

## Überwachung, Algorithmen und Selbstbestimmung

Überwachung ist kein neues Phänomen. Nicht erst seit dem Sommer 2013, als Edward Snowdens Enthüllungen die weltweite Überwachung durch die amerikanische National Security Agency (NSA) belegten, sammeln Nachrichtendienste vertrauliche Informationen, von denen sie annehmen, dass sie für ihre Regierungen nützlich sein könnten – die Bezeichnung der Spionage als »zweitältestes Gewerbe der Welt« (Grutzpalk/Zischke 2012) deutet auf diese lange Geschichte hin. Auch in analogen Zeiten hat es Ansätze staatlicher Massenüberwachung gegeben. Ein Beispiel war die umfangreiche – doppelte – Überwachung des grenzüberschreitenden Brief- und Fernmeldeverkehrs im geteilten Deutschland (Foschepoth 2012: 42), die bis zum Mauerfall 1989 praktiziert wurde: Sowohl die östlichen als auch die westlichen Geheimdienste lasen und hörten mit, was sich die Deutschen beiderseits des »eisernen Vorhangs« mitzuteilen hatten.

Auch Unternehmen begannen bereits lange vor Beginn des Digitalzeitalters mit dem systematischen Sammeln und Auswerten von Daten: Bereits ab den 1920er Jahren versahen Banken Stadtteile und ihre Bewohner mit Bonitätsnoten (»Scorewerte«). Auf Stadtplänen wurden die Viertel mit weniger zahlungskräftiger Bevölkerung rot umrandet (»Redlining«), während die besseren Stadtteile gelb oder blau gekennzeichnet wurden. Die Bewohner rot markierter Stadtteile hatten praktisch keine Chance auf einen Kredit. Die Ergebnisse dieser Klassifizierung lassen sich bis heute besichtigen: Familien, die es sich irgendwie leisten konnten, zogen aus den rot markierten Gegenden in besser klassifizierte Stadtteile, so dass die soziale Zusammensetzung der verbliebenen Bewohnerschaft immer ungünstiger geworden ist. Die schlechte Risikobewertung beschleunigte den sozialen Abstieg ganzer Stadtregionen, wobei insbesondere ethnische Minderheiten auf der Strecke blieben.

Die Marktforschung arbeitete in analogen Zeiten ganz überwiegend mit repräsentativen Methoden, bei denen aus dem Verhalten von Stichproben auf übergreifende Stimmungen und Veränderungen geschlossen wurde. Die Vorstellung, sämtliche Transaktionen – und sei es nur in einem überschaubaren Marktsegment – zeitnah zu erfassen und auszuwerten, schei-

terte weitgehend an unzureichenden Erfassungs- und Auswertungsmöglichkeiten.

## Big Data

Nach den von Gordon Moore 1965 formulierten Erkenntnissen verdoppelt sich die Verarbeitungskapazität elektronischer Komponenten seit der Erfindung der Computertechnik in den 1940er Jahren regelmäßig (»Moore'sches Gesetz«) bei unveränderten Komponentenkosten (Moore 1965). Empirisch hat sich diese These bestätigt. Bis heute verdoppeln sich die Speicherkapazitäten von Festplatten, USB-Sticks und sonstigen Speichermedien alle 18 bis 24 Monate bei unverändertem oder sogar sinkendem Preis. Ebenso schnell beschleunigt sich die Verarbeitungsgeschwindigkeit von Prozessoren und ähnlich verhält es sich mit den Übertragungskapazitäten in Netzwerken. Das anhaltend schnelle digitale Wachstum hat dramatische Folgen: Elektronische Komponenten haben inzwischen analoge Systeme in nahezu allen Bereichen der Kommunikations-, Antriebs-, Mess- und Steuerungstechnik ersetzt. Informationen werden heute fast durchgängig digital erfasst, gespeichert, übertragen und ausgewertet.

Angesichts drastisch gesunkener Preise für Speicherchips können gewaltige Datenmengen im schnellen Hauptspeicher von Computersystemen verarbeitet werden. Mit der neuen Technik können Verknüpfungen praktisch in Echtzeit vorgenommen werden. Die digitale Verarbeitung ermöglicht nicht nur die schnelle Erschließung und Auswertung der erfassten Inhalte. Bei digitalen Transaktionen entstehen »Metadaten«, die das Umfeld der jeweiligen Aktivität beschreiben: Datenmenge und -art, Uhrzeit, Dauer, Ort, Urheber, Beteiligte usw. Diese Metadaten – in der Telekommunikation »Verkehrsdaten« genannt – fallen nebenbei an, quasi als Abfallprodukte der digitalen Verarbeitung. Erst allmählich wurde erkannt, welchen Wert sie repräsentierten. So wie in der materiellen Welt versucht wird, die im Abfall gelandeten Werkstoffe zu recyceln, bilden die Metadaten das eigentliche »Öl« des Informationszeitalters: Sie können vollautomatisch erfasst und ausgewertet werden, das Datenvolumen ist nicht annähernd so groß wie dasjenige der Inhaltsdaten und aus ihnen können umfassende Beziehungs- und Verhaltensprofile abgeleitet werden.

Neuen Schub gewinnt die Digitalisierung mit dem Einbau von Informationstechnik in alle möglichen Gegenstände. Damit verschwimmen die Grenzen zwischen der virtuellen und der realen Welt. Im »Internet der Dinge« kommunizieren Geräte, Fahrzeuge, Verpackungsmaterialien und Kleidungsstücke mit ihrer technischen Umwelt. Sie können aus dem Netz

identifiziert, geortet und gesteuert werden. Im Jahr 2015 waren bereits mehr als 15 Milliarden Gegenstände per Funktechnik – mittels »Radio Frequency Identification« (RFID) – miteinander vernetzt und es wird erwartet, dass sich diese Zahl bis 2020 mindestens verdreifachen wird. Aus dem »Internet of Things« wird damit ein »Internet of Everything« (Baker 2015). Auch wenn die massenhaft und permanent generierten Daten sich zunächst auf die Gegenstände oder Gerätschaften beziehen, können sie gleichwohl auch Aussagen über Personen enthalten. Wenn festzustellen ist, wer ein Gerät mit sich führt oder bedient, wird bei der Ortung der Sache auch der Aufenthaltsort der Person festgestellt. Das digitalisierte Auto speichert alle möglichen technischen Parameter, die das Verhalten des Halters oder Fahrers beschreiben und die ggf. auch gegen ihn verwendet werden können, etwa wenn es zu einem Unfall kommt.

Zugleich rücken Sensoren immer näher an unseren Körper heran. Bereits heute werden in Kliniken Neugeborene mit einem RFID-Armband versehen, um Verwechslungen im Krankenhaus zu verhindern. Ähnliche Projekte gibt es auch für Demenzzranke, die man auf diesem Wege daran hindern möchte, ihr Krankenhaus oder ihre Wohnanlage zu verlassen (Gneuss 2006), eine Art »elektronische Fußfessel« für Alte. Recht gut verkaufen sich Fitnessarmbänder, die nicht nur die Schritte der Trägerinnen und Träger zählen und ihren Aufenthaltsort feststellen, sondern auch ihre Schlafgewohnheiten, die Puls-Frequenz und andere Vitalfunktionen überwachen und basierend auf deren Analyse Tipps für ein gesünderes Leben liefern. Schon haben Versicherungen angekündigt, jenen Kunden einen Rabatt zu gewähren, die einen gesunden Lebensstil mittels Fitness-Tracker und »Gesundheits-Apps« nachweisen (Zeh 2014). Der nächste logische Schritt sind in den Körper eingebaute Funkchips, die zur Ortung, zur Erfassung medizinischer Werte oder auch zur Identifikation verwendet werden. Bereits jetzt werden solche Techniken in einzelnen Bereichen eingesetzt, etwa in Herzschrittmachern und bei Insulinpumpen für Zuckerkrankte.

Stand zunächst bis etwa vor zehn Jahren das einzelne Datum, der jeweilige Prozess oder die zu erfüllende Aufgabe im Mittelpunkt des Interesses (»Small Data«), änderte sich die Perspektive mit den riesigen, jederzeit verfügbaren Datenmengen dramatisch. »Big Data« steht wie kein anderer Begriff für den Übergang zu einem neuen Modell des Umganges mit Informationen. Es geht um riesige Datenmengen, »die zumeist im Rahmen einer Zweitverwertung zusammengeführt, verfügbar gemacht und ausgewertet werden« (Weichert 2013: 133). Bisweilen wird auch von den »3 V's« gesprochen: »high-volume, high-velocity and high-variety information assets«.<sup>1</sup> Die vielfältigen, aus verschiedenen Quellen stammenden

Daten generieren neue Erkenntnisse. Durch Korrelation riesiger Datenmengen können Zusammenhänge sichtbar gemacht werden, die sonst niemals aufgefallen wären.

## Algorithmische Klassifikation

Bei der automatisierten Informationsverarbeitung werden Daten nach Regeln verarbeitet, sogenannten Algorithmen. Die klassischen Small-Data-Algorithmen orientieren sich an der jeweiligen Aufgabe. Es geht um möglichst effiziente Verfahren, mit denen sich aus einer definierten Datenmenge ein Ergebnis erzielen lässt – etwa die Abwicklung der Gehaltszahlung. Welche Daten erforderlich sind, ergibt sich aus der jeweiligen Aufgabe – in unserem Beispiel: Arbeitsstunden, Tarifgruppe, individuelle Zulagen. Niemand wäre vor 20 oder 30 Jahren auf die Idee gekommen, zur Gehaltsberechnung Daten über das Wetter, das Verkehrsaufkommen in einer Hauptstraße oder den Verlauf der letzten Grippeepidemie heranzuziehen.

Heute richtet sich das Interesse immer stärker auf Big-Data-Algorithmen, die sich nicht deterministisch an einer Aufgabe bzw. einem Zweck orientieren. Bei ihnen stehen Korrelationen, also statistische Zusammenhänge im Mittelpunkt. Die meisten erfolgreichen Internetangebote verwenden solche Big-Data-Verfahren, um zielgerichtete, personalisierte Werbung ohne die bei den klassischen Massenmedien unvermeidlichen hohen Streuverluste auszuliefern.

Solche Algorithmen liefern zunehmend die Grundlage für Entscheidungen, die für unser Leben von existenzieller Bedeutung sind: ob wir einen Kredit erhalten und wenn ja zu welchen Konditionen, ob wir in eine Versicherung aufgenommen werden und wie hoch die Prämie ist, die wir zu zahlen haben. Algorithmen schlagen vor, welche Bewerber auf einen Arbeitsplatz zum Vorstellungsgespräch eingeladen werden sollen, wer für eine Beförderung in Frage kommt und wer ein Entlassungskandidat ist. Die Verknüpfung einer Vielzahl von Vitaldaten ermöglicht die frühzeitige Erkennung von Krankheiten. Daten aus Anfragen bei der Internet-Suche geben Hinweise auf Epidemien und ermöglichen schnelle Gegenmaßnahmen zu deren Eindämmung.

Ein zentrales Merkmal der auf Big Data basierenden algorithmischen Steuerung ist die Klassifizierung, d. h. die Zuordnung von Datenelementen zu bestimmten Gruppen.

Heute bedient man sich angesichts einer verbesserten Datenlage und leistungsfähiger Computer sehr viel differenzierterer Methoden zur Berech-

nung individueller Risiken als beim oben beschriebenen »Redlining«. In die Bonitätsnoten fließen die verschiedensten Daten über eine Person ein, die mit Durchschnittswerten verglichen werden. Das Ergebnis, der »Scorewert«, bildet nicht das tatsächliche Verhalten einer einzelnen Person ab, sondern nur ein typisiertes, anhand statistischer Referenzwerte errechnetes Ergebnis. Das individuelle Risiko wird durch Vergleich mit den Werten anderer Personen bewertet, deren Daten hinsichtlich möglichst vieler Faktoren (etwa Wohnort, Alter, Geschlecht, Anzahl der Bankkonten und der Handy-Verträge, Social-Media-Aktivitäten) denen der betroffenen Person entsprechen.

Auch in anderen Bereichen werden Algorithmen eingesetzt, um Verhaltensmuster und Eigenschaften zu erkennen. Intelligente Videosysteme, die Aufnahmen aus digitalen Überwachungskameras analysieren, sollen Geschlecht, Alter oder andere Verhaltensinformationen der aufgenommenen Personen klassifizieren und ihr Verhalten vorhersagen. Vielfach merkt man gar nicht, dass man gerade Gegenstand einer automatisierten Bewertung ist: Der Besucher eines Einkaufszentrums sieht zwar vielleicht die Videokamera, er kann aber nicht erkennen, was mit den Aufnahmen im Hintergrund passiert. Auch bei der Internetnutzung erfolgt die individuelle Klassifizierung im Hintergrund. Zudem werden von Nutzerinnen und Nutzern, bei denen eine erhöhte Zahlungsbereitschaft vermutet wird, für dieselbe Leistung höhere Preise verlangt als von denjenigen, die vermutlich einer niedrigeren Einkommensgruppe angehören (Preisdifferenzierung) (Wilson 2014) – auch dies geschieht, ohne dass der Betroffene dies bemerkt.

Besonders problematisch sind diskriminierende Folgen der Klassifikation. Der Schutz vor Diskriminierung gehört zu den grundlegenden Menschenrechten.<sup>2</sup> Niemand darf wegen seiner Rasse, Hautfarbe, des Geschlechtes, der Sprache, der Religion, politischer oder sonstiger Anschauungen, nationaler oder sozialer Herkunft, Geburt oder seines sonstigen Standes benachteiligt werden. Nicht jede unterschiedliche Behandlung stellt allerdings eine Diskriminierung dar, insbesondere dann nicht, wenn für sie ein sachlicher Grund vorliegt. Es liegt auf der Hand, dass bei einer einzelfallbezogenen Betrachtung nachvollziehbare, auf das konkrete Individuum bezogene Gründe für eine unterschiedliche Behandlung nachzuweisen sind. Dagegen liefern Big-Data-Analysen nur scheinbar objektive Gründe, bei denen es sich bei näherem Hinsehen um nichts anderes als um Schlussfolgerungen aus Wahrscheinlichkeiten handelt. Wenn aber eine Person nicht nach ihrem tatsächlichen Verhalten, ihren Fähigkeiten und Eigenschaften, sondern nur gemäß einer mehr oder minder groben Klassifikation beurteilt wird, ist das Ergebnis zwangsläufig kein gerechtes Urteil, sondern eine besondere Form des Vorurteils.

Wie die Harvard-Forscherin und ehemalige Chefin der Technologieabteilung der *Federal Trade Commission*, Latanya Sweeney, beschreibt, führt schon die namentliche Google-Suche zur Diskriminierung (Sweeney 2013): Die Eingabe eines Namens, der eher auf einen Farbigen hinweist, führt zur Einblendung von Informationen über vermeintliche Verbindungen zu Kriminalität, Vorstrafen oder Gefängnisaufenthalte, und zwar auch dann, wenn derartige Verwicklungen in dem konkreten Fall nicht vorliegen. Dagegen führt die Suche nach »weißen« Vornamen nicht zur Anzeige derartiger diskriminierender Sachverhalte. Angesichts der Tatsache, dass heute praktisch sämtliche Bewerber um einen Job zunächst einmal vom potenziellen Arbeitgeber oder privaten Jobvermittler gegoogelt werden (Boyd u. a. 2014: 55), ist es naheliegend, davon auszugehen, dass diese Assoziationen zu einer Benachteiligung führen.

Bis heute werden die meisten Algorithmen von Menschen programmiert, wobei die Komplexität der immer ausgefeilteren Verarbeitungsmodelle selbst für Spezialisten kaum noch zu beherrschen ist. An Bedeutung gewinnen selbstlernende Systeme, die sich anhand der erzielten Ergebnisse selbst optimieren. Die dabei eingesetzten Methoden werden als »künstliche Intelligenz« (KI) bezeichnet. Die Funktionsweise dieser Modelle lässt sich allenfalls aus den erzielten Ergebnissen herleiten. Dass sich derartige KI-Systeme durchaus manipulieren lassen, zeigte im Frühjahr 2016 der selbstlernende Chat-Bot »Tay«, der allein auf Basis der Auswertung von Twitter-Meldungen selbstständig Meldungen verfassen sollte. Nachdem er von anderen Twitter-Nutzern entsprechend »gefüttert« worden war, gab er selbst rechtsradikale Antworten, leugnete den Holocaust, so dass ihn Microsoft nach kurzer Zeit wieder aus dem Verkehr zog (Graff 2016).

## Wie lassen sich Überwachung und Diskriminierung eindämmen?

Technische Systeme lassen sich gestalten – diese geschichtlich vielfach belegte Binsenweisheit darf angesichts der verbreiteten digitalen Technikgläubigkeit nicht vergessen werden. Die durch die digitale Revolution entstehenden gesellschaftlichen Risiken werden allein durch Marktmechanismen nicht verschwinden. Gerade die besonders erfolgreichen digitalen Geschäftsmodelle basieren darauf, immer mehr Daten in immer weniger Händen zu konzentrieren. Ausgangspunkt jeglicher politisch-rechtlichen Gestaltung ist eine Bestandsaufnahme, welche die Risiken nicht ausblendet. Dort, wo Fehlentwicklungen festzustellen oder zu befürchten sind, müssen Regeln, die den negativen Tendenzen und Praktiken entgegenwirken, entwickelt und durchgesetzt werden.

Ein Ansatz zur Technikregulierung ist das Datenschutzrecht, bei dem es letztlich um die Durchsetzung des vom Bundesverfassungsgericht bereits 1983 in seinem berühmten Volkszählungsurteil formulierten »Grundrecht auf informationelle Selbstbestimmung«<sup>3</sup> geht. Die daraus abgeleiteten, in den Datenschutzgesetzen und zuletzt auch in der Datenschutz-Grundverordnung der Europäischen Union (EU-DSGVO) niedergelegten Grundsätze der Erforderlichkeit und Zweckbindung<sup>4</sup> sind nicht allein deshalb obsolet, weil sie anscheinend nicht kompatibel mit Big-Data-Modellen sind. Allerdings lassen sich Analysen umfangreicher Datenbestände durchaus im Einklang mit dem Datenschutz durchführen, wenn dabei auf eine frühzeitige Anonymisierung der Daten, die Verwendung von Pseudonymen und die technische Absicherung der Verarbeitung geachtet wird.

Angesichts der zunehmenden Bedeutung von Algorithmen, die zur Klassifikation und Bewertung von Menschen herangezogen werden, wird die Frage nach ihrer Funktionsweise bedeutsamer. Nur wenn transparent ist, welche Daten in die jeweiligen Auswertungen und Bewertungsprozesse einfließen, nach welchen Kriterien die Klassifikation erfolgt und wie sie Entscheidungen beeinflussen, lassen sich Aussagen zu deren Rechtmäßigkeit und ethischen Vertretbarkeit gewinnen. Das Bundesverfassungsgericht hatte bereits im Volkszählungsurteil 1983 ausgeführt, dass die Wahrnehmung des Rechtes auf informationelle Selbstbestimmung voraussetzt, dass die betroffene Person weiß, welche Daten über sie gespeichert sind und wohin sie übermittelt werden.<sup>5</sup>

Schließlich ist zu fragen, inwieweit sich eine algorithmische Diskriminierung direkt verhindern lässt. Ein Beispiel kommt aus der Versicherungsbranche: Bis vor wenigen Jahren unterschieden sich die Versicherungstarife – insbesondere in der Kranken-, Renten- und Lebensversicherung – nach dem Geschlecht des Versicherungsnehmenden. Nach einem Urteil des Europäischen Gerichtshofes (EuGH) darf das Geschlecht, im Gegensatz zu anderen Faktoren, nicht mehr berücksichtigt werden. Unter Bezugnahme auf die Gleichbehandlungsrichtlinie der EU<sup>6</sup> entschied das Gericht am 1. März 2011<sup>7</sup>, dass Unisex-Tarife für neue Versicherungsverträge verpflichtend sind. Diese Rechtsprechung lässt sich auf andere Bereiche übertragen: Jede allein aufgrund von statistischen Wahrscheinlichkeiten erfolgende ethnische, religiöse, altersmäßige oder rassische Diskriminierung hat zu unterbleiben. Entsprechende gesetzliche Klarstellungen wären wünschenswert.

## Anmerkungen

- 1 Vgl. Eintrag »Big Data« im »IT Glossary« von Gartner, Inc., <http://www.gartner.com/it-glossary/big-data> (Stand: 17.02.2017).
- 2 Art. 2 der Allgemeinen Erklärung der Menschenrechte.
- 3 Bundesverfassungsgericht, Urteil vom 15.12.1983, BVerfGE 65, 1, S. 1.
- 4 Verordnung (EU) 2016/679 vom 27.04.2016, vgl. insb. Art. 6.
- 5 BVerfGE (Anm. 3), S. 43.
- 6 Richtlinie 2004/113/EG vom 13.11.2004.
- 7 Europäischer Gerichtshof, Urteil vom 01.03.2011 (C-236/09).

## Literatur

- Baker, Anthony (2015): Connected spaces: the next step for the internet of things, in: *The Guardian* vom 5. Februar, <https://www.theguardian.com/media-network/2015/feb/05/connected-spaces-should-be-the-next-step-for-the-internet-of-things> (Stand: 17.02.2017).
- Boyd, Danah/Levy, Karen/Marwick, Alice (2014): *The Networked Nature of Algorithmic Discrimination*, <http://www.danah.org/papers/2014/Data-Discrimination.pdf> (Stand: 17.02.2017).
- Foschepoth, Joseph (2012): Überwachtes Deutschland, Post- und Telefonüberwachung in der alten Bundesrepublik, Göttingen.
- Gneuss, Michael (2006): Funkchips für das Krankenhaus der Zukunft, in: *Handelsblatt* vom 10. November, <http://www.handelsblatt.com/technologie/forschung-medizin/medizin/rfid-funkchips-fuer-das-krankenhaus-der-zukunft-seite-all/2731124-all.html> (Stand: 17.02.2017).
- Graff, Bernd (2016): Rassistischer Chat-Roboter: Mit falschen Werten bombardiert, in: *Süddeutsche Zeitung* vom 3. April, <http://www.sueddeutsche.de/digital/microsoft-programm-tay-rassistischer-chat-roboter-mit-falschen-werten-bombardiert-1.2928421> (Stand: 17.02.2017).
- Grutzpalk, Jonas/Zischke, Tanja (2012): Nachrichtendienste in Deutschland, in: Bundeszentrale für politische Bildung (Hrsg.) *Dossier Innere Sicherheit*, <http://www.bpb.de/politik/innenpolitik/innere-sicherheit/135216/nachrichtendienste?p=all> (Stand: 17.02.2017).
- Moore, Gordon E. (1965): Cramming more components onto integrated circuits, in: *Electronics*, Heft 8, S. 114–117.
- Sweeney, Latanya (2013): Discrimination in Online Ad Delivery, Google ads, black names and white names, racial discrimination, and click advertising, in: *Search Engines*, Heft 3, <http://queue.acm.org/detail.cfm?id=2460278> (Stand: 17.02.2017).

- Weichert, Thilo (2013): Big Data – eine Herausforderung für den Datenschutz, in: Geiselberger, Heinrich/Moorstedt, Tobias (Hrsg.): Big Data, Das neue Versprechen der Allwissenheit, Berlin, S. 131–148.
- Wilson, Christo (2014): If you use a Mac or an Android, e-commerce sites may be charging you more, in: Washington Post vom 3. November, <https://www.washingtonpost.com/posteverything/wp/2014/11/03/if-you-use-a-mac-or-an-android-e-commerce-sites-may-be-charging-you-more/>(Stand: 17.02.2017).
- Zeh, Juli (2014): Wir werden manipulierbar und unfrei, in: Süddeutsche Zeitung vom 26. November, <http://www.sueddeutsche.de/kultur/juli-zeh-ueber-das-generalmodell-wir-werden-manipulierbar-und-unfrei-1.2232147> (Stand: 17.02.2017).