines Überwachungsauftrags seine menschliche Seite entdeckt.

Eine einzelne Träne läuft ihm über das reglose, ernste Gesicht. Stasi-Spitzel Wiesler (Ulrich Mühe) sitzt in seiner Überwachungszentrale und lauscht Dramatiker Georg Dreymans (Sebastian Koch) emotionalem Klavierspiel. Eine Schlüsselszene, die den Wandel Wieslers ankündigt. Die Kunst fungiert hier als Stimulus für Wieslers Menschlichkeit. Führte er zu Beginn noch den Überwachungsauftrag seines Vorgesetzten Anton Grubitz (Ulrich Tukur) gewissenhaft aus, wühlte sich ohne Mitgefühl in den Alltag des vermeintlich regimefeindlichen Künstlerpaares, hörte sämtliche Gespräche und Intimitäten mit und notierte akribisch jedes einzelne Wort, so beginnt er nun vorsichtig, das Leben der Anderen zu berühren. Nach und nach fängt er an, den Künstler vor der repressiven Stasi zu schützen. Dieser Wandel vom gefühllosen, überkorrekten und linientreuen Stasi-Mann zum mitfühlenden Menschen vollzieht sich so fließend, dass der Zuschauer nach eineinhalb Stunden Film noch nicht weiß, auf welcher Seite Wiesler steht. Eine gelungene Gratwanderung zwischen Gut und Böse, die brillant inszeniert und gespielt ist.

Eindrucksvoll und in zugleich nüchternem Erzählduktus zeigt der Film den mächtigen Überwachungsapparat der Stasi. Präzise verwanzen Wiesler und seine Männer Dreymans Wohnung. Als die Nachbarin sie dabei beobachtet, droht Wiesler, dass ihr Sohn seinen Medizinstudienplatz verliere, falls sie nur ein Wort verrate. Überwachung

ist hier das Instrument zur totalen Kontrolle und dient der Sicherstellung der Linientreue. Wer aus der Reihe tanzt, ist bald in Hohenschönhausen. So finden sich im Film Parallelen zu George Orwells Roman *1984*, der diesen dunklen Teil der deutschen Geschichte scheinbar bereits vorhergesehen hat: Niemand kann sich der Überwachung entziehen. Sogar untereinander bespitzeln sich die Agenten. Wer sich unpassend verhält, verschwindet einfach – die Stasi operiert wie die Orwell'sche Gedankenpolizei. Die permanente Überwachung manifestiert sich bei Orwell durch sogenannte Teleschirme. Diese verwandeln sich im Film gewissermaßen in Abhörsysteme: Dreyman und seine Künstler-Freunde wissen nie, ob sie gerade abgehört werden oder nicht. Wiesler fungiert als omnipräsenter Überwacher, der alles über die Überwachten weiß, während diese nicht einmal von seiner Existenz wissen. So konstituieren sich hier auch Züge von Foucaults Panopticon. Kaum verwunderlich, dass der Titel von Foucaults Buch *Überwachen und Strafen* der Einstellung der Stasi durchaus nahe kommt.

Für den Film ist jedoch auch der Faktor Mensch von erheblicher Bedeutung. *Das Leben der Anderen* macht dem Zuschauer mit Wieslers Wandel ein besonderes Angebot. Diese Wandlung zum Menschen ist das Schlüsselmotiv des Klassikers und gleichzeitig möglicher Kritikpunkt: In einem Orwell'schen totalitären Überwachungsstaat ist ein derartiges Szenario nicht vorgesehen. Entgegen der Erwartungen zeigt der Film keine Dystopie. Wiesler als neuer Mensch lässt sogar Gegensätze verschwimmen: Regisseur Florian Henckel von Donnersmarck lässt grau gekleidete Stasi-Männer, düstere Büros und Plattenbau auf den kreativen Künstler in seiner Altbauwohnung treffen. Künstlerischer Freigeist und Leidenschaft stoßen auf Wieslers Einsamkeit, der diese durch die ferne Teilhabe am Leben der Anderen zu kompensieren versucht. Nach und nach jedoch bewegt er sich aus seinem grauen Umfeld auf die bunte Künstler-Welt zu. Fraglich aber ist, ob das Bild des empathischen Stasi-Manns innerhalb des totalitären Überwachungskonstrukts realistisch ist. Macht der Film es sich zu leicht, oder dem Zuschauer ein gelungenes Identifikationsangebot?

Das Leben der Anderen beschwört im Jahr 2005 einen dunklen Teil deutscher Geschichte und trägt damit zur Vergangenheitsbewältigung bei. Gleichzeitig wirft der Film die Frage auf, ob sich Züge des totalen Überwachungsapparates auch heute wiederfinden. Diese Frage lässt sich auch kritisch im Hinblick darauf formulieren, dass wir heute ständig kleine ‚Teleschirme' bei uns tragen.

Florian Henckel von Donnersmarck (D, 2005): Das Leben der Anderen. Verfügbar u.a. auf Netflix.

Einer sieht alle

Lena Füller

Die spanische Serie *Haus des Geldes* (*La casa de papel*) zeigt eine verbotene Meisterleistung: Der spektakulärste Banküberfall Spaniens entführt nicht nur Geiselnehmer und Geiseln in eine Welt der Überwachung, sondern auch Polizei und Geheimdienst.

Ein Kammerspiel über 22 Folgen: Alle Episoden der erfolgreichen Krimi-Serie spielen in der spanischen Banknotendruckerei. Diese wird von einer Verbrecherbande überfallen, eingenommen und durch Geiselnahme verteidigt. Polizei und Geheimdienst raufen sich unter Zeitdruck die Haare, um der gewitzten Bande den Weg in die millionenschwere Freiheit abzuschneiden. Währenddessen beobachtet der sogenannte ‚Professor' und Kopf der Bande (Álvaro Morte) durch seine Überwachungskameras vom Schreibtisch das Geschehen im Inneren der Banknotendruckerei.

Schon Monate zuvor hat er die Sicherheitskameras in der Druckerei anzapfen lassen und ihr Signal in sein Versteck außerhalb des Gebäudes umgeleitet. Angespannt reibt er sich die Hände, ähnelt einem Manager vor der Abgabe eines großen Projekts. Er zoomt mit der Kamera näher heran: Unter den Ärzten, die wegen eines medizinischen Notfalls die Druckerei betreten, erkennt er einen eingeschleusten Undercover-Polizisten. Die Situation ist brenzlig, doch jedes Detail des Überfalls ist durchdacht und einstudiert: Der Polizist wird zum trojanischen Pferd, als es den Verbrechern unbemerkt gelingt, seine Brille zu verwanzen. „Wenn die Polizisten versuchen einzudringen und glauben, dass sie die Schlacht für sich gewinnen, werden wir es machen wie die Griechen," hat der Professor vorher festgelegt. Abermals ist der raffinierte Professor der Polizei einige Schritte voraus.

Álex Pina ist die Regisseurin der Erfolgsserie. Sie nimmt bei der Inszenierung des Überfalls virtuos Anleihen an Actionfilm und Liebesdrama. Durch eine gekonnte Verflechtung verschiedener Überwachungsinstrumente und -praktiken entsteht ein Netz der gegenseitigen Kontrolle zwischen Geiselnehmern, Polizei und Geheimdienst, welches in den Händen des Professors zusammenläuft. Er scheint wortwörtlich alles im Blick zu haben.

Benthams Idee des Panopticon und eine Variation von Steve Manns Sousveillance treffen hier aufeinander. Dieses Zusammenspiel wirkt wie ein Panopticon 2.0, ein neues Level der Überwachung etabliert sich. Da gibt es die Überwachungskameras im Inneren der Banknotendruckerei, mit deren Hilfe der Professor jederzeit sehen kann, was vor sich geht. Er erinnert an einen omnipräsenten Aufseher, welcher jedoch selbst nie gesehen werden kann. So wissen die Geiselnehmer im Inneren, dass sie beobachtet werden können, aber nicht, wann die Überwachung stattfindet.

Doch die Serie treibt es noch weiter mit der Überwachung. Nicht nur die Nerven der Verbrecher liegen zunehmend blank. Die verwanzte Brille des Unterinspektors führt im Laufe der Serie dazu, dass der Professor die Gespräche von Polizei und Geheimdienst stets mithören kann. Die Kommissarin (Itziar Ituño) und ihr Unterinspektor verdächtigen sich daher gegenseitig des Verrats. Die Situation eskaliert. Es ist eine Art Überwachung von unten und ähnelt Manns Sousveillance – mit der Ausnahme, dass der Ermittler nicht weiß, dass er zum Instrument des Professors geworden ist.

Diese mehrdimensionale Überwachungspraktik entpuppt sich als Wunderwaffe der Verbrecher und Erfolgsstrategie der gelungenen Serie. Die beklemmende (Un-)Gewissheit, überwacht zu werden, internalisiert sich im Bewusstsein aller Akteure. Der spannende Wechsel zwischen Sehen und Gesehen-Werden, offensichtlicher und unbemerkter Überwachung wird zum charakteristischen Gestaltungsmittel der Serie.

Dabei wirft die Serie brisante Fragen auf: Wie weit darf Überwachung gehen? Welche Regeln gelten für Verbrecher? *Haus des Geldes* verhandelt Überwachung dabei als durchaus effektives Mittel, das erfolgreich von verschiedenen Seiten in strategischen

Situationen eingesetzt wird. Es ließe sich dabei beispielsweise kritisieren, dass die Sympathie des Zuschauers für die Bande von Bankräubern zu einer Akzeptanz ihrer ausgefeilten Überwachungsmethoden beiträgt, die durchaus fragwürdig erscheint.

Álex Pina (Spanien, Antena 3, 2017). Haus des Geldes. In Deutschland verfügbar auf Netflix.

Veranstaltungen

Zeitschrift für
Semiotik
Band 40 • Heft 1-2 (2018)
Seite 135-142
Stauffenburg Verlag Tübingen

Unter der wissenschaftlichen Leitung von Klaus Sachs-Hombach und Jörg Schirra fand an der Eberhard Karls Universität Tübingen am 13. Mai 2019 die Fachtagung **Surveillance 2.0 – Zwischen Kontrolle und Komfort** statt. Anlass zur Tagung gab die Präsenz der Thematik ‚Digitale Überwachung' in aktuellen gesellschaftlichen Debatten. Das dabei entstehende Spannungsfeld zwischen „Kontrolle und Komfort" sollte durch die Fachtagung genauer beleuchtet werden. Als Referent*innen wurden vier prominente Vertreter*innen aus Wissenschaft und Praxis eingeladen, die das Phänomen Überwachung intensiv aus verschiedenen Perspektiven beleuchtet haben und dadurch einen interdisziplinären Diskurs ermöglichten: Dietmar Kammerer von der Universität Marburg, Nils Zurawski von der Universität Hamburg, Maria Wilhelm von der Stiftung Datenschutz (Referentin der Stabsstelle Europa) und Gene Engler (Marketing und Werbung). Ergänzt wurde das Programm von den Studierenden des Masterstudiengangs Medienwissenschaft der Universität Tübingen durch zwei Vorträge und eine öffentliche Debatte zu den Folgen der Überwachungsgesellschaft. An den verschiedenen Vorträgen nahmen geschätzt zwischen 15 und 40 Personen teil.

Die kurze Begrüßungsrede wurde von Lisamarie Haas (Studentin der Universität Tübingen) gehalten. Neben einem Rückblick auf das Seminar sowie die Lehrforschungsprojekte, aus denen diese Tagung hervorgegangen ist, machte die Moderatorin in ihrer Eröffnung die Grundproblematik deutlich, derer sich die verschiedenen Vorträge der Tagung widmeten. Haas machte auf die Widersprüchlichkeit unseres Verhältnisses zu Überwachung und Überwachungstechnologien aufmerksam, das einerseits kritisch unter Begriffen wie etwa ‚Kontrolle' problematisiert werde, andererseits zunehmend einen festen Bestandteil unseres Alltages ausmache, da Überwachungstechnologien mit dem Versprechen nach mehr Komfort immer mehr Einzug in unser Privatleben, Arbeitsstätten und die Öffentlichkeit hielten. Diese Ambivalenz ‚zwischen Kontrolle und Komfort' diene als Ausgangspunkt für Überlegungen über eine sogenannte ‚Surveillance 2.0'.

Anknüpfend an die Frage, was ‚Surveillance 2.0' sein könne, stellte Dietmar Kammerer (Universität Marburg) in seinem Eröffnungsvortrag *Was war Surveillance 1.0? – Ein Blick in die (Diskurs-) Geschichte von Mainframes und Zauberspiegeln* zunächst die Frage „Was war Surveillance 1.0?". Mit der Intention, eher „Forschungsfragen zu stellen, als zu beantworten" warf Kammerer in seinem Vortrag einen Blick auf verschiedene Überwachungsphänomene und jeweilige zeitgenössische Diskurse zu diesen Phänomenen. Zunächst verdeutlichte er jedoch eine Dimension des Begriffs ‚Überwachung', die er aus zwei exemplarischen Definitionen aus dem Wörterbuch der deutschen Sprache herleitete, nämlich die des Wissens. So beruhen viele Verständnisse von Überwachung auf einer Beziehung zwischen normativ festgelegten optimalen Systemzuständen und Abweichungen davon, die durch die Kategorie des Wissens sichtbar würde.

Wenn etwa im medizinischen Bereich Gesundheitswerte „überwacht“ würden, stehe hier ein Wissen über den Optimalzustand an erster Stelle. „Überwachung“ im Sinne einer kriminalistischen Praxis suche zwar auch nach einer Abweichung vom Optimalzustand, allerdings beruhe diese auf einer besonderen Form des Wissens, nämlich dem Verdacht.

Seine historische Betrachtung von Überwachungsdiskursen begann Kammerer daraufhin mit Überlegungen zur Bedeutung des Begriffs ‚Privatheit‘. Der Artikel *The Right to Privacy* von Samuel Warren und Louis Brandeis aus dem Jahr 1890 sowie ein Zeitungsartikel aus der New York Times von 1874 boten hierfür den Ausgangspunkt. In beiden Texten wurde schon vor der Etablierung klassischer technischer Überwachungsmittel das Ende der Privatheit heraufbeschworen. Ausganspunkt war hierfür das Aufkommen der Boulevardpresse, welche durch das gezielte Verfassen von Texten über das Privatleben von Individuen und das Ausfragen von deren Nachbarn darüber „the privacy of the home“ angreifen würde. Die „privacy of the home“, also eine räumliche Fokussierung von Privatheit, ließe sich als ein zentrales Kernelement des Begriffs Privatheit am Ende des 19. beziehungsweise zu Beginn des 20. Jahrhunderts verstehen. In diesem Sinne sei vor allem das Eindringen der Öffentlichkeit (beispielsweise in Form der Presse) als zentraler Feind der Privatheit verstanden worden.

Dies habe sich in den 1960er Jahren gewandelt. Durch eine zunehmende Professionalisierung des Eindringens in den privaten Lebensraum, was in gewissem Maße einer Etablierung von Überwachungsakteuren entspräche, rückten nun der Staat auf der einen Seite sowie Unternehmen auf der anderen Seite in den Blick öffentlicher Debatten über Privatheit und Überwachung. Hier sei allerdings noch immer eine Fokussierung auf das einzelne Individuum als Opfer von Überwachung zu beobachten gewesen, ähnlich wie dem Individuum als Opfer der Boulevardpresse in den oben gemachten Ausführungen. Eine Verschiebung des Blickes auf die gesamte Gesellschaft sei erst später erfolgt.

Neben den neu hinzugetretenen Akteuren (Staat und Unternehmen) und der Frage nach dem Ziel der Überwachung (Überwachung des Einzelnen vs. Überwachung der Gesellschaft) sind zu dieser Zeit allerdings auch neue technische Instrumente zur Überwachung aufgekommen, allen voran zentralisierte Datenbanken und Computer. In einem kurzen Exkurs zu sogenannten ‚Mainframes‘ und frühen Computern markierte Kammerer an dieser Stelle die Ambivalenz unseres Verhältnisses zu dieser neuen Technologie in ihren jungen Jahren, die zu Beginn zunächst als pures Werkzeug, dann als Teil einer dynamischen Mensch-Technik-Allianz und schließlich als Herrschaftsinstrument diskutiert wurde.

Seinen ‚Streifzug‘ durch Diskurse über historische Überwachungsphänomene beendete Kammerer schließlich mit einem Blick auf die Etablierung von Videokameras in der polizeilichen Praxis. So seien diese in den 1950ern zunächst nur als Instrument zur Verkehrslenkung getestet worden, bis sie dann schließlich zur Verfolgung von Ordnungswidrigkeiten (beispielsweise das Überfahren einer roten Ampel) und Straftaten beziehungsweise auch zur Prävention von Straftaten durch Abschreckung eingesetzt worden seien. Heute sei die Kameratechnologie, so Kammerer, eine „Allzweckwaffe der polizeilichen Praxis“ geworden, wie auch anhand aktueller Bemühungen zum Einsatz von Gesichtserkennungssoftware deutlich würde.

Abschließend fasste Kammerer die zentralen Erkenntnisse aus seinem Vortrag zusammen. Zum einen habe sich die Betrachtung einzelner Menschen als Individuen zunehmend aus der Überwachungspraxis verabschiedet. Stattdessen würden Menschen als „Vorgänge innerhalb eines Systems" behandelt; Kammerer fasst dies unter dem Begriff „Verhaltensmeteorologie" zusammen. Zum anderen sei gerade deswegen für Überwachungsforschung auch eine Zuwendung zu epistemischen Modellen von Überwachung notwendig, da so Fragen nach „Auffälligkeiten im System" und nach „Verdachtsmomenten" beantwortet werden können.

Um Abweichungen und Auffälligkeiten drehte sich auch die daran anschließende öffentliche Debatte über individualisierte Krankenkassenbeiträge und Überwachung, die von Masterstudierenden der Universität Tübingen geführt wurde. In der Debatte wurde die Frage nach dem Für und Wider einer Einführung von individualisierten Krankenkassenbeiträgen auf Basis von durch Smartwatches und Fitness-Wearables erhobenen Gesundheitsdaten verhandelt. Hierbei wurde besonders deutlich, dass ökonomische und auch ethische Argumente im Bereich der Überwachung eine relevante Rolle in der Abwägung von Grenzen eines Einsatzes von Überwachungsmaßnahmen spielen.

Die Grenzen von Überwachung innerhalb eines Rechtsstaates aufzuzeigen war auch die Kernbotschaft des zweiten Vortrages der Tagung unter dem Titel *Who watches the watchmen? – Datenschutzrechtliche Anforderungen an Überwachungssysteme* von Maria W i l h e l m von der Stiftung Datenschutz Stuttgart. Nachdem sie kurz die Aufgaben ihrer Behörde und des Landesdatenschutzbeauftragten skizziert hatte, benannte Wilhelm zunächst die relevanten Gesetzestexte im Bereich des Datenschutzes, das Bundes- (BDSG) und Landesdatenschutzgesetz (LDSG) auf der einen Seite sowie die EU-rechtlich festgelegte Datenschutzgrundverordnung (DSGVO). In dieser kurzen Vorstellung wurde bereits eine zentrale Problematik der aktuellen juristischen Praxis im Bereich des Datenschutzes deutlich: die neue EU-rechtliche DSGVO stelle einerseits die Rechtmäßigkeit der Bundes- und Landesgesetze in Frage, andererseits sei noch nicht geklärt, inwieweit dieses strafrechtlich zur Anwendung kommen könne, sodass im Bereich des Strafrechtes Baden-Württembergs aktuell noch vor allem das LDSG zum Einsatz komme. Da die DSGVO allerdings auf eine Vereinheitlichung von Datenschutzrechten beziehungsweise der Anwendung von Datenschutzgesetzen abziele, bestünde hier noch Nachholbedarf.

Auf Basis der geltenden Gesetze umrahmte Wilhelm daraufhin die rechtlichen Anforderungen an die (digitale) Verarbeitung von Daten. So gälten einerseits die Grundsätze der Datenminimierung und der Begrenzung der Speicherdauer von Daten, andererseits hätten Nutzer einen Anspruch auf die Richtigkeit der über sie gespeicherten Daten sowie den Schutz der Verarbeitung ihrer Daten. Zudem sei für die Verarbeitung von Daten eine Zustimmung notwendig (beispielsweise in Form eines Vertrages oder durch Nutzungsbedingungen). Des Weiteren dürften die Daten einerseits nur zweckgebunden zum Einsatz kommen, andererseits müssten die jeweiligen verarbeitenden Stellen/Unternehmen die Verarbeitungsweise und Verwendungszwecke der Daten transparent machen. Gerade die Frage nach der Transparenz sei immer wieder ein kritisch diskutiertes Problem, was auch durch Nachfragen von Zuhörern während und nach dem Vortrag deutlich wurde: Wie umfangreich muss diese Transparenzmachung sein beziehungsweise wie umfangreich darf sie sein, damit sie von Endnutzern bei der Zustim-

mung zur Datenverarbeitung auch verstanden werden kann? Und wie lässt sich diese Transparenzmachung auch im öffentlichen Raum gewährleisten, etwa bei festinstallierten Überwachungskameras? Wilhelm zeigte an dieser Stelle ein für diesen Zweck geschaffenes Hinweisschild; jedoch könne ein solches allein auch nicht die ideale Lösung sein, da dieses ja beispielsweise von sehbehinderten Menschen gar nicht wahrgenommen werden könne. Eine abschließende Antwort auf die Fragen nach der idealen Form der Transparenzmachung stehe noch aus.

Abschließend sprach Wilhelm noch über den bereits von Dietmar Kammerer in seinem Eröffnungsvortrag angeschnittenen Einsatz von Gesichtserkennungssoftware zur Überwachung im öffentlichen Raum. Damit der Einsatz solcher Software legal und somit großflächig umsetzbar würde, müsse die Erfolgsquote der Technologie annähernd 100% erreichen – wovon die aktuellen Testergebnisse noch weit entfernt seien.

Es schloss sich der Vortrag von Lena F ü l l e r, Caroline G a n z e r t und Marcel L e m m e s zum Thema *Überwachen, verführen, verkaufen – Manipulation als Schlüsselkonzept für Überwachungstheorien des 21. Jahrhunderts* an. Dieser dritte Vortrag entfernte sich inhaltlich von den eher phänomenbezogenen vorherigen Vorträgen. Marcel Lemmes präsentierte einige theoretische Überlegungen zu Überwachung, die aus einer gemeinsamen Publikation mit seinen Kommilitoninnen Lena Füller und Caroline Ganzert stammen. In einer vergleichenden Analyse von Michel Foucaults Disziplinargesellschaft, Gilles Deleuzes Kontrollgesellschaft und den Überlegungen von Zygmunt Bauman und David Lyon zu Überwachung und Konsum hat Lemmes nach der Bedeutung von Beeinflussung in Überwachungstheorien gesucht.

Zunächst stellte er einen begrifflichen Zugang zum Thema ‚Beeinflussung' anhand der Dissertation von Alexander Fischer über Manipulation vor. Fischer grenze subtile Manipulation von gewaltvollen Formen der Beeinflussung wie etwa dem Zwang oder der Nötigung ab. Manipulation zeichne sich nämlich durch eine extern verursachte, affektiv-psychologische Veränderung bei den Manipulierten aus, die deren Entscheidung in einer Wahlsituation beeinflussen soll. Ob sich diese Form der Manipulation in den Arbeiten der vier Theoretiker wiederfinden lässt, und wenn ja, welche Rolle sie jeweils spielt, sollte nun jeweils untersucht werden.

Nach einem kurzen Abriss über Foucaults Disziplinargesellschaft und die von ihm formulierten Gedanken zum Panoptismus hielt Lemmes fest, dass Beeinflussung eine sehr wichtige Rolle in Foucaults Werk einnimmt, allerdings in Form von Zwang, und nicht Manipulation.

Benthams Kontrollgesellschaft, die den Blick vor allem auf den Bereich der Ökonomie richtet und eine Ökonomisierung aller anderen Lebensbereiche konstatiert, zeichne sich dagegen durch eine manipulative Form der Beeinflussung aus. Die Kontrolle würde, im Unterschied zum Zwang, kurzfristig und kontinuierlich auftreten, und zwar beispielsweise in Form von Marketing, welches Deleuze zufolge „das neue Instrument der sozialen Kontrolle" sei. Mit der wachsenden Bedeutung des Marktes und einzelner Unternehmen ließen sich in Benthams Kontrollgesellschaft des Weiteren eine Entgrenzung der Beeinflussung und somit auch eine Entgrenzung der Überwachung beobachten. Anstatt eines Akteurs in Form des Staates wie bei Foucault würden nun viele Akteure damit beginnen, uns zu überwachen und zu beeinflussen.

An den Überlegungen von Bauman und Lyon, die Lemmes im Anschluss vorstellte, würde zudem deutlich, dass sich neben der Entgrenzung der Akteure auch immer

neue technische Möglichkeiten zum Instrumentarium der marktgesteuerten Manipulation gesellen würden. Durch ‚Datendoubles' und ‚Social Sorting' würde die Manipulation systematischer und ihr Erfolg für die Unternehmen messbar gemacht. Zudem ließe sich nach Bauman und Lyon eine Verlagerung von der Bedürfnisbefriedigung zur Bedürfniserzeugung konstatieren. Diese spiegele, so Lemmes, die manipulativen Interessen des Marktes wider.

Abschließend resümierte Lemmes, dass, genauso wie technische Möglichkeiten in Überwachungstheorien über die Zeit bedeutender wurden, auch Manipulation als mitgedachte Form der Beeinflussung zunehmend an Relevanz gewonnen habe. Darum plädierte er für eine klare, direkte Auseinandersetzung mit Beeinflussung im Allgemeinen und Manipulation im Speziellen in Überwachungstheorien, um so neue Erkenntnisse zu gewinnen.

Kunden zum Kaufen verführen – dies war auch das Kernthema des sich anschließenden Vortrags von Gene Engler: *Wir wissen besser als du, was du brauchst – Daten in der Werbung*. Engler präsentierte hierbei allerdings statt theoriegestützter Befunde vielmehr praktische Erkenntnisse und Methoden aus dem Alltag der Werbeschaffenden. Die These des Vortrages wird schon im Titel deutlich: ‚Wir wissen besser als du, was du brauchst' – aber wer ist in diesem Fall ‚wir'? Das seien einerseits – wenig überraschend – Tech-Giganten wie Google, Apple, Facebook, Amazon und Microsoft, andererseits aber auch diverse Unternehmen, mit denen man gemeinhin keinen Datenhandel in Verbindung bringt, wie der Musikstreaming-Dienst Spotify oder der Online-Modeshop Zalando. Spotify etwa könne auf Basis des Musikgeschmacks seiner Nutzer relativ akkurate Informationen über Alter, Geschlecht und verschiedene Interessen gewinnen. Zalando handele ebenfalls mit solchen Daten, die aus den Käufen ihrer Kunden hervorgingen.

Es gebe sogar eine Art digitale Datenbörse, über die Datenbroker Daten kaufen, verkaufen, kombinieren und vervollständigen würden, um so möglichst umfangreiche Datensätze und Kundenprofile zu erstellen. So könne man mit den verschiedensten Zielgruppenkriterien im Hinterkopf etwa bei Anbietern wie axciom passende Datensätze erwerben – und das mit erschreckender Genauigkeit. Demnach sei es möglich, für eine sehr detaillierte Zielgruppe ohne größere Problem passende Datensätze zu kaufen, beispielsweise männliche Autobesitzer einer bestimmten Altersgruppe, die eine bestimmte Automarke fahren, ein bestimmtes Einkommen haben und in Stadtteilen von bestimmten Großstädten wohnen. Grundlage dafür seien verschiedene statistische Verfahren sowie das Zusammenführen von Daten diverser Anbieter.

Mit verschiedenen Beispielen aus den Medien (wie etwa die US-amerikanische Einzelhandelskette Target, die die Schwangerschaft einer Teenagerin vor ihr selbst und ihren Eltern feststellen konnte) und seiner eigenen langjährigen Praxiserfahrung, schaffte es Engler, eine sehr gute Vorstellung davon zu vermitteln, welche Möglichkeiten im Bereich der Werbung und des User-Targeting derzeit bestehen. Aber den wohl alarmierendsten Befund aus der Praxis formulierte Engler wie folgt: „Es geht nur um Cash und ums Verkaufen". Ethischen Fragestellungen komme in der praktischen Sphäre der Datenüberwachung also eine nur untergeordnete Rolle zu.

Der fünfte Vortrag von Anne Diessner und Carina Konopka (Studierende der Universität Tübingen) trug den Titel *‚Alexa, kann ich dir vertrauen?' – Sprachassistenten als Wegbereiter der gläsernen Privatsphäre*. Der Vortrag, der auf einer Publikation

basiert, die die Vortragenden zusammen mit der Moderatorin der Tagung Lisamarie H a a s verfasst haben, befasste sich mit einem konkreten Phänomen aus der Sphäre der kommerziellen Datenüberwachung: Sprachassistenten. Nach einer kurzen tentativen Definition (Sprachassistenten seien technische Geräte, die menschliche Sprache aufnehmen und daraufhin mit einer synthetischen Stimme antworten und interagieren können) diskutierten die Referentinnen einen möglichen, wenn auch eher sinnbildlich zu verstehenden Vergleich zwischen den modernen, technischen Geräten und den sogenannten Dienstboten und Bediensteten aus dem 19. und frühen 20. Jahrhundert.

So seien Sprachassistenten ähnlich wie Dienstboten in den Haushalt eingebunden, sodass sie alle Geschehnisse im Haus mitbekämen und einer eher willkürlichen Arbeitszeit unterlägen. Ihr Einsatz diene allem voran der Erleichterung des Alltags der ‚Hausherren'. Gleichzeitig erinnere das den Sprachassistenten von ihren Herstellern qua Namen zugeschriebene ‚Geschlecht' (Siri, Cortana, Alexa) an die zunehmende Feminisierung des Dienstbotenwesens in dessen letzten Jahren. Die große Problematik schließlich, die durch diesen Vergleich deutlich würde, und einen markanten Unterschied zwischen Sprachassistenten und Dienstboten offenbare, sei die Frage nach der Loyalität. Da Sprachassistenten keine Menschen sind, kennen diese Werte wie Vertrauen oder Loyalität nicht, denn – wie auch aus den Vorträgen von Engler und Lemmes deutlich geworden ist – als kommerzielle Produkte dienen sie den Interessen von Konzernen.

Dieser Befund veranlasste Diessner und Konopka dazu, den Begriff der Privatheit in Frage zu stellen. Mit Blick auf Beate Rössler argumentierten sie, dass Privatheit drei Dimensionen umfasse: eine lokale, eine dezisionale sowie eine informationelle. Gleichzeitig diskutierten sie den Wert von Privatheit für eine Gesellschaft und markierten ihre Bedeutung für eine freiheitliche Öffentlichkeit, die individuelle Autonomie und als Moderationselement für die soziale Rollenverteilung. Die technische (Hacking) wie auch physikalische Angreifbarkeit (Steuerung durch fremde Personen in der eigenen Wohnung) von Sprachassistenten sowie die Problematik der fehlenden Loyalität zu ihren Besitzern stelle einen Angriff auf die drei Dimensionen der Privatheit dar und gefährde damit die mit ihr verbundenen Werte für die Gesellschaft. In diesem Sinne schlossen die Referentinnen ihren Vortrag mit dem Plädoyer, eine „Balance zwischen Bequemlichkeit und Sicherheit", zwischen Komfort und Kontrolle zu finden.

Den Schlussvortrag zum Thema *Der totale Unterhaltungsstaat – Überwachung im digitalen Zeitalter* hielt der renommierte Überwachungsforscher Nils Z u r a w s k i (Universität Hamburg). Zu Beginn seines Referats machte Zurawski zunächst den Interessenschwerpunkt seiner Untersuchung von Überwachung deutlich. Als Soziologe befrage er konkrete Überwachungsphänomene nach ihren gesamtgesellschaftlichen Zusammenhängen und interessiere sich in diesem Sinne besonders für die Beziehung zwischen Überwachung, Konsum und Bedürfnissen sowie die Frage, wie Herrschaft in einer Gesellschaft organisiert wird.

Als Ausgangsbeispiel für seine Überlegungen wählte er die nie realisierte Modellstadt *Chaux* des französischen Architekten Claude-Nicolas Ledoux aus dem 18. Jahrhundert, die um eine tatsächlich existierende Saline geplant wurde. In einer solchen Arbeiterstadt hätte der gesamte Alltag, von den Einkaufsmöglichkeiten bis hin zum sonntäglichen Kirchgang, von den Interessen des Besitzers der Saline gesteuert werden können. Diese Form der Kontrolle des Alltages durch Unternehmer versteht Zurawski als ein Sinn-

bild für die gegenwärtige Gesellschaft. Denn für ihn stelle die Frage nach der Herrschaft auch eine Frage nach der Funktionsweise des Konsums dar, der unsere heutige Gesellschaft völlig durchdringt. Grundlegend sei an dieser Stelle, den Akt des Kaufens insofern als identitätsstiftend zu verstehen, als er einerseits als klare Distinktionspraxis zum Einsatz komme, andererseits mit Werten wie ‚Modernität' und ‚Weltoffenheit' verbunden sei. Identität werde so zu einer Konsum-Identität. Die Steuerung des Konsums kann insofern als eine Steuerung der (möglichen) Identitäten verstanden werden.

Auf diesen Überlegungen basierend stellte Zurawski nun das Smartphone – ein bekanntermaßen als Überwachungsinstrument diskutiertes Gerät – in den Mittelpunkt seiner Betrachtung. Zum einen sei das Smartphone selbst etwas, das zur Distinktion des Individuums und als Symbol für dessen Modernität gekauft würde, zum anderen verändere es auch unseren Konsum: unsere Alltagsaktivitäten vereinten sich zunehmend in einem einzelnen Gerät. An dieser Stelle führte Zurawski den Begriff der ‚Optionsmaschine' an. Das Smartphone vereinfache uns das Konsumieren, da wir im Großen und Ganzen nur noch eine Auswahl nach der anderen treffen müssten. Dabei ergibt sich allerdings die Frage: Zwischen was wählen wir aus? Und was wird weggelassen – was können wir nicht wählen?

Diese „Macht, Dinge wegzulassen" konzentriere sich zunehmend in den Händen verschiedener „Plattformen" (beispielsweise die vernetzten Services von Apple). Durch die geringe Zahl an Plattformen würde unsere Welt formatiert; nur noch bestimmte Lebensweisen seien möglich. Gleichzeitig werde unser Alltag ökonomischen Prinzipien unterworfen. Denn das letzte Ziel der Plattformen als wirtschaftliche Betriebe sei es, den Konsum langfristig vorherzusagen und zu steuern und in diesem Sinne „die Zukunft zu kontrollieren". Insofern werde die Macht der Plattformen zu einer neuen Herrschaftsmacht.

Besonders problematisch sei an dieser Entwicklung, und hier schließt Zurawski an das Thema der Tagung an, dass wir durch die Konzentration und Steuerung unseres Konsums einen „großen Mehrwert" hätten. Ständig könnten wir das Gefühl haben, dass sich jemand um uns kümmert; ständig könnten wir uns unterhalten lassen – diese Ambivalenz aus Kontrolle und Komfort lässt sich wohl am besten unter einem Begriff aus dem Titel von Zurawskis Vortrag zusammenfassen: der des ‚totalen Unterhaltungsstaats'.

Vor dem Hintergrund der wissenschaftlichen Auseinandersetzung mit dem Thema Überwachung knüpften einige der Vorträge direkt oder indirekt an verschiedene vergangene sowie aktuelle Debatten und Auseinandersetzungen mit dem Thema Überwachung an. Querverbindungen konnten unter anderem bei Maria Wilhelms Vortrag gesehen werden, die darlegte, welche Mechanismen greifen, um derzeitige Überwachungssysteme mit einem selbstbestimmten Datenschutz vereinbaren zu können. Sie zeigte damit, welche Bedeutung einem staatlichen Eingreifen zukommt, um eine Dystopie des gläsernen Bürgers zu verhindern, wie etwa George Orwell sie in *1984* heraufbeschwört.

Der Vortrag von Gene Engler, der sich mit der Bedeutung von Daten in Werbung und Marketing beschäftigte, klärte hingegen darüber auf, dass trotz dieser staatlichen Maßnahmen zur Eingrenzung der Überwachung beunruhigend viele personenbezogene Informationen im Umlauf sind. Die Themen Datenhandel und ‚Dataveillance' als ‚Social Sorting' gewinnen dadurch gegenwärtig stark an Präsenz und damit einhergehend auch Fragen nach unserem alltäglichen Konsum. Wie der Vortrag von Lena Füller, Caroline Ganzert und Marcel Lemmes gezeigt hat, nimmt hier die Bedeutung mani-

pulativer Eingriffe zu. Gleichzeitig – wie Nils Zurawski herausstellte – liegt im Feld des Konsums auch ein erschreckendes Potential zur Herrschaft über Individuen und ihre Identität(en) begründet, was die zunehmende Verschmelzung von Überwachung, Herrschaft, Konsum und Manipulation als einen vielgestaltigen Forschungsgegenstand offenbar werden lässt.

Lena Füller, Caroline Ganzert und Marcel Lemmes
Eberhard Karls Universität Tübingen

Vorschau auf den Thementeil der nächsten Hefte

Nachfolgend sind die geplanten Themenhefte der Zeitschrift für Semiotik aufgeführt. Autor/-innen mit Interesse zur Abfassung von Beiträgen, Einlagen und Institutionsberichten können sich über die Adresse zsem.redaktion@tu-chemnitz.de direkt an die Redaktion der Zeitschrift für Semiotik wenden.

Themenoffenes Heft

Zeichen, Medien, Modalitäten. Semiotische Medientheorien (Georg Albert, Jörg Bücker, Mark Dang-Anh, Stefan Meier, Daniel Rellstab)

Semiotik in der Diaspora (Yuan Li, Benno Wagner)