Thomas Christian Bächle

Narrative der digitalen Überwachung

Abstract: Surveillance protects us – surveillance controls us: Whether we regard surveillance technologies and practices as either a safeguard of or a threat to individual freedoms and liberal societies is heavily shaped by long-standing and powerful narratives. This is particularly the case for digital technologies, as the value-laden expectations that are projected onto them combine modernist and Enlightenment ideas with traditional Judeo-Christian motifs. As will be argued, they form the foundation for political, journalistic and scientific discourses interpreting digital surveillance as objective and omniscient, capable of laying bare the truth about the individual self, offering God-like providence, an omnipotent, even manipulative force.

Optical surveillance (CCTV), *aerial surveillance*, *audio surveillance*, *radio-wave surveillance*, *GPS surveillance*, *Email/VoIP surveillance*, *sensors*, *computer and internet surveillance*, *biometrics*, *genetics*, *biochemical surveillance*, *mobile media surveillance* – diese hier nur unvollständig wiedergegebene Liste unterschiedlicher elektronischer Überwachungstechniken ist einer Einführung in die *Surveillance Studies* entnommen, die sich an gleicher Stelle um eine zunächst scheinbar möglichst umfassende Definition der Überwachung bemüht: „Observing, sensing or otherwise determining the presence or influence of persons, activities or phenomena of interest, especially as regards of protection of assets, territory, property, family, personal safety, power, commercial opportunities or social relationships".[1] Mit den neutral gehaltenen Variablen der Überwachungsanordnung (wer überwacht wen oder was?) verwoben ist – ein wenig überraschend – eine (fast) eindeutige, kausal-finale Bestimmung: Überwachung schützt.

Überraschend ist dies, weil Überwachung zumeist als diskursive Folie für negativ konnotierte Konsequenzen im Zusammenhang mit technischen Entwicklungen genutzt wird. ‚Schutz' tritt dabei als Antagonist von ‚Kontrolle' und damit als nur vordergründig propagierte Funktion in Erscheinung, die vor allem dazu dient, sinistre Absichten zu kaschieren. Die bloße Funktionalität der (digitalen) Technik wird daher oft zugleich als Zwecksetzung begriffen und entkommt dabei nicht einer sofortigen Wertung, die sich an tradierten Narrativen

1 Petersen (2013: S. 4).

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

orientiert. Der vorliegende Beitrag widmet sich daher zunächst drei populären Erzählsträngen, die für die Deutung und Wertung digitaler Überwachung besonders prominent genutzt werden. Sie finden sich in der politischen und medialen Öffentlichkeit genauso wie in der wissenschaftlichen Betrachtung der untersuchten Phänomene. Dies liegt zum einen an der Historizität der genutzten Motivik, die kulturell so sehr naturalisiert ist, dass sie als Referenzfolie eine besondere Wirkmacht entfaltet. Zum anderen sind die Bestrebungen, den soziotechnischen Wandel zu erklären, auch stets mit dessen Dynamik konfrontiert. Eine Strategie, sich diesem gegenüber zu verhalten, ist die Fortschreibung bekannter Narrative, die von Akteur*innen in Wissenschaft, Politik oder Journalismus wechselseitig getragen werden.

Das erste Narrativ, *(Digitale) Überwachung zerstört unsere Freiheit* (Abschnitt 1), reduziert Überwachung häufig auf ihre technischen Aspekte und erzählt ein Bedrohungsnarrativ weiter, demzufolge Technik immer in einem antagonistischen Verhältnis zum Menschen und seiner Freiheit zu denken ist. Wie sich jedoch zeigen soll, besteht nicht per se ein Widerspruch zwischen individueller Freiheit, Autonomie und Überwachung. Vielmehr sind effektive Überwachungspraktiken als eine Voraussetzung für Herstellung und Schutz individueller Freiheiten zu betrachten, die nicht nur repressiven Charakter haben. Durch ihre feste Einbettung in die geistesgeschichtliche Aufklärung ist die Funktion der Überwachung – die Sichtbarmachung – eine zentrale und konstruktive Figur der Herausbildung bestimmter Formen von Subjektivität.

Das zweite Narrativ, *Digitale Überwachung ist allwissend* (Abschnitt 2), erzählt von einer vermeintlichen Objektivität und Omniszienz digitaler Überwachung, die gar zukünftiges Verhalten oder Ereignisse antizipieren kann. Das Narrativ ist einerseits eng verflochten mit judeo-christlichen Motiven (ein wachendes Auge der Vorsehung), andererseits wird in ihm ebenfalls der Impetus der Aufklärung deutlich, nach einer objektiven und universellen Beschreibung der Welt zu streben, die vor allem in der mythischen Überhöhung des Datenwissens zum Ausdruck kommt.

Das dritte Narrativ, *Mithilfe digitaler Überwachungstechniken können wir sehr leicht manipuliert werden* (Abschnitt 3), betrachtet daran anschließende Diskursfiguren, die vor allem das Machtverhältnis zwischen Mensch und Maschine ausdeuten. In unheimlicher Weise intelligente Systeme können Wissen über den Menschen generieren, das er selbst nicht preisgeben will oder das er gar selbst nicht über sich hat. Auf diese Weise gefährdet, sind wir anfällig für gezielte Verhaltensmanipulationen, wie sie sich etwa bei Wahl- oder Konsumentscheidungen niederschlagen. Auch dieses Narrativ schließt an eine Traditionslinie der Deutung von Medientechnik an, die deren Wirkmacht tendenziell überschätzt.

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

Abschließend (Abschnitt 4) wird noch die Frage nach der narrativen Dimension der wissenschaftlichen Einordnung der ‚neuen' digitalen Überwachung aufgeworfen. In den theoretischen Konzepten, identifizierten Problemen und Lösungsansätzen stecken auch immer Erzählmuster von Anfang und Ende, von alt und neu. Ihre Widersprüchlichkeit erwächst einerseits aus der ostentativen Präsentation des Neuen und andererseits aus der impliziten Sehnsucht nach der vergangenen Ordnung der Moderne.

1. „(Digitale) Überwachung zerstört unsere Freiheit." – Digitalisierung, Surveillance und Spätmoderne

„[A] well documented, tightly reasoned, and frightening analysis of the clash between individual privacy and information-gathering technology in a computer age"[2] – so lautet das Urteil einer zeitgenössischen Rezension von Arthur R. Millers *The Assault on Privacy. Computers, Data Banks and Dossiers*[3] (1971). Computer und Datenbanken stünden im Zentrum einer ‚kybernetischen Revolution'[4], fasst Bernard A. Berkman zusammen, die in den Worten Millers folgendermaßen charakterisiert wird: „dramatically increasing man's capacity to accumulate, manipulate, retrieve, and transmit knowledge".[5] Die Leistung der computerbasierten Datennetze, so der Rezensent weiter, habe zwar einen Nutzen, bedrohe jedoch gesellschaftliche Freiheiten und die individuelle Privatheit. Die Warnung wird begleitet von einem Aufruf zu ‚einfallsreicher rechtssprecherischer Flexibilität und Erfindungsreichtum'[6], legislativen Kontrollen und administrativen Selbstbeschränkungen. Der weiterhin gelobte ‚logische Aufbau'[7] des Buchs lasse auf einen Abschnitt zu den Fähigkeiten der Informationstechnologie eine Abwägung zwischen notwendiger Datensammlung und dem ‚technologischen Angriff auf die individuelle Privatheit'[8] folgen: „the most effective portion of the book is the detailed examination of the rapidly developing computerized information-gathering techniques and the way in which they are being used to

2 Berkman (1971: S. 808).
3 Die deutsche Übersetzung des Titels – „Der Einbruch in die Privatsphäre. Datenbanken und Dossiers" (Neuwied: Luchterhand, 1973) – verzichtet auf die Nennung des Computers.
4 Vgl. Berkman (1971: S. 808).
5 Miller (1971: S. 1).
6 Vgl. Berkman (1971: S. 808).
7 Vgl. ebd.
8 Vgl. ebd.

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

create dossiers on all our citizens at a maddeningly increasing tempo".[9] Neben den staatlichen Praktiken und Institutionen, mit denen Daten über Bürger*innen gesammelt werden, liege ein besonderes Augenmerk auf Unternehmensaktivitäten wie diejenigen privater Kreditgeber*innen: „the pervasive surveillance and fact-gathering techniques that have permitted the compilation and indiscriminate dissemination and sale of personal financial information about some 50 million Americans".[10] Zu den Befürchtungen zählen in diesem Zusammenhang auch die Computerisierung von Persönlichkeits- oder IQ-Tests mit Folgen für die wirtschaftliche oder soziale Mobilität einzelner Subjekte.[11]

Als ‚tapferer erster Versuch, das Problem der Computerisierung in Amerika zu beschreiben'[12], wie der Rezensent bescheinigt, spinnt *The Assault on Privacy* wichtige Narrationsmuster, die auch heute nichts an ihrer diskursiven Prominenz eingebüßt haben. Die skizzierten Befürchtungen schreiben ‚Privatheit' rhetorisch einen erheblichen Eigenwert zu und finden nicht nur im Lichte gegenwärtiger Diskussionen Widerhall, sie entsprechen diesen in einem erstaunlichen Maße.[13]

Grundsätzlich ist in diesem Narrationsmuster bereits das antagonistisch gedeutete Verhältnis zwischen der digitalen, computerbasierten Informations- und Kommunikationstechnologie und den individuellen Freiheitsrechten, insbesondere der Privatheit, angelegt. Computergestützte elektronische Überwachung erscheint per se als Gefahr, die Debatten um den notwendigen *Schutz* von Daten, Personen und der Privatheit als einem sozialen Wert sowie der demokratisch-freiheitlichen Verfasstheit des Nationalstaats weisen der Technologie die populär-diskursive Rolle eines Aggressors zu.

Doch es besteht keine Widersprüchlichkeit zwischen Freiheit und Überwachung. Vielmehr ist Überwachung die Voraussetzung für Freiheit. Jede soziale Einheit – ob eine Paarbeziehung, die Familie oder die Dorfgemeinschaft – kann nur mithilfe bestimmter Regeln aufrechterhalten werden. An diesen orientieren sich das individuelle Verhalten und Interaktionen, sie schaffen gegenseitige Erwartungen und strukturelle Sicherheit als Voraussetzung individueller Freiheit. Die Organisation von Gemeinschaft kennt daher gegenseitige Überwachung, Kontrolle und bedarfsabhängige Sanktionierung. In Dorfgemeinschaften hatten diese Prozesse durch einen hohen Grad persönlicher Bekanntheit sowie relativ starre und homogene Normen weitgehend ohne den Einsatz technischer

9 Ebd. (S. 808f.).
10 Ebd. (S. 809f.).
11 Vgl. ebd. (S. 810).
12 Vgl. ebd. (S. 811).
13 Vgl. Zuboff (2019); Couldry/Mejias (2018).

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

Hilfsmittel Bestand. Mit der Ausbildung von Nationalstaaten als großen administrativen Einheiten in der Moderne jedoch werden neue Instrumente der sozialen Kontrolle notwendig. Betrachtet man diese mehrere Millionen Menschen umfassenden sozialen Einheiten, in denen kodifizierte Regelsysteme gelten, sind im Lichte einer weitgehenden Anonymität der einzelnen Mitglieder der Gemeinschaft sowohl die Praktiken der interpersonalen Überwachung als auch Instrumente persönlicher sozialer Sanktionierung weitgehend ineffektiv. Die Gemeinschaft eines Nationalstaats ist folglich auf andere Mittel gesellschaftlicher Steuerung durch Sanktionen oder Ausschlüsse angewiesen, die im Allgemeinen ohne Techniken und Praktiken der Überwachung nicht denkbar sind: „The social order would collapse […] if everyone felt free to lie, steal, rape or cheat whenever he or she could avoid punishment for doing so",[14] stellt Rule etwa zur selben Zeit wie Miller fest, unterstreicht dabei jedoch auch die Notwendigkeit einer zentralisierten Verarbeitung von Daten zum Zweck sozialer Kontrolle, die stets auch die Voraussetzungen für individuelle Freiheiten sichert. Es überrascht daher nicht, dass Überwachung als das dominante Organisationsprinzip der Spätmoderne identifiziert wird, das über die letzten vier Jahrzehnte immer größere Auswirkungen auf Machtstrukturen, institutionelle Praktiken und interpersonale Beziehungen entfaltet hat.[15]

Trotz der negativen Assoziationen, die oft mit staatlicher Überwachung in Verbindung gebracht werden, wird es gleichwohl als die Aufgabe des Staates betrachtet, die Bedingungen der individuellen Freiheiten sicherzustellen.[16] Wie an anderer Stelle ausgeführt,[17] sind diese Grundsätze ebenfalls als Teil der politischen Moderne und ihrer Organisationsformen zu betrachten.[18] Bürger*innen sind vor Unterdrückung oder Beschneidung ihrer Freiheiten durch Andere zu schützen. Die Umsetzung dieses Prinzips liberaler Demokratien ist undenkbar ohne die Praxis der Überwachung. Sie ist daher nicht als repressiver Antagonist zu freien und freiheitlich organisierten gesellschaftlichen Strukturen zu denken, sondern sichert in einem instrumentellen Sinn ein Regelsystem ab, ohne das individuelle Freiheit nicht möglich ist.

14 Rule (2007: S. 19).
15 Vgl. Lyon et al. (2012: S. 1).
16 Vgl. Stoddart (2014: S. 369).
17 Vgl. Bächle (2019).
18 Stoddart (2014) nennt die ‚Virginia Declaration of Rights' (1776), die ‚Déclaration des Droit de L'Homme et du Citoyen' (1789) oder die Menschenrechtserklärung (1948) als Beispiele ihrer rechtlichen Kodifizierung.

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

Das Narrativ vom Angriff auf die Privatheit durch computergestützte Überwachung wird durch eine weitere begriffliche Differenzierung getragen, die im 17. Jahrhundert entstanden ist[19] und Privatheit und Öffentlichkeit als einander wechselseitig ausschließende Konzepte definiert, die sich schließlich auch als materiell-lokalisierbare Räume beschreiben lassen. Die Dichtomie ‚öffentlich vs. privat' ist seither die Grundlage für normative Rahmenbedingungen liberaler Demokratien.[20] Sowohl der von Miller konstatierte Angriff auf die Privatheit als auch die spiegelbildlich angeordnete und in nicht minder drastischer Metaphorik diagnostizierte ‚Tyrannei der Intimität' als ‚Verfall und Ende des öffentlichen Lebens'[21] durch die Grenzüberschreitung des Privaten in die Öffentlichkeit bleiben ohne die dichotom angeordnete und normative Referenzfolie ohne Sinn. Vor dem Hintergrund dieser gilt Überwachung daher stets sowohl als staatliches Instrument, das individuelle Rechte auf Privatheit verletzt, als auch als eine Notwendigkeit, um Bürger*innenrechte zu verteidigen.[22]

Die negativen Assoziationen mit der Praxis der Überwachung – invasiv, aggressiv, repressiv – sind direkte Konsequenz aus normativen, epistemologischen (u. a. Subjektivität vs. Objektivität, siehe Abschnitt 2) sowie aus diesen politisch-institutionellen Dualismen der Moderne. Das Narrativ, das die digitalen Informations- und Kommunikationstechnologien als Antagonisten der Privatheit und individuellen Freiheit beschreibt, ist ihre Weiterführung. Doch entsteht das Subjekt – dem als einem epistemologischen Anker die individuellen Freiheiten und ein Schutzbedürfnis zugeschrieben werden können – ironischerweise erst aus der Praxis der Überwachung. Wie Foucault bekanntermaßen über die panoptische Anordnung der Sichtbarkeit (‚Gefangene' und ‚Wächter') herausarbeitet,[23] ist sie stets konstitutiv für bestimmte, räumlich definierte Subjektzuschreibungen mit klaren sozialen Rollen in Klöstern, der Psychiatrie, im Krankenhaus, im Gefängnis, in der Fabrik oder in der Schule. Die Anordnung der Sichtbarkeit und Sichtbarmachung des Subjekts hat somit einen produktiven Effekt, sie erlaubt erst die moderne Vorstellung von Subjekten als Ergebnis einer Suche nach der objektiven Wahrheit.[24]

19 Vgl. Habermas (1990).

20 Vgl. Sewell/Barker (2007: S. 354f.).

21 So der Titel von Sennett (1983).

22 Wie ebenfalls in Bächle (2019) dargestellt, sind ‚privat' und ‚öffentlich' keine universellen ontologischen Kategorien, sondern werden stets in Kontexten hergestellt. Vgl. ebenfalls Sewell/Barker (2007: S. 356).

23 Vgl. Foucault (1994: S. 258).

24 Vgl. Foucault (1983). Siehe Bächle (2019) für eine Diskussion des paradoxen Verhältnisses zwischen Autonomie, Subjekt und Überwachung.

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

Staat und Bürger*innen, Privatheit und Öffentlichkeit, Beobachtete und Beobachter*innen – dichotom angelegte Begriffe der Moderne prägen sowohl die Konzeptionierung als auch die Evaluation von Überwachungspraktiken. In der Folge orientiert sich auch die Bewertung der Technologie an diesen normativen Bezugsgrößen, verkennt jedoch zumeist die skizzierte komplexe Dynamik der Überwachung als eine notwendige strukturelle Voraussetzung für individuelle Freiheit und zugleich als notwendige und produktive Praxis zur Herstellung eines Subjekts, dem diese Freiheiten überhaupt erst zugeschrieben werden können.

Seit einigen Jahren ist eine Veränderung dieser Dynamik zu konstatieren. Die Dichotomie Bürger*innen/Staat, mit der eine hierarchische *top-down*-Relation der Überwachung einhergeht, wird ergänzt und in Teilen sogar verdrängt von effektiven und umfassenden Möglichkeiten der Überwachung, die durch große Unternehmen durchgeführt wird. Die Auseinandersetzung verläuft entlang komplexerer Relationen zwischen Staat, Unternehmen, Bürger*innen oder Konsument*innen (siehe Abschnitt 4). Auch das Begriffspaar öffentlich/privat wird in seiner wechselseitigen Exklusivität zunehmend in Frage gestellt. Dies liegt in erheblichem Maße an neuen Kommunikationsräumen, die sich von örtlich bestimmbaren und physisch manifesten Räumen (öffentliche Plätze, private Schlafzimmer) gelöst haben. Kommunikationsmedien erlauben eine zwischenzeitlich völlig ‚normalisierte', bisweilen sehr öffentliche Kommunikation aus dem Schlafzimmer. Sie sind jedoch nicht als Ursache für den Zerfall dieser Grenze zu identifizieren. Die (medien-)technologischen Praktiken decken vielmehr erst auf, dass das dichotome Schema nie in Reinform existierte.[25]

Der (kommunikative) Alltag der Gegenwart ist nicht nur sehr stark ‚durchdrungen' von digitalen Medien, sondern vielmehr durch diese *konstituiert*. Sichtbarmachung, Selbstdarstellung und Transparenz(zwänge) der mobilen Online-Kommunikation verändern den normativen Wert des Privaten.[26] ‚Seeing surveillantly' ist zu einer alltäglichen Praxis des Sehens, zu einer Form des Zugangs zu einer sozialen Welt geworden.[27] Auch die zumeist hierarchisch geprägte Zuordnung von Beobachteten, die dem Blick (verborgener) Beobachter*innen ausgeliefert sind, scheint angesichts der gezielten gegenseitigen Sichtbarmachung und Überwachung in der Online-Kommunikation oder der bewussten Inkaufnahme eines Teilens personenbezogener Daten mit Dritten obsolet. Derartig dichotome Kategorien sind nicht mehr sinnvoll anwendbar, das

25 Vgl. Sheller/Urry (2007).
26 Vgl. Bächle (2016b).
27 So der Titel von Finn (2012).

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

durch ihre normative Struktur gespeiste Narrativ der digitalen Überwachungstechnologien als Aggressor und Gefahr qua Funktionalität setzt sich jedoch fort.

2. „Digitale Überwachung ist allwissend" – Omniszienz, Vorsehung und Big Data

Auch das zweite bedeutende Narrativ der digitalen Überwachung ist stark verflochten mit einer konzeptionellen Dichotomie der Moderne entstanden, Objektivität und Subjektivität, und vereint sie zugleich mit einer judeo-christlichen Motivik: Allgegenwart und Allwissenheit. Allgegenwärtig ist die digitale Überwachung durch (medien-)technische Entwicklungen (wie Smartphones oder Tracking Devices), die soziale Interaktionen mittels datenbasierter Plattformen ermöglichen und konstituieren. Jede durch diese vollzogene oder dokumentierte kommunikative Handlung erzeugt ein detailliertes Datenwissen, das dem Narrativ zufolge in einer Allwissenheit durch universelle Datafizierung mündet. Daten geben demnach Auskunft über Alter, Geschlecht, Bildung, Arbeitssituation, sexuelle Orientierung und Identität, politische Ansichten, getätigte Einkäufe und Kaufkraft, moralische Ansichten, Kreditwürdigkeit, gesundheitsspezifische Interessen, Religionszugehörigkeit u. v. m. Die Informationen über Nutzer*innen digitaler Dienste werden dabei in Tausende einzelne Kategorien oder Attribute ausdifferenziert.[28] Sie werden in vielen Fällen allein aus dem Online-Verhalten[29] abgeleitet. In der soziologischen und kulturwissenschaftlichen Theorienbildung wird diese Veränderung einer nicht länger auf Präsenz basierten Überwachung in der Regel als Ablösung der panoptischen Allsichtbarkeit durch datenbasierte ‚Kontrollgesellschaften'[30] beschrieben.[31] An die Stelle einer visuellen Überwachung in materiell definierten Räumen tritt eine Überwachung der in Daten transponierten Subjekte („data subjects"[32]), die durch permanente Messung, Evaluation und Kontrolle von Leistung und Folgsamkeit am Arbeitsplatz, in Bildungssystemen oder in Kontexten der medizinischen Prävention oder Therapie charakterisiert ist. Die Vorstellung der Überwachung wird damit diffus: Sie wirkt überall, unbemerkt und nicht länger verortet und definiert.

28 Vgl. Christl (2017).
29 Vgl. Kosinski et al. (2013).
30 Vgl. Deleuze (1992).
31 Vgl. Bauman (2003). Vgl. zu den beiden Modellen auch die Einführung zu diesem Band.
32 Lyon (2002: S. 244).

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

Es ist ein pantheistischer Datenglaube, der sich hier mit dem Objektivitätsdiktum der Aufklärung paart. Die Daten sind nicht nur *in* allem, sie sind konstitutiv *für* alles.

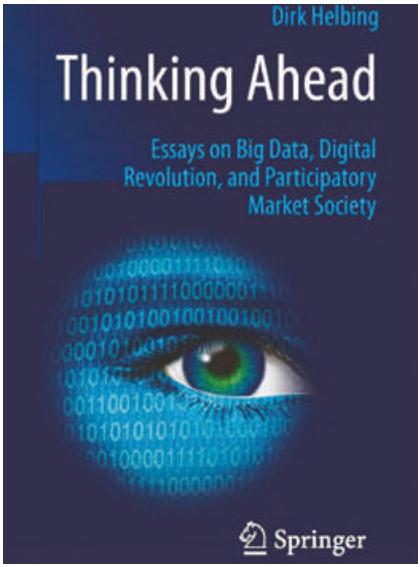

Abb. 1a: Titelseite eines Buchs von Dirk Helbing (2015).

Abb. 1b: Radierung von Daniel Chodowiecki.[33] Quelle: Chodowiecki (1787).

‚Das Auge der Vorsehung' – Ikonographie der Überwachung als Ensemble von Allwissenheit und Allsichtbarkeit, Schutz und Strafe.

Trotz einer Verschiebung der Überwachungspraxis von lokalisierten Körpern zu Datensubjekten ist der eng mit dem Panoptismus verbundene Impetus der Aufklärung, die Wahrheit aufzudecken,[34] in den heutigen digitalen Datenpraktiken sehr präsent. Überwachung als Praxis der Sichtbarmachung ist mit den Kulturtechniken der Beobachtung, Vermessung und regelgeleiteten, formalisierten

33 Siehe ausführlich zu den ‚Bildern der Überwachung' Kammerer (2008).
34 Sewell/Barker (2007: S. 358).

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

Welterschließung eine Geste der Aufklärung. Die großen Datenmengen rücken uns vermeintlich näher an die ersehnte Objektivität heran: Indem unsere sozialen Beziehungen und Interaktionen, unsere Erfahrungen, Erlebnisse, Emotionen und Gefühle vollständig zu einem computerisierbaren Datenkorpus werden, können die nur ausschnitthaften Erkenntnisse über die Welt überwunden werden.[35]

Der Datenreichtum ist als direkte Fortsetzung des objektivistischen Narrativs von der Abbildung der Welt zu verstehen. Neben einer technologischen (durch eine größere Quantität von Daten und eine verbesserte Rechenleistung) und analytischen (durch effektivere Identifikation von Mustern) Dimension von ‚Big Data' ist die mythische Zuschreibung von Wahrheit, Präzision und Objektivität an das mithilfe dieser Datenbestände konstruierte Wissen entscheidend.[36] Zwar ist der Begriff ‚Rohdaten' ein Oxymoron, da Daten niemals in einer reinen, ursprünglichen, unbearbeiteten – eben ‚rohen' – Form vorliegen können, und doch gelten sie als transparent, eigenevident, objektiv, als die kleinsten Einheiten der Wahrheit.[37]

Die Grundlagen dieses Mythos werden mit den epistemologischen Normen der geistesgeschichtlichen Moderne geschaffen, die Subjekt(ivität) und Objekt(ivität) klar voneinander scheidet[38] und neben der Möglichkeit des Objektiven auch das Streben nach Wissensaggregation und Omniszienz hervorbringt. Dieser Mythos wird in der jüngeren Vergangenheit in regelmäßigen Abständen am Leben erhalten und mit den jeweiligen technologischen Bedingungen aktualisiert. Ähnliche Narrative finden sich etwa bereits in den Diskursen der virtuellen Realität: Die Annahme einer Überführung der Welt in mathematisch definierbare Räume, die aus diskreten, manipulierbaren Einheiten (pixel) bestehen, ist nichts weniger als die computertechnische und ästhetische Realisierung des aufgeklärten Traums einer durch Formeln und Repräsentationen erschließbaren Welt.[39] Die motivischen Verflechtungen mit christlichen Traditionslinien weisen dem Körper eine sekundäre Stellung zu – das schwache Fleisch – und konzentrieren sich auf die alles durchziehenden Informationen als Einheiten der Welt: Geist über Materie.[40]

35 Vgl. Mayer-Schönberger/Cukier (2013). Für eine kritische Diskussion der (Fehl-) Annahmen des Big Data-Diskurses siehe Bächle (2016a).
36 Vgl. Boyd/Crawford (2013).
37 Vgl. Gitelman/Jackson (2013).
38 Vgl. Latour (2008).
39 Vgl. Penny (1994).
40 Vgl. Hayles (1999).

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

Die Narrative der Allwissenheit, Allsichtbarkeit und Allgegenwart werden auf der Projektionsfläche derzeitiger Daten- und Überwachungspraktiken auf zukünftige Ereignisse oder Handlungen einzelner Individuen ausgeweitet, die vermeintlich antizipiert werden können. Verbunden mit der Idee von Schutz und Strafe findet sich das Auge der Vorsehung motivisch auch in ‚Big Data'-Diskursen als eine höhere Macht (vgl. Abb. 1). Mit der Technik des *profiling* in polizeilichen, administrativen, medizinischen oder sicherheitspolitischen und militärischen Kontexten erlaubt diese Macht einen vermeintlichen Blick auf zukünftige Entwicklungen oder Szenarien. Diese Form der Überwachung des Zukünftigen ist eine Simulation von Überwachung,[41] weil das darin produzierte Wissen kein realisiertes Bezugsobjekt hat. Das durch *predictive policing* oder *predictive diagnostics* produzierte Wissen macht virtuelle, in der Möglichkeit vorhandene Ereignisse, die noch nicht eingetreten sind, gegenwärtig und damit real. Die konstruierte Beobachtung dessen, was noch nicht geschehen ist, aber vielleicht geschehen wird, erweitert die ‚Big Data'-gespeisten Narrative der Allwissenheit und das Motiv des Auges der Vorsehung als Schutz- und Bestrafungsinstanz. Praktisch ermöglicht erst die weitreichende ‚Datafizierung' die Extrapolation des Zukünftigen aus dem vermessenen Bekannten. Medientechnisch und -ästhetisch setzt sich hier die mit den Massenmedien vorgezeichnete Ablösung der Simulation von ihren Referenzobjekten fort.[42] Die simulierte Überwachung drückt sich sprachlich in Begriffen wie *pre-crime* für eine Praxis in der Kriminologie und ‚Schläfer', ‚Gefährder' oder Risikosubjekt als Kategorien für Individuen aus. Sie wird durch die kollektiv geteilten Bestrebungen, zukünftige Straftaten zu verhindern oder zukünftig entstehenden Krankheiten entgegenzuwirken, zu einer eigenen Realität vor dem eigentlichen Fakt. Das Profil als Referenzobjekt der simulierten Überwachung muss nicht legitimiert werden, es ‚funktioniert'[43], da es sich durch die Angabe seiner eigenen Irrtumswahrscheinlichkeit bereits selbst validiert. Ein falscher Blick in die Zukunft ist somit Teil der prognostischen Überwachung und sichert sie damit auch gegenüber Vorwürfen fehlerhafter Vorsehung ab.

Prospektive Überwachung deckt daher keine Wahrheiten auf, sondern konstruiert diese im Akt der Sichtbarmachung. In höchstem Maße problematisch wird dies durch bestimmte Wertungen und Wertigkeiten, die bereits in den Daten angelegt sind.[44] Eines der bekanntesten Beispiele, das die wertende Datafizierung

41 Vgl. Bogard (2007).
42 Vgl. Baudrillard (2014).
43 Vgl. Bogard (2007).
44 Vgl. Mittelstadt et al. (2016).

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

von Subjekten und deren zukünftigem Verhalten dokumentiert, ist die im Jahr 2016 von ‚ProPublica' – einer Plattform für invenstigativen Journalismus – veröffentlichte Arbeit *Machine Bias*.[45] Darin wird die Software COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*) dargestellt, die an US-amerikanischen Gerichten als Werkzeug zur Entscheidungsfindung genutzt wird, um die Wahrscheinlichkeit für eine erneute Straffälligkeit von Individuen automatisiert zu bewerten. COMPAS evaluiert dabei zusätzlich die Notwendigkeiten und/oder Bedürfnisse im Zusammenhang mit einer Resozialisierung der/des Angeklagten und gibt Empfehlungen dazu ab, wer auf Kaution entlassen werden kann, inklusive der Kautionshöhe.

Im Zuge der Recherche von ‚ProPublica' wurden die Risikobewertungen von mehr als 7.000 Personen, die in den Jahren 2013 und 2014 in Broward County (Florida) festgenommen worden waren, mit der Anzahl der von diesen tatsächlich neu begangenen Straftaten über einen Zeitraum von zwei Jahren verglichen. Die Autor*innen stellten fest, dass die Risikobewertung bei der Vorhersage gewalttätiger Straftaten ‚bemerkenswert unzuverlässig' war; eine entsprechende Prognose war nur in einem Fünftel der Fälle korrekt. Neben der sehr hohen Irrtumswahrscheinlichkeit zeigten sich auch deutliche Disparitäten bei der Risikobewertung in Abhängigkeit der Hautfarbe der Straftäter*innen: „The formula was particularly likely to falsely flag black defendants as future criminals, wrongly labeling them this way at almost twice the rate as white defendants. White defendants were mislabeled as low risk more often than black defendants".[46]

Neben der Verlässlichkeit der von der COMPAS produzierten Prognosen erscheint auch die Datengrundlage zweifelhaft. Die von der Firma Northpointe (heute: Equivant) entwickelte Software verspricht dabei eine Bewertung von Variablen wie *Anger*, *Criminal Personality*, *History of Non-Compliance*, *Residential Instability*, *Substance Abuse*, *Social Adjustment Problems* und *Socialization Failure*.[47] Als Grundlage der Prognose dienen Daten, die über eine Befragung von straffällig gewordenen Personen generiert werden. Zu den insgesamt 137 Items zählen:

> „Based on the screener's observations, is this person a suspected or admitted gang member? – No, Yes"
>
> „If you lived with both parents and they later separated, how old were you at the time? – Less than 5, 5 to 10, 11 to 14, 15 or older, does not apply"

45 Vgl. Angwin et al. (2016).

46 Ebd.

47 Diese Liste findet sich in einer Werbebroschüre auf den Seiten der Firma Northpointe (o. J.). In aktuelleren Versionen wurde diese durch zurückhaltendere Beschreibungen der Software ersetzt, vgl. Equivant (o. J.). Das aufschlussreiche Handbuch zur Software COMPAS-CORE in der Version von 2015 ist hier einsehbar: Northpointe (2015).

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

> „How many of your friends/acquaintances have ever been arrested? – None, Few, Half, Most"
> „How often have you moved in the last twelve months? – Never, 1, 2, 3, 4, 5+"
> „Thinking of your leisure time in the past few (3–6) months […] How often did you feel bored? – Never, Several times/mo [month, T. C. B.], Several times/wk [week, T. C. B.], Daily"
> „I have never felt sad about things in my life. – Strongly Disagree, Disagree, Not Sure, Agree, Strongly Agree"
> „A hungry person has a right to steal. – Strongly Disagree, Disagree, Not Sure, Agree, Strongly Agree"

Neben einer detaillierten Evaluation des sozialen Milieus stehen hier Fragen nach der persönlichen Einstellung zu einem komplexen ethischen Dilemma oder gar die subjektive Einschätzung der Interviewer*innen. Die verzerrte Prognose ist daher nicht etwa die Konsequenz aus einer automatisierten Datenanalyse, sondern vielmehr den Bedeutungen und Gewichtungen geschuldet, die einzelnen Variablen und ihren Werten im Zuge der Operationalisierung zugeschrieben werden. Mit Faktoren wie einer (durch die Interviewer*innen vermuteten) Zugehörigkeit zu einer Gang oder der Anzahl straffällig gewordenener Bekannter und Freund*innen, wird die individuelle Strafanfälligkeit u. a. durch soziale Milieus erhoben, die häufig entlang einer identitätsstiftenden ethnischen Zugehörigkeit organisiert sind. Gruppenidentität, indirekt und implizit auch definiert durch Hautfarbe, markiert Individuen. Jüngere wissenschaftliche Arbeiten stellen die Risiken dieser Art von ‚Dirty Data' („inaccurate, skewed, or systemically biased data"[48]) heraus:

> Deploying predictive policing systems in jurisdictions with extensive histories of unlawful police practices presents elevated risks that dirty data will lead to flawed or unlawful predictions, which in turn risk perpetuating additional harm via feedback loops throughout the criminal justice system.[49]

Durch die automatisierte Analyse großer – möglicherweise auch ‚schmutziger' – Datenmengen entsteht gleichwohl der Eindruck einer zusätzlichen Objektivierung eines dabei zu Tage geförderten Wissens.

Die Fokussierung des Zukünftigen im Narrativ der Überwachung ist eingebettet in den umfassenderen und für die Spätmoderne charakteristischen Diskurs der Risikominimierung[50] und des Vorsorgeprinzips[51]. Von dem

48 Richardson et al. (2019: S. 192).
49 Ebd.
50 Vgl. Beck (1986).
51 Vgl. Sunstein (2005).

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

ursprünglich deskriptiven Ziel statistischer Auswertungen kommend, über die probabilistischen Aussagen über Risiken und deren Minimierung, verschreibt sich die analytische Vision heute dem Preemptionsparadigma, dem zufolge gar die Entstehungsbedingungen für Risiken identifiziert und verhindert werden sollen. Zu den tradierten Denkfiguren auf dem Weg dorthin zählt daher auch das Vorhandensein sozialer Ordnungsmuster. Begreift man, wie Armin Nassehi es vorschlägt, Digitalisierung als „soziologisches Projekt“[52], kann seine Erkenntnis, dass „die gesellschaftliche Moderne immer schon digital war“[53] kaum überraschen, weil er damit lediglich eine Erzählung fortschreibt, die im Ursprung dieses Projekts angelegt ist und sich auf die These verkürzen lässt: Gesellschaft lässt sich in Mustern beschreiben. Neben dem ‚Muster‘ hat auch das ‚Profil‘ eine mit der Moderne verbundene Diskursgeschichte.[54] Hier wurzeln das Verschwinden des Körpers hinter seiner Übersetzung in computerisierbaren Code (‚Biometrie‘) oder die Erschaffung von in Symbole übersetzten, klassifizierbaren Datensubjekten mittels Ausweisen, Fingerabdrücken oder Passwörtern.[55] Die Macht der digitalen Überwachung rührt vom Narrativ ihrer Allwissenheit und Allgegenwärtigkeit her, mit dessen Hilfe Normen und Deutungsmuster als ‚die objektive Wahrheit‘ durchgesetzt werden und kraft technikgestützter Vorsehung gar einen vermeintlichen Blick in die Zukunft ermöglichen.

3. „Mithilfe digitaler Überwachungstechniken können wir sehr leicht manipuliert werden“ – Unheimliche KI, Medienmacht und Vulnerabilität

Das dritte Narrativ knüpft an die Vorstellung der allwissenden digitalen Überwachung an: ‚Deep neural networks are more accurate than humans at detecting sexual orientation from facial images‘, behauptet der Titel einer Studie, in der Fotos von Einzelpersonen genutzt wurden, um Rückschlüsse auf deren sexuelle Identität zu ziehen.[56] Die Einschätzungen menschlicher Proband*innen wurde dabei mit den Klassifikationen eines computergestützten Analyseverfahrens verglichen. Als Ergebnis verkünden die Autoren: „Given a single

52 Nassehi (2019: S. 18) führt zur „soziologischen Denkungsart“ der Digitalisierung aus: „Sie nutzt soziale Strukturen, sie macht soziale Dynamiken sichtbar und sie erzeugt aus diesen Formen der Mustererkennung ihren Mehrwert“.

53 Ebd. (S. 11).

54 Vgl. Bernard (2017).

55 Vgl. Lyon (2002).

56 Vgl. Wang/Kosinski (2018).

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

facial image, a classifier could correctly distinguish between gay and heterosexual men in 81% of cases, and in 71% of cases for women. Human judges achieved much lower accuracy: 61% for men and 54% for women".[57] Wie eine Form der Schädelkunde unter digitalen Bedingungen muten die Ausführungen der Autoren an, wenn zu den genutzten ‚Klassifikatoren' sowohl die Form der Nase als auch der individuelle „grooming style" zählen und sie außerdem unterstreichen: „Consistent with the prenatal hormone theory of sexual orientation, gay men and women tended to have gender-atypical facial morphology, expression, and grooming styles".[58]

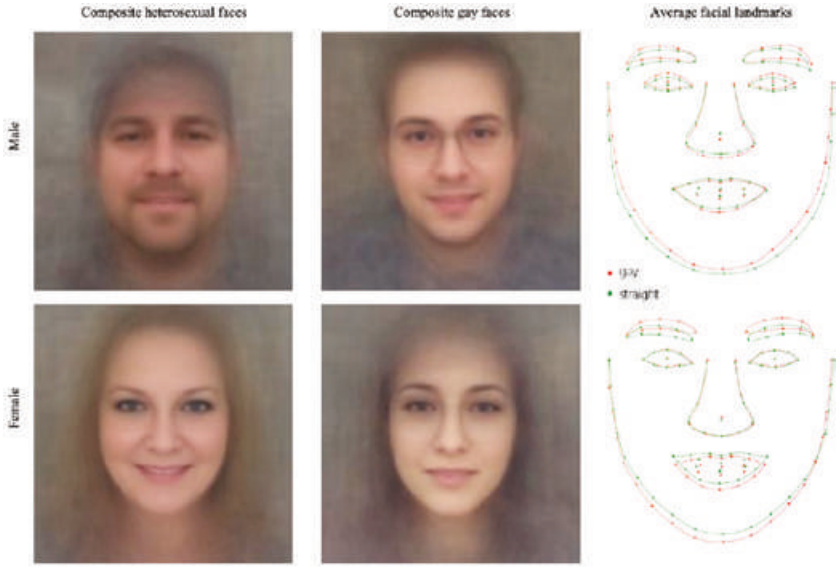

Abb. 2: Kraniometrie unter KI-Bedingungen – rechte Spalte: So sehen Homosexuelle aus. Quelle: Wang/Koskinski (2018: S. 251).

Der Ansatz ist offen naturalistisch (siehe oben: „consistent with the prenatal hormone theory of sexual orientation"), folgt einem bipolaren Schema der sexuellen Identität und verkennt völlig deren performativen Charakter: Die

57 Ebd. (S. 246).
58 Ebd.

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

Auswahl der Bilder entstammt einer US-amerikanischen Dating-Webseite, weshalb anzunehmen ist, dass sich die kulturellen Zeichen der Sexualität in der gewählten Selbstdarstellung besonders deutlich niederschlagen.[59]

Wenig überraschend wurde diese Arbeit im populären Diskurs in verbindlich klingende Schlagzeilen wie diese aus der britischen Zeitung *The Guardian* übersetzt: „New AI can guess whether you're gay or straight from a photograph".[60] Das Motiv der Allwissenheit wird dabei in ein Machtverhältnis zu den Menschen gesetzt: Die automatisierte Datenauswertung erkennt besser als wir und blickt in uns; eine unfreiwillige, unbewusste und unheimliche Offenbarung.

Dies ist das erste Element im Narrativ der Manipulationsmacht, die den digitalen Überwachungstechniken zugeschrieben wird und dabei oft angereichert ist mit Schlagworten wie ‚Künstliche Intelligenz', ‚Deep Neural Networks' oder ‚Deep Learning'. Die ‚Tiefe' letzterer, die eine komplexe Binnenstruktur zwischen Eingabe und Ausgabe im informationswissenschaftlichen Modell sogenannter neuronaler Netze beschreibt, hält eine zusätzliche Metaphorik des Unergründlichen, Unverstandenen und Unkontrollierbaren bereit. Unsere Verwundbarkeit gegenüber den Maschinen, die ein Wissen über uns generieren, das wir nicht aktiv bereitstellen, vielleicht gar verborgen halten wollen, wird in einem nächsten Schritt zur Grundlage für effektive Manipulation erklärt.[61]

Als bekanntestes Beispiel hierfür kann die *computational propaganda* gelten, die als Technik im US-amerikanischen Präsidentschaftswahlkampf des Jahres 2016 zum Einsatz kam. Wie 2018 bekannt wurde, hatte das britische Unternehmen Cambridge Analytica die Kategorisierung von Wähler*innengruppen als

59 Die bizarr anmutenden Verkürzungen und Schlussfolgerungen dieser Arbeit zeigen sich auch in der von den Autoren genutzten Rede von „gay and heterosexual faces" (Wang/Kosinski [2018: Anmerkung 6]), wenn es nicht (nur) um das Gesicht, sondern auch um dessen Ausdruck geht. Sogenannten ‚homosexuellen Gesichtern' schreiben sie eine „gender atypicality" (ebd.) zu, womit sie selbstverständlich verweiblichte männliche und vermännlichte weibliche Gesichter meinen. Gleiches gilt für Schlüsse wie diesen: „Male facial image brightness correlates 0.19 with the probability of being gay, as estimated by the DNN-based [Deep Neural Network; T. C. B.] classifier. While the brightness of the facial image might be driven by many factors, previous research found that testosterone stimulates melanocyte structure and function leading to a darker skin" (ebd.). Zu den anderen Faktoren ist wohl auch die – von der sexuellen Identität doch recht unabhängig zu betrachtende – Exposition gegenüber Sonnenlicht zu nennen, was die gesamte Absurdität einer solchen Argumentation verdeutlicht.

60 Levin (2017).

61 Dieses Narrativ kulminiert in den Annahmen um sogenannte ‚Gehirn-Computer-Schnittstellen', die als Interface zur Steuerung eines Computers genutzt werden können. Die Vorstellung jedoch, es sei möglich, als symbolische Repräsentationen vorliegende Gedanken auszulesen, entbehrt jeder seriösen Grundlage.

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

Dienstleistung verkauft und damit eine gezielte Adressierung von Nutzer*innen des sozialen Netzwerks Facebook mit selektiven Botschaften ermöglicht. Instrument hierfür war die Konstruktion von Persönlichkeitsprofilen: Die Vermessung der Psyche (‚Psychometrie') sollte besonders empfängliche Zielgruppen identifizierbar machen. Zum Einsatz kam das sogenannte ‚OCEAN-Modell'[62], das die Persönlichkeit eines Individuums in fünf Dimensionen beschreibbar machen will: Offenheit für Erfahrungen, Gewissenhaftigkeit, Extraversion, Verträglichkeit (Kooperationsbereitschaft, Empathie) und Neurotizismus (u. a. die erlebte Intensität negativer Emotionen). Seit Jahrzehnten in der psychologischen Forschung angewandt – und kritisch begleitet – kommt es seit einiger Zeit auch im Zusammenhang mit Daten zum Einsatz, die während des Gebrauchs von Medien (z. B. der Nutzung von Apps auf dem Smartphone[63]) generiert werden.

Die Ergebnisse dieser Analysen und die zielgerichteten Botschaften, so geht die Narration weiter, funktionieren, sind effektiv und haben massiv das Wahlverhalten beeinflusst.[64] Oft wird diese Erzählung mit dem derzeit populären, aus der Verhaltensökonomie stammenden Begriff *nudging* verbunden. Hinter diesem steht die Vorstellung einer gezielten – wenngleich in seiner ursprünglichen Modellierung[65] in wohlwollender Absicht verfolgten – Manipulation des Verhaltens, das auf Grundlage eines umfangreichen Datenwissens in seiner Musterhaftigkeit durchschaubar und dadurch vorhersagbar wird. Es handelt sich dabei nicht um Verbote oder finanzielle Anreize, die das individuelle

62 Vgl. Goldberg (1993).

63 Vgl. Chittaranjan et al. (2011).

64 Im US-amerikanischen *Time Magazine* (Ghosh/Scott 2018) heißt es beispielsweise am 19. März 2018 unter der Überschrift „Facebook's New Controversy Shows How Easily Online Political Ads Can Manipulate You": „Reporting by the Observer, the Guardian and the New York Times in recent days has revealed that Cambridge Analytica – the social media monitoring firm that bragged it helped put Trump in the White House – had gained access before the election to the data of 50 million Facebook users through highly questionable means. Cambridge Analytica used to that data to create a tool of ‚psychological warfare' to manipulate American voters with targeted Facebook ads and social media campaigns. This news has painted the national discussion over social media's impact on national politics in a stark new light. There was already a debate raging about how targeted digital ads and messages from campaigns, partisan propagandists and even Russian agents were sowing outrage and division in the U.S. electorate. Now it appears that Cambridge Analytica took it one step farther, using highly sensitive personal data taken from Facebook users without their knowledge to manipulate them into supporting Donald Trump."

65 Vgl. Thaler/Sunstein (2008).

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

Verhalten ändern, sondern scheinbar viel zurückhaltender um eine Wahl- und Entscheidungsarchitektur, die bestimmte Optionen begünstigt: „Putting fruit at eye level counts as a nudge. Banning junk food does not“[66]. Die sichtbarere Präsentation bestimmter Optionen oder Standardeinstellungen soll eine Auswahl begünstigen, ohne die Wahlfreiheit einzuschränken. In seiner Umsetzung in digitalen Medien[67] wirkt das Konzept *nudging* etwa durch Interface-Strukturen, die bestimmte Nutzungsweisen ermöglichen und andere ausschließen (‚affordances‘[68]). Zugleich erfolgt durch eine (mehr oder weniger) prominente Anordnung einzelner Funktionen oder ihre Einbettung in spielerische Kontexte (als *gamification* z. B. durch das Sammeln von Punkten) auch stets eine Priorisierung und Steuerung von Handlungen.

Nicht lange hat es gedauert, bis jemand im Anschluss daran eine sprachlich-konzeptionelle Originalität ersann: ‚Big Nudging‘. Dirk Helbing stellt unter diesem zusammengeschusterten Begriff in apodiktischer Eindeutigkeit fest: „Wer über große Datenmengen verfügt, kann Menschen auf subtile Weise manipulieren“.[69] Der „zu Grunde liegende Wissenschaftsansatz wird ‚Behaviorismus‘ genannt und ist eigentlich längst veraltet“ und doch würden unsere „psychologischen Unzulänglichkeiten ausgenutzt“.[70] Grundlage seien die „oft ohne unser Einverständnis gesammelten persönlichen Daten“, mit denen sich offenbare, „was wir denken, wie wir fühlen und wie wir manipuliert werden können“ und schließlich kaufen wir „überteuerte Produkte“ oder „solche, die wir nicht brauchen“ oder geben „unsere Stimme einer bestimmten Partei“[71].

Wenn doch, so mag man einwenden, der Behaviorismus veraltet ist, wie kann uns *nudging* dann überhaupt in diesem Sinne erzählt werden? Wohl weil eine solche Erzählung opportun und in hohem Maße anschlussfähig an bestehende narrative Strukturen ist. Sie gibt dem Erwartbaren eine Stimme. Das Konzept *nudging* aber beschreibt Tendenzen, die sich erst in größeren Populationen zeigen, und folgt keinem behavioristischen Ursache-Wirkungs-Prinzip, dem jede/r Einzelne unterworfen ist. Was hinter dieser dominanten Narrationsstruktur hingegen weniger sichtbar wird, sind die Konsequenzen aus der Fiktion eines klassifizierbaren ‚Psycho-Subjekts‘, das durch die psychometrischen Verfahren und die anschließende individualisierte Adressierung (etwa im genannten Beispiel

66 Ebd. (S. 6).
67 Vgl. Mirsch et al. (2017).
68 Vgl. Bucher/Helmond (2017).
69 Helbing (2017: S. 49).
70 Ebd.
71 Ebd. (S. 50).

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

der Wahlkampfkommunikation) entsteht.[72] Sie führt zu einer Fragmentierung der Öffentlichkeit in selektive Kommunikationsräume, in denen emotionalisierende oder falsche Informationen Widerhall finden.[73] Dies beschädigt potentiell die öffentliche Debatte, die politische Diskurskultur, kollektiv geteilte Identitäten als Figuren sozialen Zusammenhalts oder die Referenzfigur einer gemeinsamen (Medien-)Realität.[74]

Besondere Vulnerabilität schließlich wird im Zusammenhang mit unseren Gefühlen unterstellt. Einen relativ neuen Diskurs stellt das Paradigma des *affective computing* dar, in dessen Mittelpunkt eine Mensch/Maschine-Interaktion steht, die gezielt die Emotionen der Nutzer*innen anspricht und diese auch analysieren kann. In der ursprünglichen Definition – „computing that relates to, arises from and deliberately influences emotion"[75] – ist das manipulative Element dieser Kommunikationsdimension zwischen Menschen und Maschine bereits explizit angelegt. Heute immer populärer werdende künstliche Kommunikationsagenten wie textbasierte *chat bots*, sogenannte *smart speakers* (die über eine Sprachsynthesefunktion verfügen und damit eine menschliche Sprechstimme künstlich erzeugen können) und zu einem gewissen Grad auch *social bots,* nähern sich einer als natürlich empfundenen sprachlichen Interaktion an. Noch stärker anthropomorphisierte Elemente zeigen sich in sozialen Robotern, wie sie etwa bereits in der Pflege zum Einsatz kommen,[76] deren ausgeprägteste Form in einer humanoiden Morphologie liegt. Sie sind als Interfaces mit weitreichenden Funktionen ausgestattet, um verbale, non- und paraverbale Zeichen der menschlichen Kommunikation zu (de-)kodieren und durch eine eigene Körperlichkeit auch – in Mimik und Gesten – zu (re-)produzieren. Dies ist in der Tat ein Novum, da ein solches Interface Wissensbereiche einer computerisierbaren Form zuführt, die bislang als implizit galten.[77] Dazu zählt insbesondere ein nicht eindeutig kodifiziertes Wissen im Bereich der sozialen Normen oder ein körpergebundenes Wissen wie Annahmen über die Emotionen der menschlichen Interaktionspartner*innen.

72 Vgl. Stark (2018).

73 Vgl. Bruns (2019) für eine kritische Einordnung der damit in Verbindung stehenden Konzepte ‚Filter Bubble' oder ‚Echokammer'.

74 Siehe Susser et al. (2019) für eine differenzierte Darstellung des *nudging*-Konzepts, zum Begriff sowie den Praktiken der Manipulation.

75 Picard (1995: S. 3).

76 Vgl. Calo et al. (2011).

77 Vgl. Bächle et al. (2017).

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

Diese Entwicklungen befördern nicht weniger als eine direkte soziale Interaktion mit den uns analysierenden Medientechniken. Die natürliche Interaktionsform mit den menschenähnlichen und vertrauenserweckenden Maschinen produziert nicht nur weiteres intimes Wissen über uns, sie steigert auch die Vulnerabilität diesen gegenüber. Doch liegt die Gefahr wohl weniger im manipulativen Potential dieser Techniken selbst, sondern vielmehr in der Bedeutung, die diesem Wissen zugeschrieben wird: Die Rede von Persönlichkeitsmerkmalen, die anhand der Stimme analysiert werden oder einer computergestützten Beobachtung der Mimik, die die ‚wahren' Emotionen offenlegt, verweist auf Wissensformen, die sich aus den oben skizzierten Narrativen speisen. Sie geben vor, etwas zu erkennen, das der menschlichen Wahrnehmung entgangen ist, und sie werden zugleich mit dem Nimbus der Objektivität ausgestattet, die einer maschinellen Intelligenz unterstellt wird.

Dies sind die Gefahren, die aus den Narrativen der digitalen Überwachung entstehen. Eine Bewerberin, eine Verdächtige, ein Patient – sie alle werden möglicherweise mit einem vermeintlich objektiv qua Körperzeichen generierten Wissen über ihre Persönlichkeit und Emotionen konfrontiert, das zur ‚eigentlichen' Realität wird. Es entstehen Fiktionen des Emotionalen, die nicht objektiv vermessen werden, sondern vielmehr emotionale Zustände normieren und mit dem Zwang zur Optimierung negativ konnotierter, unerwünschter oder unproduktiver Ausprägungen versehen.[78]

Auch hier hat die Überwachung folglich keine enthüllende Funktion. Mit ihrer Hilfe wird vielmehr ein Wissen konstruiert, das soziale Machtstrukturen durchsetzt und verstärkt. Die Narrationsmuster der manipulativen Macht neuer (Medien-)technologien müssen als historische Konstante angesehen werden. Die Vorstellung, Computer als Persuasionstechnologien einzusetzen, kann auf diskursive Vorläufer wie das Mitte der 1990er Jahre ins Leben gerufene ‚Persuasive Technology Lab' der Stanford University zurückblicken, dessen Forschungsziel erklärtermaßen die computer- und mediengestützte Verhaltensänderung von Menschen ist (und nicht etwa die Erforschung der Bedingungen, unter denen uns Dritte manipulieren wollen). Blickt man weiter zurück, sei an die dem Kino oder dem Fernsehen in ihrer jeweiligen Frühphase zugeschriebenen Medienwirkungen erinnert und an die befürchteten Auswirkungen von Gewaltdarstellungen in Filmen oder die Angst vor unterschwellig gesetzten Reizen als manipulative Strategien in der Kino- und Fernsehwerbung. Die manipulative Macht der Medien – so zeigt der Blick auf diese historischen Analogien – wird

78 Vgl. ausführlich Bächle (2019).

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

jedoch tendenziell überschätzt.[79] Ihnen liegen typischerweise stark behavioristisch eingefärbte Medienwirkungsmodelle zugrunde, eine ganz offensichtliche Gemeinsamkeit mit den heutigen Ängsten um die digitale Überwachung.

4. Theorien der digitalen Überwachung – Die narrative Dimension von ‚Analyse' und ‚Lösung'

Wissenschaft und ihre Theorienbildung folgen zumeist pflichtschuldig der Geste des Neuen, suchen nach der Zäsur, der Problematisierung und daran anschließend der Lösung – was war, was ist, was könnte sein? Auch in den Versuchen, der Phänomene der computergestützten, digitalen Überwachung analytisch habhaft zu werden, steckt immer auch eine narrative Struktur, die ihrerseits Erwartungen und Befürchtungen prägt.

Überwachungspraktiken sind historisch betrachtet keine neue Entwicklung und dennoch wird ihre seit vier Jahrzehnten andauernde und stets zunehmende Bedeutung – wie bereits ausgeführt (vgl. Abschnitt 1) – als zentrales Ordnungsprinzip der Spätmoderne identifiziert.[80] Angesichts der Beschwörung einer *surveillance society*[81] und den *surveillance studies* als beigeordneter akademischer Disziplin,[82] stellt sich allerdings die Frage, ob es sich bei ihren Gegenständen tatsächlich um Ausprägungen eigenständiger Phänomene handelt, oder durch die Ausrufung eines eigenen Zeitalters die historische Kontinuität der untersuchten Entwicklungen zum Verblassen gebracht wird.

Unbestritten ist hingegen, dass qualitative Veränderungen von Überwachungspraktiken und -techniken eine theoretische Ausdifferenzierung erfordern.[83] Am prominentesten wird eine Verschiebung der Machtverhältnisse mit diesen Veränderungen verknüpft, die stets mit einer mehr oder minder impliziten Bedrohungslage assoziiert wird. Die *new surveillance*[84] der computerbasierten Überwachung erlange ein Wissen, das das beobachtete Subjekt nicht hat. Nicht länger das einzelne Individuum, sondern eine Menge aggregierter Daten seien im Fokus dieser

79 Siehe Cantril et al. (1940) als historisches Beispiel für eine Untersuchung, welche die vorherrschenden Annahmen über die Macht des ‚neuen Massenmediums' Radio relativiert, indem sie zeigt, dass die Medieneffekte weniger in der Technik selbst als vielmehr in sozialen Kontexten und psychologischen Prädispositionen zu verorten sind.

80 Vgl. Lyon et al. (2012: S. 1).

81 Vgl. Lyon (1994).

82 Vgl. Lyon et al. (2012: S. 2).

83 Die im Folgenden gestreiften theoretischen Ansätze werden in detaillierter Form in Bächle (2016a) diskutiert.

84 Vgl. Marx (2002).

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

Überwachung. Der Begriff *dataveillance*[85] beschreibt die technische Praxis des Aufbaus und der Analyse großer Datenbestände, mit denen Filterfunktionen im Sinne einer Rasterfahndung möglich werden. Begriffe wie *electronic superpanopticon*[86] stellen sich in Kontinuität zum Panoptismus, betonen jedoch zugleich, dass sich durch die Netzstruktur und die Logik der Datenbank die klassischen Grenzziehungen (innen/außen, Beobachter*innen/Beobachtete) nicht aufrechterhalten lassen. Die Rede von einer *digital enclosure*[87] wiederum unterstreicht die Spezifik der digitalen Kommunikationsmedien, in denen neben den Interaktionen selbst auch Daten *über* diese entstehen (z. B. Ort, Zeit und Dauer). Fuchs et al.[88] betonen den globalen Maßstab datenbankbasierter Internet- und Social Media-Überwachung und deren erhebliche sozialen und ökonomischen Implikationen. Zuboff[89] diagnostiziert eine neue Form des Kapitalismus – *surveillance capitalism* – mit negativen Effekten auf die demokratische Ordnung; Couldry/Mejias[90] erzählen die universelle Datafizierung vor einer narrativen Schablone des Kolonialismus (*data colonialism*), in der die massenhafte Datenextraktion als gleichbedeutend mit der Aneignung sozialer Ressourcen begriffen wird.

Doch auch eine Neujustierung der Machtverhältnisse findet sich in den wissenschaftlichen Konzepten, die neue Formen der Überwachung beschreibbar machen wollen und sie dadurch zugleich auf eine bestimmte Weise narrativieren: *Counter surveillance* wendet sich gegen bestehende Hierarchien durch den Mächtigen entgegengesetzte Praktiken der Überwachung. Dazu zählen beispielsweise die Dokumentation von Polizeigewalt durch Smartphone-Kameras, die sich in durch soziale Medien hergestellten Öffentlichkeiten einfach und schnell verbreiten kann, oder auch *leaking* von geheimgehaltenen Dokumenten. Zusammen mit Formen gegenseitiger Überwachung (der alltäglichen Recherche anderer Personen etwa) als *lateral surveillance*[91] werden die Machtverhältnisse und -dynamiken diffus und komplexer.[92] Zugleich findet sich aber auch die Gegenfigur des totalen Überwachungsstaats, die derzeit am häufigsten auf China als ein mahnendes Beispiel projiziert wird.[93]

85 Vgl. Clarke (1994).
86 Vgl. Poster (1990).
87 Vgl. Andrejevic (2007).
88 Vgl. Fuchs et al. (2012).
89 Vgl. Zuboff (2015).
90 Vgl. Couldry/Mejias (2018).
91 Vgl. Andrejevic (2005).
92 Vgl. Brakel et al. (2015).
93 So titelt etwa das britische Magazin *The Economist* am 2. Juni 2018: „The Surveillance State. Perfected in China, a Threat in the West". Vgl. The Economist (2018).

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

Die derzeit diskutierten Probleme im Kontext der digitalen Überwachung werden bestimmt von Diskursen um den Schutz von Privatheit und personenbezogenen Informationen, um technische Lösungen zur Herstellung von Datensicherheit oder den (Un-)Möglichkeiten, Verantwortungs- oder Haftungsfragen im Kontext der Verarbeitung von Daten eindeutig zu bestimmen. Die konzeptionelle Vielfalt bei der gegenwärtigen Theorienbildung zum Gegenstand der Überwachung bringt folglich auch eine erhebliche Unsicherheit zum Ausdruck.

Die Praxis der Überwachung – solange sie aus einer dyadischen Struktur aus Beobachter*innen und Beobachtetem bestand – kannte klare Zuschreibungen von Akteur*innen und damit einhergehende Konzepte. Die ‚moderne Anordnung' übersetzt dieses Schema in Relationen wie Staat/Bürger*innen oder Öffentlichkeit/Privatheit. Dies scheint konzeptionell überholt, denn die dyadischen Strukturen bilden vor allem das Verhältnis eines zentral organisierten Staats zu seinen Bürger*innen ab.[94]

Wie weiter oben dargelegt, sind die gegenwärtigen Narrative der digitalen Überwachung die direkte Folge aus noch immer prävalenten epistemologischen sowie politisch-institutionellen Dualismen der Moderne, die jedoch – angesichts der ökonomischen Akteur*innen und neuen Praktiken der Sichtbarmachung des Selbst – sowohl in konzeptioneller als auch in struktureller Hinsicht an Gültigkeit eingebüßt haben. Ließ sich etwa Verantwortung ehemals einzelnen, klar definierten Akteur*innen zuschreiben, liegt heute eine netzwerkartig organisierte *agency* vor, in der Verantwortung verteilt ist[95] und gern als Liste von Algorithmen, Programmierer*innen, Hersteller*innen, Nutzer*innen etc. ausbuchstabiert wird. Auch hierin darf man eine (narrative) Verschiebung in der Zuschreibung von Verantwortung mit dem Ziel der Kontingenzreduktion wähnen.[96] *Distributed agency* führt zu *distributed responsibility*. Was theoretisch-konzeptionell überzeugt, bleibt jedoch praktisch unbefriedigend. Das Konzept der Verteilung klärt Verantwortlichkeit nicht auf, sondern stellt lediglich ihre ‚Diffusion' fest und Verantwortbarkeit damit gleichzeitig in Frage.

Die Suche nach ‚Lösungen' als Antwort auf die diagnostizierten Probleme orientiert sich dennoch an eben jenen klaren Strukturen (z. B. Öffentlichkeit/Privatheit oder Verantwortlichkeit) als einem Ideal. Lösungen weisen damit selbst eine narrative Struktur auf, die auf die ehemals geordneten Verhältnisse rekurriert und das (prinzipiell) unerreichbare Ziel ausgibt, diese unter veränderten

94 Zu den dynamischen Kontexten des Konzepts Privatheit siehe etwa Nissenbaum (2010).

95 Vgl. Mittelstadt et al. (2016).

96 Vgl. Hempel (2017).

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

sozialen und technologischen Bedingungen wiederherzustellen. Sie müssen an der Praxis scheitern.

5. Schluss

Die nunmehr digitalen Überwachungstechniken und -praktiken sind sowohl symptomatisch als auch konstitutiv für größere gesellschaftliche und technologische Entwicklungen. Die zahlreichen Widersprüche in ihrer Bewertung rühren nicht zuletzt daher, dass die lange verlässliche Ordnung der Moderne seit Jahrzehnten an Gültigkeit einbüßt. Überwachung – reduziert meist auf eine bedrohlich entworfene Technik – wird als einer der Urheber dieses Zerfallsprozesses inszeniert. Die Sorge um ihre destruktive Macht und um ihre unkontrollierbare Allwissenheit findet Widerhall in den allgemeinen Unsicherheiten der Spätmoderne. Dabei wird nicht nur häufig verkannt, dass Überwachung nicht nur die Bedrohung ist, als die sie erzählt wird. Selbstverständlich kann sie die persönliche Freiheit und Autonomie bedrohen, doch ist sie zugleich ein wichtiges Werkzeug, diese überhaupt erst herzustellen. Auch scheint es, als würde mit den Gefahrennarrativen zugleich die strukturelle Klarheit und Sicherheit einer modernen Welt zurückgesehnt.

Überwachung erfüllt in einem instrumentellen Sinne wichtige gesellschaftliche Funktionen. Sie muss jedoch stets aufs Neue legitimiert und einer kritischen Bewertung unterzogen werden. Die narrativen Muster dürfen dabei ihre Evaluation nicht überlagern: Überwachung darf nie Selbstzweck oder *default* sein. Wie wird sie gerechtfertigt? Welche Wissensformen werden in ihr generiert und zu welchem Zweck werden sie eingesetzt? Welche Wertungen und Hierarchien werden durch Anordnungen der Überwachung bereits durchgesetzt? Welche Subjekte und sozialen Gruppen werden auf welche Weisen gedeutet?

Die Theorie selbst erzählt stets eine eigene Geschichte. Dieser Text ist keine Ausnahme.

Literaturverzeichnis

Andrejevic, Mark (2005): „The work of watching one another: Lateral surveillance, risk and governance". In: *Surveillance and Society*. Bd. 2, Nr. 4, S. 479–497.

Andrejevic, Mark (2007): *iSpy: Surveillance and Power in the Interactive Era*. Lawrence: University Press of Kansas.

Angwin, Julia et al. (2016): „Machine Bias. There's software used across the country to predict future criminals. And it's biased against blacks". In: *ProPublica* vom 23.05.2016. URL: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (02.07.2020).

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

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

Bächle, Thomas Christian (2016b): „Das Smartphone, ein Wächter. Selfies, neue panoptische Ordnungen und eine veränderte sozialräumliche Konstruktion von Privatheit". In: Beyvers, Eva et al. (Hrsg.): *Räume und Kulturen des Privaten*. Wiesbaden: Springer VS, S. 137–164.

Bächle, Thomas Christian (2019): „‚Hochinvasive Überwachung' und der Verlust der Autonomie (die es nie gab?)". In: Thimm, Caja/Thomas Christian Bächle (Hrsg.): *Die Maschine: Freund oder Feind? Mensch und Technologie im digitalen Zeitalter*. Wiesbaden: Springer, S. 231–259.

Bächle, Thomas Christian (2020): „Die Spur des simulierten Anderen – Humanoide soziale Roboter und die Imitation des Emotionalen". In: Klimczak, Peter et al. (Hrsg.): *Maschinen (in) der Kommunikation – Forschung im digitalen Zeitalter*. Wiesbaden: Springer VS, S. 143–167.

Bächle, Thomas Christian et al. (2017): „Sensor und Sinnlichkeit. Humanoide Roboter als selbstlernende soziale Interfaces und die Obsoleszenz des Impliziten". In: Ernst, Christoph/Schröter, Jens (Hrsg.): *Medien, Interfaces und implizites Wissen*. Themenheft der Zeitschrift *Navigationen*. Bd. 17, Nr. 2. Siegen: Universitätsverlag, S. 66–85.

Baudrillard, Jean (2014): *Simulacra and Simulation*. Ann Arbor: University of Michigan Press.

Bauman, Zygmunt (2003): *Flüchtige Moderne*. Frankfurt am Main: Suhrkamp.

Beck, Ulrich (1986): *Risikogesellschaft. Auf dem Weg in eine andere Moderne*. Frankfurt am Main: Suhrkamp.

Berkman, Bernard A. (1971): *The Assault on Privacy: Computers, Data Banks, and Dossiers, by Arthur R. Miller, 22 Case W. Res. L. Rev. 808 (1971)*. URL: https://scholarlycommons.law.case.edu/caselrev/vol22/iss4/10 (02.07.2020).

Bernard, Andreas (2017): *Komplizen des Erkennungsdienstes. Das Selbst in der digitalen Kultur*. Frankfurt am Main: Fischer.

Bogard, William (2007): „Surveillance, its simulation, and hypercontrol in virtual systems". In: Hier, Sean P./Joshua Greenberg (Hrsg.): *The Surveillance Studies Reader*. Maidenhead: Open University Press, S. 95–103.

Boyd, Danah/Crawford, Kate (2012): „Critical questions for big data". In: *Information, Communication & Society*. Bd. 15, Nr. 5, S. 662–679.

Brakel, Rosamunde van et al. (Hrsg.) (2015): „Surveillance Assymetries and Ambiguities". In: *Surveillance and Society*. Bd. 13, Nr. 3/4, S. 324–326.

Bruns, Axel (2019): „Filter Bubble". In: *Internet Policy Review*. Bd. 8, Nr. 4.

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

Bucher, Taina/Helmond, Anne (2017): „The Affordances of Social Media Platforms". In: Burgess, Jean et al. (Hrsg.): *The SAGE Handbook of Social Media*. London: SAGE, S. 233–253.

Calo, Christopher James et al. (2011): „Ethical implications of using the paro robot, with a focus on dementia patient care". In: AAAI (Hrsg.): *Human-Robot Interaction in Elder Care. Papers from the 2011 AAAI Workshop*. Menlo Park: AAAI Press, S. 20–24.

Cantril, Hadley et al. (1940): *The Invasion from Mars. A Study in The Psychology of Panic*. Princeton: Princeton University Press.

Chittaranjan, Gokul et al. (2011): „Who's Who with Big-Five: Analyzing and Classifying Personality Traits with Smartphones". In: *Proceedings of the 15th Annual International Symposium on Wearable Computers (ISWC)*, S. 29–36.

Chodowiecki, Daniel (1787): „Auge der Vorsehung". In: *zeno.org*. URL: http://www.zeno.org/nid/20003936503 (24.06.2020).

Christl, Wolfie (2017): „Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions". In: *Cracked Labs* vom Juni 2017. URL: https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf (02.07.2020).

Clarke, Roger (1988): „Information technology and dataveillance". In: *Communications of the ACM*. Bd. 31, Nr. 5, S. 498–512.

Couldry, Nick/Mejias, Ulises A. (2018): „Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject". In: *Television & New Media*. Bd. 20, Nr. 4, S. 336–349.

Deleuze, Gilles (1992): „Postscript on the Societies of Control". In: *October*. Nr. 59, S. 3–7.

Equivant (o. J.): *Northpointe Suite. Automated Decision Support*. URL: http://equivant.wpengine.com/wp-content/uploads/Northpointe_Suite-1.pdf (02.07.2020).

Finn, Jonathan (2012): „Seeing Surveillantly. Surveillance as Social Practice". In: Doyle, Aaron et al. (Hrsg.): *The global Growth of Camera Surveillance*. London: Routledge, S. 67–80.

Foucault, Michel (1983): *Der Wille zum Wissen. Sexualität und Wahrheit 1*. Frankfurt am Main: Suhrkamp.

Foucault, Michel (1994): *Überwachen und Strafen. Die Geburt des Gefängnisses*. Frankfurt am Main: Suhrkamp.

Fuchs, Christian et al. (Hrsg.) (2012): *Internet and Surveillance. The Challenges of Web 2.0 and Social Media*. New York/London: Routledge.

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

Ghosh, Dipayan/Scott, Ben (2018): „Facebook's New Controversy Shows How Easily Online Political Ads Can Manipulate You". In: *Time Magazine* vom 19.03.2018. URL: https://time.com/5197255/facebook-cambridge-analytica-donald-trump-ads-data/ (02.07.2020).

Gitelman, Lisa/Jackson, Virginia (2013): „Introduction". In: Gitelman, Lisa (Hrsg.): *‚Raw Data' is an Oxymoron*. Cambridge: MIT Press, S. 1–14.

Goldberg, Lewis R. (1993): „The structure of phenotypic personality traits". In: *American Psychologist*. Bd. 48, Nr. 1, S. 26–34.

Habermas, Jürgen (1990): *Strukturwandel der Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft*. Frankfurt am Main: Suhrkamp.

Hayles, N. Katherine (1999): *How We Became Posthuman. Virtual Bodies in Cybernetics Literature, and Informatics*. Chicago/London: University of Chicago Press.

Helbing, Dirk (2015): *Thinking Ahead – Essays on Big Data, Digital Revolution, and Participatory Market Society*. Cham u. a.: Springer.

Helbing, Dirk (2017): „‚Big Nudging' – zur Problemlösung wenig geeignet". In: Könneker, Carsten (Hrsg.): *Unsere digitale Zukunft*. Berlin/Heidelberg: Springer, S. 49–52.

Hempel, Leon (2017): „Verantwortungszuschreibung als Kontingenzverschiebung. Verantwortungspolitiken im Kontext von IT-Sicherheit". In: Daase, Christopher et al. (Hrsg.): *Politik und Verantwortung. Analysen zum Wandel politischer Entscheidungs- und Rechtfertigungspraktiken. Politische Vierteljahrszeitschrift*. Sonderheft Nr. 52, S. 454–476.

Kammerer, Dietmar (2008): *Bilder der Überwachung*. Frankfurt am Main: Suhrkamp.

Kosinski, Michal et al. (2013): „Private Traits and Attributes Are Predictable from Digital Records of Human Behavior". In: *Proceedings of the National Academy of Sciences of the United States of America (PNAS)*. Bd. 110, Nr. 15, S. 5802–5805.

Latour, Bruno (2008): *Wir sind nie modern gewesen*. Frankfurt am Main: Suhrkamp.

Levin, Sam (2017): „New AI can guess whether you're gay or straight from a photograph". In: *The Guardian* vom 08.09.2017. URL: https://www.theguardian.com/technology/2017/sep/07/new-artificial-intelligence-can-tell-whether-youre-gay-or-straight-from-a-photograph (02.07.2020).

Lyon, David (1994): *The Electronic Eye: The Rise of Surveillance Society*. Cambridge: Polity.

Lyon, David (2002): „Everyday surveillance. Personal data and social classifications". In: *Information, Communication and Society*. Bd. 5, Nr. 2, S. 242–257.

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

Lyon, David (2012): *Surveillance Studies. An Overview*. Cambridge: Polity.

Lyon, David et al. (2012): „Introducing Surveillance Studies". In: Ball, Kirstie et al. (Hrsg.): *Routledge Handbook of Surveillance Studies*. London/New York: Routledge, S. 1–11.

Marx, Gary T. (2002): „What's new about the ‚new surveillance'? Classifying for change and continuity". In: *Surveillance & Society*. Bd. 1, Nr. 1, S. 9–29.

Mayer-Schönberger, Viktor/Cukier, Kenneth (2013): *Big Data. A Revolution that Will Transform How We Live, Work and Think*. London: John Murray.

Miller, Arthur R. (1971): *The Assault on Privacy: Computers, Data Banks, and Dossiers*. Ann Arbor: University of Michigan Press.

Miller, Arthur R. (1973): *Der Einbruch in die Privatsphäre. Datenbanken und Dossiers*. Neuwied: Luchterhand.

Mirsch, Tobias et al. (2017): „Digital nudging: Altering user behavior in digital environments". In: Leimeister, Jan M./Brenner, Walter (Hrsg.): *Tagungsband 13. Internationale Tagung Wirtschaftsinformatik: ‚Towards Thought Leadership in Digital Transformation'*. St. Gallen: o. V., S. 634–648. URL: https://wi2017.ch/images/tagungsband_wi_2017.pdf (21.01.2020).

Mittelstadt, Brent D. et al. (2016): „The ethics of algorithms: Mapping the debate". In: *Big Data & Society*. Bd. 3, Nr. 2, S. 1–21.

Nassehi, Armin (2019): *Muster. Theorie der digitalen Gesellschaft*. München: C. H. Beck.

Nissenbaum, Helen (2010): *Privacy in Context. Technology, Policy and the Integrity of Social Life*. Stanford: Stanford University Press.

Northpointe (2015): *Practitioner's Guide to COMPAS Core*. URL: https://assets.documentcloud.org/documents/2840784/Practitioner-s-Guide-to-COMPAS-Core.pdf (02.07.2020).

Northpointe (o. J.): *COMPAS CORE Risk/Needs Assessment and Case Planning*. URL: http://www.northpointeinc.com/files/downloads/Risk-Needs-Assessment.pdf (02.07.2020).

Penny, Simon (1994): „Virtual reality as the completion of the enlightenment project". In: Bender, Gretchen/Druckrei, Timothy (Hrsg.): *Cultures on the Brink. Ideologies of Technology, Discussions in Contemporary Cultures*. Nr. 9, S. 65–77.

Petersen, Julie K. (2013): *Introduction to Surveillance Studies*. Boca Raton: CRC Press.

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

ProPublica (2016): *COMPAS Risk Assessment, COMPAS-CORE*. URL: https://www.documentcloud.org/documents/2702103-Sample-Risk-Assessment-COMPAS-CORE.html (02.07.2020).

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

Richardson, Rashida et al. (2019): „Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice". In: *New York University Law Review Online* vom 13.02.2019. URL: https://ssrn.com/abstract=3333423 (02.07.2020).

Rule, James B. (2007): „Social control and modern social structure". In: Hier, Sean P./ Greenberg, Joshua (Hrsg.): *The Surveillance Studies Reader*. Maidenhead: Open University Press, S. 19–27.

Sennett, Richard (1983): *Verfall und Ende des öffentlichen Lebens. Die Tyrannei der Intimität*. Frankfurt am Main: Fischer.

Sewell, Graham/James R. Barker (2007): „Neither good, nor bad, but dangerous: surveillance as an ethical paradox". In: Hier, Sean P./Greenberg, Joshua (Hrsg.): *The Surveillance Studies Reader*. Maidenhead: Open University Press, S. 354–367.

Sheller, Mimi/Jahn, Urry (2007): „Mobile transformations of ‚public' and ‚private' life". In: Hier, Sean P./Greenberg, Joshua (Hrsg.): *The Surveillance Studies Reader*. Maidenhead: Open University Press, S. 327–336.

Stark, Luke (2018): „Algorithmic Psychometrics and the Scalable Subject". In: *Social Studies of Science*. Bd. 48, Nr. 2, S. 204–231.

Stoddart, Eric (2012): „A surveillance of care. Evaluating surveillance ethically". In: Ball, Kirstie et al. (Hrsg.): *Routledge Handbook of Surveillance Studies*. London/New York: Routledge, S. 369–376.

Sunstein, Cass R. (2005): *Laws of Fear: Beyond the Precautionary Principle*. New York: Cambridge University Press.

Susser, Daniel et al. (2019): „Technology, autonomy, and manipulation". In: *Internet Policy Review*. Bd. 8, Nr. 2.

Thaler, Richard H./Sunstein, Cass R. (2008): *Nudge: Improving decisions about health, wealth, and happiness*. New Haven: Yale University Press.

The Economist (2018): „The Surveillance State. Perfected in China, a Threat in the West". In: *The Economist* vom 02.06.2018. URL: https://www.economist.com/printedition/2018-06-02 (02.07.2020).

Wang, Yilun/Kosinski, Michal (2018): „Deep neural networks are more accurate than humans at detecting sexual orientation from facial images". In: *Journal of Personality and Social Psychology*. Bd. 114, Nr. 2, S. 246–257.

Zuboff, Shoshana (2015): „Big Other: Surveillance Capitalism and the Prospects of an Information Civilization". In: *Journal of Information Technology*. Nr. 30, S. 75–89.

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

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access

Kilian Hauptmann, Martin Hennig and Hans Krah - 9783631827475
Downloaded from PubFactory at 06/13/2021 09:30:40AM
via free access