Von der (Un-)Möglichkeit, digital mündig zu sein

Tracking-Infrastrukturen und die Responsibilisierung des Individuums im Internet

Masterarbeit

zur Erlangung des Grades Master of Arts
im Studiengang Theorie und Geschichte der Wissenschaft und Technik
Studienrichtung Philosophie des Wissens und der Wissenschaften

Mareike Lisker

21.04.2023

Technische Universität Berlin
Fakultät I – Geistes- und Bildungswissenschaften
Institut für Philosophie, Literatur-, Wissenschafts- & Technikgeschichte

Inhaltsverzeichnis

1 Einleitung

Seit fast 25 Jahren kursiert nun die Forderung nach *digitaler Mündigkeit* im gesellschafts-, erziehungs- und netzpolitischen Diskurs. Dabei wird das Konzept als Universalmittel gehandelt, um den problematischen Entwicklungen und Herausforderungen zu begegnen, die durch digitale Technologien entstehen. Im Kontext von digitaler Mündigkeit wird häufig gefordert, dass Nutzer:innen digitaler Technologien – besonders des Internets – die Kontrolle über ihre eigenen Daten haben sollen, welche mithilfe der Technologien generiert, gesammelt und in Analysen verarbeitet werden, deren Ergebnisse direkt zurück in die Technologie fließen und dort angewendet werden. Durch diese Forderung werden Nutzer:innen also dafür verantwortlich gemacht, den Fluss ihrer eigenen Daten zu kontrollieren. Der Kontrollmechanismus, der in der Forderung nach digitaler Mündigkeit impliziert wird, ist ein individueller: Einzelpersonen sollen für die Kontrolle ihre eigenen Daten zuständig sein.

Seit wiederum fast 10 Jahren gibt es eine rege öffentliche Debatte über Diskriminierung und Bias in Systemen, die mit Methoden der künstlichen Intelligenz und des maschinellen Lernens arbeiten. Diese Systeme basieren auf Daten basieren und in automatisierten Entscheidungsprozessen eingesetzt werden, wobei sie historisch bedingte Diskriminierungsstrukturen reproduzieren und verstärken (vgl. O'Neil 2016; Benjamin 2019; Eubanks 2018; Noble 2018). Unter anderem im Marketing, in Einstellungsprozessen, bei der Vergabe von Krediten oder in der Strafverfolgung werden solche Systeme eingesetzt. Besonders prominent ist der Fall der Software COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), die in einigen Staaten der USA vor Gericht verwendet wird, um Vorhersagen über das Rückfallrisiko von Angeklagten bzw. Gefängnisinsass:innen zu treffen. Das Risikofallrisiko beschreibt das Risiko einer Person, eine weitere Straftat zu begehen, wenn sie frühzeitig auf Bewährung freigelassen würde. Journalist:innen konnten in einer Analyse der von dieser Software als potenziell rückfällige Straftäter:innen klassifizierten Personen feststellen, dass die Software auf Basis der Kategorie *race* diskriminierte. So wurden zum einen fast doppelt so häufig Schwarze Menschen fälschlicherweise als rückfällig bewertet und zugleich weiße Menschen häufiger fälschlicherweise als risikoarm eingestuft (vgl. Angwin u. a. 2016). Ein weiteres System von Amazon, das automatisiert über die Geeignetheit von Bewerber:innen für einen Job entscheidet, hat Frauen bei gleicher Qualifikation systematisch als weniger geeignet eingestuft als männliche Bewerber und somit sexistisch diskriminiert (vgl. Meyer 2018).

Die angeführten Softwaresysteme basieren zwar auf Daten, jedoch nicht notwendigerweise auf den Daten, die über uns als Nutzer:innen im Netz gesammelt werden. Doch werden die statistischen und informatischen Methoden und Techniken, die in den Softwaresystemen zum Einsatz gekommen sind, nicht nur in der Strafverfolgung oder in Einstellungsprozessen verwendet, sondern auch in automatisierten Prozessen im Internet. Es manifestieren sich also strukturell ähnliche Phänomene. So diskriminierten beispielsweise Werbeanzeigen auf Facebook sexistisch, da Frauen weniger Anzeigen für Stellen als Softwareentwickler:innen angezeigt wurden (vgl. Hao 2021). Sie diskriminierten außerdem rassistisch, denn Werbeanzeigen für Häuser, die zu verkaufen waren, wurden häufiger weißen Menschen angezeigt, während Mietshäuser häufiger BIPoC-Personen angezeigt wurden (vgl. ebd.). Es werden also historisch bedingte strukturelle Ungleichverteilungen auch von Facebooks bzw. Metas algorithmischen Werbesystem reproduziert: „Facebook's algorithms are somehow picking up on the current demographic distribution of these jobs [or housing situations, M.L.], which often differ for historical reasons." (vgl. ebd.)

Bemerkenswerterweise ‚kannte' keines dieser Systeme die Kategorien, auf Besis derer Menschen durch das System diskriminiert wurden. COMPAS ‚wusste' nicht, welcher *race* die Angeklagten angehören; die Entwickler:innen des Algorithmus von Amazon hatten die Kategorie ‚Geschlecht' ausgespart: „The team tried to stop the system from taking such factors into account, but ultimately decided that it was impossible to stop it from finding new ways to discriminate against female candidates." (Meyer 2018) Auch auf Facebook werden seit 2019 – nach mehreren Strafverfahren aufgrund von Diskriminierung – die Merkmale Standort, Alter, Geschlecht und ethnische Herkunft als Targeting-Kategorien ausgeschlossen (vgl. Facebook Meta 2019). Dass die Systeme dennoch Menschen auf Basis von sensiblen Kategorien diskriminieren, liegt daran, dass sie sogenannte Proxy-Merkmale identifizieren können: „proxy attributes [are] seemingly innocuous attributes that correlate with socially-sensitive attributes, serving as proxies for the socially-sensitive attributes themselves" (Johnson 2020, 9942) Durch Proxy-Merkmale lassen also aus vermeintlich harmlosen Daten von Personen sensible Merkmale wie Geschlecht, *race* oder Sexualität ableiten. Wie genau das funktioniert, werde ich im Laufe der Arbeit erörtern; worauf ich an dieser Stelle hinaus möchte, ist, dass diese Systeme Menschen auf Basis von Daten automatisiert diskriminieren und dass Daten deshalb geschützt und kontrolliert werden müssen.

Die automatisierte Diskriminierung ist ein gesellschaftlicher Ausgangspunkt dafür, dass es wesentlich ist, sich mit der Forderung nach digitaler Mündigkeit und der darin implizierten

Forderung nach individueller Kontrolle des Flusses der eigenen Daten auseinanderzusetzen. Dabei gilt es zu prüfen, ob es sich bei dem individuellen Ansatz tatsächlich um eine wirksamen Kontrollmechanismus handelt, was ich in dieser Arbeit tue. Ich argumentiere zum einen – und vor allem – dafür, dass es sich bei der individuellen Datenflusskontrolle *nicht* um einen wirksamen Kontrollmechanismus handelt, weil Individuen nicht dazu in der Lage sind, den Fluss ihrer eigenen Daten zu kontrollieren. Die als individuelle Datenflusskontrolle verstandene Forderung nach digitaler Mündigkeit stellt demnach uneinlösbare Ansprüche an Individuen und ist deshalb unangemessen. Zum anderen argumentiere ich in einer Nebenthese dieser Arbeit, dass Daten schützenswert sind und es daher einer nicht-individualistischen Art von Kontrolle über den Fluss der Daten im Digitalen bedarf. Ich zeige außerdem, dass die resultierende Dynamik – die Übertragung von Verantwortung auf Individuen, ohne dass sie dieser Verantwortung gerecht werden können – der neoliberalen Regierungslogik der Responsibilisierung entspricht.

Um mein Hauptargument herzuleiten, werfe ich in Kapitel 2 zunächst einen Blick auf die Diskurslandschaft, die sich um den Begriff der *digitalen Mündigkeit* entspinnt, und betrachte dabei die Teilforderung nach einer digital mündigen Kontrolle des Flusses der eigenen Daten genauer. In Kapitel 3 setze ich mich mit der neoliberalen Regierungslogik der *Responsibilisierung* auseinander. Dabei arbeite ich ‚Responsibilisierung' in Abschnitt 3.1. als inhärenten Begriff der Kritik heraus und stelle in Abschnitt 3.2. ihren Bezug zu digitalen Technologien her.

Während ich in Kapitel 2 und 3 begriffliche und konzeptuelle Vorarbeit leistete, beginnt ab dem vierten Kapitel der Hauptteil der Arbeit, der sich dem *Datensammeln im Digitalen* widmet. Im Laufe des Hauptteils ziehe ich mehrere Zwischenfazite, in denen ich charakteristische Merkmale für das Datensammeln im Digitalen ableite, auf die ich meine Argumente stütze. Ich setze mich mit der Frage auseinander, wie das Datensammeln im Digitalen die Kontrolle des Flusses der eigenen Daten für Individuen *verunmöglicht*. Dazu skizziere ich in Kapitel 4 zunächst die Problematik der Regierungstechnologie des *Nudging*. Nudging realisiert sich in der Gestaltung von digitalen Benutzeroberflächen häufig in Form von sogenannten Dark Patterns, die das Verhalten von Nutzer:innen unterbewusst beeinflussen. Die verhaltensbeeinflussende Gestaltung von Benutzeroberflächen durch Dark Patterns wirkt bereits erschwerend darauf, den Fluss der eigenen Daten kontrollieren zu können. Doch liegt der Fokus meiner Arbeit nicht auf der Oberfläche[1], sondern auf dem zugrundeliegenden System, dem ich mich ab Kapitel 5 zuwende. Zunächst nehme ich in Kapitel 5 eine eingehende

1 Auch wenn es das womöglich tut, soll dieses Wortspiel keineswegs suggerieren, dass eine Beschäftigung mit Benutzeroberflächen ein oberflächliches Unterfangen sei.

Untersuchung der Entwicklungsgeschichte von *Cookies* vor. Dabei spielt das Zusammenspiel von Cookies mit der *Werbeindustrie* – bzw. die Aneignung von Cookies durch die Werbeindustrie – eine zentrale Rolle. Aus den Ausführungen schlussfolgere ich in einem ersten Zwischenfazit 5.8., dass das Datensammeln im Digitalen *kontinuierlich*, *komplex* und *unsichtbar* ist. In Kapitel 6 widme ich mich *weiteren Trackingtechnologien* wie dem Fingerprinting oder dem Tracking auf dem Smartphone, welche mich zu dem zweiten Zwischenfazit 6.6. führen: Das Datensammeln im Digitalen ist *überall* und *unausweichlich*. In Kapitel 7 beschäftige ich mich mit der statistischen Vorhersagemethode der *prädiktiven Analytik*, deren Funktionsweise ich zunächst beschreibe, um daraufhin auf die Konsequenzen einzugehen, die sich für das Verhältnis der Daten aller Nutzer:innen zueinander ergeben, und was das für individuelle Privatsphäreeinstellungen bedeutet. In dem vierten Zwischenfazit 7.4. leite ich ab, dass das Datensammeln im Digitalen *prädiktiv* ist.

In Kapitel 8 beschäftige ich mich mit einem neben der Diskriminierung weiteren gesellschaftlichen Zusammenhang, der motiviert, weshalb es wichtig ist, sich mit der Realisierbarkeit der Forderung nach digitaler Mündigkeit als Kontrolle des Flusses der eigenen Daten zu beschäftigen. In dem Kapitel richte ich den Fokus auf das *Individuum*, welches unweigerlich Akteur:in in dem System aus Trackingtechnologien ist. Zunächst untersuche ich die Perspektive, die das Werbesystem auf Konsument:innen hat, und vergleiche die Verbrauchermodelle des traditionellen Werbesystems mit dem des heutigen programmatischen Marketings. Daraufhin stelle ich infrage, ob das Individuum tatsächlich die Einheit ist, in der Nutzer:innen des Systems aus Perspektive der Werbetreibenden gedacht werden können, und ob nicht vielmehr die Bezeichnung als *Dividuum* adäquater ist. Ebenso stelle ich die Konzeption der Personalisierung infrage. Hiernach ziehe ich das dritte Zwischenfazit 8.4., demnach das Datensammeln im Digitalen *dividuierend* ist.

Aus den im Laufe der vier Kapiteln hergeleiteten sieben charakteristischen Eigenschaften des Datensammelns im Digitalen schlussfolgere ich, dass es für Individuen unmöglich ist, ihre eigenen Daten zu kontrollieren, und dass es sich dabei um eine Art der neoliberalen Responsibilisierung handelt. In einem zweiten Zwischenfazit 8.5. arbeite ich zudem meine Nebenthese heraus, dass Daten schützenswert sind und es deshalb trotz der Verunmöglichung der Datenflusskontrolle durch Individuen einer nicht-individualistischen *Kontrolle* des Flusses der Daten im Digitalen *bedarf*. Dafür schlussfolgere ich, dass das Datensammeln im Digitalen *interdependent* ist.

Da bereits heute Alternativen zu Cookies als Trackingtechnologien sowie zu vermeintlich nicht-individuellen Kontrollmechanismen diskutiert werden, werfe ich in Kapitel 9 einen durch meine vorhergehenden Ausführungen geschärften, kritischen Blick auf zwei alternative Lösungsansätze. Zum einen betrachte ich in Abschnitt 9.1. das Modell des *Datentreuhänders* und zum anderen in Abschnitt 9.2. die Privacy Sandbox Initiative von *Google*. Abschließend ziehe ich in Kapitel 10 ein *Fazit* und gebe in Kapitel 11 einen *Ausblick* auf mögliche zukünftige Forschungsvorhaben, die sich aus meinen Untersuchungen ableiten lassen.

2 Digitale Mündigkeit

Im Jahr 2000 wurde die Forderung nach *digitaler Mündigkeit* erstmals von der Europäischen Kommission im Rahmen eines Sondergipfels verlautbart, dessen Thema die Digitalisierung sämtlicher Gesellschaftsbereiche der europäischen Staaten war (vgl. „eEurope – eine Informationsgesellschaft für alle“ 2000; belegt bei Neufert 2014, 33). Seit dem Jahr 2015 wird die Forderung nach digitaler Mündigkeit auch außerhalb staatspolitischer Räume hörbar, wenngleich weiterhin in politischen und vor allem netzaktivistischen Diskursen (vgl. Biselli 2015; Jonjic-Beitter 2015; Maurer 2015; Reinhold 2015; Neuschäfer und Hirsch 2018; Köster 2016; Wawrzyniak 2019). Seit dem Jahr 2016 hat sich der Begriff der digitalen Mündigkeit auch in wissenschaftlichen oder wissenschaftsnahen Arbeiten wie Abschlussberichten, Strategiepapieren oder Whitepapers etabliert (vgl. André 2016; „Nachwuchsforschungsgruppe 6: Digitale Mündigkeit“ 2018; Digital Autonomy Hub 2021).

Der Begriff der ‚Mündigkeit‘ ohne das Adjektivattribut ‚digital‘ ist laut Thomas Goll in den letzten Jahren zu einem Kampfbegriff geworden, welcher von Parteien des kompletten politischen Spektrums verwendet wird. Mündigkeit erweist sich dabei „nach Ansicht der sich Äußernden v. a. darin, dass andere sich so verhalten, wie es die *eigene* Position nahelegt“ (Goll 2021, 89; Herv. M.L.). Das heißt, eine Person wird dann als ‚mündig‘ bezeichnet, wenn sie oder er sich entsprechend dem Ideal verhält, welches die Partei – oder Sprecher:in – als mündig erachtet. Die Forderung nach digitaler Mündigkeit ist also nur dann sinnvoll, wenn klar ist, was in dem jeweiligen Kontext damit gefordert wird. Aus der noch jungen Debatte zu dem Begriff der digitalen Mündigkeit greife ich daher drei verschiedenen Antworten auf die Frage heraus, was genau die Forderung nach digitaler Mündigkeit beinhaltet. Ich verdeutliche, dass die drei Ansätze vor allem ein Merkmal eint: die Forderung nach einer individuellen Kontrolle des Flusses der eigenen Daten. Dabei beschränke ich mich nicht nur auf Ansätze aus der eben-

falls noch jungen wissenschaftlichen Auseinandersetzung mit dem Begriff, sondern beziehe auch den netzaktivistischen Diskurs mit ein.

Das Nationale E-Government Kompetenzzentrum (NEGZ) operationalisiert den Begriff der digitalen Mündigkeit als ein Zusammenspiel aus fünf sogenannten ‚Literacies', die die „Fähigkeiten der Bürger in Deutschland zum konstruktiven und souveränen Umgang mit digitalen Räumen" (Beck u. a. 2018, III) beschreiben. Die *Technical Literacy* beschreibt grundlegende Fertigkeiten zur Bedienung von Hardware und Software, wie beispielsweise das Bedienen eines Browsers oder einer Suchmaschine (vgl. ebd., 22). In Bezug auf die *Privacy Literacy* sprechen die Autor:innen zunächst von Datenschutzkompetenzen, die sich auf den Schutz der eigenen Privatsphäre im Internet beziehen (vgl. ebd., 22). An anderer Stelle bezeichnen sie Privacy Literacy jedoch als „Tätigkeiten verbunden mit der IT-Sicherheit und Datensicherheit" (ebd., 28). Die Autor:innen differenzieren an dieser Stelle also nicht zwischen den Begriffen „Datenschutz", „Datensicherheit" und „Privatsphäre" oder „Privacy", sondern verwenden sie synonym. Diese unscharfe Begriffsverwendung ist in der Debatte zwar weit verbreitet, birgt jedoch das Potenzial für Missverständnisse, da jedes dieser Begriffe unterschiedliche Bedeutungsdimensionen beinhaltet (vgl. S. 67 dieser Arbeit). Tätigkeiten, die die Autor:innen unter ‚Privacy Literacy' verbuchen, sind das Aktualisieren des Anti-Viren-Programms, das Löschen des Browserverlaufs, ob Cookies gelöscht oder blockiert werden, ob der Zugriff von Diensten auf Standortdaten eingeschränkt wird und ob Nutzer:innen die Privatsphäreeinstellungen ihrer Online-Nutzerprofile anpassen (vgl. ebd., 28).

Als *Information Literacy* wiederum verstehen Beck et al. „Fähigkeiten zum Finden und kritischen Beurteilen von Informationen im Internet." (2018, 22) Information Literacy geht insofern über die Technical Literacy hinaus, dass sie nicht nur die bloße Bedienung einer Suchmaschine abfragt, sondern auf die Fähigkeit abzielt, mithilfe dieser Suchmaschine auch zielgerichtet zu suchen, und die gefundenen Suchergebnisse zu bewerten und kritisch zu reflektieren (vgl. ebd., 29). *Social Literacy* beschreibt den Autor:innen zufolge die Sozialkompetenzen gegenüber anderen Nutzer:innen in Bezug auf Interaktionen in digitalen Räumen (vgl. ebd., 22). Die fünfte Dimension der *Civic Literacy* bezieht sich auf die Nutzung digitaler Medien zum Zwecke der politischen Meinungsbildung und -äußerung. Im Rahmen ihrer Studie haben die Autor:innen nun jede dieser Literacies in Alltagspraktiken im Umgang mit Computern verortet. So bezeichnen sie beispielsweise das Herunterladen von Dateien als Technical Literacy, das Löschen vom Browserverlauf als Privacy Literacy, das Nutzen einer Suchmaschine als Information Literacy, das Wertschätzen und Pflegen eines respektvollen Umgangs mit anderen

Menschen im Internet als ‚Social Literacy', oder das Nutzen von Online-Plattformen, um die eigenen politischen Ansichten auszudrücken, als ‚Civic Literacy' (vgl. ebd., 27ff.) Eine mögliche Antwort auf die Frage, was die Forderung nach digitaler Mündigkeit beinhaltet, ist also, dass digitale Mündigkeit als das Zusammenspiel der fünf Dimensionen der Technical Literacy, Privacy Literacy, Information Literacy, Social Literacy und Civic Literacy verstanden wird. Digitale Mündigkeit wird hier zu einer Art Füllstandsanzeige und damit zu etwas, dass eine Person – auch in graduellen Zwischenstufen – besitzen kann oder nicht. Je besser eine Person in den einzelnen Literacies abschneidet, desto größer ist die digitale Mündigkeit.

Eine zweite Antwort darauf, was die Forderung nach digitaler Mündigkeit beinhaltet, gibt die Netzaktivistin Leena Simon auf ihrer Website. Dort gibt sie Handlungsvorschläge bzw. -aufforderungen für eine angewandte digitale Mündigkeit (vgl. Simon 2022). Die Schritte reichen von konkreten Umsetzungsvorschlägen, wie einen bestimmten Browser, einen bestimmten App Store oder ein bestimmtes Betriebssystem zu verwenden, bis hin zu abstrakten Aufforderungen wie beispielsweise „vor allem vorsichtig und kritisch [zu sein]" und die eigenen „digitalen Handlungen [zu hinterfragen]". Die Leserin wird dazu aufgefordert, „die Kontrolle über Ihre Daten [zu behalten]", indem sie beispielsweise physische Speichermedien anstatt Cloudspeicher verwendet oder kostenlose Dienste dahingehend hinterfragt, ob diese nicht „mit Ihren Daten und Ihrer Freiheit" Umsatz machen würden. Außerdem soll sie „ihren Browser so [konfigurieren], dass [ihr] Dienste nicht mehr hinterher schnüffeln können: Installieren Sie dazu Add-ons, die Werbung und Tracking blockieren. Ändern Sie die Standardsuchmaschine und blockieren Sie (mindestens) Cookies von Drittanbietern." Die netzaktivistische Perspektive auf die Forderung nach digitaler Mündigkeit bezieht also – ähnlich wie die Studie des NEGZ – sämtliche Handlungen ein, die individuelle Nutzer:innen im Internet und an ihren Geräten vollziehen können. Vorrangig werden konkrete Handlungsforderungen gegeben, doch wird ebenso dazu aufgefordert, dass die individuellen Nutzer:innen die hinter digitalen Phänomenen liegenden Mechanismen und Machtstrukturen hinterfragen.

In einem dritten Ansatz stellt die Medienphilosophin Sybille Krämer die Frage in den Raum, ob es heutzutage einer digitalen Aufklärung bedarf, in der wir analog zur europäischen Aufklärung des 18. Jahrhunderts „lernen müssten, […] gegenüber uns selbst mündige Spurenleser zu werden" (Krämer 2019, 41:27) und „uns [.] zur Herrin und zum Herrn der Spuren machen [müssten], die wir nicht-intentional hinterlassen." (Krämer 2019, 40:53). Die Forderung nach digitaler Mündigkeit bedeutet Krämer zufolge also vor allem, darüber bestimmen zu können,

wer auf die eigenen Daten Zugriff hat und wer nicht – also die Kontrolle über die eigenen Daten zu haben.

Diese drei Ansätze werden aus verschiedenen Positionen heraus vertreten und haben daher – in Einklang mit Golls Feststellung, dass das, was unter mündigem Verhalten verstanden wird, auch von der Sprecherposition abhängt – unterschiedliche Schwerpunkte. Das Nationale E-Government Kompetenzzentrum ist ein politischer Akteur, der sich als „neutrale Plattform für Staatsmodernisierung und digitale Transformation der öffentlichen Verwaltung“ (Nationales E-Government Kompetenzzentrum e.V. 2022) begreift. Das NEGZ verfolgt einen deskriptiven Ansatz, um digitale Mündigkeit überhaupt erst einmal systematisch zu operationalisieren und auf diese Art und Weise messbar zu machen, sodass sie – so vermute ich – als analytisches Werkzeug im Rahmen der digitalen Transformation der öffentlichen Verwaltung eingesetzt werden kann. Der mündige Umgang mit den eigenen Daten betrifft dabei eine von fünf Dimensionen, die Privacy Literacy. Leena Simons Selbstverständnis ist das einer Netzaktivistin. Ihre Forderungen nach digitaler Mündigkeit sind daher vielmehr normativ und anwendungsorientiert. Bei einer dieser Anwendungen handelt es sich um den Umgang mit den, bzw. die Kontrolle der eigenen Daten. Sibylle Krämer wiederum nähert sich dem Begriff der digitalen Mündigkeit wiederum aus einem medienphilosophischen Interesse heraus an und zieht eine Analogie zwischen der europäischen Aufklärung des 18. Jahrhunderts, welche sich nicht mehr, wie bei Kant ([1784] 2004), um die Kontrolle der eigenen Gedanken, sondern um die Kontrolle der eigenen Daten drehen soll. Alle drei Ansätze eint also trotz der unterschiedlichen Schwerpunkte, dass in ihrem Verständnis oder ihrer Forderung nach digitaler Mündigkeit die Teilforderung nach einem mündigen Umgang mit den eigenen Daten oder nach der Kontrolle der eigenen Daten steckt. Daraus schlussfolgere ich, dass in der Forderung nach digitaler Mündigkeit unter anderen die Teilforderung steckt, den Fluss der eigenen Daten kontrollieren zu können.

3 Responsibilisierung

Eine rein deskriptive Charakterisierung des Begriffes der Responsibilisierung, ist, dass sie den Prozess bezeichnet, in dem die Verantwortung für Aufgaben, die vormals der Staat innehatte oder die bis dahin keine:r Träger:in zugeordnet waren, an individuelle Bürger:innen oder andere individuelle, nicht-staatliche Akteur:innen übertragen wird (vgl. Wakefield und Fleming 2009, 277). Unter der Metonymie ‚der Staat' werden in diesem Zusammenhang einerseits staatliche Akteur:innen, wie sämtliche öffentliche Behören und Verwaltungen, subsumiert. Andererseits fallen darunter auch private Organisationen, die auf einer Rechtsgrundlage vom Staat als verantwortlich ernannt wurden (vgl. Pohle 2022, 12). In dem neoliberalen Arrangement der Responsibilisierung wendet sich der Staat von dem wohlfahrtsstaatlichen Prinzip ab, demzufolge er die Aufgabe hat, „eine rechtlich verbürgte soziale Sicherung und Förderung aller seiner Bürger [zu gewährleisten, M.L.], indem er monetäre Transfers, soziale Dienste und Infrastruktur zur Verfügung stellt" (Schmid 2020). Stattdessen bietet er lediglich an Bedingungen geknüpfte ‚Hilfe zur Selbsthilfe' – wie beispielsweise durch Arbeitslosengeld – die auf eine begrenzte Dauer ausgelegt ist (vgl. Kölbel, Ralf u. a. 2021, 5).

Responsibilisierung hat sich in den letzten Jahrzehnten in einer Vielzahl gesellschaftlicher Bereichen manifestiert. Dies geschah besonders in Bereichen, in denen das Wohlergehen von Menschen und ihre Einbettung in die Gesellschaft von zentraler Bedeutung sind, wie der Gesundheits-, Sozial- oder Kriminalpolitik (vgl. Kölbel, Ralf u. a. 2021, 5). In der Gesundheitspolitik zeigt sich Responsibilisierung unter anderem in der „Adressierungen der Schwangeren in Geburtsvorbereitungskursen" (Tekin 2019, 1) oder in der Coronapolitik, in welcher ältere Menschen „zunehmend als Risikofaktor adressiert und im Rahmen von Aufforderungen zu eigenverantwortlicher sozialer (Selbst-)Isolierung in die Pflicht für das Gemeinwohl genommen [werden]" (Graefe, Haubner, und van Dyk 2020, 431). Sie zeigt sich dort auch in der Selbstvermessung von Gesundheitsdaten oder darin, dass Krankenkassen Präventionsmaßnahmen belohnen, was „Gesundheit [...] als zu erbringende Leistung nicht mehr im Gesundheitssystem, sondern bei dem je individuellen Gesundheitshandeln verortet" (Achatz und Selke 2022, 371). In die Profession der Sozialen Arbeit erhielt Responsibilisierung in dem Sinne Eintritt, dass Soziale Arbeit zunehmend „auf die Aktivierung der Individuen und deren Eigenverantwortung zielt – sowohl mit Unterstützung als auch mit Disziplinierung und Zwang" (Lutz 2018, 355). Auch in Bezug auf die Klimakrise und einen nachhaltigen Umgang mit den Ressourcen der Erde besteht „in weiten Teilen der Nachhaltigkeitsdiskussion [...] eine Tendenz, die Verantwortung auf Seiten der individuellen Akteure zu sehen" (Henkel u. a.

2018, 270). Die Responsibilisierung von Menschen in ihrer Rolle als individuelle Konsument:innen hat sich dabei „[i]nsbesondere in der öffentlichen Meinung und den Massenmedien [...] de facto weitgehend durchgesetzt“ (Henkel u. a. 2018, 422). Auch die Schulpolitik begünstigt eine Responsibilisierung der Konsument:innen, etwa wenn die Kultusministerkonferenz im Jahr 2013 die Forderung nach Verbraucherbildung in Schulen bzw. „Mündigkeit im Sinne eines verantwortlichen Konsumhandelns“ aufstellte, welche „als eine Form der Responsibilisierung von Kindern und Jugendlichen im Hinblick auf sich selbst, ihre Mit- und Umwelt gedeutet werden [kann]“ (Schütte 2020, 1088). In der Kriminalpolitik sind besonders im angloamerikanischen Raum sogenannte Neighbourhood-Watch-Vereinigungen paradigmatisch für Responsibilisierung: „through them police have encouraged communities to take responsibility for crime prevention and controlling social or physical disorder in their neighborhoods“ (Fleming 2005, 1).

Diese deskriptive Dimension macht jedoch nur einen Teil der Debatte um den Begriff der Responsibilisierung aus. Besonders in gouvernementalitätsanalytischen und machtkritischen Diskursen wird zudem untersucht, wie und wieso Responsibilisierung überhaupt funktioniert. Im Folgenden arbeite ich einige machtkritische Positionen heraus. Der Begriff der ‚Responsibilisierung‘ wandelt sich dabei von einem deskriptiven, vermeintlich neutralen Begriff in einen Begriff der Kritik. Er wandelt sich also in einen Begriff, dessen Anwendungen auf einen Sachverhalt immer auch eine kritische Perspektive auf diesen Sachverheilt impliziert.

3.1. Responsibilisierung als Begriff der Kritik

In gouvernementalitäts- und machtanalytischen Diskursen liegt die kritische Dimension des Begriffes der Responsibilisierung in dem Missstand begründet, dass die Übergabe von Verantwortung durch den Staat keineswegs auch mit einer Machtübergabe einhergehen muss. Denn den responsibilisierten Individuen werden neben der Verantwortung für eine Aufgabe nicht notwendigerweise auch die Mittel dafür übergeben, dieser Verantwortung gerecht werden zu können (vgl. Pohle 2022, 12f.).

Anstatt den Individuen mit der Verantwortung auch die Macht zu geben, behält der Staat sie nicht nur inne – er weitet sie überdies netzwerkartig aus:

> Responsibilization is not a way for the state to „pass the buck“ to other actors, but encompasses „ways of acting at a distance, of activating the governmental powers of ‚private‘ agencies, of co-ordinating interests and setting up chains of co-operative action“ (Zajko 2016, 79; nach Garland 1996, 454).

Die Akteure, denen die Verantwortung durch den Staat übergeben wurden, führen also stellvertretend seine Macht für ihn aus. Denn die Responsibilisierung führt dazu, dass Individuen oder andere Akteure die Macht des Staates verinnerlichen. Sie führen sie reflexiv aus und wenden sie auf sich selbst an, anstatt dass sie von außen kommt und sie ihr gehorchen: „an agent ‘would produce the ends of government by fulfilling themselves rather than being merely obedient’“ (Pyysiäinen, Halpin, und Guilfoyle 2017, 216; nach Rose, O’Malley, und Valverde 2006, 89).

Der Machtausweitungsprozess ermöglicht dem Staat zum einen „remote“ (vgl. Pyysiäinen, Halpin, und Guilfoyle 2017, 216) zu regieren, also aus der Ferne oder ferngesteuert seine Regierungsmacht auszuüben. Zum anderen ermöglicht er dem Staat auch, indirekt zu regieren, also gewissermaßen im Verborgenen. Denn die responsibilisierten Personen wissen nicht, dass der Staat seine Macht ausweitet, anstatt sie auch an diejenigen weiterzugeben, die die Verantwortung tragen. Und so verunmöglicht er den Individuen, der Verantwortung gerecht zu werden. Denn mit der Verschiebung der Verantwortung auf die Individuen ging auch einher, dass der metaphorische Scheinwerfer der Aufmerksamkeit auf sie gerichtet wird. Dadurch sind die responsibilisierten Personen als vermeintliche Verantwortungsträger:innen nun ebenso dafür verantwortlich, wenn sie der Aufgabe nicht gerecht werden. Es entsteht eine neue Art des „neo-liberal blaming the victim“ (Gray 2009, 330).

Dass die responsibilisierten Individuen trotz fehlender Handlungsmacht nicht die Verantwortungsannahme verweigern oder wenigstens protestieren, liegt daran, dass sie durch die der Responsibilisierung von dem Staat auf eine ganz bestimmte Art und Weise adressiert bzw. subjektiviert werden, die mit einer „creation of an attachment to a new way of thinking and behaving“ (Hache 2007, 3) einhergeht. Dabei erfolgt

> [d]ie ideologische Legitimierung [der Responsibilisierung, M.L.] [...] über die Neubestimmung der Rollen und Identitäten von Individuen als Arbeitnehmer:innen, Sozialhilfeempfänger:innen, Manager:innen, Beamt:innen, Bürger:innen, Verbraucher:innen und so weiter [...] (Pohle 2022, 12).

Die Philosophin Émilie Hache erforscht diese der Responsibilisierung zugrundeliegende Subjektivierungsprozesse bzw. Neubestimmung von Rollen und Identitäten. Responsibiliserung ist in ihren Augen „one of the major tools of this individualization“ (Hache 2007, 2). Im Folgenden schlüssele ich auf, wie Hache die Arbeitsweise der Responsibilisierung durch Subjektivierungsprozesse erklärt und inwiefern diese zu einer Individualisierung der Gesellschaft beitragen.

Responsibilisierung löst Hache zufolge zwei entgegengesetzte und komplementäre Mechanismen aus: Durch die Responsibilisierung werden zugleich ein bestimmtes Verhalten als *unerwünscht* und ein bestimmtes anderes Verhalten als *erwünscht* gedeutet.

Auf der einen Seite erscheint die Inanspruchnahme staatlicher Leistungen, wie Sozialhilfe oder Arbeitslosengeld, als unerwünscht. Sie werden als eine parasitäre Abhängigkeit vom Staat vermittelt, der dadurch eine vermeintliche Belastung erfährt. Individuen, die sich in einer solchen Abhängigkeit befinden, werden als ‚betreut' stigmatisiert. Diese Stigmatisierung beruht auf der Deutung, dass die in Anspruch nehmenden Individuen auf eine Stütze angewiesen sind und ohne diese nicht überlebensfähig seien (vgl. Hache 2007, 3).

Innerhalb der Deutungsperspektive, in der die Unterstützungsbeziehung als vermeintliche eindimensionale Abhängigkeit dargestellt wird, gilt für das Modell des Wohlfahrtstaates, dass seine Bürger:innen faul sind und sich ihren eigentlichen Pflichten entziehen (vgl. Wakefield und Fleming 2009, 277). In dieser Sichtweise bleibt verborgen, dass das Gegenteil der Fall sein kann, wenn staatliche Hilfeleistungen Individuen überhaupt erst zur Unabhängigkeit befähigen können: „Our attachment to the State is thus made undesirable by depicting it solely as a form of dependence and no longer as the condition of independence that it was for many people." (Hache 2007, 4)

Während ein bestimmtes Verhalten als unerwünscht dargestellt wird, wird auf der anderen Seite wird ein bestimmtes Verhalten als erwünscht dargestellt, welches Ausdruck von Eigenverantwortlichkeit ist. Eigenverantwortliches Verhalten zeugt davon, dass die sich entsprechend verhaltenden Individuen materiell autark sind, sie also sowohl von anderen Menschen und Institutionen unabhängig sind als auch sich selbst versorgen können:

> [C]itizens [are produced, M.L.] as individual entrepreneurs and consumers whose moral autonomy is measured by their capacity for "self-care"—their ability to provide for their own needs and service their own ambitions[2], whether as welfare recipients, medical patients, consumers of pharmaceuticals, university students, or workers in ephemeral occupations. (Hache 2007, 5 nach Brown 2006, 694).

Jede dieser durch die Responsibilisierung neubestimmten Identitäten – seien es Sozialhilfeempfänger:innen, Studierende oder Gig-Worker – werden also „als autonome, selbstbestimmte und selbsterhaltende Subjekte imaginiert [...], die als gleichberechtigte Partner:innen an einem marktlichen Austausch teilnehmen […]" (Pohle 2022, 12). Während Responsibilisierung den Subjekten Freiheit, Selbstbestimmtheit und Autonomie zuschreibt, fordert sie zugleich

2 Hache zitiert aus der französischen Übersetzung des Artikels in dem gleichen Journal, welche wiederum sich ins Englische rückübersetzt folgendermaßen liest: "moral autonomy is measured by [the] ability to take care of [oneself] – the ability to provide for one's own needs, to pursue one's own ambitions" (Hache 2007, 5)

„individual responsibility-taking, independent self-steering and ‚self-care'" (Pyysiäinen, Halpin, und Guilfoyle 2017, 216) ein.

Hache vereint all diese durch die Responsibilisierung erzeugten Identitäten und Subjekte unter dem Oberbegriff des „independent self" (2007, 14) oder ‚unabhängigen Selbst', welches in ihren Augen dasjenige paradigmatische Subjekt ist, welches durch Responsibilisierung entworfen wird. Das unabhängige Selbst ist „in theory detached from its historical and social conditions and in practice discharged of its responsibilities vis-à-vis others and of the constraints of self-reproduction" (ebd., 14). Hier verdeutlicht sich auch die Individualisierungstendenz, denn das durch die Responsibilisierung gezeichnete Idealsubjekt ist nicht in einem kollektiven, gesellschaftlichen Zusammenhang eingebettet, und befindet sich in keiner Weise in Abhängigkeit von anderen Menschen.

In seiner vermeintlichen Losgelöstheit von sozialen und historischen Bedingungen ist dieses Subjekt Hache zufolge keineswegs für alle Menschen gleichermaßen zugänglich. Ich sehe an dieser Stelle eine unmittelbare und eine mittelbare Art und Weise, wie Menschen von dem unabhängigen Selbst, das die Responsibilisierung verlangt, ausgeschlossen werden. Auf eine *unmittelbare* Art und Weise schließt Responsibilisierung nicht nur Kinder oder ältere Menschen aus, die auf gemein- bzw. gesellschaftliche Unterstützung angewiesen sind, sondern alle Menschen, die ausgerechnet aufgrund der historischen und sozialen Bedingungen, in die sie eingebettet sind, strukturell benachteiligt sind und von Diskriminierungsformen betroffen sind. Auf eine *mittelbare* Art und Weise exkludiert die Responsibilisierung außerdem Menschen, die Verantwortung für andere tragen, beispielsweise eben für Kinder oder ältere Menschen, denn sie übernehmen Sorgearbeit und haben nicht die mentalen, zeitlichen oder finanziellen Ressourcen, von wiederum anderen Menschen oder Institutionen unabhängig zu sein. Diese Verantwortung für andere wird aufgrund von hegemonialen Geschlechtervorstellungen vorrangig von Frauen übernommen.

Nun drängt sich die Frage auf, weshalb sich die Subjektivierungsform des unabhängigen Selbst weiterhin so hartnäckig hält, obwohl sie für den Großteil der Gesellschaft nicht erfüllbar ist. Die Beständigkeit der Subjektivierungsform des unabhängigen Selbst liegt Hache zufolge darin begründet, dass Responsibilisierung häufig mithilfe positiv konnotierter Begriffe wie dem des Empowerment kommuniziert wird (vgl. 2007, 5). Das Konzept des Empowerment stammt ursprünglich aus der Sozialarbeit und beruht darauf, Menschen dazu zu bewegen, (Selbst-)Verantwortung für ihre Lebenswelt anzustreben, anstatt sie von außen gestalten zu lassen. Dabei soll ihnen die Verantwortung nicht über eine neutral oder negativ assoziierte,

unidirektionale Zuweisung übertragen werden, sondern sie sollen sie aus eigenen Stücken übernehmen. Das Paradigma des Empowerment suggeriert, dass es erstrebenswert und befreiend sei, eigenverantwortlich und selbstbestimmt zu leben. Strukturelle Bedingungen werden dabei als solche verkannt. Stattdessen gelten individuelle Eigenschaften und Fähigkeiten als „learned and manufactured“ (ebd., 7). Sie werden also nicht als gegeben oder angeboren betrachtet, sondern als erlernt gedeutet, und werden somit als Attribute vermittelt, die sich individuell aneignen oder auch ablegen lassen. So gilt beispielsweise für die individuelle Gesundheit: „Considered a matter of personal choice, health becomes a sign of the ability to function in a responsible manner“ (vgl. ebd., 7). Jedoch wurde bereits vor Jahrzehnten festgestellt, dass Gesundheit auch von sozioökonomischen Faktoren sowie von sozialen und historischen Bedingungen abhängt, beispielsweise in Zusammenhang mit der Lebenserwartung: „Populations living in areas with greater income inequality have shorter life expectancies“ (Adler und Ostrove 1999, 10).

Der Soziologe Ulrich Bröckling stellt fest, dass empowered zu sein und somit frei von Abhängigkeiten zu leben, suggeriert, frei von Herrschaft zu sein (vgl. 2016). Dadurch lenkt es von der zu Beginn des Kapitels erwähnten Dynamik ab, dass durch das Regierungswerkzeug der Responsibilisierung die Macht eines Staates auf seine Bürger:innen ausgeweitet wird, indem die responsibilisierten Personen die Herrschaft internalisieren und reflexiv ausüben. Denn Bröckling zufolge sind empowerte Subjekte keineswegs frei von Herrschaft. Vielmehr ist Empowerment eine Technologie des Selbstregierens, in welcher „Autonomie, Freiheit und Eigenverantwortung [...] nicht länger die Antithese von Herrschaft dar[stellen], sondern den avanciertesten Modus ihrer Ausübung.” (ebd., 9)

Die Soziologen Jarkko Pyysiäinen, Darren Halpin und Andrew Guilfoyle sprechen in Bezug auf die Hartnäckigkeit, mit der sie sich trotz widriger Umstände als Subjektivierungsprozess hält, nicht von Empowerment, sondern differenzieren einen weiteren, komplementären Erklärungsansatz. Zunächst verweisen auch Pyysiäinen et al. auf den in Responsibilisierungstheorien populären Erklärungsansatz des ‚appeals to freedom‘, also den Anreiz der „possibilities of self-realization and maximization of quality of life“ (2017, 216). Diese Erklärung entspricht dem, was Hache mit Empowerment beschrieben hat, in dem Sinne, dass der appeal of freedom Subjekte ebenfalls über ihre positiven, also erstrebenswerten Wünsche und Ideale anruft, auf die hin sie sich entwerfen wollen. Doch stößt das Konzept des appeal of freedom laut Pyysiäinen et al. an die Grenzen seiner Erklärungskompetenz, da es folgenden Sachverhalt nicht ausreichend begründen kann:

> […] why individuals would continue to assume personal responsibility and conform to neoliberal rule even in the face of socio-economic predicament that no longer promises opportunities for personal freedom and self-realization. (ebd., 220)

Pyysiäinen et al. gehen damit noch einen Schritt weiter, als Hache es ist in ihrer Analyse gegangen ist, wenn sie feststellen, dass das Versprechen des Empowerment bzw. des appeal of freedom nicht erschöpfend erklärt, weshalb sich Menschen dem paradigmatischen unabhängigen Selbst unterwerfen, obwohl historische und soziale Bedingungen die versprochene Freiheit für sie verunmöglichen.

Die Limitationen des appeals to freedom führen Pyysiäinen et al. zu dem Modell des „threat to personal control“ (2017, 217). Der threat to personal control beruht auf der Prämisse, dass Menschen danach streben, ein Gefühl der Kontrolle über Ereignisse zu haben, sowie darüber, wie sich diese Ereignisse entwickeln und zu welchen Resultaten, oder englisch ‚outcomes‘, sie letzten Endes führen (vgl. ebd., 221).

Die Annahme, dass Menschen nach Kontrolle streben, ist ebenfalls kompatibel mit dem Modell des appeals of freedom bzw. Haches Konzept des Empowerment, welche beide auf das Gefühl von Freiheit oder Selbstermächtigung durch Kontrolle abzielen. Nun ließe sich argumentieren, dass ein logischer Zirkel vorliegt. Wenn nämlich das Subjekt, das durch Responsibilisierung entworfen wird, eines ist, das nach Kontrolle strebt, und Menschen sich als das von der Responsibilisierung propagierte unabhängige Selbst entwerfen (wollen), führt das ausgerechnet zu der Annahme, dass Menschen nach Kontrolle streben. Zu diesem möglichen Zirkelschluss äußern sich die Autoren nicht explizit. Jedoch gestehen sie ein, dass Responsibilisierung dazu beiträgt, dass Menschen nach Kontrolle streben, indem ihnen suggeriert wird, dass es möglich sei, durch eigene Entscheidungen – oder eben das Erlernen von Fähigkeiten (vgl. S. 14 dieser Arbeit) – einen Einfluss auf Ereignisse zu haben:

> people (are led to) believe [by responsibilization, M.L.] that outcomes and events are amenable to control via autonomous choices and actions and engage thus in pursuit of personal freedom, self-fulfillment and quality of life. (ebd., 222)

Um zu veranschaulichen, inwiefern der threat to personal control zu der Verfestigung von Responsibilisierung angesichts widriger Umstände beiträgt, greifen Pyysiäinen et al. auf zwei Konzepte aus der Psychologie zurück, welche beschreiben wie, Menschen auf den threat to personal control reagieren. Diese zwei Reaktionsmuster begünstigen wiederum die Responsibiliserung. Das erste psychologische Konzept ist die e*rlernte Hilflosigkeit*, welche ursprünglich als Erklärung für ein Verhalten von Tieren verwendet wurde, die über einen längeren Zeitraum hinweg periodisch unausweichlichen externen Schocks ausgesetzt waren (vgl. Over-

mier und Seligman 1967). Der Ansatz wurde daraufhin von Psycholog:innen übernommen, um auch Depressionen damit zu erklären. Die erlernte Hilflosigkeit ist ein mögliches Resultat davon, dass Individuen über eine lange Zeit hinweg erleben, dass sie keinerlei Kontrolle über externe Ereignisse ausüben können (vgl. Pyysiäinen, Halpin, und Guilfoyle 2017, 222). Sie beschreibt, dass Individuen in Anbetracht ihrer eigenen Machtlosigkeit gegenüber äußeren Umständen den Glaubenssatz verinnerlichen, ihre Kontrollfähigkeit verloren zu haben und selbst schuld an diesem Verlust zu sein. Dies führt sie dazu, zu glauben, dass sie per se unfähig seien, über externe Ereignisse Kontrolle zu haben, weshalb sie auch in Zukunft hilflos sein würden. Dieser Glaubenssatz äußert sich in einer Passivität gegenüber der eigenen Lebenssituation (vgl. Barysch 2016, 201). Pyysiäinen et al. zufolge ist erlernte Hilflosigkeit ‚stille Komplizin' der Responsibilisierung, insofern sie zu Passivität gegenüber und Akzeptanz von strukturellen Ungerechtigkeiten bzw. dem Unvermögen, einer Verantwortung gerecht zu werden, führt (vgl. 2017, 222). Zwar sind responsibilisierte Individuen möglicherweise wahrhaftig machtlos – denn es ist der Responsibilisierung inhärent, dass der Staat nicht notwendigerweise die Macht über eine Aufgabe vermittelt – doch suggeriert die Responsibilisierung stattdessen, dass sie kontrollfähig sein müssen. Denn sie haben die Verantwortung für eine Aufgabe inne und mit dieser Verantwortung geht ‚eigentlich' auch die Macht einher. Sie erleben jedoch, keine Kontrolle zu haben, woraus sie schlussfolgern, selbst schuld an ihrer Machtlosigkeit zu sein. Erlernte Hilflosigkeit trägt also insofern indirekt zur Verfestigung von Responsibilisierung bei, als dass Menschen im Angesicht von Machtlosigkeit gegenüber struktureller Ungerechtigkeiten nicht aufbegehren, sondern die Schuld bei sich selbst verorten. Hierin manifestiert sich das bereits erwähnte neoliberale Blaming-the-victim (vgl. S. 11 dieser Arbeit), demzufolge die Opfer bzw. Betroffenen sich selbst die Schuld dafür geben, der Verantwortung, der sie gar nicht gerecht werden können, nicht gerecht geworden zu sein.

Ein Gegenstück zur erlernten Hilflosigkeit, welches laut Pyysiäinen et al. mit Bezug auf den ‚threat to personal control' als zweiten Erklärungsmechanismus für die Hartnäckigkeit von Responsibiliserung im Angesicht ihrer strukturellen Verunmöglichung vorschlagen, ist die sogenannte *psychologische Reaktanz* (vgl. 2017, 222f.). Der psychologischen Reaktanz zufolge streben Individuen angesichts eines (drohenden) Kontrollverlusts umso mehr danach, ihre Kontrolle wiederherzustellen oder abzusichern – jedoch nur unter der Voraussetzung, dass sie einen Wirkzusammenhang zwischen ihrem Handeln und den Ereignissen spüren. Die Responsibilisierung wirkt hier, wie bei der erlernten Hilflosigkeit gleichermaßen indirekt: Weil Individuen die Verantwortung übergeholfen erhalten, gehen sie davon aus, dafür auch die notwen-

dige Macht zu erhalten. Da ihnen die Macht jedoch nicht notwendigerweise übergeben wird, sie aber davon ausgehen, sie zu haben, löst das in Individuen das Gefühl aus, dass ihre Kontrolle über die Aufgaben, die sie qua Responsibilisierung unter Kontrolle haben sollten, bedroht ist. Darauf reagieren sie wiederum mit einem verstärkten Kontrollbedürfnis, was dazu führt, dass sie (mehr) Verantwortung übernehmen.

3.2. Responsibilisierung im Digitalen

Die neoliberale Regierungsmodalität, die Staatsmacht indirekt vermittels Individuen oder anderen Akteuren auszuweiten, wird von Wissenschaftler:innen auch in der digitalen Sphäre identifiziert. Während in der analogen Welt – wenngleich nicht nur, so doch vor allem – Individuen die ‚Zielobjekte' der Responsibilisierung sind, wird im Digitalen auch die Responsibilisierung größerer Organisationen diskutiert. So argumentiert beispielsweise der Soziologe Mike Zajko, dass das Internet – entgegen der ursprünglich utopischen Erzählung, dass es ein Raum frei von Territorialität und Staatsgewalt sein würde – durchzogen ist von der neoliberalen Machtausweitung, beispielsweise in Form von Überwachung oder Contentfilter: „Numerous states around the world are developing and refining the exercise of state power through the internet by way of surveillance and content filtering" (Zajko 2016, 77). Zajko sieht als Zielobjekte dieser Responsibilisierung vor allem Akteur:innen in intermediären Positionen, die zwischen Endverbraucher:innen und Staat stehen und zwischen diesen vermitteln. Zu den Intermediären zählen beispielsweise alle möglichen Arten von Onlinedienstanbietern (eng. OSPs), die den Fluss verschiedenster Datenpakete zwischen Nutzer:innen und Anbietern überwachen und kontrollieren (vgl. ebd., 77). Beispiele für solche OSPs sind Zahlungsdienstleister wie PayPal, deren Metier der Geldfluss ist, oder Suchmaschinenanbieter, allen voran Google, die den Zugang zum World Wide Web ermöglichen, aber auch regulieren. Intermediäre befinden sich besonders für Staatsinteressen in einer strategisch günstigen Position: „What these intermediaries have in common is the ability to *monitor* and *control* information flows by virtue of their strategic position" (ebd., 77; Herv. M.L.). Das Überwachen, das Kontrollieren sowie das Regulieren des Informationsflusses sind dabei aus rein technischer Perspektive bereits inhärente Aufgaben der Intermediäre. So müssen beispielsweise E-Mail-Anbieter sicherstellen, dass der Betrieb ihrer Services fehlerfrei abläuft und die Datenübertragung funktioniert. Der Staat setzt also ohne großen Aufwand auf eine bereits bestehende Netzwerkinfrastruktur auf und implementiert lediglich neue Parameter, nach denen kontrolliert werden soll. Auch Internetdienstanbieter (eng. ISPs) sind wichtige Intermediäre, da sie die die Telekommunikationsinfrastruktur stellen und auf physikalischer Ebene der Glasfaserkabel den Fluss von Daten-

paketen als Stromsignale kontrollieren, und somit Zugriff auf zentrale Netzwerkknoten des Internets haben. Beispielsweise sollen Internetdienstleister eine Rolle spielen „for controlling pornography, racist materials, blasphemy, defamation, cyber-bullying, ‚anti-social' speech, and intellectual property rights" (ebd., 77). Aber auch im Hinblick auf Kriegsführung mittels Informationstechnologien befinden sich Internetdienstanbieter in den Augen des Staates in einer Schlüsselposition: „ISPs and OSPs have been enlisted as guardians of public morality, national security, and our individual privacy" (ebd., 77). So wird in einer Ansprache eines Mitarbeiters des FBIs der US-amerikanische Regierung thematisiert, dass das FBI mit dem privaten Sektor kooperiert, um sich gegen internationale Cyber-Attacken zu schützen (vgl. Wray 2022). Dabei sind „[p]rivate networks, whether they belong to a pipeline operator, some other kind of victim, or an Internet service provider, [...] most often the place we confront adversaries" (Zajko 2016, 77).

In Bezug auf Plattformen wie Google, die als Intermediäre fungieren und Zajko zufolge von Regierungen responsibilisiert werden, sollte die Frage gestellt werden, ob Regierungen in dem Falle tatsächlich ihre eigene Macht ausweiten – oder ob sie durch den responsibilisierenden Zugriff nicht auch oder vor allem versuchen, die Macht der Plattformen zu beschränken oder zumindest in sie einzugreifen. Die Frage, die außerhalb des Fokus dieser Arbeit liegt, ergibt sich daraus, dass Plattformen bereits heutzutage sehr mächtige Akteure sind. Sie sind nicht nur wirtschaftlich mächtig, weil sie vermögend sind oder Märkte dominieren. Plattformen verfügen auch eine Macht in Form von Wissen, aufgrund der vielen Daten, die sie über ihre Nutzer:innen – oder Nutzer:innen des Internets im Allgemeinen – generiert und gesammelt haben, wie in Abschnitt 5.7. dieser Arbeit deutlich wird. Mithilfe dieser ‚Wissensmacht' sind sie ind er Lage – wie Kapitel 7 zeigen wird – Nutzer:innen zu beeinflussen. Plattformen gewinnen dadurch außerdem an politischer Macht. So schreibt der Kulturwissenschaftler Michael Seemann über Mark Zuckerberg, den Geschäftsführer von Meta:

> Er hat nicht nur Macht über die 2,2 Milliarden Nutzer*innen seiner Dienste, sondern auch gegenüber nationalstaatlichen Politiker*innen, da seine Entscheidungen einen großen Einfluss auf die Geschicke von Nationalstaaten haben. (2021, 11)

Doch nicht nur Institutionen, sondern auch Individuen werden im Digitalen responsibilisiert: Die Informatiker:innen Karen Renaud et al. stellen fest, dass die Verantwortung im Umgang mit Themen der IT-Sicherheit auf die individuellen Nutzer:innen ausgelagert wird. Denn in dem Diskurs um IT-Sicherheit auf privater Ebene werden Individuen für die Sicherheit ihres eigenen Computers verantwortlich gemacht. Wie es für neoliberale Responsibilisierung cha-

rakteristisch ist, wird im Falle ihres Scheiterns den Individuen die Schuld gegeben, beispielsweise wenn sie Computerwürmer weiterverbreiten: „[people] are often blamed for not taking precautions [...]. They are given no help in dealing with the consequences of their victimhood“ (Renaud u. a. 2018, 7). IT-Sicherheit ist jedoch kein Thema, das lediglich auf individueller Ebene verhandelt werden sollte, denn Schadsoftware und Viren basieren ausgerechnet darauf, unerkannt auf möglichst vielen Computern weiterverbreitet zu werden. Sie sind keineswegs nur ein Risiko für die einzelne Benutzerin, sondern wirken sich auch auf deren Mitmenschen aus.

Bisher habe ich in dieser Arbeit zum einen gezeigt, dass in der Forderung nach digitaler Mündigkeit die Teilforderung steckt, Kontrolle über den Fluss der eigenen Daten auszuüben. Zum anderen habe ich mich eingehend mit der neoliberalen Regierungslogik der Responsibilisierung auseinandergesetzt und dargelegt, durch welche Wirkmechanismen sie funktioniert. Einer dieser Wirkmechanismen ist das Narrativ des Empowerment, welches laut Bröckling „auf nicht weniger als den ‚Ausgang des Menschen aus seiner selbstverschuldeten Unmündigkeit‘ (Kant 1784) abzielt“ (2016, 10). Die Forderung nach Mündigkeit findet sich also wieder in der neoliberalen Idee des Empowerment. Nun möchte ich die beiden Stränge – digitale Mündigkeit in Form von Kontrolle des Flusses der eigenen Daten und Responsibilisierung – zusammenführen und in den folgenden Kapiteln zeigen, dass die Forderung nach digitaler Mündigkeit in Form von indvidueller Datenflusskontrolle unangemessen ist und als eine Art der Responsibilisierung begriffen werden muss.

4 User Interfaces, Nudges und Dark Patterns

Über User Interfaces werden wir bereits heute dazu aufgefordert – und implizit dafür verantwortlich gemacht –, Kontrolle über einige unserer Daten auszuüben. Seit dem Inkrafttreten der Europäischen Datenschutzgrundverordnung (DSGVO) am 28. Mai 2018 ist die Verwendung sogenannter Cookie-Banner für alle Webseite-Betreibenden, die Cookies nutzen, um personenbezogene Daten zu verarbeiten, verpflichtend geworden.[3] Cookie-Banner sind unausweichliche Pop-Up-Fenster, die auf einer Website vorgeschaltet werden, wenn eine Nutzerin diese Website zum allerersten Mal – oder zum ersten Mal, nachdem sie alte Cookies der Website gelöscht hat – besucht. Sie fordern von der Nutzerin eine Entscheidung darüber, welche Art von Cookies die Website im Browser der Nutzerin hinterlassen darf, was somit auch eine Entscheidung darüber ist, welche Art von Daten die Website sammeln darf. In den Cookie-

3 Genau genommen sind alle Websitebetreibenden, die Erstanbieter-Analysecookies oder Drittanbietercookies sammeln, dazu verpflichtet. Werden auf einer Website lediglich funktionale Cookies wie Sitzungs- oder Warenkorbcookies gesammelt, so muss diese Website kein Cookie-Banner implementieren.

Bannern soll die Nutzerin über die Datensammelpraktiken des jeweiligen Unternehmens aufgeklärt werden, damit sie eine informierte Entscheidung treffen kann. Ob diese Entscheidung im Kontext von langen, absichtlich kompliziert und vage formulierten Ausführungen zu den Datensammelpraktiken des Unternehmens tatsächlich als informiert gelten kann, wird seit Jahrzehnten diskutiert und in Frage gestellt (Millett, Friedman, und Felten 2001; Cranor 2012; Rothchild 2018; Sloan und Warner 2013). Auf diese Debatte möchte ich an dieser Stelle jedoch nur verweisen. Stattdessen möchte ich hervorheben, dass durch die das reine Vorhandensein eines Cookie-Banners, das den Nutzer:innen eine Entscheidung dazu abverlangt, welche Daten mittels Cookies gesammelt werden. Damit wird ihnen die Verantwortung für den Umgang mit ihren eigenen Daten aufgebürdet. Cookie-Banner rufen uns als Nutzer:innen des Internets also permanent als verantwortliche Subjekte an.

Die Entscheidungen, die in Bezug auf ein Cookie-Banner getroffen werden, sind laut einer Annahme der Verhaltensökonomie, wie alle Arten von Entscheidungen, stets in eine sogenannte Entscheidungsarchitektur eingebettet. Bei Entscheidungsarchitekturen handelt es sich um „*the contexts in which people make decisions*“ (Pykett 2012, 3; Herv. i. O.), also „die sprachliche, physische, emotionale wie auch soziale Umwelt, in der Menschen Entscheidungen treffen“ (Fuhrberg 2020, 83). Die Umwelt hat direkten Einfluss auf die Entscheidung, woraus in der Verhaltensökonomie abgeleitet wird, dass eine Einflussnahme auf Entscheidungen durch die Entscheidungsarchitektur unvermeidbar ist. Wenn alles, was Teil der Umwelt ist, einen Einfluss auf die Entscheidung haben kann, kann alles zur „Stellschraube werden [...], um erwünschte Verhaltensweisen zu fördern und unerwünschte zu hemmen“ (Bröckling 2017, 191). Die Frage ist also nicht, *ob* ein Teil der Umwelt Verhalten beeinflusst, sondern *wie* dieser Teil der Umwelt Verhalten beeinflusst.

Die Entscheidungsarchitekturen werden von einer sogenannten Entscheidungsarchitektin entworfen. Indem die Entscheidungsarchitektin die Umwelt, in denen Menschen Entscheidungen trifft, moduliert, kann sie einen erheblichen Einfluss auf deren Entscheidungen ausüben und ihr Verhalten in eine bestimmte Richtung lenken. Entscheidungsarchitekt:innen sind in alltäglichen Situationen allgegenwärtig, sich jedoch nicht notwendigerweise ihrer Rolle als solche bewusst:

> Doctors describing the available treatments to patients, human-resource administrators creating and managing health-care plan enrollment, marketers devising sales strategies, ballot designers deciding where to put candidate names on a page, parents explaining the educational options available to a teenager [...] (Thaler, Sunstein, und Balz 2013, 438)

Das Einwirken auf Verhalten über die Modulation der Entscheidungsarchitektur wird gemeinhin als ‚Nudging' bezeichnet. Nudging macht sich verhaltenswissenschaftliche und psychologische Erkenntnisse darüber zunutze, wie Menschen Entscheidungen treffen, und inkorporiert diese in die Gestaltung von Umwelten, um auf Verhalten einzuwirken (Gunawan u. a. 2021, 377:3). Ein Nudge wird von anderen Arten der Verhaltensbeeinflussung abgegrenzt, insofern er gänzlich ohne Verbote oder Anreize auskommt, weshalb Nudging auch als ‚sanfte' Art und Weise gehandelt wird, Menschen zu führen (vgl. Bröckling 2017). Aus der Sanftheit resultieren zwei wesentliche Eigenschaften des Nudging. Zum einen merken Menschen aufgrund der Sanftheit häufig nicht, dass ihr Verhalten durch einen Nudge beeinflusst wurde. Sie sind sich der Entscheidung als solche womöglich gar nicht bewusst oder fühlen sich frei und nicht unter äußeren Einflüssen stehend – beispielsweise, wenn sie in einer Kantine einen Salat dazunehmen, der prominent platziert wurde, eines der bekanntesten Beispiele für einen Nudge. Durch Nudging können daher „nur jene Entscheidungen [beeinflusst werden], die ohne größeres Überlegen zustande kommen und somit nicht das Resultat einer bewussten Entscheidung sind (vgl. Kahneman 2003; 2011)." (Seitz 2022, 4) Zum anderen kann aufgrund der Sanftheit das gewünschte Verhalten nicht unbedingt hervorgerufen werden, sondern lediglich gefördert bzw. wahrscheinlicher gemacht werden. Während ein Verbot in den allermeisten Fällen bedingt, dass Menschen eine Handlung bewusst unterlassen, macht ein Nudge eine bestimmte Handlung lediglich wahrscheinlicher, aber ruft sie nicht notwendigerweise hervor. Nudging operiert daher nicht direkt auf Verhalten selbst, sondern auf Verhaltenswahrscheinlichkeiten (vgl. ebd., 164). Da ein Nugde lediglich Verhaltenswahrscheinlichkeiten beeinflusst, und somit seine Auswirkungen nie direkt in den beeinflussten Entscheidungssituationen beobachtbar sind, ist es wesentlicher Teil eines Nudges, ihn mit einer ausreichend großen Menge an Daten sichtbar zu machen und Evidenz über seine Wirksamkeit zu erzeugen (vgl. ebd., 136).

Seit dem Jahr 2008, in dem das Konzept des Nudges entwickelt und populär wurde, haben vor allem die US-amerikanische Regierung und die Regierung Großbritanniens Nudging für das Gemeinwohl ihrer Bürger:innen eingesetzt (vgl. Halpern und Sanders 2016, 54). Inzwischen wird Nudging von zahlreichen Regierungen weltweit angewendet (The World Bank 2018; Ross 2020; Aparna und Biju 2022; Reisch und Sunstein 2016; Hägele 2019). Wiederkehrend ist dabei stets die Frage – auf deren Diskussion ich in dieser Arbeit ebenfalls nur hinweise – welches Verhalten überhaupt als wünschenswert und gemeinnützig gilt, wessen Interessen davon profitieren, wer die Definitionsmacht über das Gemeinwohl hat, und ob es sich nicht vielmehr um eine Manipulation der Bürger:innen handelt.

Bei Nudging handelt es sich wie bei der Responsibilisierung um eine Regierungstechnologie. Und wie die Responsibilisierung (vgl. S. 13) ist auch Nudging „gender-blind“ (Pykett 2012, 12), insofern es strukturelle und historisch gewordene Geschlechterverhältnisse nicht mit einbezieht:

> [The proponents of nudging, M.L.] suggest policy tools which are aimed at modifying people's behaviour as opposed to seeking longer term solutions which take account of the material circumstances of differently gendered people, and discursive constructions of particular embodied behaviours as acceptable. (Pykett 2012, 12)

Weil es ein wesentlicher Teil des Nudging ist, für einen Nudge Evidenz zu erzeugen, und mit digitalen Technologien Daten automatisiert erhoben und ausgewertet werden können, und diese Auswertungen direkt zurück in das jeweilige System fließen können, werden „digitale Technologien [auch, M.L.] als Vervollkommnung ‚klassischer‘ Nudging-Ansätze“ (Grafenstein u. a. 2018, 12) diskutiert. Denn „der Bereich der elektronischen Datenverarbeitung [bereitet] einen besonders günstigen Nährboden für beeinflussende Interfacegestaltungen.“ (Kühling und Sauerborn 2022, 228)

In Bezug auf die Verhaltensbeeinflussung durch das Design von Interfaces im Internet hat sich in Abgrenzung von dem vorrangig als Regierungstechnologie gehandelten Nudging der Begriff der ‚Dark Patterns‘ etabliert. Während bei Nudges die Gemeinnützigkeit und das Wohlbefinden der Adressat:innen im Vordergrund steht und ihre Konnotation somit tendenziell ‚positiv‘ ist, sind Dark Patterns ‚negativ‘ konnotiert, weil sie hauptsächlich den wirtschaftlichen Interessen des Anwenders dienen (vgl. Gunawan u. a. 2021, 377:3). Das Kriterium der Anwenderinteressen wiegt schwer, weswegen es sich laut der Rechtsanwälte Jürgen Kühling und Cornelius Sauerborn auch bei Interfacedesigns, „die tatsächlich oder vermeintlich gemeinnützig wirken oder Adressateninteressen befriedigen“, um Dark Patterns handelt, „solange sie zumindest auch benutzt werden, um einseitig Verwenderinteressen zu dienen.“ (Kühling und Sauerborn 2022, 3) Neben Dark Patterns, die verkaufssteigernd wirken sollen, gilt eine große Aufmerksamkeit auch denjenigen Dark Patterns, aufgrund derer über Nutzer:innen mehr Daten generiert werden können, als ohne das Vorhandensein das Dark Patterns generiert werden würden (vgl. Waldman 2020; Graßl u. a. 2021).

Wie Nudging funktionieren Dark Patterns auch über das Ausnutzen verhaltenswissenschaftlicher Erkenntnisse über menschliches Verhalten, welches in niedrigschwelligen Entscheidungsfindungsprozessen von mentalen Heuristiken und kognitiven Biases geprägt ist. Eine Grundlage für diese Beschäftigung ist die Theorie des Psychologen Daniel Kahnemann, demzufolge das menschliche Denken so vorgestellt werden kann, dass es in zwei komplementären

Systemen geschieht: Das erste System, System 1, arbeitet schnell und automatisiert, ist nicht mit Anstrengung verbunden und ebenso wenig mit einem Gefühl von Kontrolle. System 2 hingegen arbeitet bei herausfordernden geistigen Aktivitäten wie komplexer Berechnungen oder Planungen und wird mit einem subjektiven Gefühl von bewusster Entscheidung, Handlungsfähigkeit und Konzentriertheit assoziiert (vgl. Kahneman 2011, 20f.). Wenngleich die empirische Adäquatheit der Theorie in Frage gestellt wird, stützt und prägt sie die Verwendung von Dark Patterns, welche gewissermaßen auf das System 1-Denken abzielen, was sie für Menschen nur schwer kontrollierbar macht (vgl. Bösch u. a. 2016, 245).

Auch wenn die Theorie der zwei Systeme umstritten ist, dient sie als Grundlage für Interface Nudges oder Dark Patterns, mithilfe derer Nutzer:innen dazu bewegt werden sollen, zu mehr Datenfreigaben zuzustimmen, als sie andernfalls würden. Dark Patterns zielen in diesem Rahmen ausgerechnet auf kognitive Prozesse ab, die automatisiert ablaufen und sich tendenziell einer Kontrolle entziehen. Unter Annahme der 2-Systeme-Theorie lassen sich also die Interfaces bzw. vermittelt über die Interfaces die Daten, die generiert und gesammelt werden sollen, von Nutzer:innen nicht erschöpfend kontrollieren.

Es gibt bereits unter anderem um den Begriff des Privacy by Designs eine breite Debatte, die die suggestive Gestaltung von Privacy Interfaces – also von Interfaces, die auf die eine oder andere Art und Weise Entscheidungen darüber beinhalten, dass Daten generiert werden – kritisiert. Viele Beiträge setzen auch an der Interfacegestaltung an und fordern, die Interfaces so zu verändern, dass Nutzer:innen eine größere Datenhoheit gewährleistet wird (vgl. Gispen 2017; Friedman u. a. 2006).

Die am Interface ansetzenden Vorgehen bleiben also wortwörtlich an der Oberfläche des Phänomens. Ich setze in dieser Arbeit hingegen tiefer an und betrachte die zugrundeliegende, komplexe Infrastruktur aus Trackingtechnologien, die das Internet durchzieht und die technologische Grundlage der Datensammelpraktiken bildet, welche durch das Interface zwar rechtlich legitimiert, aber nur schwerlich individuell kontrolliert werden kann. Ich richte den Blick somit auf die Praxis des digitalen Datensammelns oder – als Analogie formuliert – auf das zugrundeliegende ‚Backend‘, das die Hintergrundbedingungen bildet, auf Basis derer der Fluss der eigenen Daten unter Kontrolle gebracht werden müsste. Ich untersuche das Datensammeln im Digitalen aus verschiedenen Perspektiven und leite in vier Zwischenfaziten insgesamt sieben Eigenschaften ab, die zum Teil einzeln, aber vor allem in ihrer Gesamtheit bedingen, dass individuelle Nutzer:innen strukturell nicht in der Lage dazu sind, den Fluss ihrer eigenen Daten zu kontrollieren. Ich argumentiere damit, dass bereits die zugrundeliegende Struktur ver-

unmöglicht, den Fluss der eigenen Daten mündig zu kontrollieren. Den Individuen werden also der Responsibilisierungslogik entsprechend mit der Verantwortung keineswegs die Mittel bereitgestellt, um dieser Verantwortung gerecht zu werden. Ich werde zeigen, dass Individuen im Internet schlicht nicht in der Lage sind, den Fluss ihrer eigenen Daten zu kontrollieren, da weder das Backend noch das Frontend von Individuen kontrolliert werden können.

In den folgenden Kapiteln untersuche ich, was es im Nexus von Online-Marketing und Trackingtechnologien bedeutet, dafür verantwortlich zu sein, den Fluss der eigenen Daten zu kontrollieren. Als das ‚Backend' der Datensammelpraktiken betrachte ich die auf Trackingtechnologien basierende Infrastruktur, die das Internet beinahe gänzlich durchdringt. Dafür setze ich mich vorrangig mit der Trackingtechnologie der Cookies auseinander, die derzeit die präsenteste Trackingtechnologie darstellen. Zwar wird das langsame Ende der Cookies eingeläutet, seitdem Google 2019 angekündigt hat, Drittanbietercookies abzuschaffen und mit einer vermeintlich privatsphärefreundlicheren Alternative zu ersetzen (vgl. Schuh 2019), mit welcher ich mich in Abschnitt 9.2 auch beschäftigen werde. Doch ist eine eingehende Auseinandersetzung mit Cookies für die vorliegende Arbeit dennoch lohnenswert, denn zum einen beginnt die Abschaffung erst sukzessive ab 2024 (vgl. Chavez 2022). Zum anderen – und das ist wesentlich – stellen die Soziologen Kevin Mellet und Thomas Beauvisage fest, dass das System, das um Cookies herum entstanden ist, als Vorbild für derzeitige und zukünftige cookielose Märkte fungiert: „the market arrangements built around the cookie have set up an industry standard, that has been challenged and stabilized, and that is to be reproduced when the cookie technology is missing." (Mellet und Beauvisage 2020, 18) Cookies und mit ihnen auch den aktuellen Werbemarkt zu verstehen und kritisch zu betrachten, trägt also dazu bei, zukünftige Entwicklungen der Werbeindustrie einzuordnen. Ich beschäftige mich daher in diesem Kapitel zunächst ausführlich mit der Entstehungsgeschichte und der Funktionsweise von Cookies, welche sukzessive über mehrere Entwicklungsstufen hinweg von der Werbeindustrie angeeignet wurden.

5 Cookies – Entstehungsgeschichte der cookifizierten Marktinfrastruktur

Als *Magic Cookie* werden im informatischen Jargon kleine Datensätze bezeichnet, die zwischen zwei Programmen ausgetauscht werden, ohne dass sie jedoch für diese Programme eine besondere Bedeutung besitzen. Sie dienen beispielsweise lediglich dazu, die ‚Einzigartigkeit' von etwas zu belegen. HTTP-Cookies als spezielle Form des Magic Cookies sind Datensätze

– genauer gesagt eine Zeichenkette mit einer Mindestlänge von 4096 Bytes – die auf Anweisung von Websitebetreibenden in den Browsern ihrer Besucher:innen lokal gespeichert werden. Für den Browser tragen Cookies keinerlei Bedeutung. Sie fungieren vielmehr als eine Art Wiedererkennungsmerkmal für die Websitebetreibenden oder Werbetreibenden. Wenn die Nutzerin eine Seite erneut aufruft, werden die Cookies, die bei ihrem vormaligen Besuch in ihrem Browser gespeichert wurden, von dem Webserver wieder aus dem Browser geladen. Der Webserver registriert so, dass sie bereits eine ‚bekannte' Besucherin ist. Laut dem *Request For Comments* – einer Sammlung an Dokumenten, in denen die Internet Engineering Task Force einen Standard für das Internet entwickelt und Protokolle, Konzepte und Methoden vereinheitlicht und dokumentiert – müssen in einem Browser mindestens 50 Cookies pro Website und insgesamt mindestens 3000 Cookies gespeichert werden können (vgl. Barth 2011).

In diesem Kapitel zeichne ich den Entwicklungsprozess von Cookies nach, deren Ursprung in simplen Sitzungscookies liegt, aus denen sich über die vergangenen 28 Jahre hinweg eine hochkomplexe Marktinfrastruktur entwickelt hat. In Anlehnung an die Arbeit von Mellet und Beauvisage (2020) differenziere in diesem Prozess drei Entwicklungsstufen von Cookies, anhand derer sich ihre Aneignung durch die Werbeindustrie verdeutlichen lässt. Die Autoren argumentieren, dass die ‚Cookifizierung' der Online-Werbebranche einem Prozess gleicht, durch den diejenige Marktinfrastruktur entstanden ist, welche als soziotechnisches System das Internet inzwischen gänzlich durchzieht. Ihre Ausführungen enden in einer vierten Entwicklungsstufe, die zwar nicht mehr die Ontogenese von Cookies betrifft, aber für die Entwicklung der auf Cookies basierenden Marktinfrastruktur relevant ist. Im Anschluss daran ziehe ich mein erstes Zwischenfazit, in welchem ich drei charakteristische Merkmale des Datensammelns im Digitalen ableite, anhand derer ich verdeutliche, weshalb eine individuelle Kontrolle des Flusses der eigenen Daten unmöglich ist und die Forderung nach digitaler Mündigkeit in dem Sinne unangemessen.

Cookies wurden im Jahr 1994 von Lou Montulli erfunden, einem Entwickler des damals marktführenden Browsers *Netscape*. Das Problem, das durch Cookies gelöst werden sollte, war bzw. ist, dass das Hypertext Transfer Protocol (HTTP), auf dem das Internet basiert, ein zustandsloses Protokoll ist. Dies bedeutet, dass jeder Aufruf einer Website, bzw. genauer genommen einer URL, als solitär wahrgenommen wird und nicht in seinen Sitzungsverlauf eingebettet ist. Der Vorteil, der sich aus der Zustandslosigkeit von HTTP ergibt, ist eine hohe Skalierbarkeit. Das bedeutet, dass viele Nutzerinnen auf einmal auf eine Website zugreifen

können, ohne dass die Netzwerke oder Server überlastet werden. Die Zustandslosigkeit führt jedoch auch dazu, dass eine Websitenutzerin mit jedem Subdomänen-Aufruf oder Aktualisieren der Ausgangsseite von dem Websiteserver so adressiert wird, als wäre sie noch nie dagewesen. Das Browsen im Internet war wegen der Zustandslosigkeit vor der Einführung von Cookies ein „essentially private act“ (Cluley und Brown 2015, 111), da es keine Möglichkeit gab, eine:n Nutzer:in zu identifizieren oder wiederzuerkennen. Für kommerzielle Unternehmen brachte die Zustandslosigkeit jedoch auch Probleme mit sich. So war es beispielsweise nicht möglich, eine Warenkorbfunktion zu implementieren. Kund:innen hätten Artikel einzeln und direkt kaufen müssen, da es keine Möglichkeit gab, dass der Browser sich ‚merkt‘, dass einer oder mehrere Artikel bereits in einen Warenkorb gelegt wurden. Ein solcher virtueller Warenkorb war die Anforderung, die Netscape damals in einem neuartigen Shopping-Server implementieren wollte und auf die hin Cookies entwickelt wurden (vgl. Montulli 2013).

Für das Problem, dass Nutzerinnen nicht wiedererkannt werden, weil das HTTP zustandslos ist, wurden neben Cookies auch andere Lösungsvorschläge diskutiert. Einer davon war die Idee, jedem Browser eine eindeutige Identifikationsnummer zuzuteilen, mithilfe derer Nutzer:innen wiedererkannt werden. Die ID wäre dem Browser und nicht einer Nutzerin zugeordnet, da zu Zeiten der Entstehung von Cookies noch nicht überzeugend in der Dimension der Nutzerin gedacht werden konnte. Für private Zwecke wurde hauptsächlich der Personal Computer verwendet, den sich meist pro Haushalt mehrere Menschen teilten. Lou Montulli sah in der Browser-ID jedoch die Gefahr eines websiteübergreifenden Trackings und lehnte diesen Vorschlag ab. Es entbehrt nicht einer gewissen Ironie, dass das Tracking eine Eigenschaft ist, die Cookies – bzw. im Allgemeinen die Funktionalität eines Wiedererkennungsmerkmal – zum Zeitpunkt ihrer Erfindung keinesfalls erfüllen sollten (vgl. Montulli 2013). Nichtsdestotrotz werden Cookies heutzutage in erster Linie für websiteübergreifendes Tracking eingesetzt. Die Lösung für das aus der Zustandslosigkeit resultierende Problem führte also ein neues Problem mit sich: den Verlust der Privatsphäre.

Es existieren zahlreiche Maßnahmen, die das Privatsphäre der Nutzer:innen im Netz stärken oder schützen sollen, indem sie das Tracking durch Cookies blockieren, erschweren oder kontrollieren. Dazu gehören zum einen die durch die DSGVO vorgeschriebenen Cookie-Banner, aber auch das schlichte Deaktivieren von Cookies im Browser, das Einrichten individueller Browsereinstellungen, oder zahlreiche Browsererweiterungen. So ist es beispielsweise möglich, im Browser einzustellen, dass Cookies nach jedem Schließen des Browsers gelöscht werden, was das Tracking während der Sitzung zwar nicht unterbindet, es aber erschwert, Ver-

knüpfungen über Sitzungen hinweg zu erstellen. Doch sogar diese Methode können sogenannte Evercookies umgehen. Evercookies sind Cookies, die nicht nur im klassischen HTTP-Cookie-Speicher abgelegt werden, sondern an alle derzeit 17 möglichen Speicherorten, auf die eine Website über den Browser zugreifen kann (vgl. Kamkar 2010). Solange beim Löschen von Cookies auch nur einer von den 17 bestehen bleibt, lassen sich die anderen 16 daraus rekonstruieren. Optionen wie das regelmäßige Löschen von Cookies oder Add-Ons sind jedoch nicht standardmäßig im Internetgebrauch vorgesehen und müssen von Nutzerinnen individuell eingestellt werden. Browsererweiterungen wie Ghostery, Privacy Bagder oder uBlock Origin blockieren auch versteckte Tracker.

Die Wirtschaftswissenschaftlerin Shoshanna Zuboff stellt fest, dass sich mit individuellen Maßnahmen wie Browsererweiterungen immer nur einige Menschen dabei behelfen, vor bestimmten Mechanismen des Trackings geschützt zu sein (vgl. Zuboff 2019, 344). In diesen Fällen sind die Schutzmaßnahmen zwar wirksam, jedoch sorgt ihre schiere Existenz zugleich dafür, dass der Status Quo des Tracking unfreiwillig legitimiert wird: „Such measures may be effective in discrete situations, but they leave the opposing facts intact, acknowledging their persistence and thus paradoxically contributing to their legitimacy.“ (Zuboff 2019, 344) Denn indem die individuellen Schutzmaßnahmen existieren, erscheinen sie als vermeintliche Lösung für das durch Trackingtechnologien ausgelöste Datenschutzproblem. Jedoch funktionieren sie als solche immer nur individuell und partikulär, denn sie schützen nur bestimmte Menschen vor bestimmten Technologien. Dadurch tragen sie indirekt zu der Aufrechterhaltung des Problems bei, weil eine Lösung bereits zu existieren scheint und von einer gesamtheitlichen Lösung abgesehen wird. Analog würde das bedeuten, dass die Existenz eines FLINTA*-Tages in einer Sauna zur Legitimierung des patriarchalen Status Quo beiträgt. Weil es diesen Tag gibt, wirkt das Problem, das die Sauna an allen anderen Tagen ein Ort ist, an dem sich FLINTA*-Personen unwohl fühlen können, gelöst. Denn wenn sich eine FLINTA*-Person unwohl fühlt, dann steht ihr der FLINTA*-Tag als Lösung für dieses Problem zur Verfügung. Jedoch ermöglicht der FLINTA*-Tag nur den bestimmten Personen, die an dem bestimmten Tag in die Sauna gehen, sich darin unbekümmert bewegen zu können.

Im Folgenden stelle ich in Anlehnung an die drei Entwicklungsstufen drei verschiedene Arten von Cookies vor, anhand derer sich die Aneignung von Cookies durch die Werbeindustrie über die Zeit hinweg verdeutlichen lässt. Zunächst entstanden Sitzungscookies, daraufhin folgten Erstanbieter-Analysecookies und zuletzt kulminierte die Cookifizierung in Drittanbietercookies.

5.1. Erste Entwicklungsstufe: Sitzungscookies

Wie in dem vorigen Abschnitt des Kapitels deutlich wurde, beginnt die Entwicklungsgeschichte der Cookies bei Warenkorb- und Sitzungscookies. *Sitzungscookies* dienen dazu, den reibungslosen Ablauf einer Sitzung zu gewährleisten. Sie werden als eine eindeutige Sitzungsidentifikationsnummer im Browser der Nutzerin gespeichert. Eine Sitzung beschreibt die Zeitspanne vom Aufrufen einer Website bis zum Schließen der Registerkarte oder des Browsers. Der Ablauf wird durch die Sitzungscookies deswegen reibungslos, weil bereits authentifizierte Nutzerinnen als solche auf Basis der Sitzungscookies von dem Server wiedererkannt werden, und von den Webseitenbetreibenden somit zu einem eingeloggten Mitgliederbereich oder einem Status im Sitzungsverlauf zugeordnet werden können. Andernfalls wäre für jeden neuen Unterseitenaufruf auf der Website (beispielsweise von `www.sport.de` zu `www.sport.de/boxen`) eine erneute Authentifizierung erforderlich. Dies gilt insbesondere, wenn es innerhalb eines Prozesses notwendig ist, Pop-Up-Fenster zu verwenden oder auf der Webseite zu navigieren, wie beispielsweise im Online-Banking. Sitzungscookies werden mit dem Ende der Sitzung, also dem Schließen des Browserfensters bzw. der spezifischen Registerkarte, wieder gelöscht. *Warenkorbcookies* wiederum dienen dazu, dass der Warenkorb einer Nutzerin in einem Online-Shop die ganze Sitzung über erhalten bleibt und auch dann nicht verlorengeht, wenn die Nutzerin sich auf Unterseiten weitere Artikel anschaut. Im Gegensatz zu Sitzungscookies sind Warenkorbcookies *persistent*, das heißt, sie überdauern eine einzige Sitzung und bleiben über einen längeren Zeitraum hinweg bzw. bis zu ihrem Ablaufdatum bestehen. So können sich Nutzerinnen auch nach mehreren Tagen, Wochen oder dem ungewollten Schließen des Browsers noch dazu entscheiden, zum Warenkorb zurückzukehren, in dem ihre Artikel noch vermerkt sind.

Sitzungscookies und Warenkorbcookies gehören heutzutage zu denjenigen Cookies, die für das Funktionieren einer Website als notwendig klassifiziert werden und keinerlei Einwilligung bedürfen. Notwendige Cookies gehören zu den sogenannten *Erstanbietercookies*, da sie ausschließlich von den Betreibenden der Website – den Erstanbietern – gesetzt und gelesen werden. Davon zu unterscheiden sind *Drittanbietercookies*, welche von einem weiteren, außenstehenden Server gesetzt werden.

Notwendige Cookies benötigen keine vorhergehende Einwilligung und können somit auch nicht abgelehnt werden. In Browsern gibt es jedoch die Möglichkeit, Cookies im Allgemeinen zu deaktivieren. Das führt aufgrund der Zustandslosigkeit von HTTP beispielsweise dazu, dass Services, die nur über die Authentifizierung in einem eingeloggten Mitgliederbereich er-

reichbar sind, nicht mehr nutzbar sind. Als Folge würde die Nutzer:in in einer Authentifizierungsschleife feststecken, weil jeder Loginversuch wieder auf die Ausgangsseite führt. Außerdem führt das Blockieren von Cookies dazu, dass mit jedem (Unterseiten-)Aufruf das DSGVO-konforme Cookie-Banner erneut beantwortet werden muss – denn auch die Entscheidung zum Cookie-Banner wird in einem notwendigen Cookie gespeichert.

5.2. Das traditionelle Werbesystem

Zu dem Zeitpunkt, zu dem Sitzungscookies entstanden sind, basierte das Schalten von Anzeigen und die Preisgestaltung von Internetwerbung auf den Werbemechanismen der bis dato traditionellen Medien wie Printmedien oder Fernsehen. Die Verhandlungsrundlagen für Werbekampagnen waren auf der einen Seite quantitative Aussagen über die Konsumentinnen des Mediums, im Falle von Fernsehen beispielsweise Aussagen darüber, wie viele Zuschauer die Tagesschau um 20 Uhr auf ARD hat. Auf der anderen Seite standen qualitative Aussagen über die Eigenschaften der Konsumentinnen, die auf einigen wenigen, festen und vorgefertigten Kategorien beruhten wie Alter, Geschlecht, Einkommen oder grobe Interessen (vgl. Mellet und Beauvisage 2020, 10). Ein zwischen den Werbeflächenanbietern und Werbetreibenden agierendes Werbenetzwerk führte nun basierend auf diesen Informationen mit den Werbetreibenden Verhandlungen darüber, wann und in welchem Medium die Werbekampagne laufen sollte, also ob in einem Printmedium, im Fernsehen oder online, und wie viel sie kosten würde (vgl. ebd.). Werbekampagnen waren damals im Vergleich zu dem heutigen vollautomatisierten Anzeigenhandel an der Werbebörse in Echtzeit sehr ‚grobe' Unterfangen:

> [T]he system is large-grained: segments are large, the means to target them are made at a media or a section (sports, economics, fashion, etc.) level, and no individual measurement of exposure and its effects exists at a global scale. (ebd., 10)

Im Internet wurde beispielsweise eine Kampagne für neue Sportschuhe nur auf Unterseiten von Websites beworben, auf denen auch Sportschuhe verkauft werden, wodurch sichergestellt werden sollte, dass das Segment der ‚Sportinteressierten' adressiert wird. Eine Werbefläche zu kaufen, bedeutete im traditionellen Werbesystem also, das Recht zu erwerben, die eigene Werbung neben ganz bestimmten Inhalten zu zeigen.

Sitzungs- und Warenkorbcookies wurden von der Werbeindustrie noch nicht eingesetzt, doch wurde mit ihrem Aufkommen die zugrundeliegende Technologie eingeführt, welche sich die Werbeindustrie in den folgenden Jahren aneignete.

5.3. Zweite Entwicklungsstufe: Erstanbieter-Analysecookies

Die zweite Entwicklungsstufe der Cookies waren *Erstanbieter-Analysecookies*, also Cookies, die von den Websitebetreibenden eingesetzt werden, um das Verhalten ihrer Nutzerinnen zu analysieren. Erstanbieter-Analysecookies können von Websitebetreibenden zum Beispiel genutzt werden. um nachzuvollziehen, über welche Klickpfade Nutzerinnen auf einer Website navigieren. Wenn dabei beispielsweise erkannt wird, dass ein Großteil der Nutzerinnen, die Informationen zum Suchwort *X* möchten, sich auf Seite *Y* verlaufen und ihre Suche abbrechen, können mögliche Fehlerquellen in der Architektur der Website identifiziert werden. In Erstanbieter-Analysecookies werden daher unter anderem Informationen darüber gespeichert, was für Suchbegriffe eine Nutzerin eingibt, wie lange sie auf welcher Seite ist, wohin sie auf einer Seite scrollt oder klickt, oder in welcher Reihenfolge sie Seiten besucht.

Der Einsatz von Erstanbieter-Analysecookies ermöglicht jedoch nicht nur Fehlerquellenidentifikation, sondern wird faktisch auch dafür eingesetzt, die wirtschaftlichen Interessen von Websitebetreibenden zu realisieren. Denn Websitebetreibende vollziehen beispielsweise mithilfe von Analysecookies nach, wie eine Kaufentscheidung oder ein Kaufabbruch zustande kommt, während eine potenzielle Kundin die Website navigiert, und ob dieser Prozess optimiert werden kann.

Der Navigationsprozess, den eine Nutzerin auf einer Website vollzieht, wird im Marketing-Fachvokabular als ‚Customer Journey' oder ‚Kundenerfahrung' bezeichnet. Eine Kaufentscheidung führt zu einer sogenannten *Konversion*, einer Transformation einer Interessentin bzw. *potenziellen* Kundin in eine *tatsächliche* Kundin. Der Begriff der Konversion bezeichnet dabei jede Art von Realisierungswunsch der Websitebetreibenden, welcher von einer Besucherin erfüllt werden kann: der Kauf von Artikeln, Dateidownloads, das Abschließen von Mitgliedschaften, die Anmeldung für einen Newsletter oder das Ausfüllen eines Kontaktformulars. Eine hohe Konversionsrate ist ein gängiges Ziel für die meisten Unternehmen bzw. Websites. Durch die Nachverfolgung der Customer Journey können vermeintlich kritische Momente identifiziert werden, an denen Interessentinnen abspringen und aus Sicht des Anbieters verloren gehen.

Im Gegensatz zu Sitzungs- und Warenkorbcookies, die als notwendig gelten, erfordert das Setzen von Erstanbieter-Analysecookies, deren Zweck die Nutzungsanalyse ist, seit Inkrafttreten der DSGVO die vorherige Einwilligung der Nutzerin. Erstanbieter-Analysecookies sind persistent, bleiben also über eine Sitzung hinweg bestehen. Dadurch können die Anbieter eine

Nutzerin und deren Präferenzen ‚kennenlernen' und die Website auf ihre vermeintlichen Bedürfnisse abgestimmt darstellen.

5.4. Erste Berührungen mit der Werbeindustrie

Während die ursprünglichen Sitzungscookies für die Werbeindustrie noch nicht brauchbar waren und lediglich die Vorlage boten, ermöglichten die Erstanbieter-Analysecookies den ersten Schritt in Richtung der ‚Cookifizierung': „the [first party] cookie led to the birth of profiling and behavioral targeting." (Mellet und Beauvisage 2020, 11). Denn Erstanbieter-Analysecookies erlaubten, Nutzerinnen auch über sämtliche Unterseiten der Website hinweg mit der passenden Werbung anzusprechen. Während zu Zeiten des Sitzungscookies Werbung für Sportschuhe nur auf der Sportschuh-Unterseite eines Online-Shops angezeigt wurden, ermöglichten Erstanbieter-Analysecookies, Werbung für Sportschuhe auch einer Person zu zeigen, die sich gerade auf der gleichen Website Bücher anschaute, solange sie bereits mindestens ein Mal zuvor in einer anderen Sitzung auf der Sportschuh-Unterseite gewesen war. Die groben Segmente wie ‚Sportinteressierte', die aus dem traditionellen Werbesystem geerbt wurden, blieben erhalten.

Die Werbeindustrie veränderte sich durch das Aufkommen von Erstanbieter-Analysecookies vor allem für Anbieter von großen Websites oder Onlineshops, die eine breite Palette an Artikeln vertrieb, welche verschiedene Interessen widerspiegelten. Denn Erstanbieter-Analysecookies ermöglichten ihnen, ihre Zielgruppen viel granularisierter zu erkennen und anzusprechen. Das zugrundeliegende Werbesystem beruhte weiterhin auf dem der traditionellen Medien. Allerdings wurde bereits nebenher experimentiert und erforscht, welche Möglichkeiten Erstanbieter-Analysecookies im Marketingbereich eröffneten: „this first step of the cookification of the advertising industry had a lot to do with experiencing and domesticating browsing information." (Mellet und Beauvisage 2020, 11)

5.5. Dritte Entwicklungsstufe: Drittanbietercookies

Die dritte Entwicklungsstufe von Cookies sind Drittanbietercookies, die heute auch als *Trackingcookies* bezeichnet werden. Diese Cookies werden von einem dritten Akteur implementiert, also einem weiteren Akteur neben dem Browser der Nutzerin zum einen und dem Server der Website zum anderen. Das Internet war bereits darauf ausgelegt, Inhalte von Drittanbietern zu laden, da nicht der komplette Inhalt einer Website nur auf dem die Website betreibenden Server gespeichert wird. Die Möglichkeit zum Einbinden von Drittanbieterinhalten war also bereits inhärent. Beispielsweise liegen Bilder, Codeschnipsel, oder Designvorgaben

auf einem dritten Server und werden von der Zielwebsite lediglich verlinkt. Der Browser der Nutzerin ruft diesen Link auf, wenn er die Zielwebsite lädt und zusammenbaut, und ruft die Inhalte von dem dritten Server automatisch ab. Um Drittanbietercookies setzen zu dürfen, ist ebenfalls gemäß DSGVO die Einwilligung der Nutzerin erforderlich. Die drei Browser Brave, Firefox und Safari haben Drittanbietercookies standardmäßig deaktiviert.

Drittanbieter- oder Trackingcookies ähneln den Analysecookies, sind dabei jedoch nicht auf die ‚Customer Journey' der Nutzerin auf einer einzigen Website beschränkt, sondern zeichnen vielmehr einen Weg nach, der sich passender als die ‚Internet Journey' der Nutzerin bezeichnen lässt. Drittanbietercookies funktionieren sowohl sitzungs- als auch websiteübergreifend und speichern – im Extremfall – jede besuchte Website, jeden Klick, jede Sucheingabe, jede Mausbewegung. Auf diese Art und Weise wird ein detailliertes Profil über die Nutzerin angelegt, um möglichst passende Werbung zu schalten. Den Drittanbietern gelingt „the fabrication of a statistical knowledge of these users across these sites: interests, inferred socio-demographic properties, etc." (Mellet und Beauvisage 2020, 12). Drittanbietercookies ermöglichen also, dass auf einer Website, die sich ausschließlich mit Pflanzen beschäftigt, dennoch Werbefläche beispielsweise für eine Sportschuhwerbung verkauft werden kann, wenn eine Person, die auf ihr browst, vor mehreren Tagen auf einer anderen Website Sportschuhe angeschaut hatte. Die Werbetreibenden erwerben also nicht mehr den Anspruch, ihre eigene Werbung neben *bestimmten Inhalten* auf einer Website zu zeigen wie es zu Beginn war, sondern sie erwerben die Möglichkeit, ihre Werbung *bestimmten Kund:innen* zu zeigen, und zwar unabhängig von dem Inhalt der Website, die diese gerade besuchen. An diesem Punkt löste sich die Werbung also von dem Ort bzw. Kontext der Werbefläche und orientierte sich ausschließlich an ihrer Betrachterin. Es vollzog sich eine „transformation of single-media audiences into networked audiences" (Mellet und Beauvisage 2020, 12).

Die ersten Drittanbieter waren diejenigen Firmen, die bereits zuvor in der Werbeindustrie tätig waren, um Daten über Kund:innen und mögliche Zielgruppen zu erheben. Die Platzierung ihrer Drittanbietercookies haben sie sich ermöglicht, indem sie den Websitebetreibenden ein Tauschgeschäft anboten: Im Gegenzug dafür, dass die Drittanbieter ihr Cookie auf einer Website setzen durften, erhielten die Websitebetreibenden kostenlose und wertvolle Informationen über die Profile und Interessen ihrer Besucher:innen (vgl. Mellet und Beauvisage 2020, 12). Die Menge an neugewonnenem, wertvollem Wissen verlieh den Drittanbietern eine größere Handlungsmacht, sodass sie sich zu Betreibenden von Werbenetzwerken weiterentwickelten

und den Werbeflächenverkauf zwischen Werbetreibenden und Werbeflächenanbietenden eigenständig organisierten (vgl. ebd., 12).

5.6. Programmatische Werbung in Echtzeit

Mit Drittanbietercookies mündet der Entwicklungsprozess von Cookies in die Gegenwart, doch folgte in den 2010er-Jahren eine weitere Entwicklung, die wesentlich dazu beitrug, dass sich durch die ‚Cookifizierung' eine komplexe Marktinfrastruktur herausbildete. Diese Entwicklung war die Einführung der sogenannten *programmatischen Werbung*. Während zuvor die Verhandlungen, in denen Werbetreibende und Werbeflächenanbietende sich auf Kampagne und Preis einigen, von den Werbenetzwerken manuell moderiert wurden und möglicherweise über einige Runden gingen, finden in der programmatischen Steuerung von Werbekampagnen keine iterativen Verhandlungen mehr statt. Stattdessen werden die Werbeflächen automatisiert und in Echtzeit an Werbebörsen gehandelt: „Ad exchanges automate the process of advertising inventory purchasing: buyers' and sellers' strategies are implemented by algorithmic mechanisms which assess the appropriateness of displaying a banner and determine the optimal price" (Mellet und Beauvisage 2020, 13).

Die Werbenetzwerke, die im Auftrag der Werbetreibenden an der Werbebörse handeln, konkurrieren durch das sogenannte *Cookie Matching* miteinenander. Beim Prozess des Cookie Matchings verschlüsselt die Werbebörse das Cookie der aktuellen Besucherin so, dass nur noch eine eindeutige Identifikationsnummer ableitbar ist und keine Interessens- oder Verhaltensdaten enthalten sind. Die ID wird an interessierte Werbetreibende gesendet, welche sie wiederum abgleichen mit ihren eigenen Cookies der Besucherin und so beispielsweise in Erfahrung bringen können, ob die Besucherin bereits auf einer der Websites war, auf denen sie Drittanbietercookies platziert haben. Basierend auf dieser Information geben die interessierten Werbetreibenden mittels Algorithmen automatisierte Gebote ab. Unabhängig davon, ob Werbetreibende die Auktion gewinnen oder verlieren, wird durch das Cookie-Matching-Verfahren ein weiteres Cookie in ihrer Datenbank gespeichert, was also für alle Teilnehmenden der Auktion neues Wissen birgt. (Vgl. Ghosh u. a. 2015, 2)

Von den technischen Voraussetzungen her können in Cookies jede Art von Informationen gespeichert werden, die sich durch die Interaktion mit einer Website ergeben. Denn Cookies sind – metaphorisch gesprochen – leere Behälter, in die jede erdenklich mögliche Information gefüllt werden kann, die sich mithilfe eines Javascript-Skriptes aus einer Interaktion auslesen lässt. Was unter anderem generiert oder festgehalten werden kann, sind der Benutzername, die

IP-Adresse, der Standort, die weiteren auf einen Klick auf eine Werbeanzeige folgenden Aktionen (der Klickpfad), die Suchwörter, die Uhrzeit, Formulareingaben, Käufe oder angeschaute Artikel, personalisierte Einstellungen wie die Währung, die Sprache oder das Erscheinungsbild, jede weitere auf einer Website getroffene Einstellung, der verwendete Browser, die Hardware, oder das Betriebssystem. Theoretisch können auch Passwort, Name, Emailadresse oder andere personenbezogene Daten gespeichert werden, was jedoch gegen die Datenschutzgrundverordnung verstößt.

5.7. Die cookifizierte Marktinfrastruktur

Ich habe bisher die Entwicklungsgeschichte von Cookies rekonstruiert und nachvollzogen, wie sich die Werbeindustrie die Cookies angeeignet hat. Mellet und Beauvisage (2020) zufolge hat sich durch diesen Prozess der ‚Cookifizierung' eine trackingbasierten Marktinfrastruktur entwickelt. Diese Entwicklung geschah auf eine unscheinbare Art und Weise und keineswegs eingebettet in eine gesellschaftliche oder fachliche Debatte: „The cookie-based market infrastructure has emerged in a silent way, outside of any discussion, even among advertising professionals." (Mellet und Beauvisage 2020, 8).

Wenn die Forderung nach digitaler Mündigkeit als die Forderung formuliert wird, den Fluss der eigenen Daten zu kontrollieren, so bedeutet das, dass diese mündige Datenflusskontrolle im Kontext der trackingbasierten Marktinfrastruktur passieren muss. Was genau das bedeutet, erarbeite ich in diesem Abschnitt. Dafür werde ich im Folgenden zunächst darlegen, wodurch sich Märkte auf der einen, und Infrastrukturen auf der anderen Seite auszeichnen. Ich leite zu einer Untersuchung der Frage über, aufgrund welcher Merkmale des Marktinfrastrukturbegriffs und der Cookifizierung Mellet und Bauvisage ihre These formulieren, dass sich durch den Prozess der Cookifizierung eine trackingbasierten Marktinfrastruktur entwickelt hat. In einem ersten Zwischenfazit leite ich aus den vorhergehenden Ausführungen die drei Eigenschaften ab, dass das Datensammeln im Digitalen *kontinuierlich*, *komplex* und *unsichtbar* ist. Auf Basis dieser Eigenschaften argumentiere ich, dass die Forderung nach digitaler Mündigkeit in Form der Teilforderung, den Fluss der eigenen Daten zu kontrollieren, unangemessen ist.

Märkte sind physische oder virtuelle Orte, an denen Marktteilnehmer:innen Waren gegen Geld oder andere Waren handeln. Auf dem Markt werden Angebot und Nachfrage koordiniert und Preise bzw. Werte für Güter bestimmt. Außerdem zeichnen sich Märkte durch einen Wettbewerb aus. Börsen wiederum sind eine spezielle Form des Marktes, an der weder die Markt-

teilnehmer noch die Handelsobjekte präsent sind. In der durch die Akteur-Netzwerk-Theorie geprägten soziologischen Forschung zu Märkten ist die materialistische Seite von Märkten in den Fokus gerückt, die sich in sogenannten *Market Devices* manifestiert (vgl. Velthuis 2020, 83). Als ‚Market Devices' werden technische Instrumente bezeichnet, die an der Konstruktion und Umgestaltung von Märkten beteiligt sind und Marktfähigkeit bestimmen. Beispiele für Market Devices sind Preismodelle und Handelsprotokolle (vgl. Callon, Millo, und Muniesa 2007) oder Kundenrezensionen (vgl. Mellet und Beauvisage 2020, 7).

Bei *Infrastrukturen* handelt es sich der Ethnografin Susan Star zufolge um im Hintergrund liegende Ressourcen, die die Handlungen von Akteuren zugleich ermöglichen und begrenzen. Sie begrenzen sie insofern, dass sie nur eine bestimmte Menge an Handlungen ermöglichen, die durch Konventionen und Standards bestimmt werden (vgl. Star 1999, 381). Beispiele für solche Konventionen ist die Zustandslosigkeit von HTTP – denn darauf wurde sich geeinigt, das Protokoll hätte jedoch auch anders funktionieren können – oder Konventionen darüber, auf welche Art und Weise Begriffe beim Programmieren[4] geschrieben werden. Infrastrukturen sind Star zufolge stets relational, was bedeutet, dass es von der Perspektive einer Person abhängt, ob eine Ressource für sie als Infrastruktur dient oder eine andere Aufgabe erfüllt. Beispielsweise kann eine Treppe für die Person, die zur Bahn sprintet, eine Infrastruktur sein, die im Hintergrund liegt und ihr erlaubt, die eigentliche Handlung – das zur Bahn sprinten – auszuführen. Für das Putzpersonal ist sie hingegen ein im Vordergrund liegendes Arbeitsobjekt, und für eine Person, die sich mit einem Rollstuhl bewegt, eine Behinderung, da sie die Treppe nicht benutzen kann (vgl. ebd., 380). Für die Personen, die Infrastrukturen auch als solche nutzen, sind sie transparent, wobei transparent hier bedeutet, dass sie in den Hintergrund treten und nicht mehr sichtbar sind, sondern die Aufgaben, für die die Personen sie benutzen, unsichtbar unterstützen (vgl. ebd., 381). Infrastrukturen sind zwar stets realisiert durch materielle Objekte – wie Treppen, Stromkabel, oder Wasserleitungen – doch ist diese Materialität für den Infrastrukturbegriff irrelevant bzw. ein Fokus darauf sogar irreführend, da er ablenkt von den immateriellen Eigenschaften einer Infrastruktur wie beispielsweise ihrer Relationalität (vgl. 1999, 380).

Marktinfrastrukturen wiederum vereinen diese materiellen und immateriellen Aspekte. Mellet und Beauvisage bezeichnen sie als die Gesamtheit von Objekten, die die Grundlage für das Funktionieren von Märkten bilden: „the material and discursive objects and assemblages that create the grounds on which markets silently operate." (Mellet und Beauvisage 2020, 3) Ihnen zufolge gehen mit Marktinfrastrukturen hauptsächlich drei Prozesse einher: Als Erstes sind

4 Vgl. z.B. die ungarische Konvention, Camel Case und Snake Case.

Marktinfrastrukturen vor allem *Wissensinfrastrukturen*, die sowohl die Produktion als auch die Verbreitung von Wissen ermöglichen, welches für wirtschaftliche Transaktionen wie beispielsweise den Kauf und Verkauf von Gütern nützlich sind (vgl. ebd., 7). Dass durch die Cookifizierung eine Wissensinfrastruktur entstand, machen Mellet und Beauvisage an der zweiten Entwicklungsstufe von Cookies fest, den Erstanbieter-Analysecookies. Zwar vergrößerte sich die Wissensproduktion mit dem Aufkommen von Drittanbietercookies noch einmal mehr, jedoch fand sie ihren Ursprung in den Informationen, die Erstanbieter-Analysecookies über Nutzer:innen zu sammeln erlaubten und an denen sich wirtschaftliche Transaktionen im Werbesystem zu orientieren begannen (vgl. ebd., 11).

Zweitens zeichnen sich Marktinfrastrukturen durch eine *Kapitalisierung* aus, was bedeutet, dass das Wissen bzw. die Informationen über das Nutzerinnenverhalten kapitalisiert werden bzw. einen wirtschaftlichen Wert erhalten (vgl. Mellet und Beauvisage 2020, 7). Mit dem Aufkommen von Drittanbietercookies bauten die Drittanbieter ihre Wissensbasis aus und hatten im Vergleich zu den Erstanbietern, die durch Erstanbieter-Analysecookies lediglich das Wissen über die Nutzer:innen ihrer eigenen Website haben, das weitaus größere Kapital. Dies erlaubte den Drittanbietern, den Zugang zu der sich noch im Entstehen befindenden Marktinfrastruktur zu sichern, und ihn zu organisieren, indem sie ein Werbenetzwerk gründeten (vgl. ebd., 12).

Drittens sind Marktinfrastrukturen auch *Koordinationsinfrastrukturen*. Dies bezieht sich vor allem auf die materielle Seite von Märkten, auf denen Angebot und Nachfrage zusammengeführt und koordiniert werden, sodass die jeweiligen individuellen Entscheidungen von Anbietenden und Nachfragenden miteinander kompatibel sind und Transaktionen gelingen (vgl. Mellet und Beauvisage 2020, 7). Genau diese Koordinierung findet in den Werbebörsen statt, auf denen in Echtzeit und automatisiert Werbeflächen und Gebote mittels Cookie-Matching gehandelt und koordiniert werden (vgl. ebd., 13f.). Mellet und Beauvisage zufolge entsteht um die cookifizierte Marktinftrastruktur herum ein komplexes soziotechnisches System:

> [T]he cookie is at the centre of a sociotechnical system that feeds a knowledge base produced from the tracking of consumers, the capitalization of this knowledge into marketable segments, and its operationalization in advertising and marketing actions. (ebd., 3)

Das Ausmaß der aus der Cookifizierung hervorgegangenen Marktinfrastruktur beschränkt sich nicht nur auf – beinahe – das gesamte World Wide Web bzw. die darin aufgeführten Websites, sondern schließt auch uns als dessen Nutzer:innen mit ein. Fast jede Website – und besonders die meistbesuchten Websites – verwenden Cookies. Auf den insgesamt 1 Mio. meistbesuchten

Seiten wurden über 3 Mio. verschiedene Trackingtechnologien gefunden (vgl. builtwith 2022). Im Durchschnitt verwendet also jede der Websites drei Trackingtechnologien. Dies ist nicht gleichbedeutend damit, dass jede Website im Schnitt drei Cookies setzt, sondern bedeutet, dass jede Website im Schnitt drei Trackingtools wie Google Analytics, Meta Pixel oder LinkedIn Insights verwendet, mithilfe derer verschiedene Cookies oder auch andere Trackingtechnologien (vgl. Kapitel 6) eingesetzt werden können. Wenn die meistbesuchten Websites Trackingtechnologien einsetzen, heißt das im Umkehrschluss für die meisten Besucher:innen, dass fast jede von ihnen ebenfalls von Trackingtechnologien betroffen ist. Im Gegensatz dazu wird der Werbemarkt nur von einer Handvoll Akteuren beherrscht, welche keineswegs mehr nur reine Marketingunternehmen sind. Einige wenige Unternehmen – allen voran Google und Meta (vgl. builtwith 2022) – verfügen also über Unmengen an Wissen über fast alle Nutzer:innen des Internets.

Plattformunternehmen wie Google oder Facbeook sind zwar keine reinen Marketingunternehmen, weil ihr vermeintlicher Schwerpunkt abseits vom Marketing auf einem anderen Service liegt. Beispielsweise bietet Google eine Vielzahl an Services an, wie Maps, Docs, Meet etc. Auch Meta liefert mit Facebook vordergründig eine Social Media Plattform. Dennoch ist laut den Konsumforschern Joel Hietanen, Oscar Ahlberg und Andrei Bozet unter Bezug auf die Arbeit von Nick Srnicek (2017) zum Plattformkapitalismus das eigentliche Zentrum ihrer Geschäftsmodelle das Datensammeln und Marketing:

> Their business is not the service they market to consumers, but rather the intensification and commodification of recordable consumer information. As Srnicek (2017) notes, the very business model of any platform economy enterprise is the future potential of the user data it amasses. (Hietanen, Ahlberg, und Botez 2022, 6)

Was bedeutet es also im Angesicht dieser Marktinfrastruktur digital mündig zu sein? Können wir digital mündig sein angesichts eines soziotechnischen Systems, das beinahe das gesamte Internet durchdringt und angesichts einer Marktinfrastruktur, die auf invasiven Trackingtechnologien basiert, mit denen Daten über Nutzerverhalten erhoben wird, um sie dem Werbemarkt als Produkte zu handeln?

5.8. Zwischenfazit I: Das Datensammeln ist kontinuierlich, komplex und unsichtbar

In Kapitel 5 habe ich bisher gezeigt, wie sich die Technologie des Cookies in drei Schritten entwickelt hat, deren Richtung und Verlauf maßgeblich von der Aneignung der Technologie durch die Werbeindustrie geprägt wurde. Die Entwicklung resultierte in der heute vorherr-

schenden cookifizierten Werbemarktinfrastruktur, die sich laut Mellet und Beauvisage durch drei charakteristische Prozesse auszeichnete. Der erste, grundlegendste Prozess der Marktinfrastruktur ist die Generierung von Wissen, welches notwendig ist für die darauffolgende zweite Operation – die Kapitalisierung eben jenes Wissens in einem Markt –, sowie die dritte Operation der Koordinierung dieses Marktes. Das Wissen basiert auf den durch Cookies und andere Trackingtechnologien generierten und gesammelten Daten über uns als Nutzer:innen des Internets. Die Grundbedingung dafür, dass die Marktinfrastruktur überhaupt funktionieren kann, sind also gewissermaßen wir als Nutzer:innen – bzw. die cookiebasierte Verdatung unserer Handlungen im Internet. Den Unternehmen und Konzernen, die aus dem daraus generierten Wissen Kapital schlagen und den Markt organisieren, ist es also ein zentrales Anliegen, diese Daten zu generieren und zu sammeln. Sie werden alles in ihrer Macht stehende tun, um weiterhin den Fluss der Daten generieren und verwerten zu können. Auch, aber nicht nur aufgrund dessen trägt das Datensammeln verschiedene Eigenschaften, welche ich im Folgenden mithilfe einer Analogie verdeutliche.

Meine bisherigen Ausführungen haben gezeigt, dass das Datensammeln im Digitalen in einer hochkomplexen Marktinfrastruktur eingebettet ist. Um zu veranschaulichen, was die Forderung nach digitaler Mündigkeit in diesem Kontext bedeutet, setze ich sie mit der Forderung gleich, sich in einem Raum voller Überwachungskameras mündig beobachten zu lassen. Sich mündig beobachten zu lassen würde hier bedeuten, selbst kontrollieren zu können und zu müssen, welche der zahlreichen Kameras was, wie, und wie viel filmt. Die Analogie dieses Raumes voller Überwachungskameras ist im Einklang mit Gegenwartsdiagnosen wie beispielsweise Shoshana Zuboffs These des Zeitalters des Überwachungskapitalismus, welcher sich dadurch auszeichnet, dass Technologieunternehmen wie Google private menschliche Erlebnisse und Gefühlsregungen für ihren eigenen Profit verdaten, verarbeiten und für Vorhersagen verwenden (vgl. 2015, 8f.). Auch Hietanen et al. stellen fest: „marketing now blossoms as surveillance through and through.“ (2022, 7)

Als erste These lässt sich feststellen, dass in der Analogie des Raumes voller Überwachungskameras die Kameras permanent laufen und also *kontinuierlich* filmen. Daran lässt sich zunächst verdeutlichen, weshalb es sinnvoll ist, davon zu sprechen, den *Fluss* der eigenen Daten zu kontrollieren, anstatt lediglich davon, die eigenen Daten zu kontrollieren. Denn die Daten werden kontinuierlich und nicht nur einmalig gesammelt, so wie die Kameras in der Analogie kontinuierlich filmen.[5] Die Möglichkeiten, welche die gefilmte Person hat, um ihre Mündigkeit auszuüben, sind beschränkt. Eine Möglichkeit, die sie beispielsweise hat, ist, dass sie Fil-

5 Vgl. dazu auch Jörg Pohles (2022) Verwendung des Begriffes der Daten(-fluss-)kontrolle.

ter oder Blenden auf die Linsen der Kameras klebt. Außerdem fragen manche der Kameras sie, bevor sie filmen, in welcher Auflösung oder welchen Ausschnitt sie filmen dürfen – vorausgesetzt, dass diese Kameras überhaupt sichtbar sind und nicht versteckt.

Mit der Analogie des Raumes voller Überwachungskameras lässt sich eine weitere These herleiten: Datensammeln im Internet ist zudem *unsichtbar*. Unsichtbarkeit herrscht hier in zweierlei Aspekten: Zum einen sind die getarnten oder versteckten Kameras für die Person im Raum zunächst einmal unsichtbar. Dadurch weiß sie gar nicht, von wie vielen Kameras sie gefilmt wird, wann sie gefilmt wird oder welche Ausschnitte gefilmt werden. Zum anderen ist Unsichtbarkeit in dieser Analogie auch in dem Sinne gegeben, dass das Videomaterial, das von der Person erzeugt wird, für diese Person ebenfalls unsichtbar ist. Wenn sie sich mündig (nicht) beobachten lassen soll, kann sie lediglich Annahmen darüber treffen, wie das Filmmaterial aussehen könnte, und basierend auf ihrer Annahme entscheiden, ob und wie sie sich beobachten lassen möchte. Sie kann jedoch nicht in der Beobachtungssituation selber einen Blick auf das Kameradisplay werfen und den Winkel ändern, die Aufnahme abbrechen oder sie sogar löschen.[6]

Allein die Vielzahl an Kameras macht den Raum und die Entscheidung, welche Kamera wie viel, was, wann und wo filmen darf, *komplex*. Hinzukommend tauschen die Kameras Videomaterial an einem zentralen Sammelplatz miteinander aus, und während die Person der einen Kamera womöglich einen Unschärfefilter aufgelegt hat, hat sie übersehen oder vergessen, dass sie einer anderen schon längst einmal erlaubt hatte, sie in höchster Auflösung zu filmen. Diesen Materialaustausch zwischen den Kameras mitzudenken, erschwert die Entscheidung der Person, sich mündig (nicht so) beobachten zu lassen, zusätzlich.

Es wird deutlich, dass die Eigenschaften, *kontinuierlich*, *unsichtbar* und *komplex* zu sein, es der Person in dem Raum schier unmöglich machen, sich mündig beobachten oder nicht beobachten zu lassen. Dies verunmöglicht es dem Individuum, den Fluss der eigenen Daten mündig zu kontrollieren. Dennoch werden die Nutzer:innen des Internets individuell für die Kontrolle des Flusses ihrer eigenen Daten verantwortlich gemacht. Da die Forderung nach digita-

6 Auch die Datenauskunft ließe sich in dieser Analogie verdeutlichen. Nutzer:innen können bei den datensammelnden Unternehmen eine Auskunft über die über sie generierten Daten anfragen. Die Datenauskunft bietet jedoch lediglich einen zusammenfassenden, statischen Überblick über die personenbezogenen Daten, statt einen Einblick in die dynamische Marketinginfrastruktur zu bieten, in der ihre Daten in Echtzeit weiterverarbeitet werden und zu algorithmischen Entscheidungen führen. Die Analogie dazu verliefe folgendermaßen: Zwar könnte die Person einzelne Filmstudios anfragen, welches Material sie über sie gefilmt haben, und auf diese Art und Weise ein besseres Verständnis dafür erhalten, was für Videomaterial erzeugt wird. Doch bekäme sie von den Filmstudios lediglich Standfotos anstatt des gesamten Filmmaterials. Sie könnte also maximal antizipieren, dass oder wie sie von den Kameras gefilmt wird, ohne sich dessen ganz sicher zu sein.

ler Mündigkeit als Kontrolle des Flusses der eigenen Daten Individuen für etwas verantwortlich macht, für das sie keine Verantwortung übernehmen können, erfüllt die Forderung Merkmale der neoliberalen Regierungslogik der Responsibilisierung. Deshalb ist die Forderung nach digitaler Mündigkeit unangemessen.

6 Weitere Trackingtechnologien

Tracking betrifft längst nicht mehr nur das World Wide Web, sondern findet auch auf dem Smartphone oder anderen digitalen Geräten statt. Denn die Ausbreitung der auf Cookies basierenden Marktinfrastruktur hat dazu geführt, dass Tracking zu einem Industriestandard wurde. Im Folgenden skizziere ich anhand von *URL-Tracking* und *Fingerprinting*, wie Tracking im Browser ohne Cookies funktioniert. Daraufhin stelle ich *Trackingpixel* vor, die auch per Mail verschickt werden können, und gebe einen Einblick, wie Tracking zum einen auf dem *Smartphone* und zum anderen auf *Internet-of-Things-Geräten* funktioniert. Mit den Ausführungen verdeutliche ich, dass die trackingbasierte Marktinfrastruktur das Internet in weiten Teilen durchzieht und nicht nur auf Cookies reduziert werden kann. Daraus schlussfolgere ich das zweite Zwischenfazit, in dem ich zwei weitere Eigenschaften des Datensammelns im Digitalen ableite.

6.1. URL-Tracking

Einige der weiteren Trackingtechnologien funktionieren, indem Zusatzinformationen in die Browser-URL eingefügt werden. ‚URL' ist das Akronym für ‚Uniform Resource Locator'. URLs dienen als eine Art eindeutige Adresse im Adressraum des Internets und sie ermöglichen, jede dort veröffentlichte Ressource wie beispielsweise eine Website im Internet zu lokalisieren. An das Ende einer URL können sogenannte Parameter angehangen werden, mit denen die URL und damit auch die Nutzer:in getrackt werden kann. Sie werden mittels Fragezeichen angeführt:

```
http://www.website.de/home.html?param_a=1&param_b=2
```

Parameter sind für die Lokalisierung einer Ressource nicht notwendig, werden aber vom Webserver verarbeitet und gegebenenfalls in Aktionen umgesetzt, bevor er die Website zur Verfügung stellt. Während einige wenige Parameter standardisiert und weit verbreitet sind oder ihre Funktion aufgrund ihrer Bezeichnung leicht identifizierbar ist, gilt es „als gut gehütetes Betriebsgeheimnis, welche Informationen die verschiedenen übermittelten Parameter genau codieren." (Mühlhoff 2019, 88) Im Folgenden skizziere ich mit der *Sitzungsidentifika-*

tionsnummer einen nicht-standardisierten, jedoch identifizierbaren Parameter, sowie mit dem *Google Click Identifier* und den *UTM-Parametern* zwei standardisierte Formate. Zuletzt stelle ich einen nicht-standardisierten, nur schwer identifizierbaren Parameter vor, der für die Nutzerin tendenziell unsichtbar bleibt.

Sitzungsidentifikationsnummern als URL-Parameter sind das cookielose Pendant zu Sitzungscookies. Mit ihnen können eine Sitzung und der beispielsweise dazugehörige Warenkorb auch wiedererkannt werden, wenn Cookies in einem Browser deaktiviert worden sind:

```
https://www.website.de/home/subpage/content.htm?
shop=life&SessionId=2772x0549e38110a28d5930733492f6d37470&a=catalog
```

Allerdings setzt dieses Vorgehen voraus, dass der Anbieter abgesehen von der Sitzungsidentifikationsnummer mit einem weiteren Mechanismus absichert, dass es sich jedes Mal um die gleiche Person handelt, die den Link aufruft, da er andernfalls eine Schwachstelle darstellt, die mit böswilligen Absichten ausgenutzt werden kann.[7] Denn andere Menschen, die die Sitzungsnummer kennen, hätten sonst die gleichen Zugriffsrechte wie die Person, die den Link ursprünglich geöffnet oder geteilt hat. Sitzungsidentifikationsnummern sind daher kein standardisiertes URL-basiertes Trackingverfahren.

Ein weiteres URL-Trackingverfahren ist der proprietäre Google Click Identifier (`gclid`), der in eine URL integriert wird, um die Performanzauswertungen von Werbekampagnen zu ermöglichen. Wenn Menschen auf eine Anzeige klicken, die über eine Werbekampagne von dem Werbesystem Google Ads ausgestrahlt wird, kann über die `gclid` nachverfolgt werden, über welches Medium sich welche Person für welche Kampagne interessiert hat und in welcher Zielgruppe die Person war. Das Werbesystem Google Ads verknüpft wiederum die `gclid` mit dem dazugehörigen Analysetool Google Analytics, welches für die Messung und Auswertung der Werbekampagne zuständig ist.

Die `gclid` ist die jüngere Version der sogenannten *UTM-Parameter*, welche ebenfalls von Google Analytics erfunden wurden und in URLs übergeben werden. Insgesamt können fünf verschiedene UTM-Parameter gesetzt werden, welche das Nutzerverhalten in Bezug auf eine Werbekampagne analysieren: `utm_id`, `utm_source`, `utm_medium`, `utm_campaign`, `utm_term` und `utm_content`. UTM-Parameter sammeln also unter anderem Daten darüber, welche Wer-

7 Diese Schwachstelle machen sich einige Hacking-Methoden zunutze, denen es dadurch gelingt, sich in eine eingeloggte Benutzersitung einzuklinken. Deshalb – aber auch um im Allgemeinen URL-Tracking zu vermeiden – ist es ratsam, den Teil der URL, der nach dem Fragezeichen „`?`“ steht, zu löschen, wenn eine URL mit anderen Menschen geteilt wird.

beanzeige mit welcher Identifikationsnummer angeklickt wurde oder wo die Werbung angeklickt wurde (z.B. bei einer Google Suche oder in einem Newsletter per Mail).

Die Sitzungsidentifikationsnummer, der Google Click Identifier und die UTM-Parameter lassen sich als URL-basierten Trackingverfahren von der Nutzerin in der Adressleiste ihres Browsers ablesen. In anderen Fällen sind diese Parameter jedoch nur für einen Sekundenbruchteil Teil der aufgerufenen URL. So hat Mühlhoff (2019) mithilfe von Reverse Engineering ermittelt, dass Google Klicktracking betreibt, also die Suchanfragen seiner Nutzer:innen mithilfe von URL-Parametern nachverfolgt. Allerdings passiert dieses Klicktracking im Verborgenen,

Anhand der Untersuchung von Mühlhoff konstruiere ich ein Szenario, um die Funktionsweise des Klicktrackings zu veranschaulichen. In diesem Szenario gibt die Nutzerin in der Suchmaschine von Google den Suchbegriff ‚Reverse Engineering' ein und entdeckt unter den aufgelisteten Ergebnissen den entsprechenden Wikipedia-Artikel, den sie lesen möchte. Der Link zu dem Wikipedia-Artikel hat folgende URL:

```
https://de.wikipedia.org/wiki/Reverse_Engineering
```

In dem Moment, in dem die Nutzerin auf diesen Link klickt – bzw. noch spezifischer: in dem kurzen Moment, in dem die Nutzerin den Mauszeiger für wenige Millisekunden heruntergedrückt hält, um auf den Link zu klicken, wird die Ziel-URL jedoch umgeschrieben. Statt auf die Seite von Wikipedia zu führen, zeigt der Link plötzlich auf eine URL von Google, die die Ziel-URL wiederum nur als Parameter enthält. Zusätzlich ist ein weiterer Parameter mit dem Bezeichner `ved=GTa…` eingefügt worden, wobei unklar ist, was genau er bedeutet:

```
https://google.com/?url=https://de.wikipedia.org/wiki/Reverse_Enginee-
ring&ved=GTaanUTzEfb1mvUOFRjO3dgMBWaa4wa00lE3lp0T
```

Nachdem der Mauszeiger losgelassen wird, leitet Google den Browser an die Ziel-URL weiter, die nun auch in der Adressleiste des Browsers erscheint. Der Zwischenschritt, der über die Google-eigene URL führt und dabei einen Parameter anhängt, bleibt dem menschlichen Auge verborgen. Mühlhoff stellte fest, dass sich der Wert des Parameters `ved` im Laufe einer kompletten Suchsitzung nicht veränderte und schlussfolgert daraus, dass hier mittels Parameter das Suchverhalten einer Nutzer:in nachverfolgt wird. (Vgl. Mühlhoff 2019, 88f.)

6.2. Fingerprinting

Das Trackingverfahren des sogenannten *Fingerprintings* basiert nicht wie Cookies oder URL-Parameter auf dem Einsetzen von zusätzlichem Code, sondern macht sich zunutze, wie personalisiert und dadurch einzigartig die Browser bzw. die Browserkonfigurationen heutzutage geworden sind. Denn Browser übergeben von sich aus eine Vielzahl an Konfigurationsinformationen an den Webserver, wenn sie eine Ressource wie beispielsweise eine Website laden wollen, damit diese dem System der Nutzerin entsprechend korrekt dargestellt wird. Zu den Konfigurationsinformationen gehören – unter vielen anderen – die Version des Browsers und des Betriebssystems, die installierten Schriftarten, die Zeitzone, Spracheinstellungen, Hardwaremedien wie Kopfhörer oder Kamera. Aber auch Informationen darüber, welche Plugins im Browser installiert sind oder darüber, wie bestimmte Grafiken gerendert werden, also wie der Browser aus Rohdaten ein Bild erzeugt, gehören dazu (vgl. Electronic Frontier Foundation 2023). Es gibt sogar eine Methode, die eine Audiodatei mit einer Länge von 1/2000 Sekunde im Browser abspielen lässt, und den Browser auf diese Art und Weise identifizieren (vgl. Copland 2021). Die Kombination aus all diesen Merkmalen macht den Browser eindeutig und verleiht ihm gewissermaßen einen Fingerabdruck. Dieser Fingerabdruck ermöglicht es, den Browser mit einer hohen Wahrscheinlichkeit zu identifizieren. Sobald der ‚Fingerabdruck' eines Browsers identifiziert worden ist, ist es im Gegenteil zu Cookies, die gelöscht werden können, viel schwieriger, Anonymität zurückzuerlangen. In einer Studie wurde festgestellt, dass von 470.161 Browsern 83.6% einen eindeutigen Fingerabdruck besaßen, und dass sich daraus für einen randomisierten Browser eine Wahrscheinlichkeit von 1:286,777 ableiten lässt, dass ein anderer Browser den gleichen Fingerabdruck besitzt (Eckersley 2010, 2).

6.3. Trackingpixel

Trackingpixel wiederum sind winzige Grafiken von einer Größe von 1x1 Pixel, die auf einer Website oder in einer E-Mail eingebunden werden. Im Gegensatz zu den anderen Grafiken in einem Interface dienen Trackingpixel jedoch keineswegs dazu, von den Nutzer:innen gesehen zu werden. Stattdessen sind sie farblich entweder transparent gestaltet oder in der Hintergrundfarbe gehalten, sodass sie für das menschliche Auge nicht sichtbar sind. Trackingpixel sind dabei jedoch nicht fest in eine die Website oder E-Mail integriert. Stattdessen enthält der Code für ein Trackingpixel, der in den Quelltext einer Website oder E-Mail eingefügt ist, nicht direkt das Pixel, sondern nur einen Link zu einem weiteren, dritten Server, der die Pixelgrafik bereitstellt. Wenn die betreffende Website oder die E-Mail geöffnet wird, wird der Download

des Trackingpixels durch den Browser oder das E-Mailprogramm automatisch angestoßen. Das Herunterladen des Trackingpixels wird wiederum von dem dritten Server registriert, der zusätzlich zu der Information, dass der Pixel heruntergeladen wurde, noch weitere Informationen von dem Browser sammelt. So können Trackingpixel beispielsweise Daten über das verwendete Betriebssystem, den Browser oder das E-Mailprogramm, die Uhrzeit, die Bildschirmauflösung oder die IP-Adresse sammeln, und über letztere auch Rückschlüsse auf den Standort ziehen. Werden Trackingpixel auf jeder Unterseite einer Website verwendet, ermöglichen sie es außerdem, die Aktivitäten einer Nutzerin während der gesamten Sitzung nachzuverfolgen. Sämtliche große Plattformen wie Meta, LinkedIn oder Twitter stellen Trackingpixel bereit, um die Performanz der Werbekampagnen, die Unternehmen auf diesen Plattformen schalten, nachzuvollziehen. (Vgl. Ryte 2020)

6.4. Tracking auf dem Mobiltelefon

Während Cookies auf HTTP basieren, welches nur in Browsern funktioniert und somit auf den meisten Computern präsent sind, spielen Browser auf mobilen Geräten nur eine untergeordnete Rolle. Hier sind mobile Apps von größerer Bedeutung. Es wurden jedoch wurden alternative Mechanismen entwickelt, mit denen Tracking auch auf mobilen Geräten möglich ist, um eine den Drittanbietercookies ähnliche Funktionalität zu gewährleisten. Die Entwicklung von Trackingtechnologien für mobile Geräte stellt somit ein anschauliches Beispiel dafür dar, wie die cookiefizierte Infrastruktur des World Wide Webs als Vorbild für cookielose Märkte funktioniert. Zu den Trackingtechnologien auf mobilen Geräten, die ich im Folgenden vorstellen werde, gehören Werbeidentifikationsnummern, proprietäre Apps und der sogenannte Single-Sign-On-Service (SSO).

Als die ersten Smartphones entwickelt wurden und sich allmählich verbreiteten, haben Anbieter mobiler Betriebssysteme wie Android und Apple an jedes Gerät eine feste Geräteidentifikationsnummern vergeben, welche sie ohne das Wissen der Nutzer:innen mit Drittanbietern teilten. Nachdem Kritik an diesem Vorgehen aufkam, ersetzten die Anbieter vor ungefähr zehn Jahren die festen Geräteidentifikationsnummern mit den Werbeidentifikationsnummern. Android kooperiert dabei mit Google, indem es deren Google Advertising ID (GAID) einsetzt, und Apple nutzt den eigenen Identifier for Advertisers (IDFA). Die Neuerung an Werbe-IDs ist, dass sie von der Nutzerin eigenständig zurückgesetzt und inzwischen auch selbstständig deaktiviert werden können. Dennoch sind die Werbe-IDs standardmäßig gesetzt und die Nutzerin muss aktiv auf die Suche nach der Einstellung gehen, mit der sie die Werbe-ID deakti-

vieren kann. Diese standardmäßige Annahme von erteilter Erlaubnis, der aktiv widersprochen werden muss, nennt man Opt-out-Verfahren.

Eine weitere Methode, mit der große Plattformen ihre Nutzer:innen auch auf Mobiltelefonen tracken, sind ihre proprietären Apps. So betreibt Google insgesamt 90 verschiedene Apps für Mobiltelefone, darunter Google Mail, Google Maps, Google Chrome oder YouTube. Diese Apps verleiten die Nutzerin mithilfe des Interfacedesigns dazu, permanent eingeloggt zu sein, auch wenn sie den Login zum Teil gar nicht voraussetzen, denn Services wie Google Maps lassen sich auch ohne Google-Account nutzen. Besonders, wenn die Nutzer:innen eingeloggt sind, erlaubt das den Unternehmen jedoch, die Daten aus vielen verschiedenen Apps geräteübergreifend miteinander zu verknüpfen. So erhalten die Unternehmen ein immer komplexer und genauer werdendes Profil der Nutzerin.

Auch die Facebook Messenger App für Mobiltelefone existiert seit ungefähr zehn Jahren. Sie ermöglicht, auf den Nachrichtenverlauf des eingeloggten Facebookprofils zuzugreifen. Standardmäßig bleiben deren Nutzer:innen permanent eingeloggt, wodurch Facebook die über die Messenger App auf dem Mobiltelefon gesammelten Daten verknüpfen kann mit den Daten, die sowohl über das Facebookprofil als auch über Cookies und andere Verfahren im Browser gesammelt werden. Auf diese Art und Weise kann Meta eine über Geräte hinweg verteilte Wissensbasis ausbauen.

Metas Wissensbasis ist inzwischen so groß, dass es eine eigene Vermarktungsmöglichkeit anbietet, die sich Lookalike-Targeting nennt. Beim Lookalike-Targeting erstellt das werbetreibende Unternehmen zunächst eine Sammlung mit all den Informationen, die es über seine wertvollsten Kund:innen hat. Was genau für das Unternehmen wertvoll ist – beispielsweise die Personen, die viel kaufen, oder Personen, die auf Facebook oder Instagram viel mit ihrer Marke interagieren – bestimmt das Unternehmen selbst. Meta analysiert daraufhin die Gruppe der wertvollen Kund:innen und identifiziert gemeinsame Eigenschaften der darin enthaltenen Personen. Auf Basis dieser Gemeinsamkeiten filtert Meta nun Nutzer:innen heraus, die die gemeinsamen Eigenschaften teilen und der Ausgangsgruppe von wertvollen Kund:innen somit ähnlich zu sein scheinen. Diesen Nutzer:innen wird daraufhin die Werbung des werbetreibenden Unternehmen angezeigt. Das Lookalike-Targeting arbeitet mit dem statistischen Verfahren der sogenannten prädiktiven Analytik, auf welche ich in Kapitel 8 eingehen werde.

Diese Wissensbasis nutzt Meta wiederum, um innerhalb der cookifizierten Infrastruktur eine eigene Meta-Tracking-Infrastruktur zu schaffen, die so funktioniert, die die gleiche Funktionsweise hat, jedoch nur die firmeneigenen Daten zulässt. Dadurch entstehen „‚logged‘ or

walled-garden environments, i.e. autonomous milieus built around identifiers specific to an actor“ (Mellet und Beauvisage 2020, 18). Wenn Unternehmen auf Facebook oder Instagram Werbung schalten wollen, können in ihre Werbekampagne keine Informationen einfließen, die durch beliebige Drittanbieter gesammelt wurden – wie es normalerweise auf Werbebörsen wie dem Google Ad Exchange passiert – sondern nur das firmeneigene Wissen sowie das Erstanbieterwissen der Unternehmen über ihre Kunden- bzw. Zielgruppe sowie das dürfen für die Werbekampagne verwendet. Zum einen ist das abgeschlossene Werbeökosystem für Plattformen wie Facebook und Google eine Strategie, um Datenschutzvorgaben zu entsprechen und Drittanbietern den Zugang zu den Daten zu verbieten. Zum anderen gewährt es ihnen jedoch auch mehr Macht über die Daten, die sie haben, und führt zu Monopolbildung.

Nicht nur mithilfe proprietärer Apps haben Plattformen ihr Trackingnetzwerk auf unterschiedliche Geräte wie Mobiletelefone, Tablets oder Computer ausgeweitet. Eine weitere Technologie, die sie sich zunutze machen, ist der Single-Sign-On-Service, der sich sowohl in mobilen Apps als auch in Online-Services im Browser implementieren lässt. Über den SSO können sich neue Nutzer:innen einer App oder für einen Online-Service registrieren und anmelden, ohne dabei ihre eigenen Daten einzugeben. Stattdessen wählen sie beispielsweise aus, sich über den Google-Dienst zu registrieren, woraufhin Google der App oder der Website die entsprechenden Daten der Person zur Verfügung stellen.[8] Die Nutzerin spart sich dadurch die erneute Eingabe ihrer zur Registrierung notwendigen Daten, die sie bereits in ihrem Google-Account hinterlegt hat. Gleichzeitig vereinfacht der SSO den erneuten Anmeldeprozess, nachdem die Nutzerin bereits erfolgreich registriert wurde, da sie nur das Passwort für ihren Google-Account verwenden muss und sich keine weitere Kombination aus E-Mail oder Benutzername und Passwort merken muss. Die meisten großen Plattformen wie Google, Meta, Apple, Microsoft, Amazon, Twitter oder LinkedIn bieten inzwischen einen Single-Sign-On-Service an, der in Apps oder für Online-Service genutzt werden kann. Vordergründig soll durch den SSO zwar der Registrierungs- und Anmeldeprozess für (Neu-)kund:innen erleichtert werden, wovon die Apps und Online-Services profitieren, die den SSO der Plattformen in ihre Anmeldefläche integrieren. Doch ein viel größerer Nutzen liegt in dem SSO für die Plattformen, die ihn anbieten: Denn nicht nur die App oder die Website, die den SSO von Google integriert, erhält Daten von Google – Google erhält gleichzeitig neue Daten über die Nutzer:innen der App, über die Google zuvor nicht verfügen konnte.

8 Siehe auch Mühlhoff (2019, 92) für eine ausführliche Aufstellung der übertragenden und übertragbaren Daten sowie eine Analyse des Single-Sign-On-Service im Kontext von Nudging und Entmündigung.

6.5. Internet of Things

Das *Internet of Things* (IoT) oder Internet der Dinge ist ein visionärer Begriff und beschreibt das Netzwerk, das sich zwischen mit Sensoren ausgestatteten, physischen Objekten entspinnt, die mit dem Internet verbunden sind, und auf diese Art und Weise miteinander kommunizieren. Die physischen Objekte erhalten im IoT zusätzlich eine digitale Identität, als die sie beispielsweise in WLAN oder Bluetooth-Netzwerken erkannt werden können. Wenn die physischen Objekte IoT-tauglich sind, werden sie durch das Adjektivattribut ‚smart' identifiziert. So lässt sich beispielsweise ein smartes Licht per Smartphone-App steuern, ein smarter Kühlschrank füllt automatisch die Einkaufsliste aus und ein smarter Fitness-Tracker am Handgelenk misst und wertet Gesundheitsdaten aus. Auch vernetzte Fahrzeuge sind Teil des Internet of Things.

Durch Sensoren generieren IoT-Geräte kontinuierlich Daten, die als Grundlage für weiterführende Analysen und Berechnungen dienen, ohne welche die Daten – und mit ihnen der Service, der das Gerät ‚smart' macht – bedeutungslos wären. Diese Weiterverarbeitung der Daten mittels Analysen und Berechnungen geschieht vorwiegend in einer Cloud, also in einem Verbund aus Servern. Häufig werden diese Clouds von Drittanbietern betrieben und nicht von dem Unternehmen, welches das Gerät herstellt. Wenn das der Fall ist, ist eine Einwilligung in der Verarbeitung von Daten durch Drittanbieter von den Nutzer:innen erforderlich. Zwar ist es zum Teil möglich, diese Daten lokal, also beispielsweise direkt auf dem Endgerät zu verarbeiten, wie es im Edge-Computing passiert, doch wird Edge Computing derzeit hauptsächlich in industriellen Kontexten verwendet und nicht in Anwendungen, die für Konsument:innen vorgesehen sind (vgl. Qiu u. a. 2020). Es gilt ebenso wenig für alle Geräte, dass sie mit dem Internet verbunden sein müssen (vgl. Farnell 2018), jedoch betrifft auch diese Ausnahme keine smarten Verbrauchergeräte. IoT-Geräte generieren und teilen demnach per definitionem Daten mit einem Cloud-Service, wobei unter anderem die großen Unternehmen Microsoft, Amazon und Google prominente IoT-Clouds anbieten. Google stellt den Service allerdings noch in diesem Jahr 2023 alternativlos ab.

Die Daten, die IoT-Geräte generieren, geben unter anderem Aufschluss über Verbraucherpräferenzen, Nutzerverhalten, Gesundheit oder Aktivitäten allgemein. Dabei gehen sie jedoch über klassische online generierte Verhaltensdaten hinaus, beispielsweise erzeugen IoT-Staubsaugerroboter Grundrisse der Lebensräume, in denen sie verwendet werden (vgl. Webb 2022). In Staubsaugerrobotern der Firma der Firma iRobot, die vor Kurzem von Amazon akquiriert wurden, sind inzwischen häufig Kamerasensoren integriert. Im Jahr 2020 wurden Aufnahmen

von diesen Kamerasensoren aus privaten Wohnräumen in privaten Facebookgruppen gepostet von ‚Klickarbeitern' aus dem globalen Süden, die damit beauftragt waren, die Bilder zu annotieren und die einzelnen Objekte, die darauf erkennbar sind, zu labeln (vgl. Goa 2022). Es handelte sich hierbei jedoch nur um eine begrenzte Anzahl an Staubsaugerroboter, die nicht im Verkauf waren und deren Besitzer:innen zumindest wussten, dass der Roboter filmen würde. Sie wussten jedoch vermutlich nicht, dass andere Menschen damit beauftragt wurden, das Material zu sichten. Auch andere Staubsaugerroboter wie beispielsweise die der Firma Dreame haben Kameras und zumindest Vorrichtungen dafür, Daten mit einer Cloud der Firma zu teilen, wenngleich das laut Datenschutzrichtlinie nicht getan wird (vgl. ebd.). Wie ich zuvor beschrieben habe, ist das Tracking auf Smartphones bereits ein Mechanismus, der es Unternehmen erlaubt, ein komplexeres und detaillierteres Profil von Nutzer:innen über ihre Endgeräte hinweg zu erstellen. Mit IoT-Geräten wird diese Entwicklung noch einmal potenziert, und den Unternehmen ermöglicht, „to paint a more complete and accurate picture of the lives and activities of consumers, individuals in their households, and communities." (Elvy 2018) Da die Unternehmen diejenigen Akteur:innen sind, welche sich das dadurch generierte Wissen aneignen und zunutze machen, spricht die Juraprofessorin Stacy-Ann Ely im Zuge dessen von einer „*corporate colonization and surveillance* [which] may limit individuals' ability to determine what happens to their information and may decrease their ability to shield themselves, their emotions and their daily activities from various actors." (2022; Herv. M.L.).

6.6. Zwischenfazit II: Das Datensammeln ist überall und unausweichlich

In Zwischenfazit I habe ich aus den Ausführungen zu Cookies und ihrer Aneignung durch die Werbeindustrie abgeleitet, dass digitales Datensammeln *kontinuierlich*, *komplex* und *unsichtbar* ist. Diese drei Eigenschaften gelten auch für einen Großteil der weiteren Trackingtechnologien, die ich soeben vorgestellt habe. Eine weitere Eigenschaft, die ich nun aus der Kombination von Kapitel 5 und 6 für das digitale Datensammeln ableite, ist, dass das Datensammeln *überall* stattfindet, das heißt auf allen Websites, die wir besuchen, in allen Apps, die wir verwenden, auf all unseren Smartphones und Rechnern – auf jedem mit dem Internet vernetzten Gerät.[9] In den Worten der Analogie des komplett mit Überwachungskameras ausgestatteten Raumes bedeutet dies, dass es keinen Winkel des Raumes gibt, der nicht gefilmt wird und

9 Natürlich werden nicht streng logisch auf jedem einzelnen Gerät, das mit dem Internet verbunden ist, Daten gesammelt. Jedoch werden auf dem Großteil der Geräte Daten gesammelt, sodass es sich im Sinne des Argumentes lohnt, von pragmatisch nach oben und skalieren und von ‚jedem Gerät' zu sprechen.

dass selbst, wenn die Person den Raum verlässt – indem sie beispielsweise ihr Smartphones aus der Hand legt – weiterhin überall Kameras laufen.

Dass das Datensammeln im Digitalen überall passiert, verunmöglicht *per se* nicht, den Fluss der eigenen Daten auf jedem einzelnen Gerät zu kontrollieren[10]. Allerdings macht die Eigenschaft es zu einer sehr komplexen Angelegenheit, die im Zusammenspiel mit den anderen sechs Eigenschaften des digitalen Datensammelns dazu beiträgt, dass Individuen nicht dazu in der Lage sind, den Fluss ihrer eigenen Daten zu kontrollieren, wie es im Diskurs um digitale Mündigkeit gefordert wird. Dass das digitale Datensammeln überall stattfindet, beschreibt indessen, dass immer mehr Lebensbereiche datafiziert werden, die zuvor nicht die Zielobjekte einer Verdatung waren. Gleichsam werden in diesen Lebensbereichen nicht mehr nur Verhaltensdaten über die Nutzung von Websites oder Suchmaschinen generiert, sondern alle möglichen anderen Arten von Daten wie Bewegungsdaten, Gesundheitsdaten oder wie im Falle der Staubsaugerroboter der Grundriss der eigenen Wohnfläche. Auf diese Art und Weise wird ein immer detaillierteres Bild über die entsprechenden Individuen gezeichnet.

Aus einer Kombination der Merkmale aus Zwischenfazit I, dass das Datensammeln im Digitalen pausenlos ist, und dem Merkmal aus diesem Zwischenfazit II, dass das Datensammeln im Digitalen *überall* ist, ergibt sich ein weiteres Merkmal: Das Datensammeln im Digitalen ist *unausweichlich*. Denn wenn Menschen das World Wide Web nutzen wollen, welches sich unter anderem in einer Infrastruktur aus Trackingtechnologien manifestiert, dann agieren sie unweigerlich in der Infrastruktur aus Trackingtechnologien. In die Analogie des Raumes voller Überwachungskameras übertragen, bedeutet das, dass bestimmte notwendige Reproduktionsaufgaben, die den Haushalt betreffen, ausschließlich in diesem Raum durchgeführt werden können. Beispielsweise, weil sich der Wasseranschluss für die Waschmaschine in dem Überwachungsraum befindet und es so unausweichlich ist, beim Wäsche waschen gefilmt zu werden.

7 Prädiktive Analytik

In diesem Kapitel widme ich mich einem mathematischen bzw. statistischen Verfahren, welches in der Datenanalyse zahlreich zum Einsatz kommt. Mithilfe der *prädiktiven Analytik* werden auf Basis von Daten Prognosen über zukünftige Ereignisse oder unbekannte Sachverhalte aufgestellt. Prädiktive Analytik wird im Marketing beispielsweise bei der Auswahl der Artikel eingesetzt, die einer Person von einem Onlineshop empfohlen werden, weil eine Pro-

10 abgesehen von der Technik des Fingerprinting, die jede Kontrolle umgeht.

gnose darüber getroffen wird, was die Person mit hoher Wahrscheinlichkeit kaufen wird. Aber auch in anderen Bereichen der automatisierten Entscheidungsfindung wird prädiktive Analytik genutzt, etwa bei der Vergabe von Krediten durch Banken (vgl. Torvekar und Game 2019), in der Gesundheitsversorgung (vgl. Hahn, Nierenberg, und Whitfield-Gabrieli 2017; Harris, May, und Vargas 2016) oder in der Polizeiarbeit (vgl. Bachner 2013). Prognostiziert wird nicht nur zukünftiges Verhalten oder persönliche Risikofaktoren, sondern auch persönliche Attribute wie die ethnische Zugehörigkeit, sexuelle Identität oder Wohlstand. Die Prognosen fließen typischerweise in die automatisierten Entscheidungsfindungsprozesse ein, durch die sich die Geschäftsmodelle der Betreiber:innen der prädiktiven Methoden auszeichnen (vgl. Mühlhoff 2022, 32f.).

Ich werde in diesem Kapitel zunächst die Funktionsweise des statistischen Verfahrens erläutern, um anschließend darauf einzugehen, was sich daraus für die Wirksamkeit zum einen von Anonymisierungsverfahren und zum anderen für individuelle Privatsphäreeinstellungen ergibt. Daraufhin schlussfolgere ich das dritte Zwischenfazit.

7.1. Funktionsweise des statistischen Verfahrens

Prädiktive Analytik als statistisches Verfahren ermöglicht es, sensible Attribute oder zukünftiges Verhalten einer beliebigen Person vorherzusagen oder abzuleiten – sogar, wenn nur unvollständige Informationen, wenige personenbezogene oder nicht-personenbezogene Daten über diese Person vorliegen. Bei der prädiktiven Analytik geht es also darum, „anhand leicht zugänglicher Daten schwer zugängliche Informationen über Individuen abschätzen.“ (Mühlhoff 2022, 34). Die Abschätzung der schwer zugänglichen Informationen mittels leicht zugänglicher Daten beruht in der prädiktive Analytik vereinfacht ausgedrückt darauf, eine beliebige Person P_1 mit einer umfangreichen Menge anderer Personen $P_{2, 3 \dots n}$ zu vergleichen, und aus diesem Vergleich Informationen über die Person P_1 abzuleiten. Zu Anschauungszwecken transponiere ich dieses Vergleichsverfahren in die analoge Welt: Über die Personen $P_{2, 3 \dots n}$ sind bereits zahlreiche und vielfältige Informationen vorhanden. Diese Informationen sind in einigen Fällen durch bloßes Hinschauen leicht feststellbar – wie beispielsweise welche Kleidung die Personen $P_{2, 3 \dots n}$ tragen. In anderen Fällen reicht das bloße Hinschauen jedoch nicht aus, um Informationen zu ermitteln, sondern sie werden explizit, beiläufig oder auch indirekt erfragt – wie beispielsweise die Essvorlieben. Über P_1 hingegen ist beispielsweise lediglich bekannt, dass P_1 weiße Turnschuhe trägt. Es ist aber nun von Interesse, ob P_1 Vanilleeis mag. Um abzuschätzen, ob P_1 Vanilleeis mag, wird P_1 verglichen mit der Grundgesamtheit, also all

den anderen Personen $P_{2, 3 \dots n}$, über die eine Vielzahl an Informationen vorliegen. Ein Blick in die Grundgesamtheit auf das Verhältnis von weißen Turnschuhen und einer Vorliebe für Vanilleeis zeigt, dass eine Person, die weiße Turnschuhe trägt, im Durchschnitt zu 80% auch Vanilleeis mag. Daraus wird abgeleitet, dass P_1 wahrscheinlich Vanilleeis mag.

In der tatsächlichen Verwendung von prädiktiver Analytik wird ein mathematisches Modell auf den Daten über $P_{1, 2 \dots n}$[11] berechnet und auf einen vorliegenden Fall angewendet, um basierend auf dieser Anwendung Vorhersagen über den Fall zu treffen. Das mathematische Modell wird auch als *prädiktives Modell* bezeichnet, und wird nicht nur auf Basis der Grundgesamtheit zum Zeitpunkt der Berechnung konstruiert, sondern auf Basis aller möglichen historischen Daten. Historische Daten umfassen alle seit Beginn der Datengenerierung gesammelten Daten, die von einem Unternehmen in einer Datenbank gespeichert werden, und beinhalten also auch Daten aus der Vergangenheit. Die Datenbank wächst und verändert sich mit jedem neu generierten und hinzugefügtem Datum. Durch die Konstruktion des prädiktiven Modells werden die Daten aggregiert, was bedeutet, dass die große Menge an Datenpunkten bzw. Einzelbeobachtungen beispielsweise als Mittelwert zusammengefasst und für weitere statistische Analysen aufbereitet werden.

Das prädiktive Modell bildet ab, welche Ereignisse e_1, e_2, e_3, …, e_n mit welcher Wahrscheinlichkeit auftreten. In dem vorhergehenden Beispiel könnte e_1 beispielsweise das Ereignis sein, weiße Turnschuhe zu tragen, und e_2 das Ereignis, Vanilleeis zu mögen. Dieses prädiktive Modell wird nun auf die neuen, ungesehenen Daten der Person P_1 angewendet. Dabei werden die Datenpunkte von P_1 in den mathematischen Wahrscheinlichkeitsraum eingeordnet und Methoden der Mustererkennung angewendet, um den Fall von P_1 mit allen anderen bisher gesehenen Fällen zu vergleichen. Aus diesem Vergleich wird daraufhin abgeleitet, mit welcher Wahrscheinlichkeit im Hinblick auf die Datenpunkte von P_1 beispielsweise das Ereignis e_2 – also Vanilleeis mögen – auftritt, gegeben dass e_1 vorliegt.

Die UN beschreibt sensible Daten in den Leitlinien für die Regulierung von digitalen Personendateien als „data likely to give rise to unlawful or arbitrary discrimination“ (UN General Assembly 1990). Eine Vorliebe für Vanilleeis stellt in unserer heutigen Gesellschaft also keine sensible Information über eine Person dar, da sie keine Diskriminierungskategorie ist. Jedoch können mithilfe von prädiktiver Analytik sensible Informationen auch aus Hilfsdaten über Nutzer:innen vorhergesagt oder abgeleitet werden. Zu den sensiblen Informationen gehören etwa *race*, die ethnische Herkunft, die sexuelle Orientierung sowie die religiöse, philosophis-

11 Weil typischerweise auch Daten von P_1 bereits in der Datenbank vorliegen, schreibe ich die Datenhistorie hier als ‚$P_{1, 2 \dots n}$‘ und nicht wie zuvor als die Menge ‚$P_{2, 3 \dots n}$‘, in der P_1 noch nicht enthalten war.

che oder politische Anschauung oder die Gesundheit (vgl. Kosinski, Stillwell, und Graepel 2013). Auch die Mitgliedschaft in einem Verein oder einer Gewerkschaft gelten als sensible Daten (vgl. UN General Assembly 1990).

Die Nutzer:in muss der Datenbank weder bekannt sein, um sensiblen Informationen über sie vorherzusagen, noch müssen bereits andere sensible Informationen über sie generiert worden sein. Stattdessen sind die „Inputdaten“, mit deren Hilfe sensible Daten abgeleitet werden, „typischerweise leicht verfügbare Hilfsdaten, zum Beispiel Trackingdaten, der Browser- oder Standort-Verlauf, oder Social Media Daten (Likes, Postings, Freund:innen, Gruppenmitgliedschaften).“ (Mühlhoff 2022, 33) Auch der Philosoph James Brusseau (2020) betont in Bezug auf das Interesse von Unternehmen an Daten, dass dieses keineswegs den sensiblen oder intimen Informationen über ein spezifisches Individuum gilt:

> Because today’s watchers want profit, not personal intimacy, they are interested in profiles, not specific people, and their attention is drawn to opportunities, not embarrassing information. If they are interested in vulnerability at all, they mean vulnerable to *appeals* […]. (Brusseau 2020, 8)

Vielmehr geht es den Unternehmen also darum, welche ‚Empfehlungen‘ sich darüber aus den Daten ableiten lassen, auf welche Art und Weise sie beliebige Nutzer:innen mittels beispielsweise Werbung ansprechen sollten, sodass diese Ansprache möglichst profitsteigernd wirkt.

Zwischen den zunächst wenig Aufschluss gebenden Hilfsdaten von P_1 und sensiblen Informationen über P_1 können mittels prädiktiver Analytik Korrelationen berechnet werden, weil die historischen Daten sämtlicher Personen $P_{1, 2 \ldots n}$ so mannigfaltig sind, und neben vielen Hilfsdaten von vielen Personen auch einige sensible Informationen über einige Personen beinhalten.

Dass dieses Vorgehen, aus wenig Aufschluss gebenden Hilfsdaten sensible Informationen abzuleiten, funktioniert, wurde bereits vielfach gezeigt und angewendet. Beispielsweise hat eine US-amerikanische Supermarktkette aus einer Kombination von 15 bestimmten Produkten, die von einer Person gekauft werden, abgeleitet, dass mit einer hohen Wahrscheinlichkeit eine Schwangerschaft vorliegt (vgl. Hill 2012). Darüber hinaus haben Wissenschaftler:innen gezeigt, dass sich aus Facebook-Likes von beliebigen, unbekannten Personen mit hoher Wahrscheinlichkeit Aussagen über sensible Informationen abschätzen lassen. Basierend auf einer Datenhistorie von 58.000 Facebook-Nutzer:innen, die ihre Profil- und Likes-Daten freiwillig zur Verfügung gestellt haben, konnten sie unter anderem sensible Informationen wie die Sexualität, *race*, Persönlichkeitsmerkmale, den Suchtmittelkonsum oder die mentale Gesundheit abschätzen (vgl. Kosinski, Stillwell, und Graepel 2013). Genauso könnte ein Unterneh-

men Zyklusdaten über eine Zyklustrackingapp sammeln, und mit hoher Wahrscheinlichkeit vorhersagen, wann oder dass eine Person an dem Prämenstruellen Syndom (PMS) leidet und daher besonders anfällig für Impulskäufe ist (vgl. Pine und Fletcher 2011). Ein kommerzielles Unternehmen, das ein entsprechendes prädiktives Modell anwendet, könnte in der Zeit, in der eine beliebige Person wahrscheinlich unter PMS leidet, gezielt Werbung schalten. Bei den in der Werbung beworbenen Produkten könnte es sich um Artikel handeln, die die Person bereits vorher schon einmal angeschaut hat, oder um Artikel, die andere Personen, über die abgeleitet wurde, dass sie an PMS leiden, in dieser Zeit gekauft haben.

7.2. Zur (Un-)Wirksamkeit von Anonymisierung und individuellen Datenschutzeinstellungen

In vielen Zusammenhängen wird die Anonymisierung von Daten als Datenschutzlösung betrachtet. Es ist zum einen jedoch möglich, auch in anonymisierten Daten bestimmte Individuen zu identifizieren. Beispielsweise hat 2021 ein konservatives katholisches Nachrichtenportal in den USA über einen Datenhändler anonymisierte Standortdaten von der Dating-App Grindr gekauft. In diesen Daten konnte der Nachrichtendienst einen ranghohen katholischen Priester identifizieren, indem sie ihre eigenen Daten über dessen Aufenthalt mit den anonymisierten Standortdaten abglichen. Der Priester war daraufhin gezwungen, sein Amt abzulegen.

Zum anderen ist es für die technische Funktionalität von prädikativer Analytik jedoch auch unwesentlich, ob die Daten anonymisiert sind oder nicht. Denn auch in einer großen Menge an komplett anonymisierten Daten lassen sich Muster und Korrelationen erkennen, die mittels Proxy-Attributen ermöglichen, sensible Attribute beliebiger Individuen abzuleiten oder vorherzusagen. Die Identität der Individuen als eine bestimmte Person mit einem bestimmten Namen und ggfs. Geburtsdatum ist in diesem Moment irrelevant, da es vielmehr darum geht, ihre Wünsche und Bedürfnisse zu erkennen, diese gewinnbringend zu nutzen – oder sogar zu konstruieren (s. Abschnitt 8.5.). Rechtlich betrachtet spielt es hingegen eine wesentliche Rolle, ob Daten anonymisiert sind, denn anonymisierte Daten fallen nicht in den Geltungsbereich von Datenschutzgesetzen wie beispielsweise der DSGVO (vgl. Datenschutz-Grundverordnung, Erwägungsgrund 26). Gegenstand der DSGVO sind vielmehr personenbezogene Daten, also Daten „die sich auf eine identifizierte oder identifizierbare lebende Person beziehen.“ (Europäische Kommission 2022) Die Daten, die in die Berechnung prädiktiver Modelle einfließen, sind in dem Moment ihrer Generierung und Sammlung häufig anonymisiert und gelten also nicht als personenbezogen. Doch stellt Mühlhoff in Frage, ob der Personenbezug im Falle prädiktiver Analytik eine valide Unterscheidungskategorie ist:

> Im Laufe der Verarbeitung *abgeleitete* Informationen können die Unterscheidung von anonymen vs. personenbezogenen somit unterlaufen, [...] weil durch Verknüpfungen anonymer Daten neue Erkenntnisse in Bezug auf beliebige Dritte gewonnen werden können. (Mühlhoff 2022, 48; Herv. i. O.)

Es ist für prädiktive Analytik also unerheblich, ob Daten personenbezogen oder anonymisiert sind, und die Ausführungen gelten für beide Arten von Daten.

Dass mittels prädiktiver Analytik sensible Informationen über Nutzer:innen abgeleitet werden können, über die lediglich Hilfsdaten vorliegen, liegt daran, dass die von allen Nutzer:innen gesammelten Daten sich in dem prädikativen Modell wechselseitig beeinflussen. Daraus kann geschlussfolgert werden, dass die individuellen Datenschutzeinstellungen eines datensparsamen Individuums – also eines Individuums, welches nicht mehr als die notwendigen Daten über sich preisgeben möchte – dieses Individuum nur bedingt davor schützen, identifiziert zu werden. Die Identifikation eines Individuums bezieht sich an dieser Stelle ebenfalls nicht notwendigerweise darauf, dass es als die Person ‚Vorname Nachname' lokalisierbar ist, sondern vielmehr als eine Person, die mit hoher Wahrscheinlichkeit bestimmte Eigenschaften und Bedürfnisse hat. Selbst wenn nur notwendige, wenig Aufschluss gebende Hilfsdaten über dieses Individuum generiert und gesammelt werden, lassen sich aus diesen wenigen Daten andere, auch sensible Informationen ableiten oder Vorhersagen aufstellen, solange bereits genügend aussagekräftige Daten über andere Nutzer:innen gesammelt wurden oder in Zukunft gesammelt werden. Denn sogar dann, wenn die Hilfsdaten in dem Moment der Generierung noch wenig aussagekräftig sind, kann es sein, dass in Zukunft neue Daten über andere, zukünftige Nutzer:innen generiert werden, die in den bis dato wenig aussagekräftigen Daten der Vergangenheit neue Muster zu erkennen ermöglichen. Individuelle Datenschutzvorkehrungen sind daher nur bedingt relevant.

Im Gegensatz dazu haben die Datenschutzeinstellungen von Individuen, die sich unabsichtlich oder absichtlich datenfreigiebig verhalten – beispielsweise, weil sie „nichts zu verbergen haben" (Mühlhoff 2022, 32), einen umso stärkeren Effekt darauf, wie identifizierbar sie selbst und andere Individuen werden. Denn ihre Daten bilden den Input des prädikativen Modells und haben somit einen unmittelbaren Einfluss darauf, welche Cluster gebildet werden und welche Vorhersagen über andere Personen getroffen werden können:

> Wir stehen hier also vor einer Situation, in der die *Datenfreigiebigkeit einer Minderheit von Nutzer:innen* (zum Beispiel die prozentual wenigen Facebook-Nutzer:innen, die Angaben über ihre sexuelle Orientierung machen) den Standard der über *alle* Gesellschaftsmitglieder ableitbaren Informationen setzt. (ebd., 35f.; Herv. i. O.)

Die Entscheidungen, die Menschen in Bezug auf die über sie generierten Daten treffen, stehen also in einem interdependenten Verhältnis, und die Entscheidung einer einzelnen Person ist keineswegs nur eine individuelle, sondern wirkt sich auch auf die anderen Nutzer:innen aus. Mühlhoff schlussfolgert aus diesem Verhältnis, dass die Validität des Rechtsmechanismus der Einwilligung, mit welcher heutzutage vorwiegend das Sammeln von Daten rechtlich abgesichert wird, in Frage gestellt werden muss. Denn die Konsequenzen der Einwilligungsentscheidung – anders als in der Einwilligung vorgesehen – betreffen nicht nur das einwilligende Individuum, sondern auch andere Nutzer:innen (vgl. Mühlhoff 2022, 53):

> [W]enn eine Nutzer:in nach einer Einwilligung gefragt wird, dann trifft sie eine Entscheidung *auch für viele andere Menschen*, die anhand dieser Daten diskriminiert werden können, sofern auch noch einige weitere Nutzer:innen solche Daten über sich preisgeben [...] (ebd., 45; Herv. M.L.)

Auch die Philosophin Carissa Véliz betont, dass Privatheit oder ‚Privacy' – ein Begriff, der den Diskurs um Datenkontrolle prägt und in Abschnitt 9.1. erläutert wird – nicht nur ein persönliches, sondern auch ein kollektives Unterfangen ist (vgl. 2020, 75). Sie spricht davon, dass wir nicht nur für die eigenen Daten bzw. die eigene Privacy Verantwortung tragen, sondern auch für die Privacy unserer Mitmenschen: „Since we are intertwined in ways that make us vulnerable to each other, we are responsible for each other's privacy." (ebd., 79)

7.3. Normierung

Der Einfluss, den die Entscheidungen von denjenigen Personen, die absichtlich oder unabsichtlich viele Informationen über sich preisgeben, auf die anderen Nutzer:innen hat, wirkt dabei normierend. Denn die Entscheidungen beeinflussen, welche Daten über sie generiert und in die Datenhistorie eingespeist werden. Auf der Datenhistorie werden wiederum die prädiktiven Modelle trainiert. Auf Grundlage der prädiktiven Modelle werden wiederum Entscheidungen darüber getroffen, wie Menschen begegnet wird, welche Werbung ihnen angezeigt wird, ob sie einen Kredit erhalten, oder für eine Anstellung geeignet sind. Dadurch bilden die historischen Daten die Hintergrundfolie für das, was in einer Gesellschaft überhaupt vorhersagbar ist, und somit auch vorhergesagt wird.

Übertragen auf das vorhergehende Beispiel bedeutet das, dass womöglich nur ein paar Menschen, die weiße Turnschuhe tragen, auch mitgeteilt haben, dass sie Vanilleeis mögen, während viele andere die Information darüber, ob und wenn ja welches Speiseeis sie präferieren, lieber für sich behalten. Auch wenn es nicht viele Personen sind, die ihre Speiseeispräferenz transparent gemacht haben, erkennt das auf diesen Informationen trainierte prädiktive Modell

ein Muster und berechnet, dass eine Person mit weißen Turnschuhen mit hoher Wahrscheinlichkeit Vanilleeis mag. Dem Unternehmen, das Lebensmittel verkauft, reicht diese Information, um einer neuen Person mit weißen Turnschuhen ebenfalls ein Vanilleeis vorzusetzen, denn die Wahrscheinlichkeit, dass die Person Vanilleeis mag, ist immer noch höher als die Wahrscheinlichkeit, dass sie eine andere Sorte bevorzugt.

7.4. Zwischenfazit III: Das Datensammeln ist prädiktiv

Aus Mühlhoffs Ausführungen zur prädiktiven Analytik schlussfolgere ich, dass das digitale Datensammeln *prädiktiv* ist. Es ist prädiktiv insofern, dass es ermöglicht, Informationen über ein beliebiges Individuum abzuleiten oder vorherzusagen, welche dieses nicht preisgegeben hat. Dies ist möglich, weil über andere Personen bereits unzählige Daten generiert und gesammelt wurden. Diese Dynamik hat zur Folge, dass die Forderung, Kontrolle über die *eigenen* Daten zu haben, impliziert, Kontrolle über die Daten *aller* Menschen haben zu müssen. Denn für das Ableiten und Vorhersagen von sensiblen Informationen über ein beliebiges Individuum ist es nur marginal, welche konkreten Privatsphäreeinstellungen dieses Individuum getroffen hat und wie streng diese sind. Denn solange ein wenig Hilfsdaten über dieses Individuum vorliegen, können über dieses Individuum Informationen abgeleitet und vorhergesagt werden. Somit beeinflussen die Entscheidungen, die die Nutzer:innen in ihren Privatsphäreeinstellungen treffen, sich indirekt. Wenn eine Nutzerin ihre Daten insofern kontrollieren möchte, dass keinerlei sensible Informationen über sie bekannt sind, sensible Informationen über sie jedoch mittels prädiktiver Analytik ableitbar sind, dann reicht es nicht, nur die eigenen Daten zu kontrollieren – es müssten auch die Daten aller anderen Nutzer:innen kontrolliert werden. Und mit ‚alle anderen Nutzer:innen' sind nicht nur alle anderen Nutzer:innen in dem Moment der Entscheidung in Bezug auf Privatsphäreeinstellungen gemeint, sondern auch die vergangenen Nutzer:innen der letzten Jahrzehnte sowie alle zukünftigen Nutzer:innen. Dafür wird dem Individuum durch die Forderung nach digitaler Mündigkeit implizit die Verantwortung aufgebürdet. Doch eine Kontrolle der Daten aller vergangenen, derzeitigen und zukünftigen Nutzer:innen kann ein Individuum nicht leisten. Dies stützt mein Argument, dass die Forderung nach digitaler Mündigkeit in Form der Teilforderung der Kontrolle des Flusses der eigenen Daten unangemessen ist und dass es sich bei der Forderung um eine Spielart der neoliberalen Regierungslogik der Responsibilisierung handelt, bei der Individuen für Aufgaben verantwortlich gemacht werden, die zu bewältigen sie strukturell nicht in der Lage sind.

8 Das (In-)dividuum in der Marktinfrastruktur

Ich untersuche in dieser Arbeit die Hintergrundbedingungen, vor denen wir fragen müssen, was es bedeutet, als Nutzer:innen des Internets digital mündig zu sein und unsere Daten kontrollieren zu sollen. In den vorhergehenden drei Kapiteln habe ich bereits die technologischen, (markt-)infrastrukturellen und methodischen Hintergrundbedingungen kondensiert. In drei Zwischenfaziten habe ich gezeigt, dass das Datensammeln im Digitalen die Merkmale hat, *kontinuierlich*, *komplex*, *unsichtbar*, *überall*, *unausweichlich* und *prädiktiv* zu sein. Darin zeichnete sich bereits ab, dass die individuellen Nutzer:innen eine essentielle Rolle in der cookifizierten Marktinfrastruktur spielen. In diesem Kapitel möchte ich nun die Perspektive des Werbesystems untersuchen, und welche Rolle individuelle Nutzer:innen darin spielen. Dafür arbeite ich die Transformationsprozesse heraus, die die Verbrauchermodelle des Werbesystems den Ausführungen der Marketingforscher Robert Cluley und Steven D. Brown (2015) zufolge aufgrund von Trackingtechnologien durchlaufen haben. Damit werde ich zum einem in Zwischenfazit IV weiterhin für die Hauptthese dieser Arbeit argumentieren – dass individuelle Datenflusskontrolle verunmöglicht wird – und mich in Zwischenfazit I' der Nebenthese zuwenden, dass Daten schützenswert sind und es deshalb dennoch einer nicht-individualistischen Kontrolle des Flusses der Daten bedarf.

8.1. Verbrauchermodelle im traditionellen und im programmatischen Werbesystem

Dem Werbesystem, das auf traditionellen Medien wie Print oder Fernsehen beruhte, lagen bestimmte Modelle zugrunde, die Annahmen darüber trafen, was das Wesen von Konsument:innen ist, wie sie sich in bestimmten Situation verhalten und was ihre Vorlieben sind. Cluley und Brown bezeichnen diese Modelle als ‚Masken', die den Konsument:innen durch die Medien aufgesetzt werden, bzw. die sich die Konsument:innen selbst aufsetzen, da sie eine Rahmung für die Konstruktion der eigenen Identität bieten. Beispiele für solche Masken sind die der „rational decision-makers, information processors, communicators, rebels, activists, workers, prosumers and so on" (Cluley und Brown 2015, 108). Diese Masken sind zwar im Allgemeinen voneinander verschieden, doch haben sie Cluley und Brown zufolge alle die gleiche Grundannahme, dass die Konstument:innen, die sie tragen, als individuelle Subjekte adressiert werden (vgl. ebd., 108).

Die Masken entsprechen den Gruppierungen von Konsument:innen, wie sie im traditionellen Werbesystem der Neunzigerjahre mithilfe von festen, vorgefertigten Kategorien vollzogen

wurden (vgl. Kap. 5.1.). Parameter, die in die Konstruktion der Gruppierungen hineinflossen, waren beispielsweise Alter, Geschlecht, Einkommen oder allgemeine Interessen. Auf diese Art und Weise wurden die Individuen entlang ihrer Ähnlichkeiten gruppiert und es ergaben sich unter anderem Kategorien wie die der „silver surfers“ oder der „dog owners“ (Cluley und Brown 2015, 115).

Durch die durch Cookies bedingte Entwicklung von Werbebörsen und dem dort stattfindenden programmatischen Werbehandel in Echtzeit (vgl. Kap. 5.5.) haben sich diese Verbrauchermodelle verändert. Konsument:innen werden im heutigen, programmatischen Marketing nicht mehr wie im traditionellen Werbesystem nach ihren vermeintlichen Ähnlichkeiten und auf Basis von bereits bestehenden Kategorien gruppiert. Stattdessen werden sie auf Basis aller über alle möglichen Nutzerinnen gesammelten und aggregierten Daten in *fluide Cluster* gruppiert. Im Gegensatz zu den Gruppen im traditionellen Werbesystem, in die Verbraucher:innen aufgrund ihrer Ähnlichkeiten zueinander und ihrer Ähnlichkeit zu einem Prototypen der jeweiligen Kategorie eingeordnet werden, zeichnen sich fluide Cluster vor allem durch die Differenz zueinander aus (vgl. Cluley und Brown 2015, 115). Clusteralgorithmen beziehen dabei zwar mit ein, welche Datenpunkte zueinander ähnlich sind, allerdings ist diese Ähnlichkeit nur insofern relevant, dass es lediglich eine Rolle spielt, ob die Datenpunkte zueinander ähnlicher sind als zu Datenpunkten in anderen Clustern, von denen sie im Umkehrschluss verschieden sind. Cluster basieren also nicht auf vordefinierten, externen Kategorien wie die ‚silver surfer‘ oder ‚dog owner‘, sondern einzig und allein auf dem internen Verhältnis aller Datenpunkte zueinander. Ein Cluster wird von einem Algorithmus ‚gefunden‘, sobald Datenpunkte zueinander weniger verschieden sind als zu allen anderen Datenpunkten.

Die Cluster sind das funktionale Pendant zu den im traditionellen Marketing festen, externen Kategorien, die bereits existieren, bevor eine Werbekampagne gestartet wird. Die Cluster existieren jedoch nicht vorab, sondern entstehen erst in dem Prozess der Vermarktung selber, da sie von dem internen Verhältnis der aktuellen Datenpunkte zueinander abhängen. Dass Cluster einzig vom internen Verhältnis der Datenpunkte zueinander abhängen, bedingt auch, dass die Cluster fluide sind, da jeder neue Datenpunkt das interne Verhältnis und somit gegebenenfalls auch die Cluster verändert: „[a] consumer’s position is fluid as new differences are sought out to place them into new segments.“ (Cluley und Brown 2015, 117)

8.2. Der Divisionsprozess

Cluley und Brown argumentieren, dass Nutzer:innen in diesem Werbesystem, in dem sie basierend auf der Differenz zueinander geclustert werden, nicht mehr wie zuvor im traditionellen Werbesystem als Individuen aufgefasst werden, sondern zu sogenannten *Dividuen* werden: „a cybernetic subject made up of data point, codes and passwords“ (Cluley und Brown 2015, 108), „that is endlessly divisible and reducible to data representations via the modern technologies of control, like computer-based systems“ (Williams 2005, 104). Hietanen et al. sprechen von dem „dividual as a predictive data profile“, welches sich „at the heart of technologically-mediated consumer culture“ (Hietanen, Ahlberg, und Botez 2022, 1) befindet. Die Nutzer:innen im programmatischen Werbesystem werden also keineswegs individualisiert und auf bestimmte, feste Kategorien abgebildet, mit denen sie sich identifizieren können. Stattdessen werden sie durch Clusteralgorithmen auf Basis der Differenz zueinander voneinander dividiert: „people [are not imagined, M.L.] as individuals with emotions, attitudes, behaviours, but as data that can be divided and reassembled through analysis.“ (Cluley und Brown 2015, 117)

Die Autoren konzipieren den kybernetischen Divisionsprozess, der repetitiv neue Dividuen hervorbringt, in drei Schritten. Der erste Schritt ist, Menschen nicht als Individuen mit Emotionen, Einstellungen oder Verhaltensweisen zu betrachten, sondern als Daten, die durch Analyse geteilt und neu zusammengesetzt werden können (vgl. Cluley und Brown 2015, 117). In dem Moment, in dem Menschen als teilbare Daten konzipiert und zu Dividuen werden, geht auch die Verknüpfung zwischen dem individuellen Menschen und den über ihn generierten Datenpunkten verloren. Im cookiebasierten Werbesystem entspricht diesem ersten Schritt das Setzen eines Cookies, welches ermöglicht, Daten über die Nutzer:innen zu sammeln.

In einem zweiten Schritt werden technologische Instrumente auf die so generierten Daten angewendet und Berechnungen durchgeführt, durch die neue Kombinationen von Menschen und Daten hervorgebracht werden (vgl. Cluley und Brown 2015, 117). Ein in dieser Arbeit relevantes Beispiel für ein solches technologisches Instrument ist der sogenannte *Cookie-Matching-Prozess*. Als Ergebnis der Verarbeitung durch den Cookie-Matching-Prozess wird eine Werbefläche an diejenigen Werbetreibenden verkauft, die bereits spezifische Information über die Besucherin der Werbefläche besitzen, wodurch das Cookie für sie am ‚wertvollsten‘ ist. Diese Information besitzen sie beispielsweise durch ein anderes Cookie über die Besucherin, durch das sie wissen, dass sie schon einmal im Onlineshop war und den Bestellvorgang für

einen bestimmten Artikel abgebrochen hat. Der Algorithmus berechnet, dass der Besucherin als Werbung dieser und weitere ähnliche Artikel angezeigt werden soll.

Im dritten Divisionsschritt wird deutlich, weshalb Cluley und Brown den Prozess bzw. das Dividuum als ‚kybernetisch' bezeichnen. Denn im dritten Schritt erscheint das Ergebnis der Berechnungen aus dem zweiten Schritt in Form von Werbung auf den graphischen Interfaces der in das spezifische Cluster eingeteilten Nutzer:innen. Von dort beeinflusst es unmittelbar deren Handeln und Wahrnehmen, welches wiederum erneut im ersten Schritt als Daten über die Nutzer:innen einfließt: „This then shapes the marketing communications uttered to this group of consumers which are, subsequently, measured and analysed, feeding back into further clustering of consumers" (Cluley und Brown 2015, 115). Der Divisionsprozess ist kybernetisch, weil in einer endlosen Feedbackschleife jedes neue Datum das User Interface beeinflusst, was wiederum neue Daten generiert, die in die Berechnung mit einfließen, die das neue Interface regeln. Deshalb gilt für die Cluster, in die Nutzer:innen eingeteilt werden, dass sie fluide und flüchtig sind und sich mit jedem neu generierten Datum verändern.

Weil die fluiden Cluster flüchtig sind, und immer erst in dem aktuellen Durchlauf ihrer Berechnung entstehen, existiert Cluley und Brown zufolge im programmatischen Werbesystem keineswegs eine ‚Maske' im Sinne der traditionellen Werbebranche, in welcher es eine endliche Anzahl an Masken gibt. Vielmehr gilt im programmatischen Marketing:

> [R]ather than imagine some menu of possible masks that marketing can place on consumers, we have to conceptualise a relationship where masks are constantly constituted through marketing as consumers are constantly reassembled as new collections of difference. (Cluley und Brown 2015, 115)

Hietanen et al. betonen ebenfalls, dass es sich bei der Dividualität keineswegs nur um einen anderen Modus des Konsums oder um einen andere, aber ähnliche Art der Maske für die Konsument:innen handelt, sondern um eine fundamentale Veränderung (vgl. 2022, 2).

Weil es im traditionellen Werbesystem eine endliche Sammlung an distinkten ‚Masken' gab, war es den Individuen möglich, ihre Maske gegen eine andere auszutauschen oder sich zu weigern, sie gänzlich aufzusetzen, und auf diese Art Widerstand zu leisten:

> An individual consumer wearing a mask designed by marketing devices and marketing theory can refuse to wear that mask. They might take on another, switching from the rational decision-maker to the hedonist, but they are able to take it off. (Cluley und Brown 2015, 118)

Im Gegensatz dazu können Dividuen im heutigen, programmatischen Werbesystem nicht zwischen sich und der sich überhaupt erst im Vollzug konstituierenden Maske differenzieren, die

ihnen unweigerlich aufgesetzt wird, sobald sie in der vernetzten Marketingwelt des Internets agieren (vgl. Cluley und Brown 2015, 118). Deshalb können sich Dividuen der Maske nicht widersetzen, indem sie sich verweigern oder sie mit einer anderen austauschen. Cluley und Brown finden unter Rückgriff auf Gilles Deleuze (1992) zum Dividuum nur eine einzige Möglichkeit des Widerstandes für die Dividuen:

> Resistance […] is thus to be found in ‚out-gaming' the combinatorial logic of control: find a way to move faster, discover a ‚line of flight', become something utterly unrecognisable to the devices that continuously attach themselves to your movements. (Cluley und Brown 2015, 118)

Die einzige Möglichkeit zum Widerstand liegt also darin, nicht von Trackingtechnologien erkannt zu werden. ‚Nicht erkannt zu werden' meint hier keineswegs – wie in diesem Kontext angenommen werden könnte – in einer anonymen Masse als ein bestimmtes Individuum identifiziert und lokalisiert zu werden. Es meint vielmehr, in keiner Weise verdatet zu werden; auch nicht in Form von vermeintlich anonymen Aktivitäten wie Klicks oder dem Browserverlauf, welche nicht notwendigerweise Rückschlüsse auf ein bestimmtes Individuum zulassen (vgl. Kap. 7).

Dadurch, dass die Trackinginfrastruktur die Cluster kreiert, in die wir als Nutzer:innen des World Wide Webs ständig gruppiert werden, ist sie verwoben mit jeder einzelnen Handlung, die wir online ausführen. Unsere Handlung wird wiederum von Unternehmen durch Cookies oder anderen Trackingtechnologien als eine Aktion registriert und verdatet. Ohne diese Handlungen – oder korrekter gesagt: ohne, dass Unternehmen mittels Trackingtechnologien ständig Daten erzeugen, aggregieren und zueinander in Bezug setzen, die diese Handlungen abbilden sollen, – würde der programmatische Werbemarkt nicht existieren. Denn ohne die stets wachsenden, datenbasierten Wissensschätze würde dem Markt die Ware fehlen: „the market, in this sense, does not exist outside of traces consumers leave within databases" (Cluley und Brown 2015, 115). Hietanen et al. gehen sieben Jahre später einen Schritt weiter als Cluley und Brown und schlussfolgern für das Verhältnis von Markt und Dividuum, dass der Markt nicht nur nicht mehr außerhalb des Dividuums und seiner Daten existiert, sondern sich im Dividuum selbst realisiert: „The dividual does not ‚take part' in the market, *it is the market fully realised* as a global modulation of flows" (Hietanen, Ahlberg, und Botez 2022, 3; Herv. i. O.).

Was bedeutet es nun, dass Individuen zu Dividuen werden? Im Laufe dieses Abschnitts wurde deutlich, dass die Konsument:innen im programmatischen Werbesystem nicht mehr, wie im traditionellen Werbesystem, im Verhältnis zu externen, festen Kategorien konzipiert und angesprochen werden. Dass Kategorien des traditionellen Marketings fest und referenzierbar sind,

ermöglichte den Nutzer:innen, sich mit ihnen zu identifizieren und die Konstruktion ihrer Identität an ihnen auszurichten. Es ermöglichte ihnen ebenfalls, die damit einhergehenden ‚Masken' abzulehnen oder zu wechseln. Da die Clusteralgorithmen der programmatischen Werbung indessen lediglich das Verhältnis der Daten zueinander abbilden und ohne externe Kategorien auskommen, fehlen den Nutzer:innen – zumindest in Bezug darauf, wie sie von Marketing und Werbung angesprochen werden – die referenzierbaren Kategorien.

Zwar bleibt zu erforschen, ob sich tatsächlich psychologische Aussagen über den Zusammenhang von Verbrauchermodellen und Persönlichkeitsstruktur treffen lassen, aber dass es keine festen Kategorien mehr gibt, an denen die eigene Identität ausgerichtet werden kann, könnte Brusseau zufolge Auswirkungen auf die Identitätsbildung haben. Dies setzt die Annahme voraus, dass es prinzipiell so etwas wie ein kohärentes Selbst geben kann, welches sich in einem Individuum manifestiert. Brusseau spricht beispielsweise davon, dass dadurch, dass die Werbeindustrie Individuen nicht mehr als solche wahrnehmen, sondern nur als Eigenschaftscluster, sich auch die Wünsche und Bedürfnisse von jenem Selbst ablösen. Stattdessen realisieren sie sich in Form von fragmentierten Teilaspekten: „That is, our desires and purchases are no longer aspects of a coherent self so much as disconnected spurts of purchasing corresponding with market segments." (Brusseau 2020, 15) Der Philosoph veranschaulicht dieses Verhältnis folgendermaßen:

> And, it is not *me* who wants to visit the Whitney Museum on Saturday, it is the person whose name appears on three lists: Land Rover owners, Manhattan residents, Amazon Alexa users. The Whitney marketing department – with the help of big data operators like LiveRamp – has found that when those three slices of *dividuality* come together, the offering of a discounted membership likely receives an affirmative response. (Brusseau 2020, 14; Herv. i. O.)

Im traditionellen Werbesystem, in welchem die Kategorien statisch und referenzierbar waren, konnten Nutzer:innen aufgrund von externen Merkmalen wie Alter, Interesse, Einkommen oder Geschlecht ableiten oder vermuten, in welche Kategorie sie eingeordnet würden bzw. welche ‚Maske' ihnen als Verbraucher:innen aufgesetzt werden würde. Diese externen Merkmale spielen zwar auch heute weiterhin eine Rolle in der Persönlichkeitsstruktur, jedoch hängen die dividuierenden Cluster zusätzlich auch von Datenpunkten ab, die Handlungen und unbewusstes Verhalten von Menschen abbilden sollen. Wenn sie Verhalten abbilden sollen, welches für die Nutzer:innen unbewusst ist, und dieses unbewusste Verhalten dazu beiträgt, in welche Kategorie eine Person geordnet wird, so ist es für sie auch nicht mehr so leicht nachvollziehbar, aufgrund welcher Merkmale eine Nutzerin in diese Kategorie eingeordnet wird. Darüber hinaus geschieht das unbewusste Verhalten, auf Basis dessen Daten generiert werden,

vorwiegend unbeobachtet von anderen Menschen, auf deren Bildschirm wir selten Einblick haben. Diejenigen Merkmale, die die Gruppierungen in Cluster determinieren, bleiben für uns also größtenteils im Verborgenen. Ebenfalls eher im Verborgenen geschieht heute der Konsum von Werbung, weil Nutzer:innen nicht wissen können, welche Werbung anderen Person auf der gleichen Werbefläche auf der gleichen Website angezeigt wird, ohne dass diese Personen das offenlegen würden. Nutzer:innen erhalten also kaum Einblick darüber, wie Dividuen in anderen Clustern angesprochen werden.

Verbraucher:innen im traditionellen Werbesystem haben die Möglichkeit, sich eine neue Zeitung zu kaufen oder den Fernseh- oder Radiokanal zu wechseln, um sich so ein Bild darüber zu machen, wie andere Verbrauchermodelle konstruiert und adressiert werden. Sie können durch den Vergleich mit und Abgrenzung von anderen Modellen eventuell auch Rückschlüsse darüber ziehen, was ihre eigene ‚Maske' für Annahmen enthält und wie sie selber als Konsument:innen angesprochen und konzipiert werden. Sowohl sich von anderen Verbrauchermodellen abzugrenzen als auch, die eigene ‚Maske' zu erkennen, ist heutzutage im programmatischen Werbemodell erschwert.

8.3. Personalisierung

Es kann beim Lesen der Eindruck entstehen, dass Werbung im programmatischen Werbesystem individueller sei, als im traditionellen Werbesystem, insofern sie in Echtzeit auf die vorliegenden und abgeleiteten Informationen über die Konsument:innen angepasst ist und auf den jeweils aktuellen Zustand reagiert. Weil das programmatische Marketing jedoch auf Basis des internen Verhältnisses von unzähligen Datenpunkten Cluster dividiert, ist die Werbung jedoch nur bedingt individuell, sondern vor allem unterschiedlich. Denn in die Werbung, die einer Person angezeigt wird, fließen neben ihren eigenen vorhergehenden Entscheidungen und ihrem bisherigen Verhalten auch alle möglichen Entscheidungen und das Verhalten von allen möglichen anderen Nutzer:innen ein. Werbung als ‚personalisiert' zu bezeichnen, ist also nur in dem Sinne adäquat, dass sie für unterschiedliche Personen auch unterschiedlich aussieht. Doch die Bedeutungsdimension des Begriffes der Personalisierung, die eine individuelle Zuschneidung von Werbung auf ein einzigartiges Subjekt suggeriert, muss in Frage gestellt werden.

Den Marketingforschern Darmody und Zwick zufolge erfüllt das Narrativ der Personalisierung von Werbung einen anderen Zweck: Dass Werbung personalisiert ist, suggeriert, dass sie für die Konsument:innen von besonderer Relevanz sei, und daher einen größeren Wert habe

(vgl. 2020, 6). Die Relevanz wird wiederum als Begründung von Werbetreibenden verwendet, um die permanente Überwachung der Konsument:innen mittels Trackingtechnologien zu legitimieren. Denn in dieser Erzählung führt die Überwachung und Kontrolle von Konsument:innen über die dadurch erzeugte Relevanz des Marketings zu empowerten, autonomen und befreiten Subjekten: „relevance allows marketers to believe that in the age of surveillance capitalism, the manipulation of choice contexts and decision-making is the same as consumer empowerment.“ (ebd., 1). Es herrscht also ein Paradoxon: Die Konsument:innen werden überwacht und kontrolliert und sind zugleich frei und autonom. Dieses Paradoxon lösen die Werbetreibenden durch die Idee der Relevanz symbolisch – also nicht tatsächlich – auf, und schaffen sich somit eine moralische Legitimation für das trackingbasierte Marketing, das sie betreiben (vgl. ebd., 2).

8.4. Zwischenfazit IV: Das Datensammeln ist dividuierend

Mithilfe von Cluleys und Browns Ausführungen können wir folgern, dass das Datensammeln im Internet *dividuierend* ist, weil individuelle Nutzer:innen nicht mehr als solche konzipiert werden, sondern vielmehr als eine Ansammlung von Daten, die durch Analyse geteilt und neu zusammengesetzt werden. Das bedeutet, dass sich in dem Moment, in dem Nutzer:innen als teilbare und verrechenbare Daten konzipiert werden, die Verknüpfung zwischen der individuellen Nutzerin und den zahlreichen, über sie generierten Datenpunkten löst.

Weil das Datensammeln im Internet dividuierend ist, bzw. auf Dividuen operiert, verlieren Individuen sämtliche Zugriffspunkte auf den Fluss ihrer eigenen Daten, sobald diese generiert und erhoben worden sind. Das Referenzobjekt dieser Daten sind nicht mehr die Individuen, sondern in Cluster gruppierte Dividuen. Eine individuelle Nutzerin verliert also den eindeutigen Zugriff auf den Fluss ihrer Daten, den es jedoch gemäß der Forderung nach digitaler Mündigkeit braucht, um die individuellen Daten zu kontrollieren. Denn in dieser Forderung werden Individuen durch das neoliberale Regierungswerkzeug der Responsibilisierung dafür verantwortlich gemacht, den Fluss ihrer eigenen Daten zu kontrollieren. Da individuelle Nutzer:innen eine Kontrolle ihrer *eigenen* Daten jedoch gar nicht leisten können, ist die Forderung nach digitaler Mündigkeit in diesem Sinne unangemessen.

Nun könnte eine zweite mögliche Schlussfolgerung bzw. ein Einwand lauten, dass dividuierendes Datensammeln im Digitalen die Forderung nach digitaler Mündigkeit in einem weiteren Sinne unangemessen macht. Denn wenn individuelle Nutzer:innen den Zugriff auf den Fluss ihrer Daten verlieren und es insofern gar nicht mehr *ihre eigenen* Daten sind, sondern ir-

gendwelche Daten, dann stellt sich die Frage, warum Nutzer:innen den Fluss ihrer Daten überhaupt kontrollieren sollten. Eine individuelle Kontrolle des Flusses der eigenen Daten wäre in dieser Annahme unnötig, weil es sich gar nicht um den Fluss der Daten des Individuums handelt.

Die Antwort auf diesen Einwand liegt in dem zweiten Merkmal, welches sich für das Datensammeln im Digitalen aus den Ausführungen zu dem Dividuum ableiten lässt. Mit diesem zweiten Merkmal argumentiere ich jedoch nicht für die Hauptthese dieser Arbeit – dass die Forderung nach digitaler Mündigkeit unangemessen ist, weil eine individuelle Kontrolle des Flusses der eigenen Daten nicht geleistet werden kann – sondern für die Nebenthese. Deshalb ziehe ich im Folgenden das Zwischenfazit I' als Fazit für die Nebenthese, dass Daten schützenswert sind und es deshalb dennoch einer nicht-individualistische Kontrolle bedarf.

8.5. Warum es dennoch einer Kontrolle bedarf – oder Zwischenfazit I': Das Datensammeln ist interdependent

Das zweite Merkmal für das Datensammeln im Digitalen, welches ich aus den Ausführungen zum Dividuum in Kombination mit dem Merkmal der *Prädiktivität* herleite, funktioniert nicht als Argument für die Hauptthese, sondern für die Nebenthese dieser Arbeit. Das Merkmal lautet: Das Datensammeln im Digitalen ist *interdependent*. Mit ‚interdependent' beschreibe ich den Sachverhalt, dass die Daten von unterschiedlichen Nutzer:innen sich gegenseitig beeinflussen. Denn zum einen fließen sie jeweils in die Clusterbildung ein und zum anderen bestimmen sie – im Sinne der prädiktiven Analytik –, welche Informationen über andere Personen vorhersagbar sind. Die Daten stehen somit in einem interdependenten Verhältnis. Die auf diesen interdependenten Daten basierenden, dynamisch berechneten Cluster haben wiederum einen erheblichen Einfluss auf uns als individuelle Nutzer:innen. Denn die Informationen, die Unternehmen über eine Nutzerin ableiten oder vorhersagen können, beeinflussen beispielsweise, welche Werbeanzeigen dieser Nutzerin angezeigt werden oder wie die graphischen Interfaces der Websites gestaltet sind, die die Nutzerin sieht. Der Aktivist Eli Pariser, der bereits im Jahr 2011 unter dem Schlagwort der ‚Filter Bubbles' zu diesem Phänomen geschrieben hat, beschreibt den Zusammenhang zwischen Daten und Interfaces folgendermaßen: „personalization algorithms can cause identity loops, in which what the code knows about you [or people like you, M.L.] constructs your media environment" (Pariser 2011, 233). Das, was wir auf den Interfaces bzw. in der Medienumgebung sehen, basiert also auf unserem Verhalten im Netz und auf den Wünschen und Bedürfnissen, die dieses vermeintlich ausdrückt. Außerdem basiert es auf dem Verhalten und den vermeintlichen Wünschen und Bedürfnissen anderer,

wie in Kapitel 7 zu prädiktiver Analytik deutlich wurde. Zugleich wirkt das, was wir auf den Interfaces sehen, jedoch auch zurück auf uns und formt unsere Wünsche und Bedürfnisse: „your media environment helps to shape your future preferences“ (ebd., 233). Weil die Cluster also einen großen Einfluss auf uns haben, und auf Basis der (in)dividuellen Daten berechnet werden, sind Daten dennoch schützenswert. Das macht es notwendig, den Fluss dieser Daten zu kontrollieren.

Nachdem ich gezeigt habe, dass daraus, dass die Daten dividuiert werden und nicht mehr individuellen Nutzer:innen zugeordnet, nicht folgt, dass sie deshalb gar nicht mehr kontrolliert werden müssten, möchte ich auf einen Sachverhalt aufmerksam machen, der wiederum tatsächlich daraus folgt. Weil das Datensammeln dividuierend ist, verlieren Individuen sämtliche Zugriffspunkte auf den Fluss ihrer eigenen Daten, sobald diese generiert und erhoben worden sind. Das spricht dafür, dass die Kontrolle, die es über diese Daten geben muss, eine nicht-individualistische sein muss. In der akademischen Diskurslandschaft um Privacy-Themen gibt es bereits einige Konzepte, die eine nicht-individualistische, kollektive Dimension in Bezug auf den Schutz von Daten fordern, so z.B. die Group Privacy (vgl. Mittelstadt 2017), Collective Privacy (vgl. Mantelero 2016), oder Inferential Privacy (vgl. Loi und Christen 2020). Auch Rainer Mühlhoff setzt sich dafür ein, mit der sogenannten *prädiktiven Privatheit* ein Schutzgut in den Datenschutz aufzunehmen, welches kollektiven, durch prädiktive Analytik erzeugten Schaden abfängt (vgl. Mühlhoff 2022, 42ff.).

9 Kritische Betrachtung alternativer Lösungsansätze

Seit einigen Jahren werden Cookies sukzessive von Browsern und Plattformen abgebaut. Auch in der Regulierung werden neue Datenschutzkonzepte diskutiert. Ich habe bereits zum Ende von Kapitel 4 hervorgehoben, dass eine eingehende Auseinandersetzung mit Cookies dennoch lohnenswert ist, da das komplexe Werbesystem, das um das Cookie herum entstanden ist, als Vorbild für derzeitige und zukünftige cookielose Märkte fungiert. Das aktuelle Werbesystem zu verstehen, verhilft dazu, auch zukünftige Entwicklungen der Werbeindustrie einzuordnen. Ich möchte daher auf zwei mögliche zukünftige Entwicklungen eingehen und sie im Lichte dieser Arbeit kritisch betrachten. Zum einen werfe ich in Abschnitt 9.1. einen Blick auf das in der Gesetzgebung verhandelte Konzept des Datentreuhänders, welcher ebenfalls im Lichte der neoliberalen Responsibilisierung verstanden werden kann. In Abschnitt 9.2. setze ich mich mit von Google vorgestellten Alternativen zu Cookies auseinander, an de-

nen sich auf den ersten Blick eine vermeintliche Rückentwicklung des Werbesystems erkennen lässt.

9.1. Datentreuhänder

Als Alternative zu Cookie-Bannern werden mit dem Inkrafttreten des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTGSG) Datentreuhänder als „vielversprechendes Konzept, um Datennutzung zu ermöglichen und dabei Datenschutz beizubehalten“ (Blankertz und Specht 2021, 2) diskutiert. Der Soziologe und Rechtswissenschaftler Jörg Pohle befragt das Konzept als „allgemeines Lösungsmodell für den Datenschutzbereich“ (Pohle 2022, 4) jedoch kritisch, da es ihm zufolge in der neoliberalen Logik der Responsibilisierung funktioniert und sie begünstigt. Pohle unterscheidet in seiner Argumentation zwischen den historisch gewachsenen Paradigmen des Rechtsstaatmodell einerseits, in welchem es um den Schutz von Grundrechten geht und unter welches auch Datenschutz fällt, und dem individualistischen Datenkontrollparadigma andererseits, welches den Diskurs um Privacy prägt (vgl. ebd., 8).

In folgendem Exkurs möchte ich die Differenzierung zwischen den Konzepten des Datenschutzes sowie der Privacy, welche häufig miteinander vermengt werden, schärfen. Zunächst sei jedoch festgehalten, dass es sich laut Pohle bei diesen Begriffen[13] um „wesensmäßig umstrittene Konzepte“ handelt, wobei damit „Konzepte bezeichnet [werden], die ihre Bedeutung im Wesentlichen durch die Perspektive derjenigen gewinnen, die sie betrachten.“ (Pohle 2022, 7; auch Mulligan, Koopman, und Doty 2016) Der Philosoph Walter Bryce Gallie führte den Begriff der ‚essentially contested concepts‘ ein, um damit beispielsweise die Konzepte der Kunst, der Demokratie, der sozialen Gerechtigkeit oder der Religionspraxis zu beschreiben (vgl. 1955, 180). Sie zeichnen sich dadurch aus, dass umstritten ist, wie die Begriffe gebraucht werden, dass es unterschiedliche Verwendungen dieser Begriffe gibt und keine davon als die eine prototypische Verwendung verallgemeinerbar ist (vgl. ebd., 168).

Mit diesem Wissen nähern wir uns nun den Begriffen ‚Privacy‘ und ‚Datenschutz‘. Für den Datenschutz gilt, dass „[d]as Problem, das [er] zu lösen sucht, [...] als technikvermitteltes gesellschaftliches Machtproblem verstanden [wird]“ (Pohle 2022, 10). Das Machtproblem entfaltet sich dabei zwischen Organisationen auf der einen Seite, und Personen auf der anderen Seite:

> Datenschutz bezeichnet insofern all diejenigen Vorkehrungen, die auf Seiten der Organisationen zu treffen sind, um die Machtasymmetrie zwischen Organisationen und Personen so zu formen, dass

13 Und bei vielen anderen in frequentistischer Nähe dazu: „von (Computer, Information oder Data) Privacy, Privatheit, Privatsphäre, digitaler Intimsphäre oder informationeller Selbstbestimmung über Surveillance oder Dataveillance bis hin zu Datenschutz.“ (Pohle 2021, 7)

> Personen vor der Willkür der Organisationen geschützt sind oder sich schützen können. (Rost 2017, 64)

Datenschutz schützt Menschen also vor Grundrechtseingriffen infolge von Datenverarbeitung. Die Grundrechtseingriffe können sowohl von verarbeitenden Organisationen als auch vom staatlicher Verwaltung ausgehen (vgl. Pohle 2022, 10).

Privacy ist wiederum eine Realisierungsform des individualistischen Datenflusskontrollparadigmas (vgl. Pohle 2022, 8f.), welche sich als Kontrolle und somit Schutz des eigenen Informations- bzw. Datenflusses manifestiert (vgl. ebd., 9). Als Schutzmechanismus wird vor allem „‚Selbstdatenschutz' durch informationstechnische Systeme [propagiert, M.L.], die von den Betroffenen kontrolliert werden und es ihnen ermöglichen, für ihren eigenen Schutz zu sorgen" (ebd., 9).

Diesen ‚Selbstdatenschutz' sollen Datentreuhänder nun im Auftrag von Individuen übernehmen. Datentreuhänder fungieren in ihrer neutralen Erzählung „als unabhängige Vermittler zwischen Datengebern und Datennutzern [...]. Sie sichern Datenzugänge, organisieren Zugriffe und pseudonymisieren Daten" (Bundesdruckerei GmbH 2022). In diesem Deutungsrahmen steht der Datentreuhänder zwischen den Bedürfnissen von Datensubjekt[14] und Datenverarbeitern und erfüllt die Anliegen beider Seiten gleichermaßen: Für das Datensubjekt gewährt er Datenschutz sowie den Schutz der Privatsphäre, und für die Datenverarbeiter organisiert er den Zugang zu bzw. Zugriff auf die Daten der Datensubjekte. Dass der Datentreuhänder als intermediärer Akteur durch den Staat responsibilisiert wird, deckt sich auch mit den Erkenntnissen des Soziologen Mike Zajko (s. Abschnitt 3.2.), denen zufolge sich Intermediäre in einer für eine Responsibilisierung besonders geeigneten Position befinden.

Doch Pohle zufolge ist „[d]as wichtigste Ziel, das mit Datentreuhändern verfolgt werden soll, [...] eindeutig das des ‚erleichterten Datenteilens'" (2022, 17). Also ist das Anliegen der datenverarbeitenden Unternehmen zentral. Nebensächlich ist hingegen der vermeintliche Schutz der Datensubjekte durch den Rechtsmechanismus der individuellen Einwilligung, einer Operationalisierung des individualistischen Datenflusskontrollparadigmas. Ich bezeichne den Schutz als „vermeintlich", da die Wirksamkeit der individuellen Einwilligung dem Richter Malte Engeler zufolge, den Pohle zitiert, überbewertet wird und „in der Praxis (fast) keine Schutzwirkung auf die Grundrechte hat" (ebd., 17). Pohle argumentiert also, dass Datentreuhänder keineswegs die Grundrechte im Sinne eines gesellschaftspolitischen Datenschutz gemäß der Europäischen Datenschutzgrundverordnung (Art. 1 Abs. 1 und 2 DSGVO) schützen

14 „Datensubjekt" wird hier im Sinne der DSGVO verstanden und bezeichnet diejenige Person, über die personenbezogene Daten vorliegen.

(können), sondern vielmehr das individualistische Datenkontrollparadigma befeuern (vgl. ebd., 4):

> [Datentreuhändermodelle] zielen nicht auf eine gesellschaftliche Lösung eines gesellschaftlichen Problems, sondern auf eine individuelle Lösung für ein als individuell verstandenes Problem. Sie reproduzieren das Problem [des Datenschutzes, M.L.] damit als individuelles, selbst im Scheitern – dann haben sich die Betroffenen eben schlicht den falschen Datentreuhänder ausgesucht, um ihre Interessen und Präferenzen zu vertreten. (ebd., 18)

Durch einen Datentreuhänder würden sich eine Vielzahl der Eigenschaften des Digitalen Datensammelns, die digitale Mündigkeit für Individuen verunmöglichen, von deren Schultern auf die des Datentreuhänders verlagern, dessen Aufgabe es wäre, sich mit diesen Eigenschaften wie z.B. der *Komplexität* der Trackinginfrastruktur auseinanderzusetzen. Jedoch geschieht hier strukturell das gleiche wie bei der Responsibilisierung der Individuen, nur auf einer ‚höheren' Ebene bei einem intermediären Akteur. Zum einen steht also infrage, ob wenige Datentreuhänder wirklich zu leisten in der Lage wären waas Individuen nicht möglich ist. Zum anderen werden die Eigenschaften, die bedingen, dass es eine nicht-individualistische Art von Datenflusskontrolle geben muss – beispielsweise, dass das Datensammeln im Digitalen *interdependent* ist – in dem Modell des Datentreuhänders außer Acht gelassen. Dadurch ist der Datentreuhänder als vermittelnde Instanz zwischen Nutzer:innen und Plattformen kein zufriedenstellender Lösungsansatz, da es den Schutz der Daten von Individuen weiterhin nur im Rahmen des individualistischen Datenflusskontrollparadigmas begreift.

9.2. Googles Privacy Sandbox

Google kündigte im Jahr 2019 an, Drittanbietercookies im Chrome Browser abzuschaffen und es somit anderen Browserbetreibern wie Apple (Safari) oder dem Tor-Browser gleichzutun. Jedoch soll die Abschaffung nicht ohne einen unmittelbar einsetzbaren Nachfolger geschehen. Denn, so argumentiert Google, wenn es keine funktionale Alternative zu Trackingcookies gäbe, dann würden Werbetreibende noch invasivere Methoden anwenden, um Nutzer:innen zu tracken (vgl. Bohn 2021). Um einen Ersatz zu entwickeln, hat Google die Privacy Sandbox gestartet; eine Initiative, mit der das Unternehmen zwei Dinge gleichzeitig zu ermöglichen behauptet, die einander bisher ausschließen: Die Privacy Sandbox soll den Nutzer:innen zum einen Datenschutz bieten und dabei gleichzeitig den Werbemarkt, wie er bisher funktioniert, nicht einschränken (vgl. Chavez 2022).

Im Januar 2021 hat Google im Rahmen der Privacy Sandbox das Konzept des Federated Learning of Cohorts (FLoC) vorgestellt, welches im Chrome Browser implementiert werden soll-

te. Das Konzept wurde zwar bereits überworfen, sah aber vor, anstatt die komplette Browserhistorie mittels Cookies nachzuverfolgen und an einen Server zu senden, die Browserhistorie der Nutzerin auf ihrem Rechner zu belassen. Dort sollte die Historie von dem Browser lokal verarbeitet werden, indem er ungefähr alle sieben Tage mithilfe eines Algorithmus die Zugehörigkeit der Nutzerin zu einer von 34.000 Interessens-Kohorten berechnet hätte. In einer Kohorte hätte sich eine Mindestanzahl von mehreren Tausend Nutzer:innen mit ähnlicher Browserhistorie befunden. Anstatt einer eindeutigen ID wie bei Cookies hätte sich aus der Berechnung ein einziges Kohortenlabel ergeben, welches im Anschluss von dem Browser an die aufrufende Website übergeben worden wäre. Die Bedeutung, die das Label getragen hätte, bzw. das, was eine jeweilige Kohorte auszeichnen sollte, wollte Google hingegen nicht festlegen, sondern die Festlegung den Werbetreibenden überlassen.

Das Modell des Federated Learning of Cohorts stieß auf vehemente Kritik. Es wurde unter anderem bemängelt, dass das Verhalten der Nutzer:innen über alle Seiten hinweg offengelegt würde: „Users begin every interaction with a confession: here's what I've been up to this week, please treat me accordingly." (Cyphers 2021) Das Label, das dafür verwendet wäre, wäre auf den ersten Blick undurchschaubaren gewesen, jedoch für die Werbetreibenden von großer Bedeutung. Im Falle von Drittanbietercookies konnten Nutzer:innen für jede Seite theoretisch noch entscheiden, welche Cookies zugelassen würden, oder Cookies ganz löschen, bei FLoC wäre das nicht gegangen. Darüber hinaus würde das Kohortenlabel ein weiteres Merkmal sein, das in die Technologie des Fingerprinting einfließen würde (vgl. Kap. 6.2).

Vermutlich weniger wegen der Kritik, sondern vielmehr weil die Testläufe von FLoC nicht erfolgreich waren (vgl. Kleinz 2022), hat Google die Arbeit an dem Service eingestellt. Im Januar 2022 wurde der Nachfolger, die Topics API, vorgestellt. In der Topics API finden ebenfalls Berechnung im nutzereigenen Browser statt. Allerdings wird hier nicht die Zugehörigkeit zu einer Kohorte maschinell berechnet, sondern die fünf ‚top interests' der vergangenen Woche wie ‚Reisen' oder ‚Sport'. Es soll eine Liste zwischen mehreren Hundert und mehreren Tausend solcher Themen geben, die von Mitarbeiter:innen von Google sowie dem Wirtschaftsverband des Interactive Advertising Bureaus (IAB) kuratiert wurden. Im Gegensatz zu den in FLoC maschinell erzeugten Clustern sollen die Themen ihre externe Bedeutung im Titel tragen. Für die Vertestung existiert eine vorläufige Taxonomie mit insgesamt 349 Themen wie beispielsweise „/Sports/Martial Arts", „/People & Society/Family & Relationships/Parenting/Adoption" oder „/Travel & Transportation/Tourist Destinations/Theme Parks" (Karlin

[2022b] 2023). In der Taxonomie sollen keine sensiblen Kategorien, wie Geschlecht, sexuelle Orientierung oder *race*, abgebildet werden.

Um die Themen von Websites zu labeln sollen in einem ersten Durchlauf einer bestimmten Anzahl von Websites per Hand Themen zugewiesen werden. Diese von Menschen durchgeführten Annotationen dienen daraufhin als Trainingsdaten für ein Machine Learning Modell, welches im weiteren Verlauf die Themenzuweisung automatisiert (vgl. Titone 2022). Für die Vergabe von Themen bezieht sich die Topics API dabei nur auf die aufrufende Domain oder Subdomain – z.B. `https://www.website.de/` – und nicht auf die individuelle Seite, wie z.B. `https://www.website.de/home/subpage`.

In einem Zyklus von drei Wochen werden in jeder Woche die jeweiligen fünf Top-Themen der Woche gesammelt. Nach drei Wochen werden die Themen der ältesten Woche wieder gelöscht. Die Themen sollen überdies hinaus auch von den Nutzer:innen eingesehen und gegebenenfalls gelöscht werden können. Beim Aufruf einer Website werden der Website bis zu drei der insgesamt 15 bzw. 18 Themen übergeben, und zwar eines aus der jeweiligen Liste von fünf Themen pro Woche der letzten drei Wochen (vgl. Goel 2022). In jeder Woche wird außerdem ein randomisiertes sechstes Thema generiert, das in 5% der Fälle übergeben werden soll. Welches Thema jeweils genau aus den fünf (bzw. sechs) Themen einer Woche ausgewählt wird, wird durch eine Zufallsmethode ermittelt, was dafür sorgen soll, dass zwei unterschiedliche Websites nur mit einer Wahrscheinlichkeit von 33% unterschiedliche Themen erhalten. So erhält Website *a.com* beispielsweise die Themen ‚Sport' für Woche 1, ‚Musik' für Woche 2 und ‚Essen' für Woche 3. Website *b.com* erhält die Themen ‚Reisen' für Woche 1, ‚Politik' für Woche 2 und ‚Essen' für Woche 3. So soll das Risiko von Fingerprinting und websiteübergreifendem Tracking vermindern werden (vgl. Guy 2022). Außerdem erhält wiederum jede Werbeplattform – beispielsweise WP_1 und WP_2 –, die auf einer Website *a.com* eingebunden ist, das gleiche Thema ‚Sport'. Wenn WP_1 jedoch auch auf Website *b.com* läuft, erhält WP_1 auch das Thema ‚Reisen' (vgl. Titone 2022). In bestimmten Fällen erhalten die Werbeplattformen auch eine leere Liste, wenn die Nutzer:in beispielsweise zum ersten Mal surft, gerade die alten Themen sowie Browserhistorie gelöscht hat, sich im Inkognito-Modus befindet oder mit einem Kinderaccount den Browser verwendet.

Eine Werbeplattform wie WP_1 – oder Google Ads – erfährt nur dann von einem bestimmten Thema einer Nutzerin, wie beispielsweise ‚Sport', wenn die Werbeplattform auf irgendeiner Website eingebunden ist, die dem Thema ‚Sport' zugeordnet ist und von der Nutzerin in den letzten drei Wochen besucht wurde (vgl. Karlin [2022a] 2023). Sie muss allerdings eben *nur*

auf einer Website mit dem Thema ‚Sport' laufen, um über eine Nutzerin beispielsweise der Website *a.com* erfahren zu dürfen, dass eines ihrer Themen ‚Sport' ist. Bei Drittanbietercookies muss die Werbeplattform WP_1 noch eine direkte oder indirekte Geschäftsbeziehung mit der Website *a.com* pflegen, um dort Cookies setzen zu dürfen, um abzuleiten, dass die Nutzerin sich für Sport interessiert. (Vgl. Titone 2022).

Zwar erlaubt Topics wesentlich eingeschränkteres Targeting als Drittanbietercookies, steht aber dennoch in der Kritik von Akteur:innen der Internetgemeinschaft. Beispielsweise seitens des World Wide Web Consortiums (W3C), einer Organisation, die die Techniken, Protokolle und Methoden des Internets standardisiert; Mozilla, die den Firefox Webbrowser entwickeln; oder WebKit, eine von Apple weiterentwickelte Software zum Rendern von HTML-Seiten. So schlussfolgert Mozilla in einer Prüfung der Topics API, dass das durch Cookies eingeschränktere Tracking zwar weniger aussagekräftige Informationen an die Unternehmen liefert, jedoch die die Privatsphäre der Nutzer:innen nicht notwendigerweise schützt:

> Fundamentally, we just can't see a way to make this work from a privacy standpoint. Though the information the API provides is small, our belief is that this is more likely to reduce the usefulness of the information for advertisers than it provides meaningful protection for privacy. (Thomson 2023)

Der W3C kritisiert unter anderem, dass die Nutzer:innen wie bei FLoC auch bei Topics nicht entscheiden können, welche Informationen über sie – bzw. welche ihrer Themen – in welchem Kontext an welche weiteren Akteur:innen gelangen (vgl. Guy 2022). Das Generieren und Teilen von websiteübergreifenden Daten sowie die websiteübergreifende Gestaltung von Werbung wird somit zum Standard (vgl. Kesteren 2022). Da der Browser diejenige Instanz ist, die diese Informationen im Hintergrund mit anderen Akteur:innen teilt, würde dies das Vertrauen der Nutzer:innen in den Browser untergraben, welcher als ‚user agent' hauptsächlich die Aufgabe hat, den Nutzer:innen zu ermöglichen, Webinhalte abzurufen und darzustellen (vgl. Kesteren 2022; User Agent Working Group W3C 2011; Guy 2022).

Wenngleich die im Idealfall drei an eine Werbeplattform kommunizierten Themen im Einzelnen wenig Informationen zu beinhalten scheinen, so ist die Kombination der drei Themen bereits aussagekräftiger. Wird diese Kombination wiederum mit anderen Daten verknüpft, lassen sich weitere Informationen ableiten. Das hat die Werbeplattform Weborama herausgefunden, die in einer kleinen App die Funktionsweise der Google Topics API nachempfunden hat. Weborama hat dabei die jeweils drei Themen in ihre gesamte Datenbank an Nutzungshistorien eingeordnet und konnte Korrelationen mit anderen Informationen finden, die über die drei Themen hinausgehen (vgl. Tastevin 2022). Das bedeutet, dass Websites, die bereits

Informationen über eine Nutzerin haben – insbesondere Suchmaschinen und Soziale Netzwerke – sowohl ihren Wissensbestand durch die drei Themen anreichern können als auch den Informationsgehalt der Themen durch ihren Wissensbestand ergänzen können. Denn mithilfe von Machine Learning Methoden – wie beispielsweise der prädiktiven Analytik – können durch eine Verknüpfung der drei Themen mit einer großen Wissensbasis Informationen abgeleitet werden, die in ihrer Spezifizität und Sensibilität über die 349 Kategorien hinaus gehen werden (vgl. Kesteren 2022).

Überdies werden Websites mittels der Topics API im Laufe der Zeit in der Lage sein, wenn sie die Themen einem Nutzer:innenprofil zuordnen können. In diesem Kontext wird kritisiert, dass die 5% Quote, mit der ein randomisiertes Thema versendet wird, nicht ausreichend Schutz davor bietet, dass Websites feststellen können, ob ein Thema nutzer:innenspezifisch ist oder randomisiert (vgl. Thomson 2023). Das W3C schlussfolgert daraus: „the proposed API appears to maintain the status quo of inappropriate surveillence on the web, and we do not want to see it proceed further.“ (Guy 2022)

Der Fakt, dass eine Werbeplattform nur dann von einem Thema einer Nutzerin erfährt, wenn die Plattform innerhalb der letzten drei Wochen auf einer Website mit dem gleichen Thema für die gleiche Nutzerin bereits einmal die Topics API aufgerufen hat (z.B. eine Website zum Thema ‚Sport‘), verschafft überdies hinaus etablierten Werbeplattformen, die bereits eine große Marktmacht haben, einen weiteren Vorteil. Denn ihre Tools und Codeschnipsel sind bereits in vielen Websites eingebunden, woraus mit großer Wahrscheinlichkeit folgt, dass eine weitverbreitete Werbeplattform bereits in einer anderen Website eingebunden ist, die das Thema ‚Sport‘ betrifft und von der Nutzerin in den letzten drei Wochen besucht wurde (vgl. Thomson 2023; Kesteren 2022).

Auf weitere Kritik stößt die Taxonomie bzw. die Kategorisierung der Themen, die der Topics API zugrunde liegen. Einerseits wird kritisiert, dass eine Kategorisierung der Themen in ‚sensibel‘ und ‚nicht-sensibel‘ nicht angemessen ist. Denn es handelt sich bei den Adjektiven nicht um kontradiktorische Antonyme – wenn das eine nicht gegeben ist, muss notwendigerweise das andere gelten –, sondern um konträre Antonyme, was bedeutet, dass es graduelle Abstufungen zwischen ‚sensibel‘ und ‚nicht-sensibel‘ gibt. Der Grad der Sensibilität verändert sich je nach aktuellem Kontext und hängt von dem betreffenden Individuum in seiner situativen sozialen Einbettung ab. Eine endgültige Aufteilung in sensible und nicht-sensible Themen ist somit nicht möglich (vgl. Kesteren 2022; Guy 2022). Andererseits wird an der Taxonomie kritisiert, dass sie – trotzdem sie nur vorläufig und nur zu Testzwecken eingesetzt

wird – bereits ein Bias gegenüber westlichen Lebensstilen aufweist. Beispielsweise wird die Bezeichnung „World Music“ als Begriff für nicht-westliche Musik verwendet (vgl. Kesteren 2022). Die Taxonomie sollte jedoch gewährleisten, alle Browsernutzer:innen der Weltbevölkerung abzubilden, ohne dabei zu normieren. Überdies hinaus ist bisher unklar, wie genau die Zuweisung von Themen zu bestimmten Websites geschehen soll. Infrage steht beispielsweise, ob die Websites diese Aufgabe erledigen, oder wie der Zugang zur und die Wartung der Taxonomie geregelt werden. Es könnte eine einzige globale Liste geben, deren Zugang von Google organisiert wird, oder unterschiedliche Browser könnten unterschiedlich verfahren (vgl. Kesteren 2022).

Auch FloC und die Topic API von Google lassen sich mithilfe von Erkenntnissen dieser Arbeit betrachten. Während der Datentreuhänder vor allem im Lichte der neoliberalen Responsibilisierung (s. Kapitel 3) diskutiert wurde, lassen sich Googles Federated Learning of Cohorts und die Topic API mithilfe der Ausführungen zu Verbrauchermodellen und dem Dividuum (s. Kapitel 8) begreifen.

Zum einen weist das Vorgehen von FLoC Ähnlichkeiten zu dem von Cluley und Brown diskutierten Divisionsprozess auf. Es lässt sich feststellen, dass Googles FLoC identisch zur Berechnung der Cluster im Divisionsprozess funktioniert hätte. In beiden Fällen werden Individuen zunächst als Datenpunkte konzipiert, welche daraufhin voneinander dividiert werden. Lediglich auf Basis des internen Verhältnis dieser – ggfs. google-eigenen – Datenpunkte werden die resultierenden Dividuen in fluide Cluster gruppiert – oder eben in Kohorten eingeteilt. Weder die Cluster des Divisionsprozesses noch die FLoC-Kohorten tragen dabei eine Bedeutung, die ihnen durch externe Referenzpunkte verliehen worden wäre, sondern die Bedeutung wird den Clustern bzw. Kohorten nachträglich zugeschrieben. Darüber hinaus sind Cluster und FLoC-Kohorten fluide. Während sich die Cluster mit jedem neuen Datenpunkt verändern, hätten sich auch die Kohorten, die gebildet worden wären, mit jedem neuen Datenpunkt verändert. Zwar wäre die Anzahl an Kohorten auf 34.000 beschränkt gewesen, aber durch welche Größe und Zusammenstellung sich die Kohorten ausgezeichnet hätten, wäre stets neu berechnet worden. Ein Unterschied zwischen den zwei Modellen liegt darin, dass das Kohortenlabel die aggregierte Browserhistorie enthalten hätte, anstatt wie im Falle der Cluster alle Datenpunkte der einzelnen durch Cookies generierten Verhaltensinformationen über die Nutzer:innen. Dennoch lässt sich schlussfolgern, dass FLoC das Vorgehen, das bereits im Jahr 2015 – dem Erscheinungsjahr des Textes von Cluley und Brown – in der Werbeindustrie präsent war, reproduziert hätte.

Der Nachfolger von FLoC, die Topics API, wirkt hingegen wie ein Schritt zurück in Richtung des traditionellen Werbesystems (s. Abschnitt 5.2.) thematisiert wurde. Denn die Topics API arbeitet ebenfalls mit externen, referenzierbaren Kategorien, wie es im traditionellen Werbesystem der Fall war. Diese heißen in der Topics API ‚Themen'. Die Themen klassifizieren jedoch auf den ersten Blick nicht – wie im traditionellen Werbesystem – das Zielpublikum, sondern das Zielprodukt bzw. die Inhalte der Website. Sie basieren auch nicht in erster Linie auf demographischen und zum Teil sensiblen Merkmalen wie Alter oder Geschlecht, wie es bei den Kategorien des traditionellen Werbesystems der Fall war. Auf einen zweiten Blick wird jedoch auch hier deutlich, dass die Klassifikation des Zielprodukts eng mit der Klassifikation des Zielpublikums verknüpft ist bzw. sich durch die große Wissensbasis der Unternehmen dennoch Annahmen über das Zielpublikum treffen lassen. Es bleibt allerdings in Zukunft zu untersuchen, ob und inwiefern das auf der Topics API basierende Werbesystem tatsächlich wieder mehr von den Eigenschaften aufweist, die Cluley und Brown mit dem traditionellen Werbesystem in Verbindung bringen und welche der Eigenschaften dem heute vorherrschenden programmatischen Werbesystem entsprechen.

10 Fazit

Ich habe mich in dieser Arbeit mit der politischen Forderung nach digitaler Mündigkeit bzw. nach mündigen Individuen kritisch auseinandergesetzt. Mein Fokus lag dabei auf der Teilforderung, dass es von Mündigkeit zeugt, den Fluss der eigenen Daten zu kontrollieren, welche ich in Kapitel 2 erarbeitet habe. Diese Teilforderung setzt voraus, den Fluss der eigenen Daten tatsächlich kontrollieren zu können – eine Voraussetzung, deren Realisierbarkeit ich in dieser Arbeit überprüft habe. Meine Hauptthese ist, dass es Individuen nicht möglich ist, den Fluss ihrer eigenen Daten zu kontrollieren. Dass sie dennoch dafür verantwortlich gemacht werden, muss im Kontext der neoliberalen Responsibilisierung verstanden werden; einem Prozess, in dem Individuen oder andere nicht-staatliche Akteure für Dinge verantwortlich gemacht werden, für die Verantwortung zu übernehmen sie nicht in der Lage sind (vgl. Kapitel 3).

In Kapitel 4 habe ich mich in einem Exkurs mit dem ‚Frontend', also mit der Gestaltung von graphischen User Interfaces, befasst, mithilfe dessen Menschen ihre Daten kontrollieren können sollen. Diese Interfaces müssen im Kontext von Nudging verstanden werden. Nudging ist eine Regierungstechnologie, welche Menschen auf unmerkliche Art und Weise beeinflusst, indem sie sich verhaltenswissenschaftliche Erkenntnisse zunutze macht. Nudging realisiert sich neben zahlreichen anderen Gesellschaftsbereichen auch im Internet. Dort tritt es vor allem als

Dark Patterns im Kontext von Entscheidungen auf, die Nutzer:innen mit Bezug auf die über sie generierten Daten treffen sollen. Die Dark Patterns ‚nudgen' die Nutzer:innen in eine Datenfreigiebigkeit. Während es durch die Interfacegestaltung im Frontend also bereits erschwert wird, Kontrolle über den Fluss der eigenen Daten auszuüben, habe ich ab Kapitel 5 den Blick auf das ‚Backend' justiert und überprüft, ob das dahinter- und zugrundeliegende System eine Kontrolle des Flusses der eigenen Daten zulässt.

Dafür habe ich mich in Kapitel 5 zunächst mit der Entwicklungsgeschichte von Cookies auseinandergesetzt, und nachvollzogen, inwiefern die Werbeindustrie sich ihrer angeeignet hat. Diese Erarbeitung hilft, zu verstehen, was für ein System es ist, in dem wir als Nutzer:innen dazu aufgefordert werden, unsere Daten zu kontrollieren. Die Entwicklungsgeschichte der Cookies kulminierte in der hochkomplexen, cookifizierten Marktinfrastruktur, wie wir sie heute kennen. Als Analogie zu dieser Marktinfrastruktur habe ich einen Raum voller Überwachungskameras beschrieben, mithilfe dessen ich zeigen konnte, dass das Datensammeln im Digitalen *kontinuierlich*, *komplex* und *unsichtbar* ist, was Eigenschaften sind, die dazu beitragen, dass eine individuelle Datenflusskontrolle unmöglich ist.

In Kapitel 6 habe ich einen weiteren Winkel verwendet und andere Trackingtechnologien untersucht, wie unter anderem das Fingerprinting oder das Tracking auf dem Smartphone und IoT-Geräten. Daraus konnte ich ableiten, dass das Datensammeln im Internet außerdem *überall* und *unausweichlich* ist, die ebenfalls zu einer Verunmöglichung individueller Datenflusskontrolle beitragen.

In Kapitel 7 habe ich das statistische Verfahren der prädiktiven Analytik nachvollzogen, welches von Unternehmen sowohl im Werbekontext als auch in anderen Bereichen eingesetzt wird, um auf Basis von statistischen Wahrscheinlichkeiten Vorhersagen über Menschen zu treffen, die in automatisierte Entscheidungsprozesse einfließen. In dem Zwischenfazit dieses Kapitels habe ich die Ebene der Analogie verlassen und geschlussfolgert, dass das Datensammeln *prädiktiv* ist, was bedeutet, dass Informationen über eine beliebige Person aus den Daten anderer abgeleitet werden können, welche diese Person gar nicht preisgegeben hat. Auch diese Eigenschaft trägt dazu bei, dass eine individuelle Datenflusskontrolle unmöglich ist.

In dem folgenden Kapitel 8 habe ich zunächst den Fokus auf das Individuum gerichtet und erarbeitet, welche Annahmen im Werbesystem über das Wesen von Verbraucher:innen getroffen werden und wie diese sich durch das Aufkommen von Trackingtechnologien verändert haben. Ich habe festgestellt, dass Verbraucher:innen nicht mehr als Individuen konzipiert werden, sondern als eine Menge an Daten, die von- und durcheinander teilbar ist, was der Eigenschaft

des Datensammelns im Digitalen entspricht, *dividuierend* zu sein. Dadurch, dass es dividuierend ist, verlieren Individuen den Zugriff auf ihre Daten, was es ihnen ebenfalls verunmöglicht, Kontrolle über ihre vermeintlich eigenen Daten auszuüben. Die vereinten sechs Eigenschaften des digitalen Datensammelns, die ich in den bisherigen Kapiteln herausgearbeitet habe, verunmöglichen die individuelle Kontrolle des Flusses der eigenen Daten. Dadurch wird die Forderung nach digitaler Mündigkeit unangemessen und es wird deutlich, dass digitale Mündigkeit zu fordern der neoliberalen Regierungslogik der Responsibilisierung entspricht. Mit dem zweiten Merkmal, das ich aus diesem Kapitel abgeleitet habe – dass das Datensammeln im Digitalen *interdependent* ist –, habe ich für die Nebenthese dieser Arbeit argumentiert und gezeigt, dass Daten schützenswert sind und es also dennoch eine nicht-individualistische Kontrolle des Flusses der Daten braucht.

In Kapitel 9 habe ich einen kritischen Blick auf zwei unterschiedliche Ansätze geworfen, die zugleich den Nutzen von Daten zum einen und den Schutz von Daten zum anderen balancieren sollen. So werden im Datenschutzbereich Datentreuhänder als Alternative dazu diskutiert, dass Individuen ihre Privatsphäreeinstellungen selbst vornehmen. Auch hier ließen sich Züge der neoliberalen Responsibilisierung identifizieren, was Datentreuhänder als Lösungsansatz infragestellt. Als technologische Alternative zu Cookies, die Tracking und gleichzeitig den Schutz der Nutzer:innen ermöglichen soll, wurde Googles Privacy Sandbox Initiative vorgestellt. Während deren erster, inzwischen eingestellter Aufschlag – das Federated Learning of Cohorts – eine eindeutig dividuierende Qualität besaß, habe ich festgestellt, dass das Nachfolgeprojekt Google Topics strukturelle Ähnlichkeiten zu dem traditionellen Werbesystem aufweist.

Im Wesentlichen habe in dieser Arbeit gezeigt, dass die Forderung nach digitaler Mündigkeit kritisch hinterfragt werden muss, da es aufgrund zahlreicher Merkmale des digitalen Datensammelns für Individuen *nicht* möglich ist, den Fluss ihrer eigenen Daten zu kontrollieren. Dass sie dennoch dafür verantwortlich gemacht werden, entspricht der neoliberalen Regierungsmodalität der Responsibilisierung. Ich habe außerdem argumentiert, dass es dennoch einer nicht-individualistischen Kontrolle des Flusses der Daten bedarf.

11 Ausblick

Durch meine Arbeit ergeben sich für mich und für die Forschungsgemeinschaft, die sich mit Themen des Internets und der Gesellschaft auseinandersetzt, fünf interessante und lohnenswerte Anknüpfungspunkte für zukünftige Untersuchungen. Erstens liegt es nahe, eine umfas-

sende Theorie digitaler Mündigkeit zu entwickeln, die, beispielsweise, über die Operationalisierung von digitaler Mündigkeit als fünf Literacies bzw. Kompetenzen hinausgeht (vgl. Beck u.a. 2018). Eine Theorie der digitalen Mündigkeit sollte unter anderen folgende Fragen beantworten können: Was bedeutet ‚digitale Mündigkeit'? Welche Eigenschaften gelten als ‚digital mündig'? Welche Bedingungen müssen für digitale Mündigkeit gegeben sein? Wie wird digitale Mündigkeit von dem Konzept einer ‚analogen' Mündigkeit abgegrenzt? Im Rahmen einer solchen Theorieentwicklung ließe sich untersuchen, inwiefern andere Bedeutungsdimensionen digitaler Mündigkeit – wie beispielsweise, dass digital mündig zu sein bedeutet, Fake News zu erkennen – überhaupt einlösbar sind. Denn in meiner Arbeit argumentiere ich nicht notwendigerweise dafür, dass die Forderung nach digitaler Mündigkeit *im Allgemeinen* unangemessen ist, schließe es jedoch auch nicht aus. Ich gebe vielmehr den Anstoß, auch andere Bedeutungsdimensionen der Forderung hinsichtlich ihrer Einlösbarkeit und ihres Zusammenspiels mit neoliberalen Regierungsdynamiken zu hinterfragen.

Ein zweiter Anknüpfungspunkt für weitere Forschung liegt darin, den Blick auf andere, zur digitalen Mündigkeit ähnliche Bezeichner auszuweiten, in denen die Forderung nach der Kompetenz, den Fluss der eigenen Daten zu kontrollieren, ebenfalls auftaucht. So wird in einem Bericht des Digital Autonomy Hubs folgende Diagnose aufgestellt:

> „Digitale Selbstbestimmung", „digitale Autonomie" oder „digitale Mündigkeit" – aktuell vollzieht sich in digitalpolitischen Diskussionen ein Tauziehen um verschiedene Begriffe, die beschreiben, wie Menschen in digitalisierten Gesellschaften ihr Recht auf Selbstbestimmung ausüben. Menschen sollen beispielsweise in die Lage versetzt werden, selbstbestimmt zu entscheiden, welche personenbezogenen Daten sie für welche Dienste einsetzen oder der Allgemeinheit zur Verfügung stellen. (Mollen und Haas 2021, 3)

Verwandte Rufe nach digitaler Autonomie, digitaler Selbstbestimmung oder digitaler Souveränität wären insofern möglicherweise ebenfalls von meiner Argumentation betroffen, dass auch sie das Individuum empowern wollen und dabei strukturelle Faktoren außer Acht lassen. Wenngleich ich mich in dieser Arbeit auf den Begriff der digitalen Mündigkeit beziehe, schließe ich nicht aus, dass die Ausführungen auch auf andere Bezeichner angewendet werden können.

Drittens ließe sich der Zusammenhang zwischen dem programmatischen Werbesystem und Persönlichkeitsstrukturen erforschen. In Abschnitt 8.2. habe ich den Philosophen James Brusseau angeführt, der von einer Fragmentierung der Identität im Zusammenhang mit der dividuierenden Clusterbildung durch Plattformen und Internetdienstleister spricht (Brusseau 2020, 14f.). Zum einen könnte die Untersuchung mithilfe von empirischer Subjektivierungsforschung geschehen. Zum anderen könnte überprüft werden, inwiefern sich empirisch belegte

psychologische Aussagen über den Zusammenhang von Werbesystem und Persönlichkeitsstruktur treffen lassen.

Der vierte Forschungsgegenstand hat sich in dem vorhergehenden Kapitel 9 eröffnet. Denn ich halte es für lohnenswert, die Projekte der Google Privacy Sandbox Initiative kritisch zu hinterfragen und mithilfe von Literatur über die Entwicklung des Werbesystems und Verbrauchermodellen vertiefend einzuordnen.

Als fünften Punkt halte ich eine vergleichende Untersuchung der Regierungsmodalitäten der Responsibilisierung und und des Nudging für lohnenswert. Während es sich bei der Responsibilisierung um eine neoliberale Regierungsmodalität handelt, wird das Nudging zwar häufig als post-neoliberale Regierungstechnologie eingeordnet, doch dem Soziologen Nicholas Gane zufolge gilt: „the nudge agenda is less a form of 'post-neoliberalism' than a new, hybrid form of neoliberalism“ (vgl. 2021, 139). Diese beiden Modalitäten – die Responsibilisierung zum einen, die als die Forderung nach digitaler Mündigkeit artikuliert wird, und des Nudgings zum anderen, das als in Form von Dark Patterns korrumpiert betrachtet wird – treffen im Internet aufeinander. Möglicherweise entstehen dabei Interferenzen und folgende Fragestellungen ergeben sich: Funktioniert Responsibilisierung überhaupt im Angesicht von Nudging bzw. Dark Patterns? In welchem Verhältnis stehen neoliberale Responsibilisierung und die neuen, hybriden Formen des Nudging? Welche Subjektivierungsformen sind den Modalitäten inhärent? Welche Annahmen der Responsibilisierung finden sich im Nudging wieder, und wurden sie weiterentwickelt? Was bedeutet das für die Machtverhältnisse zwischen Staat, Plattformen und Menschen? Im Kontext dieser Untersuchung liegt es auch nahe, das Verhältnis von Responsibilisierung und Plattformen dahingehend zu befragen, ob der Staat seine Macht ausweitet, wenn er Plattformen responsibilisiert, oder ob er nicht gleichzeitig oder vor allem versucht, die Macht von Plattformen zu beschränken.

Achatz, Johannes, und Stefan Selke. 2022. „Der Realität auf die Sprünge helfen. Zum Kontingenzdilemma im Kontext von popularisierten Praktiken digitaler Selbstvermessung von Gesundheitsdaten“. In *Gesundheit – Konventionen – Digitalisierung: Eine politische Ökonomie der (digitalen) Transformationsprozesse von und um Gesundheit*, herausgegeben von Valeska Cappel und Karolin Eva Kappler, 361–91. Soziologie der Konventionen. Wiesbaden: Springer Fachmedien. https://doi.org/10.1007/978-3-658-34306-4_13.

Adler, Nancy E., und Joan M. Ostrove. 1999. „Socioeconomic Status and Health: What We Know and What We Don't“. *Annals of the New York Academy of Sciences* 896 (1): 3–15. https://doi.org/10.1111/j.1749-6632.1999.tb08101.x.

André, Julia. 2016. „Die digitale Welt selbst mitgestalten können – Fünf Thesen zum Fokusthema »Digitale Mündigkeit«“. Körber-Stiftung. https://www.koerber-stiftung.de/themen/digitale-muendigkeit.

Angwin, Julia, Jeff Larson, Surya Mattu, und Lauren Kirchner. 2016. „Machine Bias“. *ProPublica* (blog). 23. Mai 2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

Aparna, a S, und a V Biju. 2022. *Behavioural Nudges for Public Policies in India – Opportunities and Criticisms*.

Bachner, Jennifer. 2013. *Predictive Policing: Preventing Crime with Data and Analytics*. IBM Center for the Business of Government.

Barth, A. 2011. „HTTP State Management Mechanism“. 6265. Request for Comments (RFC). Internet Engineering Task Force (IETF). https://www.rfc-editor.org/rfc/rfc6265.

Barysch, Katrin Nicole. 2016. „Selbstwirksamkeit“. In *Psychologie der Werte: Von Achtsamkeit bis Zivilcourage – Basiswissen aus Psychologie und Philosophie*, herausgegeben von Dieter Frey, 201–11. Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-662-48014-4_18.

Beck, Roman, Vanessa Greger, Christian Hoffmann, Wolfgang König, Helmut Krcmar, Jasmin Weber, Nico Wunderlich, und Robert Zepic. 2018. „Digitale Mündigkeit. Eine Analyse der Fähigkeiten der Bürger in Deutschland zum konstruktiven und souveränen Umgang mit digitalen Räumen“. Abschlussbericht. Nationales Kompetenzzentrum E-Governance (NEGZ). https://www.researchgate.net/publication/325756267_Digitale_Mundigkeit_Eine_Analyse_der_Fahigkeiten_der_Burger_in_Deutschland_zum_konstruktiven_und_souveranen_Umgang_mit_digitalen_Raumen.

Benjamin, Ruha. 2019. *Race After Technology: Abolitionist Tools for the New Jim Code*. 1. edition. Medford, MA: Polity.

Biselli, Anna. 2015. „Was tut die Bundesregierung zur Medienbildung? An die Länder verweisen.“ *netzpolitik.org* (blog). 17. März 2015. https://netzpolitik.org/2015/was-tut-die-bundesregierung-zur-medienbildung-an-die-laender-verweisen/.

Blankertz, Aline, und Louisa Specht. 2021. „Eine Regulierung für Datentreuhänder“. Policy Brief. Stiftung Neue Verantwortung. https://www.stiftung-nv.de/de/publikation/eine-regulierung-fuer-datentreuhaender.

Bohn, Dieter. 2021. „Privacy and Ads in Chrome Are about to Become FLoCing Complicated“. *The Verge* (blog). 30. März 2021. https://www.theverge.com/2021/3/30/22358287/privacy-ads-google-chrome-floc-cookies-cookiepocalypse-finger-printing.

Bösch, Christoph, Benjamin Erb, Frank Kargl, Henning Kopp, und Stefan Pfattheicher. 2016. „Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns“. *Proceedings on Privacy Enhancing Technologies* 2016 (Juli): 237–54. https://doi.org/10.1515/popets-2016-0038.

Bröckling, Ulrich. 2016. „Auch Aufrichten ist Zurichten. Das Paradox des Empowerment.“ *Medien + Erziehung*.
———. 2017. *Gute Hirten führen sanft*. Frankfurt am Main: Suhrkamp Taschenbuch Verlag.
Brown, Wendy. 2006. „American Nightmare: Neoliberalism, Neoconservatism, and De-Democratization“. *Political Theory* 34 (6): 690–714.
Brusseau, James. 2020. „Deleuze’s Postscript on the Societies of Control: Updated for Big Data and Predictive Analytics“. *Theoria* 67 (164): 1–25. https://doi.org/10.3167/th.2020.6716401.
builtwith. 2022. „Analytics technologies Web Usage Distribution“. 17. November 2022. https://trends.builtwith.com/analytics.
Bundesdruckerei GmbH. 2022. „Der Datentreuhänder als neutrale Schutzinstanz“. 7. Juni 2022. https://www.bundesdruckerei.de/de/innovation-hub/der-datentreuhaender-als-neutrale-schutzinstanz.
Callon, Michel, Yuval Millo, und Fabian Muniesa, Hrsg. 2007. *Market Devices*. 1. Aufl. Oxford: Wiley-Blackwell.
Chavez, Anthony. 2022. „Ausweitung der Tests für die Privacy Sandbox im Web“. *Google* (blog). 28. Juli 2022. https://blog.google/intl/de-de/produkte/android-chrome-mehr/ausweitung-der-tests-fur-die-privacy-sandbox-im-web/.
Cluley, Robert, und Steven D. Brown. 2015. „The dividualised consumer: sketching the new mask of the consumer“. *Journal of Marketing Management* 31 (1–2): 107–22. https://doi.org/10.1080/0267257X.2014.958518.
Copland, Savannah. 2021. „How the Web Audio API Is Used for Audio Fingerprinting“. 18. März 2021. https://fingerprint.com/blog/audio-fingerprinting/.
Cranor, Lorrie Faith. 2012. „Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice“. *Journal on Telecommunications and High Technology Law* 10: 273.
Cyphers, Bennett. 2021. „Google’s FLoC Is a Terrible Idea“. *Electronic Frontier Foundation* (blog). 3. März 2021. https://www.eff.org/de/deeplinks/2021/03/googles-floc-terrible-idea.
Datenschutz-Grundverordnung (DSGVO). „Erwägungsgrund 26 - Keine Anwendung auf anonymisierte Daten“.
Deleuze, Gilles. 1992. „Postscript on the Societies of Control“. *October* 59: 3–7.
Digital Autonomy Hub. 2021. „Mensch und Technik in Interaktion – Wie gelingt individuelle digitale Souveränität?“ https://digitalautonomy.net/studie.
Eckersley, Peter. 2010. „How Unique Is Your Web Browser?“ In *Privacy Enhancing Technologies*, herausgegeben von Mikhail J. Atallah und Nicholas J. Hopper, 1–18. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-642-14527-8_1.
„eEurope – eine Informationsgesellschaft für alle“. 2000. Mitteilung über eine Initiative der Kommission für den Europäischen Sondergipfel von Lissabon am 23./24. März 2000 28/00. Drucksache des Bundesrates.
Electronic Frontier Foundation. 2023. „Cover Your Tracks“. 2. Februar 2023. https://coveryourtracks.eff.org/learn.
Elvy, Stacy-Ann. 2018. „Commodifying Consumer Data in the Era of the Internet of Things“. *Boston College Law Review* 59 (2): 423.
———. 2022. „Data Privacy and the Internet of Things | UNESCO Inclusive Policy Lab“. Inclusive Policy Lab. UNESCO. https://en.unesco.org/inclusivepolicylab/analytics/data-privacy-and-internet-things.

Eubanks, Virginia. 2018. *Eubanks, V: Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. Illustrated edition. New York, NY: St Martin's Press.
Europäische Kommission. 2022. „Was sind personenbezogene Daten?" Text. *EU-Kommission - European Commission* (blog). 24. März 2022. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_de.
Facebook Meta. 2019. „Updates im Werbeanzeigenmanager zu Anzeigen für Immobilien, Jobangebote und Kredite". Meta for Business. 26. August 2019. https://de-de.facebook.com/business/news/updates-to-housing-employment-and-credit-ads-in-ads-manager.
Farnell. 2018. „Braucht man für das IoT überhaupt Internet? | Farnell Deutschland". 15. Januar 2018. https://de.farnell.com/does-the-iot-really-need-the-internet.
Fleming, Jenny. 2005. *„Working Together": Neighbourhood Watch, Reassurance Policing and the Potential of Partnerships*. Canberra: Australian Institute of Criminology.
Friedman, Batya, Peter Kahn, Alan Borning, Ping Zhang, und Dennis Galletta. 2006. „Value Sensitive Design and Information Systems". In *The Handbook of Information and Computer Ethics*. https://doi.org/10.1007/978-94-007-7844-3_4.
Fuhrberg, Reinhold. 2020. „Verhaltensökonomie in der Verwaltungskommunikation – Der Staat als Entscheidungsarchitekt". In *Öffentliche Verwaltung – Verwaltung in der Öffentlichkeit: Herausforderungen und Chancen der Kommunikation öffentlicher Institutionen*, herausgegeben von Klaus Kocks, Susanne Knorre, und Jan Niklas Kocks, 77–101. Wiesbaden: Springer Fachmedien. https://doi.org/10.1007/978-3-658-28008-6_5.
Gallie, W. B. 1955. „Essentially Contested Concepts". *Proceedings of the Aristotelian Society* 56: 167–98.
Gane, Nicholas. 2021. „Nudge Economics as Libertarian Paternalism". *Theory, Culture & Society* 38 (6): 119–42. https://doi.org/10.1177/0263276421999447.
Garland, David. 1996. „The Limits of the Sovereign State: Strategies of Crime Control in Contemporary Society". *The British Journal of Criminology* 36 (4): 445–71.
Ghosh, Arpita, Mohammad Mahdian, R. Preston McAfee, und Sergei Vassilvitskii. 2015. „To Match or Not to Match: Economics of Cookie Matching in Online Advertising". *ACM Transactions on Economics and Computation* 3 (2): 12:1-12:18. https://doi.org/10.1145/2745801.
Gispen, Jet. 2017. „Ethics for Designers". Ethics for Designers. 2017. https://www.ethicsfordesigners.com.
Goa, Eileen. 2022. „A Roomba Recorded a Woman on the Toilet. How Did Screenshots End up on Facebook?" *MIT Technology Review*, 19. Dezember 2022. https://www.technologyreview.com/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy/.
Goel, Vinay. 2022. „Get to Know the New Topics API for Privacy Sandbox". *Google* (blog). 25. Januar 2022. https://blog.google/products/chrome/get-know-new-topics-api-privacy-sandbox/.
Goll, Thomas. 2021. „Kant, Adorno und Covid-19 – Politische Mündigkeit in den Zeiten der Pandemie". In *Demokratie im Stresstest: Reaktionen von Politikdidaktik und politischer Bildung*, herausgegeben von Carl Deichmann und Marc Partetzke, 87–102. Politische Bildung. Wiesbaden: Springer Fachmedien. https://doi.org/10.1007/978-3-658-33077-4_6.
Graefe, Stefanie, Tine Haubner, und Silke van Dyk. 2020. „»Was schulden uns die Alten?« Isolierung, Responsibilisierung und (De-)Aktivierung in der Corona-Krise". *Leviathan* 48 (Januar): 407–32. https://doi.org/10.5771/0340-0425-2020-3-407.

Grafenstein, Max von, Julian Hölzel, Florian Irgmaier, und Jörg Pohle. 2018. „Nudging: Regulierung durch Big Data und Verhaltenswissenschaften“. *Abida – Assessing Big Data*. http://www.abida.de/sites/default/files/ABIDA-Gutachten_Nudging.pdf.

Graßl, Paul, Hanna Schraffenberger, Frederik Zuiderveen Borgesius, und Moniek Buijzen. 2021. „Dark and Bright Patterns in Cookie Consent Requests“. *Journal of Digital Social Research* 3 (1): 1–38. https://doi.org/10.31234/osf.io/gqs5h.

Gray, Garry C. 2009. „The Responsibilization Strategy of Health and Safety: Neo-liberalism and the Reconfiguration of Individual Responsibility for Risk“. *The British Journal of Criminology* 49 (3): 326–42. https://doi.org/10.1093/bjc/azp004.

Gunawan, Johanna, Amogh Pradeep, David Choffnes, Woodrow Hartzog, und Christo Wilson. 2021. „A Comparative Study of Dark Patterns Across Web and Mobile Modalities“. *Proceedings of the ACM on Human-Computer Interaction* 5 (CSCW2): 377:1-377:29. https://doi.org/10.1145/3479521.

Guy, Amy. 2022. „Early Design Review for the Topics API · Issue #726 · W3ctag/Design-Reviews“. *GitHub*. https://github.com/w3ctag/design-reviews/issues/726.

Hache, Émilie. 2007. „La Responsabilité, Une Technique de Gouvernementalité Néolibérale ? [Is Responsibility a Tool of Neo-Liberal Governmentality?]“. *Raisons Politiques* 28 (4): 49. https://doi.org/10.3917/rai.028.0049.

Hägele, Ramona. 2019. „Nudging with Chinese characteristics: an adapted approach from the Global North to achieve a sustainable future?“ In *Reassessing Chinese politics: national system dynamics and global implications*, herausgegeben von Nele Noesselt, 172–99. Baden-Baden: Tectum Wissenschaftsverlag.

Hahn, Tim, Andrew A. Nierenberg, und Susan Whitfield-Gabrieli. 2017. „Predictive Analytics in Mental Health: Applications, Guidelines, Challenges and Perspectives“. *Molecular Psychiatry* 22 (1): 37–43. https://doi.org/10.1038/mp.2016.201.

Halpern, David, und Michael Sanders. 2016. „Nudging by government: Progress, impact, & lessons learned“. *Behavioral Science & Policy* 2 (2): 52–65. https://doi.org/10.1353/bsp.2016.0015.

Hao, Karen. 2021. „Facebook’s Ad Algorithms Are Still Excluding Women from Seeing Jobs“. MIT Technology Review. 9. April 2021. https://www.technologyreview.com/2021/04/09/1022217/facebook-ad-algorithm-sex-discrimination/.

Harris, Shannon L., Jerrold H. May, und Luis G. Vargas. 2016. „Predictive Analytics Model for Healthcare Planning and Scheduling“. *European Journal of Operational Research* 253 (1): 121–31. https://doi.org/10.1016/j.ejor.2016.02.017.

Henkel, Anna, Nico Lüdtke, Nikolaus Buschmann, und Lars Hochmann, Hrsg. 2018. *Reflexive Responsibilisierung: Verantwortung für nachhaltige Entwicklung*. transcript Verlag. https://doi.org/10.14361/9783839440667.

Hietanen, Joel, Oscar Ahlberg, und Andrei Botez. 2022. „The ‘dividual’ is semiocapitalist consumer culture“. *Journal of Marketing Management* 38 (Februar): 1–17. https://doi.org/10.1080/0267257X.2022.2036519.

Hill, Kashmir. 2012. „How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did“. *Forbes* (blog). 16. Februar 2012. https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.

Johnson, Gabbrielle M. 2020. „Algorithmic Bias: On the Implicit Biases of Social Technology“. *Synthese* 198 (10): 9941–61. https://doi.org/10.1007/s11229-020-02696-y.

Jonjic-Beitter, Andrea. 2015. „Digital-Manifest: Zehn Prinzipien gegen die Entmündigung der Bürger“. *netzpolitik.org* (blog). 13. November 2015.

https://netzpolitik.org/2015/digital-manifest-zehn-prinzipien-gegen-die-entmuendigung-der-buerger/.
Kahneman, Daniel. 2003. „Maps of Bounded Rationality: Psychology for Behavioral Economics“. *The American Economic Review* 93 (5): 1449–75.
———. 2011. *Thinking, fast and slow*. 1st ed. New York: Farrar, Straus and Giroux.
Kamkar, Samy. 2010. „Samy Kamkar - evercookie - virtually irrevocable persistent cookies“. 20. September 2010. https://samy.pl/evercookie/.
Kant, Immanuel. (1784) 2004. „Was ist Aufklärung?“ *Utopie Kreativ*, Nr. 159 (1784): 5–10.
Karlin, Josh. (2022a) 2023. „The Topics API: GitHub Repository“. Bikeshed. Private Advertising Technology Community Group Individual Draft Space. https://github.com/patcg-individual-drafts/topics.
———. (2022b) 2023. „The Topics API: taxonomy_v1.md“. *GitHub*. https://github.com/patcg-individual-drafts/topics/blob/daa954e56a25cbf3a8898e50610b95b1379f7382/taxonomy_v1.md.
Kesteren, Anne van. 2022. „The Topics API · Issue #111 · WebKit/Standards-Positions“. *GitHub*. https://github.com/WebKit/standards-positions/issues/111.
Kleinz, Torsten. 2022. „Privacy Sandbox: Googles Cookie-Nachfolger gehen in den Praxistest“. *heise online* (blog). 31. März 2022. https://www.heise.de/news/Privacy-Sandbox-Googles-Cookie-Nachfolger-gehen-in-den-Praxistest-6658725.html.
Kölbel, Ralf, Demichel, Sébastien, Grollmann, Felix, Tushingham, Poppy, Förg, Katharina-Luise, Gadebusch Bondio, Mariacarla, Hengerer, Mark, Lepsius, Susanne, und Radner, Karen. 2021. „Responsibilisierung – Überlegungen zu einer geistes- und sozialwissenschaftlichen Kategorie, Anregungen zu einem heuristischen Instrument“. 02/21. Working Paper des SFB 1369 „Vigilanzkulturen“..
Kosinski, Michal, David Stillwell, und Thore Graepel. 2013. „Private traits and attributes are predictable from digital records of human behavior“. *Proceedings of the National Academy of Sciences* 110 (15): 5802–5. https://doi.org/10.1073/pnas.1218772110.
Köster, Max. 2016. „Internet of too many things | Digitalcourage“. *digitalcourage* (blog). 13. April 2016. https://digitalcourage.de/blog/2016/internet-too-many-things.
Krämer, Sybille, Reg. 2019. *Sybille Krämer: Digitalität und die Kulturtechnik der Verflachung*. re:publica 2019. https://www.youtube.com/watch?v=g2w_pyu4wgg.
Kühling, Jürgen, und Cornelius Sauerborn. 2022. „‚Dark Patterns‘ Unter Der DSGVO Und Dem DSA – Neue Herausforderung Für Die Digitale Rechtsordnung — Klassifikation Und Datenschutzrechtliche Steuerungsvorgaben“. *Computer Und Recht* 38 (4): 226–35. https://doi.org/10.9785/cr-2022-380409.
Loi, Michele, und Markus Christen. 2020. „Two Concepts of Group Privacy“. *Philosophy & Technology* 33 (2): 207–24. https://doi.org/10.1007/s13347-019-00351-0.
Lutz, Tilman. 2018. „Wandel der Sozialen Arbeit: von der Pathologisierung zur Responsibilisierung“. In *Politik der Verhältnisse - Politik des Verhaltens: Widersprüche der Gestaltung Sozialer Arbeit*, herausgegeben von Roland Anhorn, Elke Schimpf, Johannes Stehr, Kerstin Rathgeb, Susanne Spindler, und Rolf Keim, 355–67. Perspektiven kritischer Sozialer Arbeit. Wiesbaden: Springer Fachmedien. https://doi.org/10.1007/978-3-658-17954-0_25.
Mantelero, Alessandro. 2016. „Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection“. *Computer Law & Security Review* 32 (Februar): 238–55. https://doi.org/10.1016/j.clsr.2016.01.014.
Maurer, Kathrin. 2015. „Anhörung: Digitale Bildung und Medienkompetenz“. *netzpolitik.org* (blog). 24. April 2015. https://netzpolitik.org/2015/anhoerung-digitale-bildung-und-medienkompetenz/.

Mellet, Kevin, und Thomas Beauvisage. 2020. „Cookie monsters. Anatomy of a digital market infrastructure“. *Consumption Markets & Culture* 23 (2): 110–29. https://doi.org/10.1080/10253866.2019.1661246.
Meyer, David. 2018. „Amazon Killed an AI Recruitment System Because It Couldn’t Stop the Tool from Discriminating Against Women“. Fortune. 10. Oktober 2018. https://fortune.com/2018/10/10/amazon-ai-recruitment-bias-women-sexist/.
Millett, Lynette I., Batya Friedman, und Edward Felten. 2001. „Cookies and Web browser design: toward realizing informed consent online“. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 46–52. CHI ’01. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/365024.365034.
Mittelstadt, Brent. 2017. „From Individual to Group Privacy in Big Data Analytics“. *Philosophy & Technology* 30 (4): 475–94. https://doi.org/10.1007/s13347-017-0253-7.
Mollen, Anne, und Leonard Haas. 2021. „Digitale Selbstbestimmung - Eine begriffliche Abgrenzung für eine menschenzentrierte Digitalpolitik“. 4. Policy Brief. Digital Autonomy Hub.
Montulli, Lou. 2013. „The irregular musings of Lou Montulli: The reasoning behind Web Cookies“. *The irregular musings of Lou Montulli* (blog). 14. Mai 2013. https://montulli.blogspot.com/2013/05/the-reasoning-behind-web-cookies.html.
Mühlhoff, Rainer. 2019. „Big Data Is Watching You“. In *Affekt Macht Netz - Auf dem Weg zu einer Sozialtheorie der Digitalen Gesellschaft*, 22:81–106. Bielefeld: transcript.
———. 2022. „Prädiktive Privatheit: Kollektiver Datenschutz im Kontext von Big Data und KI“. In Künstliche Intelligenz, Demokratie und Privatheit, herausgegeben von Michael Friedewald, Alexander Roßnagel, Jessica Heesen, Nicole Krämer, und Jörn Lamla, Künstliche Intelligenz, Demokratie und Privatheit:31–58. Nomos Verlagsgesellschaft mbH & Co. KG.
Mulligan, Deirdre K., Colin Koopman, und Nick Doty. 2016. „Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy“. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374 (2083): 20160118. https://doi.org/10.1098/rsta.2016.0118.
„Nachwuchsforschungsgruppe 6: Digitale Mündigkeit“. 2018. Graduiertenkolleg NRW - Digitale Gesellschaft. 2018. https://digitalemuendigkeit.netlify.app/.
Nationales E-Government Kompetenzzentrum e.V. 2022. „ÜBER UNS“. Nationales E-Government Kompetenzzentrum e.V. 24. November 2022. https://www.negz.org/blank-1.
Neufert, Nikolai. 2014. „Der ‚eEducation Berlin Masterplan‘ als Planungs- und Umsetzungsinstrument für die Ausbreitung der informationstechnischen Bildung und die Entwicklung der Medienkompetenz“, Januar. https://doi.org/10.14279/depositonce-3909.
Neuschäfer, Markus, und Nele Hirsch. 2018. „Digitale Mündigkeit gibt es nicht umsonst: Fünf Forderungen aus der Bildungspraxis“. netzpolitik.org. 19. Juni 2018. https://netzpolitik.org/2018/digitale-muendigkeit-gibt-es-nicht-umsonst-fuenf-forderungen-aus-der-bildungspraxis/.
Noble, Safiya Umoja. 2018. *Algorithms of Oppression: How Search Engines Reinforce Racism*. Illustrated edition. New York: Combined Academic Publ.
O’Neil, Cathy. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown.
Overmier, J. Bruce, und Martin E. Seligman. 1967. „Effects of inescapable shock upon subsequent escape and avoidance responding“. *Journal of Comparative and Physiological Psychology* 63: 28–33. https://doi.org/10.1037/h0024166.

Pariser, Eli. 2011. *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*. Penguin.
Pine, Karen J., und Ben C. Fletcher. 2011. „Women's Spending Behaviour Is Menstrual-Cycle Sensitive". *Personality and Individual Differences* 50 (1): 74–78. https://doi.org/10.1016/j.paid.2010.08.026.
Pohle, Jörg. 2022. „Datenschutz: Rechtsstaatsmodell oder neoliberale Responsibilisierung? Warum Datentreuhänder kein Mittel zum Schutz der Grundrechte sind". Verbraucherzentrale Nordrhein-Westfalen e.V. https://www.hiig.de/publication/datenschutz-rechtsstaatsmodell-oder-neoliberale-responsibilisierung-warum-datentreuhaender-kein-mittel-zum-schutz-der-grundrechte-sind/.
Pykett, Jessica. 2012. „The New Maternal State: The Gendered Politics of Governing through Behaviour Change". *Antipode* 44 (1): 217–38. https://doi.org/10.1111/j.1467-8330.2011.00897.x.
Pyysiäinen, Jarkko, Darren Halpin, und Andrew Guilfoyle. 2017. „Neoliberal governance and 'responsibilization' of agents: reassessing the mechanisms of responsibility-shift in neoliberal discursive environments". *Distinktion: Journal of Social Theory* 18 (2): 215–35. https://doi.org/10.1080/1600910X.2017.1331858.
Qiu, Tie, Jiancheng Chi, Xiaobo Zhou, Zhaolong Ning, Mohammed Atiquzzaman, und Dapeng Oliver Wu. 2020. „Edge Computing in Industrial Internet of Things: Architecture, Advances and Challenges". *IEEE Communications Surveys & Tutorials* 22 (4): 2462–88. https://doi.org/10.1109/COMST.2020.3009103.
Reinhold, Theresia. 2015. „Coding für die Kleinen – ‚Programmieren ist die Sprache des 21. Jahrhunderts'". *netzpolitik.org* (blog). 6. Februar 2015. https://netzpolitik.org/2015/programmieren-fuer-alle/.
Reisch, Lucia, und C. Sunstein. 2016. „Do Europeans Like Nudges?" *Judgment and decision making* 11 (August): 310–25. https://doi.org/10.2139/ssrn.2739118.
Renaud, Karen, Stephen Flowerday, Merrill Warkentin, Paul Cockshott, und Craig Orgeron. 2018. „Is the Responsibilization of the Cyber Security Risk Reasonable and Judicious?" *Computers & Security* 78 (September): 198–211. https://doi.org/10.1016/j.cose.2018.06.006.
Rose, Nikolas, Pat O'Malley, und Mariana Valverde. 2006. „Governmentality". 2. Annual Review of Law and Social Science. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=1474131.
Ross, Meghan. 2020. „CHIBE To Establish First-of-Its-Kind HIV ‚Nudge Unit' in South Africa". *Center for Health Incentives and Behavioral Economics* (blog). 5. Februar 2020. https://chibe.upenn.edu/chibeblog/chibe-to-establish-first-of-its-kind-hiv-nudge-unit-in-south-africa/.
Rost, Martin. 2017. „Bob, es ist Bob!" *FIfF-Kommunikation*, FIfF-Kommunikation, 4 (17): 63–66.
Rothchild, John. 2018. „Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else)". SSRN Scholarly Paper ID 3126869. Rochester, NY: Social Science Research Network.
Ryte, Marketing. 2020. „Was bedeutet Tracking Pixel? - Ryte Digital Marketing Wiki". 22. Januar 2020. https://de.ryte.com/wiki/Tracking_Pixel.
Schmid, Josef. 2020. „Wohlfahrtsstaat in Europa". *Bundeszentrale für politische Bildung* (blog). 2020. https://www.bpb.de/kurz-knapp/lexika/das-europalexikon/177357/wohlfahrtsstaat-in-europa/.

Schuh, Justin. 2019. „Building a More Private Web“. *Google* (blog). 22. August 2019. https://blog.google/products/chrome/building-a-more-private-web/.
Schütte, André. 2020. „Verbraucherbildung an Schulen. Bestandsaufnahme und Kritik eines Responsibilisierungsprogramms“. *Zeitschrift für Erziehungswissenschaft* 23 (5): 1079–96. https://doi.org/10.1007/s11618-020-00971-9.
Seemann, Michael. 2021. *Die Macht der Plattformen: Politik in Zeiten der Internetgiganten*. 1. Aufl. Berlin: Ch. Links Verlag.
Simon, Leena. 2022. „Digitale Mündigkeit – Angewandte Mündigkeit“. Digitale Mündigkeit. 14. März 2022. https://muendigkeit.digital/#angewandte_muendigkeit.
Sloan, Robert H., und Richard Warner. 2013. „Beyond Notice and Choice: Privacy, Norms, and Consent“ Rochester, NY: Social Science Research Network.
Srnicek, Nick. 2017. „The Challenges of Platform Capitalism: Understanding the Logic of a New Business Model“. *Juncture* 23 (4): 254–57. https://doi.org/10.1111/newe.12023.
Star, Susan Leigh. 1999. „The Ethnography of Infrastructure“. *American Behavioral Scientist* 43 (3): 377–91. https://doi.org/10.1177/00027649921955326.
Tastevin, Nicolas. 2022. „Decoding Google Topics (2/3)“. *Weborama* (blog). 12. September 2022. https://medium.com/weborama/decoding-google-topics-2-2-8415b14d11f7.
Thaler, Richard H., Cass R. Sunstein, und John P. Balz. 2013. „Chapter 25. Choice Architecture“. In *Chapter 25. Choice Architecture*, 428–39. Princeton University Press. https://doi.org/10.1515/9781400845347-029.
The World Bank. 2018. „Behavioural Science Around the World – Profiles of 10 Countries“. World Bank Documents.
Thomson, Martin. 2023. „Request for Position: Topics API · Issue #622 · Mozilla/Standards-Positions“. *GitHub*. https://github.com/mozilla/standards-positions/issues/622.
Titone, Trey. 2022. „Topics API - The Google FLoC Replacement Explained“. *Ad Tech Explained* (blog). 31. Januar 2022. https://adtechexplained.com/google-topics-api-explained/.
Torvekar, Nupura, und Pravin Game. 2019. „Predictive analysis of credit score for credit card defaulters“. *International Journal of Recent Technology and Engineering* 7 (Januar): 283–86.
UN General Assembly. 1990. *Guidelines for the Regulation of Computerized Personal Data Files*. *A/RES/45/95*. UN. https://digitallibrary.un.org/record/105299.
User Agent Working Group W3C. 2011. „Definition of User Agent - WAI UA Wiki“. https://www.w3.org/WAI/UA/work/wiki/Definition_of_User_Agent.
Véliz, Carissa. 2020. *Privacy is power: why and how you should take back control of your data*. London: Bantam Press.
Velthuis, Olav. 2020. „Market Devices“. *Pragmatic Inquiry*, 80.
Wakefield, Alison, und Jenny Fleming. 2009. „Responsibilization“. In *The SAGE Dictionary of Policing*, 277–78. London: SAGE Publications Ltd. https://doi.org/10.4135/9781446269053.
Waldman, Ari Ezra. 2020. „Cognitive Biases, Dark Patterns, and the ‘Privacy Paradox’“. *Current Opinion in Psychology*, Privacy and Disclosure, Online and in Social Interactions, 31 (Februar): 105–9. https://doi.org/10.1016/j.copsyc.2019.08.025.
Wawrzyniak, Jessica. 2019. „Digitale Bildung & Datenschutzwissen im Bücherregal | Digitalcourage“. 28. Februar 2019. https://digitalcourage.de/pressemitteilungen/2019/digitale-bildung-und-datenschutzwissen-im-buecherregal.
Webb, Alex. 2022. „Amazon’s Roomba Deal Is Really About Mapping Your Home“. *Bloomberg.Com*, 5. August 2022.

https://www.bloomberg.com/news/articles/2022-08-05/amazon-s-irobot-deal-is-about-roomba-s-data-collection.
Williams, Robert. 2005. „Politics and Self in the Age of Digital (Re)producibility“. *Fast Capitalism* 1 (Januar). https://doi.org/10.32855/fcapital.200501.008.
Wray, Christopher. 2022. „FBI Partnering with the Private Sector to Counter the Cyber Threat“. Speech. Federal Bureau of Investigation. 22. März 2022. https://www.fbi.gov/news/speeches/fbi-partnering-with-private-sector-to-counter-the-cyber-threat-032222.
Zajko, Mike. 2016. „Telecom Responsibilization: Internet Governance, Surveillance, and New Roles for Intermediaries“. *Canadian Journal of Communication* 41 (Januar): 75–93. https://doi.org/10.22230/cjc2016v41n1a2894.
Zuboff, Shoshana. 2015. „Big Other: Surveillance Capitalism and the Prospects of an Information Civilization“. *Journal of Information Technology* 30 (1): 75–89. https://doi.org/10.1057/jit.2015.5.
———. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. 1. Aufl. New York, NY: PublicAffairs.