Digitale Selbstverteidigung

Der Schutz der Privatheit als aktuelle Herausforderung der Erwachsenen- und Weiterbildung

Masterarbeit

zur Erlangung des akademischen Grades
Master of Arts

an der Karl-Franzens-Universität Graz

vorgelegt von

Thorsten STOCKNER

am Institut für Erziehungs- und Bildungswissenschaft

Begutachterin Annette SPRUNG, Univ.-Prof.in Mag.a Dr.in phil.

Graz, 2021

CC BY-SA 3.0 DE

Kurzzusammenfassung

Digitale Selbstverteidigung - Der Schutz der Privatheit als aktuelle Herausforderung der Erwachsenen- und Weiterbildung

Thorsten Stockner

Die vorliegende Arbeit beschäftigt sich mit dem Schutz und dem Verfall der Privatsphäre und den aktuellen Herausforderungen, die sich dabei ergeben. Ziel ist es, zu einem grundlegenden Verständnis von Datenschutz für die Erwachsenenbildung beizutragen, vor allem aber die große Bedeutung und Notwendigkeit einer kritischen Reflexion von Datenverarbeitungsprozessen aufzuzeigen und zu begründen. Der pandemiebedingte Digitalisierungsschub führte Menschenleben in eine digital repräsentierte Wirklichkeit. Dabei lauern viele Gefahren. Von Hackings, Identitätsdiebstahlen, bis hin zur elektronischen Überwachung. Vor allem letzterer Punkt ist für diese Arbeit ausschlaggebend, da die elektronische Überwachung einen maßgeblichen Eingriff in die Privatsphäre von Nutzern und Nutzerinnen mit sich bringt. Paradoxerweise ist Nutzern und Nutzerinnen der Schutz der eigenen Daten durchaus ein Anliegen, doch sie handeln entgegen dieser Einstellung. In einer ökonomisch motivierten Datengesellschaft sind Daten das neue Kapital – das Öl des 21. Jahrhunderts. Egal, ob personenbezogen oder nicht: Aus Daten lassen sich Rückschlüsse auf das Verhalten ziehen und Vorhersagen treffen. Aufgrund einer dünnen Schicht erwachsenen-pädagogischer Literatur wurde eine Sekundäranalyse über die Gefahren, die sich dabei für die Erwachsenen- und Weiterbildung ergeben, aufgezeigt. Von Verhaltensmanipulation, Informationsmacht und informationeller Asymmetrie. Die Erwachsenen- und Weiterbildung trägt hierbei die Verantwortung aufzuklären und eine Datenkompetenz zu schaffen, denn rein regulatorische Maßnahmen sind heutzutage nicht mehr ausreichend, um den Schutz der Privatsphäre zu gewährleisten.

Abstract

Digital Self-Defense - The Protection of Privacy as a Current Challenge for Adult and Continuing Education

Thorsten Stockner

The present work deals with the protection and deterioration of privacy and the current challenges that arise in this context. The aim is to contribute to a fundamental understanding of privacy for adult education, but above all to demonstrate and justify the great importance and necessity of critical reflection on data processing. During the pandemic, the surge of digitization led human lives into a digitally represented reality. But in this surge, many dangers lurk. From hackings and identity theft to electronic surveillance. The latter point in particular is crucial for this work, as electronic surveillance entails a significant intrusion into the privacy of users. Paradoxically, users are concerned about protecting their own data, but their actions contradict this. In an economically motivated data society, data is the new capital – the oil of the 21st century. Whether personal or not, data can be used to draw conclusions about behaviour and make predictions. Based on a thin layer of adult education literature, a secondary analysis of the dangers this poses to adult and continuing education was highlighted. That of behavioural manipulation, informational power, and informational asymmetry. Adult and continuing education has a responsibility to educate and create data literacy, because purely regulatory measures are no longer sufficient enough to ensure privacy protection today.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

„*Software will eat the world.*“

Marc Andreessen[1]

Daten sind das neue Öl und Datenschutz der neue Umweltschutz. Ölverschmierte Meeresvögel, das Kalben eines endenden Gletschers, das Lodern der Flammen eines Waldbrandes, oder ein verwüsteter Straßenzug nach einem Wirbelsturm. Während der Umweltschutz ein Gesicht trägt, geschehen Eingriffe in die Privatsphäre – still und heimlich im Verborgenen. Den datenverschmierten Homo sapiens gibt es nicht. Daten sind digitale Repräsentationen unserer Welt und somit nicht greifbar. Die Nutzung von webbasierten Anwendungen wird immer anfälliger für Hacker und bösartige Software, aber auch für Überwachung, Verfolgung, Kontrolle und für die Ausbeutung von Nutzerdaten – sowohl durch den Staat als auch durch private Organisationen. Das Hauptinteresse des Staates liegt dabei in der vermeintlichen Sicherheit, während das Hauptziel der Privatunternehmen die Beschaffung von Daten in großem Umfang ist.

Das Leben eines jeden und einer jeden Einzelnen wurde als Konsequenz der andauernden COVID-19-Pandemie - mehr noch, als es die in der Erwachsenenbildung heißumwogene Digitalisierung vorsehen vermochte – online gelebt. Aufgrund von Ausgangssperren wanderten Workshops, Seminare, sogar ganze Arbeitsplätze in die digital repräsentierte Wirklichkeit. Dies trug zu einer Verbreitung und Einflussnahme von technologischen Hilfsmitteln und webbasierten Anwendungen auf den Lebensalltag von Menschen bei – bedauernswerterweise „zum Teil unter grob fahrlässiger Nichtbeachtung jeglicher datenschutzrechtlicher Warnhinweise und unter Suspendierung oder zumindest situationselastischer Anpassung pädagogisch-ethischer Erwägungen.“ (Hug & Madritsch, 2020, S. 19)

[1] Der US-amerikanische Softwareentwickler ist 2011 davon überzeugt, dass Technologieunternehmen, welche sich auf webbasierte Anwendungen spezialisieren, in etablierte Industriestrukturen eindringen und diese umstürzen. Andreessen, M. (2011). *Why Software Is Eating The World*. Genius. Abgerufen 16. November 2021, von https://genius.com/Marc-andreessen-why-software-is-eating-the-world-annotated.

Die Erwachsenenbildung sieht sich demnach konfrontiert mit einigen Herausforderungen. In dieser Arbeit wird deswegen der Schutz der Privatheit, der Datenschutz und der Schutz vor Überwachung im Kontext der Erwachsenenbildung behandelt. Dies sind keine neuen Phänomene, bedürfen aber durch den Digitalisierungsschub, den social-distancing und home-office als Maßnahmen gegen die Pandemie hervorgerufen haben, besonderer Aufmerksamkeit. Für die vorliegende Arbeit relevant steht allen voran hierbei die Frage nach dem Schutz der Privatheit von Individuen. Neben der Installation von Videoüberwachungsanlagen, dem Sammeln von biometrischen Informationen und der Nutzung von DNA werden persönliche Daten vor allem dann gesammelt, wenn elektronische Endgeräte eingesetzt werden. Geräte, die vor allem in kontaktlosen Zeiten zu treuen Weggefährten in einer vernetzten und doch distanzierten Welt geworden und auch in der Erwachsenenbildung nicht mehr wegzudenken sind. Einerseits trugen sie in hohem Maße dazu bei Lockdowns erträglicher zu machen, doch andererseits ergibt sich daraus ein Problem, dem sich Individuen nur schwer entziehen können: Die kontinuierliche Sammlung und Ausbeutung persönlicher Daten und die immanente elektronische Überwachung.

Jedes elektronische Endgerät sammelt im eingeschalteten Zustand ununterbrochen Informationen, speichert diese ab, und verarbeitet sie weiter. Jeden Tag. Jede Stunde. Jede Sekunde. Ohne Zutun des Wissens und selten mit der gänzlich freiwilligen Einwilligung auf Seiten der Nutzer und Nutzerinnen, werden individuelle Stärken und Schwächen, Interessen, Präferenzen, Krankheiten, Erfolge, Misserfolge, Geheimnisse und insbesondere unser Einkaufsverhalten dokumentiert und analysiert. Die Menge an gesammelten Daten von Unternehmen ist in den letzten Jahren drastisch gestiegen (Christl & Spiekermann, 2016, S. 7).

Dieser Umstand führt zur Prägung des Begriffs des Überwachungskapitalismus. Der von der Wirtschaftswissenschaftlerin Zuboff eingeführte Begriff beschreibt ein marktwirtschaftliches, kapitalistisches System, das mit technischen Hilfsmitteln persönliche Daten von Menschen erhebt und wie diese in weiterer Folge verwendet werden, um Informationen über Verhaltensweisen zu sammeln, diese zu analysieren und für marktökonomische Entscheidungsfindungen aufzubereiten, um daraus Verhaltensvorhersagen generieren zu können, welche wiederum zu Gewinnzuwachs führen.

> Das industrielle Erbe eines Klimadesasters erfüllt uns mit Schrecken, Gewissensbissen und Angst. Vor welchem ungeahnten Erbe von Schädigungen und Gewissensbissen werden sich dann künftige Generationen sehen, wenn der Überwachungskapitalismus die beherrschende Form des Informationskapitalismus unserer Zeit werden sollte? (Zuboff, 2018, S. 27)

Während es Abtreibungsgegner, Black-Lives-Matter-Demonstrierende oder Gegner und Gegnerinnen von Corona-Schutzmaßnahmen gelingt, die Menschen in Scharen auf die Straßen zu bringen und für ihren Standpunkt einzustehen, treffen sich Verfechter der Privatheit und Datenschutzaktivistinnen nur selten außerhalb ihrer eigenen vier Wände. Es gibt keine konzertierte weltweite Bewegung, die sich für den Schutz der Privatheit einsetzt, welche auch nur annähernd das Ausmaß, die Ressourcen oder die öffentliche Anerkennung bekommt, die Organisationen im Umwelt-, Frauen- oder Menschenrechtsbereich (Bennett, 2008, S. 199) genießen. Zugleich warnen sie nicht vor der Zerstörung des Planeten, wie es Umweltschützer seit Jahren tun, und dennoch gibt es Parallelen, die Schneier folgendermaßen zieht: „Data is the pollution problem of the information age, and protecting privacy is the environmental challenge.“ (Schneier, 2016, S. 238) Im Bereich des Schutzes der Privatsphäre gibt es ein vielfältiges, offenes und fließendes Spektrum von Gruppen und Organisationen, die von traditionellen Bürgerrechtsorganisationen bis hin zu Verbraucherverbänden reichen und spezialisierten Gruppen, die sich mit Einzelfragen der Problematik auseinandersetzen (Bennett, 2008, S. 199).

Dabei wird die Debatte um den Datenschutz von Interessensgruppen geführt, die sich nicht von den bereits genannten unterscheiden lassen. Schlussendlich glauben sie alle daran, für etwas einzustehen, das unabdingbar ist für eine funktionierende Zivilgesellschaft (Hosein, 2006, S. 121). „Through participation in political processes, without regard to differing political persuasions and methods, all these people work for change and for the attention of the silent majority.“ (Hosein, 2006, S. 121)

Edward Snowden, US-Amerikanischer Whistleblower, hat die Aufmerksamkeit der „silent majority“, wie sie von Hosein (2006) genannt wird, im Jahr 2014 auf sich gezogen, als er aufdeckte, inwiefern die schlimmsten Befürchtungen von George Orwell aus seinem Roman „1984“ bereits in der heutigen Zeit angekommen sind und inwieweit sie für das Individuum als auch für die Gesellschaft problematisch werden können. Trotz dessen haben die Bedeutung der Privatheit und die Bemühungen, diese zu schützen, nie den Stellenwert in der Gesellschaft beansprucht, wie es beispielsweise der Umweltschutz oder das Selbstbestimmungsrecht der Frau geschafft haben (Hosein, 2006, S. 121).

Der Einzug in den öffentlichen Diskurs geht langsam voran. In der Erwachsenen- und Weiterbildung wird das Thema der Privatheit im Netz oft vernachlässigt. Doch gerade die Erwachsenenbildung, die Interesse an einer funktionierenden Zivilgesellschaft haben muss, muss sich im Zuge der Digitalisierung mit dem Schutz der Privatheit auseinandersetzen. Eine Umfrage des deutschen Bundesverbandes für Informationswirtschaft, Telekommunikation und neuen Medien aus dem Jahre 2015 hat ergeben, dass lediglich drei Prozent der befragten Internetnutzer und Internetnutzerinnen angaben, dass es ihnen egal sei, was mit ihren Daten im Internet passiert (BITKOM, 2011; Gerber et al., 2017, S. 142). Dennoch spiegelt sich dies im Verhalten der Nutzer und Nutzerinnen kaum wider und wird als Paradox der Privatheit bezeichnet.

Was es damit auf sich hat und welche weiteren Herausforderungen auf die Erwachsenenbildung im Kontext der Privatheit und Digitalisierung warten, ist Thema dieser Arbeit.

1.1 Motivation

Meine eigene Motivation entstammt zu einem Teil aus persönlicher Bestürzung über die mangelnden datenschutzrechtlichen Bedenken Mitstudierender gegenüber der Videokonferenzsoftware Zoom. Eine Standardfloskel auf die Konfrontation, in welchem Ausmaß dabei personenbezogene Daten erhoben werden, ist „Ich habe ja nichts zu verbergen“, gepaart mit einem resignierenden Schulterzucken. Nichts zu verbergen und nichts zu befürchten. Diese zynische Grundhaltung in Bezug auf Datenschutz und die eigene Privatsphäre schlägt sich mit der hohen Bedeutung, die dem Datenschutz in Umfragen zugeschrieben wird. Dem Privatheitsparadox ist dementsprechend ein eigenes Kapitel in dieser Arbeit gewidmet.

Ich frage mich, woran es liegt, dass auf der einen Seite Menschen mit Leichtsinn ihre persönlichen Daten im Internet preisgeben und andererseits andere alles tun, um so wenig wie möglich von sich selbst online preiszugeben. Dabei beziehe ich mich nicht auf das Teilen von privaten Informationen in Sozialen Medien, sondern auf die unachtsame und wenig reflektierte Nutzung von webbasierten Anwendungen und technischen Hilfsmittel.

Ich gehe dieser Frage im Laufe der Arbeit nach. Mittlerweile zähle ich mich zweifellos zur letztgenannten Gruppe von Personen. Über die Jahre habe ich ein Interesse zu den Themen Privatheit und „Digitale Selbstverteidigung“ entwickelt. Dieses Interesse möchte ich in meiner Abschlussarbeit mit meiner Expertise als Student der Erwachsenen- und Weiterbildung paaren.

1.2 Relevanz und Problemstellung

„Datenschutz ist eines der großen gesellschaftlichen und politischen Themen des 21. Jahrhunderts. Kaum ein Gegenstand wird gegenwärtig derart breit und kontrovers diskutiert.“ (Beyvers, 2018, S. 25) Dennoch finden sich im österreichischen Bibliotheksverbund kaum Einträge, welche die beiden Schlagwörter Erwachsenenbildung und Privatsphäre und/oder Privatheit beinhalten. Aus dem Blickwinkel der Erwachsenen- und Weiterbildung wird die Thematik rund um Datenschutz und Privatsphäre im Internet eher stiefmütterlich behandelt. Maßgebend lassen sich Arbeiten finden, die sich dem Thema aus rechtswissenschaftlicher Sicht annähern.

Oftmals als rein individuelles Problem angesehen, betreffen die persönlichen Daten eines Individuums allerdings vermehrt auch die Daten anderer Individuen, und es kann dementsprechend als Problemstellung gesehen werden, die bei der Suche nach Antworten auf kollektive Koordination angewiesen ist (Fairfield & Engel, 2015, zit. n. Beyvers, 2018, S. 304).

Privatheit wird verstanden als „a crucial underpinning of interpersonal relationships, of society itself and its groups and categories of persons, and of the workings of democratic political systems." (Raab, 2017, S. 87) Allgemein festzustellen ist ein Verfall des Privaten. Wenn Privatheit allerdings essenziell für das Funktionieren einer Demokratie ist: Was passiert mit dem demokratisch politischen System, wenn diese Voraussetzung nicht mehr gegeben ist? Welche Rolle nimmt die Erwachsenenbildung hierbei ein? Dies führt zur Methodik und zur Forschungsfrage der vorliegenden Arbeit.

1.3 Methodik

Das Ziel der Forschung ist es, einen Einblick zu gewinnen, mit welchen Herausforderungen sich die Erwachsenenbildung aufgrund einer voranschreitenden Digitalisierung und einer damit einhergehenden kontinuierlichen Expropriation von persönlichen Daten und elektronischer Überwachung konfrontiert sieht. Ich habe mich dabei bewusst gegen empirische Forschungsmethoden entschieden.

Dieses aufgrund der Dichotomie zwischen Einstellung und tatsächlichem beobachtbaren Verhalten beim Teilen von Informationen im Internet, aber auch aufgrund von Zustimmungstendenzen und sozialer Erwünschtheit, die bei datenschutzrelevanten Umfragen oft zutage kommen. Ebenso schien mir die Repräsentativität bei der Auswahl von Interviewpartnern und Interviewpartnerinnen in der Erwachsenenbildung als schwierig zu erreichen.

Dementsprechend entschied ich mich für eine Sekundärforschung zur Erreichung zuvor genannter Zielsetzung. Die Arbeit bezieht jedoch einige Ergebnisse aus empirischen Erhebungen und Experimenten mit ein, um meine Argumentation zu untermauern. Die vorliegende Arbeit ist somit eine Literaturarbeit und basiert auf einer sorgfältigen Auswahl relevanter wissenschaftlicher und gesellschaftskritischer Literatur.

Eine inhaltliche Zusammenfassung der Basisliteratur mit Ergänzungen weiterführender Literatur wird dabei kritisch beleuchtet und stets im Kontext der Erwachsenen- und Weiterbildung erläutert. Aufgrund der Interdisziplinarität des behandelten Themas wurden bei der Auswahl der Literatur Disziplinen wie Rechtswissenschaften, Psychologie, Wirtschaftswissenschaften, Soziologie und Ethik miteinbezogen. Vor allem die Rechtswissenschaften beanspruchen die Thematik seit jeher für sich, schaffen es allerdings nicht, die volle Bedeutungsbreite der Problematik zu erfassen.

In den Bildungswissenschaften und in der erwachsenen-pädagogisch relevanten Literatur gibt es kaum Arbeiten, die sich im Speziellen mit der zugrundeliegenden Thematik auseinandersetzen. Gezielte Suchanfragen, bei denen einerseits die Schlagwörter „Privatheit“, „Privatsphäre“, „Datenschutz“ und „Datenkompetenz“ und andererseits „Erwachsenenbildung“, „Weiterbildung“, „Pädagogik“ und „Bildung“ miteinander kombiniert wurden, ergaben wenige auswertbare Treffer.

Aus diesem Grund suchte ich in weiterer Folge nach englischsprachiger Literatur und wurde fündig. Aufgrund der Interdisziplinarität konnte ich dennoch auf eine breite Auswahl an Literatur, Videodateien und wenige Internetartikel zurückgreifen. Bei der Auswahl dieser lag mein Augenmerk auf Wissenschaftlichkeit und Aktualität, da vor allem die technologischen Aspekte rund um die Thematik eine gewisse Kurzlebigkeit und ständige Aktualisierungen aufweisen.

Aus diesen Gründen soll die vorliegende Arbeit einen Beitrag zum Verständnis des Forschungsgebiets in der Erwachsenen- und Weiterbildung leisten, bestehende Forschungslücken aufzeigen und bestmöglich zur Schließung derselben beisteuern. Im Laufe der Arbeit werden diesbezüglich folgende Fragestellungen beantwortet:

Hauptfragestellung

Welche Herausforderungen ergeben sich für die Erwachsenenbildung angesichts einer kontinuierlichen Datensammlung und immanenten elektronischen Überwachung von Individuen im 21. Jahrhundert?

Unterfragen

Bei der Beantwortung der Hauptfrage beschäftigte ich mich ebenfalls mit dem Verhältnis zwischen Erwachsenenbildung und dem Wert, den sie der Privatheit zuschreibt. Die Fragestellung lautet demnach:

Welche Bedeutung hat der Verlust der Privatsphäre für die Erwachsenen- und Weiterbildung und welchen Stellenwert gibt sie dem Datenschutz aktuell?

Des Weiteren skizziere ich am Ende der Arbeit mögliche Schritte, um die in dieser Arbeit erläuterten Herausforderungen zu meistern und frage:

Welche Bildungsmaßnahmen kann die Erwachsenen- und Weiterbildungsbranche präventiv zum Schutz der Privatsphäre einsetzen?

1.4 Aufbau der Arbeit

Die vorliegende Arbeit ist in sieben inhaltliche Kapitel mit abschließender Conclusio aufgebaut. Dabei wird die Leserschaft mit illustrativen Beispielen aus der digitalen Erwachsenenarbeit durch die Arbeit geleitet. Dabei wird stets auf die Bedeutung für die Profession des bzw. der Erwachsenenbildner bzw. Erwachsenenbildnerin hingewiesen.

In Kapitel 2 gehe wird der Frage nachgegangen, was Privatheit im wissenschaftlichen Sinne ist, und inwiefern sie sich vom Begriff der Privatsphäre unterscheidet. Des Weiteren wird die Problematik der Asymptomatik von Verletzungen bzw. Eingriffen in die Privatheit erläutert. Neben der Bedeutung von Privatheit sowohl für Individuum als auch für Gesellschaft befasse ich mich anschließend mit der historischen Entwicklung des Konzepts und erstelle einen prägnanten Vergleich zwischen Vergangenheit und Gegenwart, ehe ich mich mit der schwierigen Definition der Begriffsthematik auseinandersetze. Das Kapitel endet mit einer Kategorisierung von Privatheit und Privatsphäre und grenzt die zu behandelnde Thematik näher ein.

Das dritte Kapitel ist der Entwicklung zur Informationsgesellschaft und dem Traum der Wissensgesellschaft gewidmet. Ich stelle ein deskriptives Modell zur Begriffsunterscheidung von Daten, Informationen und Wissen bis hin zur Entstehung von Wissen vor. Ein metaphorischer Vergleich von Daten mit Rohöl hilft bei der Veranschaulichung von Daten und deren Nutzen zur Erwirtschaftung von Gewinn in einer ökonomisch motivierten Datengesellschaft. Ich gehe der Frage nach, welche Rolle Big Data dabei spielt, und unterscheide zwischen personenbezogenen und sogenannten Metadaten. Weiters wird aufgezeigt, inwiefern blindes Vertrauen in Auswertungsverfahren und der Irrglaube, mit Daten lasse sich jedes Problem lösen, zu einer gefährlichen Entwicklung, insbesondere zur Beeinflussung von Individuen, führen kann.

Das vierte Kapitel beginnt mit der Vorstellung eines Modells zur Entscheidungsfindung von Individuen bei der Preisgabe von Daten, um deren oftmals widersprüchlichem Verhalten im Internet auf die Spur zu kommen. Das sogenannte Privatheitsparadox wird erläutert und kritisch betrachtet. Warum geben Individuen Daten preis – trotz Bedenken. Und welche Rolle spielt hierbei das „Ich-habe-nichts-zu-verbergen“ Argument? Dabei wird auf unterschiedliche Erklärungsansätze zur Datenpreisgabe eingegangen und untersucht, inwiefern Individuen aus freien Stücken Daten preisgeben.

Kapitel 5 widmet sich der elektronischen Überwachung allgemein und inwiefern diese mit permanenter Datenerhebung möglich ist. Ich widme mich dem sogenannten Überwachungskapitalismus und untersuche, inwiefern dieser eine Gefahr für unsere Gesellschaft darstellt. Informationelle Asymmetrie und Informationsmacht führen zu einem Machtungleichgewicht und einem enormen Einfluss von wenigen Unternehmen, die sich ein Oligopol teilen, dessen Geschäftszweck auf den Daten von Nutzern und Nutzerinnen beruht.

Als vorletztes inhaltliches Kapitel beschäftigt sich Kapitel 6 damit, inwiefern gültige Rechtsprechung Daten und die Menschen dahinter schützt und ob es wirksam dabei ist, dieses Machtungleichgewicht auszutarieren. Es werden dabei der Schutz der Privatheit in den Menschenrechten und der europäischen Grundrechtcharta bis hin zur relativ neuen Europäischen Datenschutzgrundverordnung und wie diese den Umgang mit personenbezogenen Daten regelt abgehandelt. Das Kapitel schließt mit einer ernüchternden Folgerung bezüglich des rechtlichen Schutzes und dessen Wirksamkeit für den Schutz der Privatheit von Einzelpersonen.

Ehe ich mich der Conclusio der Arbeit widme, schließe ich den inhaltlichen Teil mit Ebenen von Kontrollmechanismen, die Individuen bedienen können, um einen effektiven Schutz ihrer Daten gewährleisten zu können. Im Weiteren wird erläutert, welche Maßnahmen bei der Bewältigung von den in der Arbeit beschriebenen Herausforderungen helfen können – von regulativen Mechanismen und technischen Hilfsmitteln bis hin zu pädagogischen Maßnahmen, in denen insbesondere die Rolle der Erwachsenen- und Weiterbildung herausgestellt wird. Zusätzlich werden zwei Beispiele vorgestellt, die einen maßgeblichen Beitrag zur Schaffung von Datenkompetenz leisten können.

Die Arbeit endet mit einer inhaltlichen Zusammenfassung des Geschriebenen und liefert einen Ausblick auf die zukünftige Forschung.

2 Einführung in die Privatsphäre

„Whenever a conflict arises between privacy and accountability, people demand the former for themselves and the latter for everybody else.“

David Brin[2]

Im Folgenden wird auf die Unterscheidung zwischen den Begriffen Privatheit und Privatsphäre eingegangen, welche im Alltag oft synonym gebraucht werden.

2.1 Privatheit vs. Privatsphäre

Das englische Wort „Privacy“ steht im Deutschen für den Neologismus „Privatheit“. Im Alltagsgebrauch als auch im wissenschaftlichen Diskurs wird der Ausdruck „Privatsphäre“ häufiger verwendet. In der vorliegenden Arbeit verwende ich dennoch bewusst größtenteils den Begriff „Privatheit“, denn Diskussionen über die Privatsphäre nehmen eine explizite oder implizite räumliche Dimension an und beruhen auf der Annahme, dass es einen geschützten Ort gibt – eine „Zone“ oder einen „Bereich“, in den andere Personen oder Organisationen nicht eindringen dürfen.

Die Bedeutungsbreite des Begriffs „Privatheit“ bezieht daneben allerdings ebenso dezisionale und informationelle Bereiche mit ein, für die eine Ortsmetapher gänzlich ungeeignet ist (Behrendt et al., 2019, S. 1; Bennett, 2008, S. 3).

> Wird also die Vorstellung einer „digitalen“, „virtuellen“ oder „elektronischen Privatsphäre“ artikuliert, ist damit kein (auch kein „virtueller“) Raum, sondern die informationelle Dimension des Privaten gemeint. (Eichenhofer, 2019, S. 166)

Eben diese von Eichenhofer beschriebene Dimension ist es, die maßgebend ist für den Diskurs der Privatheit im 21. Jahrhundert.

---

[2] David Brin ist ein US-amerikanischer Wissenschaftler und Science-Fiction-Autor.

Brin, D. (1998). *The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom?* Print. S. 12.

2.2 Eingriffe in die Privatheit

Auf der einen Seite trug die sorgfältige Zusammentragung und unablässige Wiederholung von Fakten über Sklaverei, Rassendiskriminierung, Folter, Kinderarbeit, Prostitution usw. dazu bei, diese Themen auf die Tagesordnung der Institutionen zu setzen, um somit Veränderungen herbeizuführen (Bennett, 2008, S. 96). Auf der anderen Seite stellt sich Bennett die Frage, was die entsprechenden Fakten für Verfechter des Datenschutzes sind. Was sind die „Schäden", die dokumentiert und schonungslos als unwiderlegbarer Beweis für die Notwendigkeit von Reformen dargestellt werden können? Was ist das Äquivalent der Zeugenaussagen von Menschenrechtsverletzungen? (2008, S. 97).

Eine Verbrennung ist eine durch Hitze verursachte Verletzung und äußert sich durch bestimmte Symptome. Es lassen sich verschiedene Grade der Verbrennung unterscheiden. Wenn ein Arzt eine Verbrennung diagnostiziert, weiß er sofort, wie er oder sie diese am besten behandeln kann. Andere Ursachen können ausgeschlossen werden. Empfehlungen werden ausgesprochen, wie diese Verletzung in Zukunft vermieden werden kann (Calo, 2010, S. 1132).

Im Unterschied hierzu attestiert Bennett, dass diese Art von spezifischer Dokumentation einer direkten Verletzung der Privatheit von Einzelpersonen selten ist und führt dafür folgende Gründe an: Erstens werden viele Eingriffe in die Privatheit oft nicht als solche aufgrund ihrer Asymptomatik erkannt. Ihre Auswirkungen sind eher indirekt und zeigen sich erst, wenn andere Konsequenzen eintreten, wie beispielsweise die Verweigerung eines Kredits, der Erhalt unerwünschter Telefonmarketing-Anrufe, personalisierte Werbeanzeigen, eine ungerechtfertigte Steuerprüfung, oder eine zweite Kontrolle bei der Flughafensicherheit. Die eigentliche Ursache dieser Auswirkungen, der Eingriff in die Privatheit, kann den Betroffenen verborgen bleiben und wird daher nicht als solcher erkannt (Bennett, 2008, S. 97). Dies trifft logischerweise nur auf Eingriffe in die informationelle Dimension des Privaten zu. Hierzu liefert Corn (2020) ein interessantes Gedankenspiel, um die Bedeutung dieser Dimension zu erkennen:

> Imagine you come to work one day and find someone has put a nude picture of you on the wall. You quickly have it removed but the embarrassment and anger lingers. Eventually, even that fades — maybe you even move to a new job where no one knows you as 'the naked person.' Embarrassing, but you recover. For those who have had their personal information stolen, there is no 'but you recover.' It is impossible to fully remove published information from the digital web. Even if you could miraculously convince every legitimate web service to remove your data, you can never convince those who illicitly deal in personal data to erase it. (Corn, 2020)

Im Gegensatz zu einer körperlichen Wunde, die heilt, heilt eine Wunde der digitalen Privatheit nie. Aus diesem Grund, so argumentiert Corn (2020), wird ein schrittweiser regulatorischer Ansatz zum Schutz persönlicher Daten immer scheitern. „We can't wait for a loss, then regulate the circumstances that led to it. By then it is too late." (Corn, 2020)

Weiter ist offensichtlich, dass Verletzungen der Privatheit kein einziges wesentliches Merkmal besitzen, das alle gemeinsam haben (Bennett, 2008, S. 4).

2.3 Die Bedeutung von Privatheit bei der Entscheidungsfindung

Der Rechtsphilosoph Solove trifft mit folgender Aussage einen wunden Punkt in der Debatte um den Schutz der Privatheit: „Privacy seems to be about everything, and therefore it appears to be nothing." (Solove, 2006, S. 479) Obwohl für die einen ein unverzichtbarer Bestandteil westlicher Industriestaaten, für andere ein notwendiges Übel, wird im gesellschaftlichen Diskurs oft aneinander vorbeigeredet.

Auf der allgemeinsten Ebene umfasst die Idee der Privatheit den Wunsch, in Ruhe gelassen zu werden, frei zu sein, selbst zu sein. Dies bedingt frei zu sein von Beeinflussung und der Neugier anderer. Von unaufgeforderter Werbung bis hin zu Eingriffen in den „Raum", in dem intime, persönliche Entscheidungen ohne die Einmischung Dritter getroffen werden (Wacks, 2015, S. 34 f.). Dieses Maß, individuelle Entscheidungsmacht ausüben zu können, definiert ein Individuum in dem Sinne, dass Individuen in dem Maße existieren, in dem sie in der Lage sind, Entscheidungen zu treffen und sich als autonome Wesen darzustellen (PRESCIENT, 2011, S. 20).

2.4 Datenschutz

Privatsphäre wird als pluralistisches Konzept verstanden und von Finn et al. als heterogenes, fließendes und multidimensionales Konzept beschrieben. Dies führt somit unausweichlich dazu, dass – wie soeben beschrieben – aneinander vorbeigeredet wird, wenn Fragen der Privatheit diskutiert werden (Finn et al., 2013, S. 26; Solove, 2006, S. 772). Aus diesem Grund widmet sich der nächste Abschnitt der vorliegenden Arbeit mit den Begrifflichkeiten Privatheit und Datenschutz.

Das Konzept der informationellen Privatsphäre, oftmals synonym mit Datenschutz, entstand in den 1960er und 1970er Jahren etwa zur gleichen Zeit, als der Begriff „data protection“ (abgeleitet vom deutschen Wort Datenschutz) in das englische Vokabular der europäischen Experten aufgenommen wurde.

Der Begriff steht in engem Zusammenhang mit den Informationsverarbeitungsmöglichk eiten von Computern und der Notwendigkeit, Schutzvorkehrungen zu treffen, als in verschiedenen fortgeschrittenen Industriestaaten große nationale Datenintegrationsprojekte ins Auge gefasst wurden. Diese Projekte schürten die Angst vor einer omnipräsenten „Big Brother“-Regierung mit beispiellosen Überwachungsbefugnissen (Bennett, 2008, S. 6).

Ein differenzierter Blick auf die heimische Medienberichterstattung offenbart regelmäßige Schlagzeilen über diverse Datenskandale und räumt jegliche Zweifel aus dem Weg, dass Privatheit heutzutage ein knappes und bedrohtes Gut zu sein scheint (Piegsa & Trost, 2018, S. 7) und unsere Daten mehr denn je dem Kapitalismus als verwertbare Ware zum Opfer gefallen sind.

Am 1. Januar 2010 startete das von der Europäischen Union mitfinanzierte Projekt PRESCIENT. Das Projekt setzte sich zum Ziel, Fragen des Schutzes der Privatsphäre im Zusammenhang mit neu entstehenden Wissenschaften und Technologien zu ermitteln und zu bewerten. Dabei wurde besonderes Augenmerk auf die Entwicklung neuer Instrumente für die Steuerung von Wissenschaft und Technologie gesetzt. Das Projekt zeigt auf, inwiefern die Gesellschaft gespalten ist: Bei der Diskussion über den gesellschaftlichen Wert der Privatheit und dem Datenschutz konkurrieren zwei Denkschulen. Die eine argumentiert, dass „Privatsphäre tot sei“, während die andere sie für ihren sozialen Wert lobt (PRESCIENT, 2011, S. 11).

2.5 Die Bedeutung von Privatheit für Individuum und Gesellschaft

Privatsphäre ist ein Eckpfeiler in demokratisch regierten Staaten. Sie ermöglicht die individuelle Selbstbestimmung, die Autonomie der Beziehungen, die Verhaltensunabhängigkeit, die existenziellen Entscheidungen und die Entwicklung des eigenen Selbst, den spirituellen Seelenfrieden und die Fähigkeit, Macht und Verhaltensmanipulationen widerstehen zu können (Gutwirth, 2002, S. 30). Der Begriff Privatsphäre wird verwendet, um einen als „privat“ abgegrenzten Bereich bzw. eine Sphäre zu beschreiben. In dieser hat beispielsweise eine Frau ohne äußeren Eingriff die Wahl, ob sie abtreiben möchte, oder eine Person ihre Sexualität frei zum Ausdruck bringen kann (Wacks, 2015, S. 35).

Verhaltensmanipulationen äußern sich durch den Eingriff in oben genannten Entscheidungsprozessen von intimen und persönlichen Angelegenheiten (Bennett, 2008, S. 3), in abgegrenzten Bereichen als auch in offenen, grenzenlosen Sphären wie dem World Wide Web. Ein verstörendes Beispiel für Verhaltensmanipulationen beschreibt der US-amerikanische Journalist Duhigg in einem New York Times Artikel im Jahr 2012. Das US-amerikanische Einzelhandelsunternehmen Target sammelte genug Daten über eine Frau, um ihre Schwangerschaft vorherzusagen:

> My daughter got this in the mail he said. ‚She’s still in high school, and you’re sending her coupons for baby clothes and cribs? Are you trying to encourage her to get pregnant?‘ The manager didn’t have any idea what the man was talking about. He looked at the mailer. Sure enough, it was addressed to the man’s daughter and contained advertisements for maternity clothing, nursery furniture and pictures of smiling infants. The manager apologized and then called a few days later to apologize again. On the phone, though, the father was somewhat abashed. ‚I had a talk with my daughter,‘ he said. ‚It turns out there’s been some activities in my house I haven’t been completely aware of. She’s due in August. I owe you an apology.‘ (Duhigg, 2012)

Im Verlauf der Arbeit wird noch näher auf die Schlüsse eingegangen, die aus persönlichen Daten gezogen werden können. Privatheit ist im Weiteren essenziell, um Mitmenschen zu respektieren, zu lieben, ihnen zu vertrauen, Zuneigung für sie zu empfinden, und um uns selbst als Objekte der Liebe, des Vertrauens und der Zuneigung zu betrachten. Privatheit agiert als Kern unserer Vorstellung von uns selbst als Person unter Personen (Wacks, 2015, S. 38). „[P]rivacy is the necessary atmosphere for these attitudes and actions, as oxygen is for combustion." (Fried, 1968, S. 477)

Privatheit stellt somit den „Sauerstoff" zur Verfügung, die Bereiche wie Kreativität, psychologisches Wohlbefinden und die Fähigkeit zu lieben, soziale Beziehungen zu knüpfen und Vertrauen, Intimität und Freundschaft aufzubauen, zum Atmen brauchen und ermöglicht diese in erster Instanz überhaupt erst (Wacks, 2015, S. 38). Oftmals als individuelle Privatheit bezeichnet, bedürfen Freundschaften, Intimität und Vertrauen stets mehr als nur ein Individuum.

Privatheit ist eine entscheidende Grundlage für zwischenmenschliche Beziehungen, für die Gesellschaft selbst und ihre Gruppen und Kategorien von Personen sowie für die Funktionsweise demokratischer politischer Systeme (Raab, 2017, S. 87). „Privatheit lässt sich demnach als sowohl gesellschaftliches wie auch gesellschaftstheoretisches Problem verstehen." (Ochs, 2019, S. 14)

Dennoch wird der Schutz der Privatheit vielerorts als rein individuelles Problem angesehen, doch betreffen die von einem Individuum erzeugten Daten regelmäßig auch die Daten anderer Individuen. Beispielsweise überlappen Informationen über ein soziales Netzwerk oder Standortdaten einer Einzelperson Daten mehrerer Individuen. Dementsprechend kann der Schutz der Privatheit als eine Problemstellung gesehen werden, die bei der Suche nach Antworten auf kollektive Koordination angewiesen ist (Fairfield & Engel, 2015, zit. n. Beyvers, 2018, S. 304).

Regan drückte es 1995 folgendermaßen aus: „[T]echnology and market forces are making it hard for any one person to have privacy without all persons having a similar minimum level of privacy.“ (Regan, 1995, S. 213) Diese Aussage veranschaulicht die Bedeutung von Datenschutz und den Entscheidungen, die tagtäglich dazu von Individuen getroffen werden.

Dabei verhält es sich ähnlich wie mit lebensrettenden Impfungen. Es ist die soziale Verantwortung aller. Wenn kein Wert auf die eigene Privatheit gelegt wird, sollte zumindest anerkannt werden, dass der Schutz der Daten wichtig ist, dass ihm eine interindividuelle Bedeutung zuzuschreiben ist, und, dass notwendige Schritte zum Wohle der Allgemeinheit unternommen werden müssen.

Die Auseinandersetzung mit Privatheit und Datenschutz sind somit Fragen der kollektiven Koordination (Fairfield & Engel, 2015, zit. n. Beyers, 2018, S. 304). Denn schlussendlich erlaubt uns Privatheit „to remove our social mask.“ (Wacks, 2015, S. 38)

Wird im Verlauf der vorliegenden Arbeit somit der Begriff individuelle Privatheit verwendet, so wird diesem stets die Bedeutung für die Gesellschaft subsumiert.

> Erst wenn gleichgerichtete Belange vieler Beteiligten zu einer überindividuellen Einheit verschmelzen, können letztere als zumindest nicht mehr rein private Interessen erscheinen, soweit der Staat diese ‚Interessenhäufung‘ als überindividuelles Ziel verfolgt. (Beyvers, 2018, S. 190)

2.6 Der Verfall der Privatheit

In der westlichen politischen Philosophie geht die erste Konzeptualisierung der privaten Sphäre im Gegensatz zur öffentlichen Sphäre auf die Antike zurück. Die erste historische Vorstellung von Öffentlichkeit im Sinne einer verallgemeinerten Vorstellung von anderen Menschen als Quelle von Verpflichtungen und Autorität entstand in der antiken griechischen Demokratie (PRESCIENT, 2011, S. 19). Erst im 16. Jahrhundert wurde der Begriff des „Privaten“ von der deutschen Sprache geprägt. Zu dieser Zeit bezeichnete er die Bereiche des Lebens, die vor einem Eingriff der Herrschaftsgewalt des Staates und der Öffentlichkeit geschützt waren (Westermann et al., 2018, S. 4).

Theoretische und rechtliche Diskussionen über die Beziehung zwischen Technologie und Privatheit beginnen hingegen erst in den 1890er Jahren, als tragbare Fotoausrüstungen aufkamen, die für die allgemeine Bevölkerung zugänglich waren. Zur selben Zeit fand der akademische Diskurs über individuelle Privatsphäre seinen Anfang. Er geht auf einen Artikel der Harvard Law Review von Warren und Brandeis (1890) zurück.

> Instantaneous photographs and newspaper enterprises have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that ‚what is whispered in the closet shall be proclaimed from the house-tops’. (Warren & Brandeis, 1890, S. 193)

Die ehemaligen Kanzleipartner sahen in der Berichterstattung der Presse und der einfachen Verbreitung und Veröffentlichung von Fotografien eine Bedrohung für den Schutz der Privatsphäre.

> These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone. (Warren & Brandeis, 1890, S. 205)

Die beiden Juristen verstanden unter Privatsphäre das Recht, allein gelassen zu werden („the right to be let alone“). Laut Warren und Brandeis sei ein Angriff auf das Recht auf Privatsphäre ein Angriff auf die Freiheit des Einzelnen (Warren & Brandeis, 1890). Und auch die zeitgenössische Definition der Privatheit ist mit dem Konzept der Autonomie verbunden, d.h. mit der Fähigkeit, Abstand zwischen uns und anderen zu schaffen (PRESCIENT, 2011, S. 19).

In den 1970er und frühen 1980er Jahren wurde allgemein davon ausgegangen, dass Problematiken bezüglich des Schutzes der Privatheit von zentralen und koordinierten Kontrollmechanismen persönlicher Informationen herrührten, welche von Regierungen in westlichen Industriestaaten in diskreten großangelegten distinkten Datenbanken gespeichert wurden (Bennett, 2008, S. 14).

Soweit privatwirtschaftliche Organisationen ein Thema waren, konzentrierten sich Verfechter der Privatheit auf die sichtbarsten und am monopolistischten Unternehmen und auf den Gegenstand der meisten Beschwerden, nämlich die Verbraucherkreditbranche (Bennett, 2008, S. 14).

In den 1980er und 1990er Jahren war es jedoch offensichtlich, dass der private Sektor ebenso viel Aufmerksamkeit verdiente wie der öffentliche, und dass es immer schwieriger wurde, den Unterschied zwischen beiden zu erkennen (Bennett, 2008, S. 14).

Vor allem seit der Entwicklung von innovativen Technologien zum Auffinden von Informationen und zur Kommunikation im Internet hat sich das Verständnis von Privatsphäre dramatisch verändert (Weigend, 2017, S. 44). Denn die Fähigkeit, Abstand zur Wahrung der Privatsphäre zu schaffen, mag im Sinne der Ortsmetapher durchaus gegeben sein, scheint in hochdigitalisierten Gesellschaften in aller Bedeutungsbreite des Begriffes allerdings eingeschränkt zu sein.

In einer hochdigitalisierten Gesellschaft kommt auch der Erwachsenenbildung eine besondere Rolle zu: Ob mehr eLearning-Angebote, vermehrtes digitales Arbeiten oder die Entwicklung von Standards für digitale Erwachsenenbildungsangebote: Die Digitalisierung hat die Erwachsenenbildung fest im Griff. Trotzdem stimmen in einer von Gugitscher und Schlögl durchgeführten Studie allerdings nur knapp mehr als ein Drittel aller befragten Erwachsenenbildner und Erwachsenenbildnerinnen der Aussage zu, dass sie Bedarf nach Maßnahmen zum Datenschutz und zur Datensicherheit sehen (Gugitscher & Schlögl, 2021, S. 32).

Weigend (2017) argumentiert, dass sich Schaffung und Abschaffung des Konzeptes der Privatheit innerhalb von nur wenigen Jahrhunderten vollzogen. Während sie in den letzten einhundert Jahren gepriesen wurde, verfällt ihr Wert zunehmend (Weigend, 2017, S. 47).

2.7 Definitionsversuche

Westliche Philosophen sehen sich mit der Herausforderung konfrontiert, eine umfassende und zufriedenstellende Definition von Privatheit zu finden. Es gibt eine große Meinungsvielfalt darüber, was Privatheit bedeutet, wie sie geschützt werden kann, und wie sie zu bewerten ist (PRESCIENT, 2011, S. 19).

Der Begriff der Privatsphäre und der Privatheit ist oftmals verbunden mit dem der Autonomie. Sie beinhaltet die Fähigkeiten, unsere Überzeugungen und Wünsche ohne Einfluss Dritter zu entwickeln, ein gewisses Maß an Kontrolle über die inneren Sphären des Selbst zu behalten. Alan Westin, Vater des modernen Datenschutzrechtes, beschreibt Privatheit als „the ‚claim' of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." (Westin, 1967, zit. n. Wacks, 2015, S. 42)

Gutwirth behauptete 2002, der Begriff der Privatsphäre entziehe sich dem festen Griff all jener, die versuchen, ihn zu greifen. Selbst wenn er durch zusätzliche Modifikatoren wie „unsere" oder „individuelle" Privatsphäre in die Enge getrieben wird, findet er immer noch einen Weg, sich zu entziehen (Gutwirth, 2002, S. 30).

Eine allgemein anerkannte Definition der Begrifflichkeiten Privatheit und Privatsphäre bleibt demnach der Wunsch aller Akademiker und Akademikerinnen. Aufgrund der vielfältigen und sich verändernden Dimensionen, die sich aus den verschiedenen Disziplinen ergeben, die sich mit dem Konzept befassen, ist es nicht möglich, das Wesen des Privaten bzw. den ontologischen Kern des Konzepts zu erfassen (PRESCIENT, 2011, S. 57). Aus diesem Grund ist es zielführend, Privatheit zu kategorisieren und die Kategorien zu bestimmen, welche zur Beantwortung der eingangs gestellten Forschungsfrage relevant sind.

2.8 Arten von Privatsphäre

Finn et al. veröffentlichten 2013 eine auf Clarkes vier Kategorien der Privatsphäre aufbauende nützliche, logische, strukturierte und kohärente Typologie, die dabei hilft, Studien zum Datenschutz und der Privatheit einordnen zu können.

Clarke definierte 1997 vier Kategorien von Privatheit. Diese lauten wie folgt:

- Privacy of the person
- Privacy of personal behaviour
- Privacy of personal communication
- Privacy of personal data (Clarke, 1997).

Aufgrund der rasanten technologischen Entwicklung sind Clarkes Kategorien allerdings nicht mehr ausreichend, um sämtliche technische Bedrohungen individueller Privatheit einzuordnen. Technologien wie Ganzkörperscanner, RFID-fähige Reisedokumente, unbemannte Luftfahrzeuge oder DNA-Sequenzierungstechnologien der zweiten Generation erfordern eine Erweiterung der vier Kategorien (Finn et al., 2013, S. 7).

Finn et al. stellen 2013 infolgedessen drei weitere Kategorien von Privatheit vor und erweitern die Kategorie „privacy of personal data“ um „privacy of personal data and image“:

- Privacy of thoughts and feelings
- Privacy of location and space
- Privacy of association (including group privacy) (Finn et al., 2013, S. 9).

Diese Kategorien dienen als Sinnbild, inwiefern sich Privatheit als Grundwert bereits im Verfall befindet, wenn sogar Gedanken und Gefühle bereits zur kapitalisierbaren Ware geworden sind. Im Folgenden wird im Detail auf die Kategorien eingegangen und erläutert, aus welchen Gründen ein Schutz dieser tagtäglich an Bedeutung gewinnt.

2.8.1 Die Privatsphäre der Person (Privacy of the person)

Auch als „körperliche Privatsphäre“ bezeichnet, bezieht sie sich speziell auf die Integrität des Körpers einer Person und umfasst das Recht, Körperfunktionen und Körpermerkmale wie genetische Codes und biometrische Daten privat zu halten. Dabei wird der Schutz vor körperlichen Eingriffen, einschließlich Folter, medizinischer Behandlung, der zwangsweisen Bereitstellung von Proben von Körperflüssigkeiten und Körpergewebe und die Aufforderung zur biometrischen Messung, abgedeckt. Für Clarke (1997) ist die Privatsphäre der Person durch viele medizinische Überwachungstechnologien und -praktiken gefährdet. Die Privatsphäre der Person wird als förderlich für das individuelle Freiheitsgefühl angesehen und hilft, eine gesunde, gut angepasste demokratische Gesellschaft zu unterstützen (Clarke, 1997; Finn et al., 2013, S. 7 f.).

2.8.2 Die Privatsphäre des persönlichen Verhaltens (Privacy of personal behaviour)

Wird von Finn et al. (2013) erweitert um die Privatsphäre des persönlichen Verhaltens und Handelns. Sie beinhaltet den Schutz vor der Offenlegung von sensiblen persönlichen Angelegenheiten wie religiöse Praktiken, sexuelle Vorlieben, politische Aktivitäten und Gewohnheiten. Clarke (1997) attestiert, dass ein räumliches Element in der Privatsphäre des persönlichen Verhaltens enthalten ist, in dem Menschen ein Recht auf privaten Raum haben, in dem bestimmte Aktivitäten ausgeübt werden können fernab einer Aufzeichnung und Speicherung von Informationen über diese Aktivitäten. Dies impliziert das Recht, frei von systematischer Überwachung im öffentlichen Raum zu sein (Clarke, 1997; Finn et al., 2013, S. 7 f.).

2.8.3 Die Privatsphäre der persönlichen Kommunikation (Privacy of personal communication)

Sie inkludiert den Schutz der Kommunikation und zielt darauf ab, das Abhören von Unterhaltungen zu vermeiden. Dabei miteingeschlossen ist das Abfangen von Postsendungen und Paketen, der Einsatz von Wanzen, Richtmikrofonen, das Abhören von Telefonen, die Aufzeichnung von drahtloser Kommunikation und der Zugriff auf E-Mail- und Chat-Nachrichten. Dieses Recht wird von vielen Regierungen durch die Forderung anerkannt, dass generelle Kommunikationsüberwachung von einer Justizbehörde beaufsichtigt werden muss. Dieser Aspekt der Privatsphäre kommt Individuen und der Gesellschaft gleichermaßen zugute, weil er eine freie Diskussion einer Vielzahl von Ansichten und Einstellungen ermöglicht (Clarke, 1997; Finn et al., 2013, S. 7 f.).

2.8.4 Die Privatsphäre der personenbezogenen Daten (Privacy of personal data)

Die Autoren und Autorinnen fügen der Kategorie des Schutzes personenbezogener Daten die Erfassung von Bildern hinzu, da diese u. a. von der Europäischen Union im Rahmen der Datenschutzrichtlinie von 1995 und von der Europäischen Datenschutzgrundverordnung als eine Art personenbezogener Daten betrachtet werden. Die Privatsphäre von Daten und Bildern beinhaltet das Anliegen sicherzustellen, dass die Daten von Einzelpersonen nicht automatisch für andere Einzelpersonen und Organisationen verfügbar sind und dass die Menschen ein erhebliches Maß an Kontrolle über diese Daten und ihre Verwendung ausüben können. Eine solche Kontrolle über die persönlichen Daten stärkt das Selbstvertrauen und ermöglicht es dem Einzelnen und der Einzelnen, sich selbstbestimmt zu fühlen (Clarke, 1997; Finn et al., 2013, S. 7 f.).

2.8.5 Die Privatsphäre der Gedanken und Gefühle (Privacy of thoughts and feelings)

Fallstudien von Finn et al. (2013) zeigen, dass neue und aufkommende Technologien das Potenzial haben, sich auf die Gedanken und Gefühle von Individuum auszuwirken. Menschen haben ein Recht darauf, ihre Gedanken und Gefühle nicht mit anderen zu teilen und dass diese Gedanken und Gefühle nicht offengelegt werden. Der und die Einzelne sollte das Recht haben zu denken, was er/sie will. Die Privatsphäre der Gedanken und Gefühle kann von der Privatsphäre der Person unterschieden werden, so wie der Geist vom Körper unterschieden werden kann. In ähnlicher Weise kann zwischen Gedanken, Gefühlen und Verhalten unterschieden werden. Ein Gedanke führt nicht automatisch zu

einem Verhalten. Ebenso kann sich gedankenlos verhalten werden (Clarke, 1997; Finn et al., 2013, S. 8 f.).

2.8.6 Die Privatsphäre in Bezug auf Ort und Raum (Privacy of location and space)

Nach der Auffassung von Finn et al. (2013) von Privatsphäre in Bezug auf Ort und Raum hat der Einzelne oder die Einzelne das Recht, sich im öffentlichen oder halb-öffentlichen Raum zu bewegen, ohne identifiziert, verfolgt oder überwacht zu werden. Diese Auffassung von Privatsphäre umfasst sowohl ein Recht auf Einsamkeit als auch ein Recht auf Privatsphäre in Räumen wie beispielsweise eine Wohnung, ein Auto oder Sanitäranlagen. Eine solche Auffassung von Privatsphäre hat einen sozialen Wert. Wenn sich Bürger und Bürgerinnen frei im öffentlichen Raum bewegen können, ohne Angst vor Identifizierung, Überwachung oder Verfolgung zu haben, haben sie das Gefühl, in einer Demokratie zu leben und Freiheit zu erleben. Diese beiden subjektiven Gefühle tragen zu einer gesunden, gut funktionierenden Demokratie bei. Darüber hinaus fördern sie die Versammlungsfreiheit, die beide für eine funktionierende Demokratie unerlässlich sind. Dieser Aspekt der Privatsphäre war 1997, als Clarke über die vier Kategorien schrieb, nicht akut bedroht, hat sich allerdings mit dem technologischen Fortschritt in den letzten 24 Jahren maßgeblich verändert (Clarke, 1997; Finn et al., 2013, S. 9).

2.8.7 Vereinigungsfreiheit (Privacy of association)

Die letzte Kategorie von Privatsphäre, die Finn et al. (2013) identifizieren, ist die Privatsphäre der Assoziation und schließt die Gruppenprivatsphäre mit ein. Sie betrifft das Recht, sich mit Personen zu treffen, ohne dabei überwacht zu werden. Dies ist notwendig für eine demokratische Gesellschaft, da es die Redefreiheit, einschließlich der politischen Rede, fördert, ferner die Freiheit der Religionsausübung und andere Formen der Vereinigung. Die Gesellschaft profitiert von dieser Art von Privatsphäre, da eine große Vielfalt von Interessengruppen gefördert wird, was dazu beitragen kann, dass marginalisierte Stimmen, von denen einige auf mehr politischen oder wirtschaftlichen Wandel drängen, gehört werden. Dieser Aspekt der Privatsphäre wurde von Clarke nicht berücksichtigt, und eine Reihe von neuen Technologien kann sich dabei negativ auf diese Kategorie auswirken (Clarke, 1997; Finn et al., 2013, S. 9).

2.9 Ein düsterer Ausblick

In einem Abschlussbericht des PRESCIENT Projekts haben die Autoren und Autorinnen eine detaillierte Tabelle über die von Clarke (1997) entworfenen Kategorien, ihre Grenzen, Beispiele, Vorteile für Individuen als auch auf gesamtgesellschaftlicher Ebene und die Gefahren bei Einschränkung derselben erstellt (PRESCIENT, 2011, S. 63 f.).

Für den weiteren Verlauf der vorliegenden Arbeit und die Bearbeitung der eingangs gestellten Forschungsfrage macht eine Fokussierung auf die beiden Kategorien „Privacy of personal communication“ und „privacy of personal data“ Sinn. Durch die enge Kopplung zwischen Informatik und Kommunikation, insbesondere seit den 1980er Jahren, sind diese beiden Kategorien eng miteinander verknüpft. Gemeinhin werden sie heutzutage unter dem Begriff Datenschutz subsumiert (Holvast, 1993, zit. n. Kokolakis, 2017, S. 123; Rosenberg, 1992, zit. n. Kokolakis, 2017, S. 123).

In einer hochdigitalisierten Welt lassen sich mittlerweile Daten in allen Lebensbereichen erheben, speichern, verarbeiten und verbreiten. Nicht nur personenbezogene Daten können eine Gefahr für die Privatheit darstellen. Dementsprechend sind sämtliche Kategorien der Privatsphäre davon bedroht, in einer Informationsgesellschaft unterlaufen zu werden.

3 Daten im Informationszeitalter

„Und wenn du lang genug in einen Abgrund blickst, dann blickt der Abgrund auch in dich hinein.“

Friedrich Nietzsche[3]

Dass der technologische Wandel unser Leben verändert, darüber besteht Konsens. Ebenso offensichtlich ist, dass dieser für die weitere Entwicklung der Gesellschaft und „für die Chancen individueller Emanzipation zentrale Relevanz besitzt.“ (Faulstich, 2018, S. 947)

Bridle vertritt die Ansicht, dass sich unsere Gesellschaft rascher entwickelt als die Fähigkeit, diese Entwicklungen einzuordnen und abzuschätzen. „Over the last century, technological acceleration has transformed our planet, our societies, and ourselves, but it has failed to transform our understanding of these things.“ (Bridle, 2018, S. 2)

Faulstich unterstreicht die Aussage und fügt hinzu, dass es mehr als ungewiss ist, in welche Richtungen sich die derzeitigen gesellschaftlichen Entwicklungen bewegen und welche Konsequenzen das für die Möglichkeit von Mündigkeit mit sich bringt (Faulstich, 2018, S. 947), denn der Aufstieg des World Wide Web hat nicht nur die Art und Weise, wie wir kommunizieren, handeln, uns präsentieren und wie wir lernen radikal verändert, sondern das Internet ist eine Umgebung, in der viele Erwachsene zunehmend, freiwillig oder unausweichlich leben (Wacks, 2015, S. 135).

Keineswegs verwunderlich ist, dass der Begriff der Digitalisierung längst Einzug in die Bildungsbranche und in das Feld der Erwachsenen- und Weiterbildung gehalten hat. Innovationen mit disruptivem Potential wurden einerseits erhofft und andererseits befürchtet. Digitalisierung nimmt ihren Einfluss sowohl auf die Programm- und Angebotsplanung inhaltlich und methodisch, und andererseits führt der verstärkte Einsatz von digitalen Technologien am Arbeitsplatz zu einem erhöhten Bildungsbedarf und beeinflusst infolgedessen Lerninhalte als auch Themen von Bildungsangeboten für Erwachsene (Dörner et al., 2020, S. 182).

[3] Nietzsche, F. (1886). *Jenseits von Gut und Böse*. 11. Aufl.. ed. 1991. Print. Kröners Taschenausgabe. Aph. 146.

Die Digitalisierung verändert nicht nur die Art und Weise, wie Wirtschaft, Politik, Erziehung und Bildung verstanden werden, sie hat auch einen enormen Einfluss auf die Privatheit der Debatte um den Datenschutz (Thies, 2018, S. 137). In drastischeren Worten formuliert es die Wirtschaftswissenschaftlerin Zuboff so:

> Der Vormarsch der Digitalisierung sorgt für eine Neudefinition auch des letzten Aspekts unserer eben noch so vertrauten Welt, ohne uns auch nur eine Chance zu lassen, eine durchdachte Entscheidung darüber zu fällen. Wir loben die vernetzte Welt der vielschichtigen Bereicherung unserer Möglichkeiten und Aussichten wegen über den grünen Klee, aber da sie uns der Geborgenheit einer berechenbaren Zukunft beraubt, beschert sie uns auch eine Vielzahl neuer Ängste, Gefahren und Formen von Gewalt. (Thies, 2018, S. 18)

Unter Digitalisierung wird ein Prozess verstanden, durch den analoge Entitäten in digitale transformiert werden (Thies, 2018, S. 138). Piegsa und Trost unterscheiden zwischen den Begrifflichkeiten Digitalisierung und Digitalität. Während unter letzterer „aus technischer Sicht zunächst eine neue Stufe der elektronischen Datenherstellung und -verarbeitung“ verstanden (Thies, 2018, S. 10) und von Thies als „das technische Rückgrat der Globalisierung“ (Thies, 2018, S. 138) bezeichnet wird, ist erstere eine Nominalisierung für „deren kulturelle und soziale Niederschläge.“ (Piegsa & Trost, 2018, S. 10) Allerdings steht viel zu oft weniger der Prozess der Digitalisierung selbst im Vordergrund „als vielmehr seine Indienstnahme für kapitalistische Verwertungslogiken.“ (Rummler, 2020, S. 33)

3.1 Informations- / Wissensgesellschaft

In der Geburtsstunde des Internets am 12. März 1989, als der britische Informatiker Tim Berners-Lee am CERN (Conseil européen pour la recherche nucléaire) in Genf konkrete Vorschläge für ein grenzüberschreitendes elektronisches Netz einreichte, welches Wissenschaftlern aus aller Welt den Datenaustausch ermöglichen sollte, war der Begriff – vor allem in den 1990er Jahren – verbunden mit Hoffnungen auf eine befreiende und emanzipatorische Kraft und neuen Möglichkeiten des Informationsaustausches und der Kommunikation. Mittlerweile haben sich diese Hoffnungen in vielen Bereichen verflüchtigt und sind der Ernüchterung gewichen. Gar als größte Bedrohung für die

Privatheit wird das Internet beschrieben (Banse et al., 2006, zit. n. Grunwald, 2018, S. 40; Matzner, 2016, zit. n. Piegsa & Trost, 2018, S. 11 & Thies, 2018, S. 138).

Wir leben in einer Zeit, die sehr stark auf Information und Wissen ausgerichtet ist. Der gleichberechtigte Zugang zu Informationen und der freie Austausch von Ideen sind große Herausforderungen der modernen Informations- und Kommunikationstechnologien. Diese entwickeln und verbreiten sich in einem Tempo, welches es schwierig macht, die sozialen und ethischen Auswirkungen ihrer Entwicklung und Nutzung vorherzusagen oder auch nur zu beschreiben (PRESCIENT, 2011, S. 46).

Die Pandemie, welche die Welt zum Zeitpunkt dieser Arbeit noch fest im Griff hat, hat diesen technologischen Wandel und das Voranschreiten der Digitalisierung noch einmal beschleunigt und den Aufruf nach technischem Grundverständnis, digitaler Kompetenz und kritischer Medienbildung in der Erwachsenen- und Weiterbildung verschärft. Aufgrund dessen soll im folgenden Abschnitt auf die Begrifflichkeiten Daten, Information und Wissen und deren Relationen zueinander näher eingegangen werden.

3.1.1 Informationsgesellschaft

Die Bezeichnung von wohlhabenden Industriegesellschaften als Informationsgesellschaf-ten begann sich nach Ende des Zweiten Weltkriegs zu etablieren. In der unmittelbaren Nachkriegszeit gab es bedeutende Fortschritte bei der Anwendung elektronischer Informationssysteme zur Unterstützung der Organisation und Kontrolle von Informationen für militärische und nicht-militärische Zwecke. Viele der Schlüsselideen waren jedoch schon lange vorher im Umlauf. Bereits Mitte des 15. Jahrhunderts wurde der Begriff „Information“ erstmalig für eine Anweisung oder „Tatsache“ verwendet (Mansell, 2012, S. 38).

Die Zusammenführung von Information, bestehend aus Daten, welche sich wiederum aus Bits und Bytes zusammensetzen und Information als verwertbares Wissen, ist schlussendlich ein Merkmal der Erkenntnistheorie der ökonomischen Disziplin. Die Ursprünge einer Theorie der modernen Gesellschaft als Wissensgesellschaft liegen Ende der 1960er, Anfang der 1970er Jahre, als die beiden Begriffe Information und Wissen als Synonyme verwendet wurden (Kade et al., 2018, S. 277; Mansell, 2012, S. 41).

Der Wechsel „einer Güter produzierenden Industriegesellschaft in eine auf Dienstleistungen basierende postindustrielle Gesellschaft“ führt zu einer Fokussierung von Wissen und Information als Wirtschaftsfaktor Nummer Eins (Kade et al., 2018, S. 277). Aus diesem Grund war der Wechsel von den Debatten über die „Informationsgesellschaft“ zur „Wissensgesellschaft“ für viele Ökonomen ein leichter (Mansell, 2012, S. 43).

Hintergrund dieses Verständnisses ist das Konzept der „Informationsökonomie“, ein Zweig der neoklassischen mikroökonomischen Theorie, der untersucht, wie sich Informationen auf die wirtschaftliche Entscheidungsfindung auswirken. Im Kontext dieser Arbeit befasst sich die Informationsökonomie hauptsächlich mit zwei Themen: Informationsasymmetrie und Informationsgüter.

Informationsasymmetrien beziehen sich auf Entscheidungen in Transaktionen, bei denen eine Partei über mehr oder bessere Informationen verfügt als die andere. Dadurch entsteht ein Machtungleichgewicht bei Transaktionen. Für George J. Stigler, einen der wichtigsten Vertreter der Chicagoer Schule der Wirtschaftswissenschaften und der geistige Vater der Informationsökonomie (Nobelpreisträger 1982), ist die Privatsphäre ein Faktor, der Informationsasymmetrien verstärkt, weil eine Partei (persönliche) Informationen zurückhalten kann, die für die Entscheidungsfindung der anderen Partei wichtig sein könnten (Stigler, 1980, zit. n. PRESCIENT, 2011, S. 15). Das Vorhandensein solcher Informationsasymmetrien führt zu Problemen wie Moral Hazard (in den Wirtschaftswissenschaften liegt Moral Hazard vor, wenn ein Unternehmen einen Anreiz hat, sein Risiko zu erhöhen, weil es nicht die vollen Kosten dieses Risikos trägt) und adverse Selektion (adverse Selektion beschreibt, dass Teilnehmer mit Schlüsselinformationen selektiv an Geschäften auf Kosten anderer Parteien teilnehmen können, die nicht über dieselben Informationen verfügen).

Problematisch dabei ist, dass die orthodoxe neoklassische Theorie den Datenschutz aus diesen Gründen als unerwünschte Marktstörung ablehnt (PRESCIENT, 2011, S. 15). Im weiteren Verlauf der Arbeit wird eine Typologie aufgezeigt, die eindeutig zwischen den synonym verwendeten Begriffen Wissen und Information differenziert.

Nicht nur deswegen ist die Verwendung des Begriffes der Wissensgesellschaft mit Vorsicht zu genießen und in Zeiten von postfaktischer Politik und Fake News kaum haltbar, wie der folgende Abschnitt näher erläutert. „Man sollte Akademikern kaum sagen müssen, dass Information eine wertvolle Ressource ist: Wissen ist Macht." (Stigler, 1961, zit. n. Mansell, 2012, S. 41) Und auch Weigend konstatiert, dass sich Information im Zentrum aller Macht befindet (Weigend, 2017, S. 11).

3.1.2 Wissensgesellschaft

Als zentrale Ressourcen gesellschaftlicher und wirtschaftlicher Entwicklung dienen Information und Wissen, welche auf dem Rücken des technologischen Fortschritts getragen werden, als Treiber des Wirtschaftswachstums in Informations- und Wissensgesellschaften (Mansell, 2012, S. 42; Stang & Schüller-Zwierlein, 2018, S. 858). Können wir somit den Sprung von Informations- zur Wissensgesellschaft wagen oder bleibt es ein langersehnter Traum der Menschheit?

Im Zentrum einer Wissensgesellschaft stehen die Fragen: „Was ist Wissen, wie gehen wir damit um und wie wenden wir es an?" (Mainzer, 2002, S. 15) Müller plädiert dafür, dass die Wissensgesellschaft ein Mythos bleibt, denn ein Erreichen dieser aus dem gegenwärtigen Zustand der Digitalisierung ist in weite Ferne rückt. Die oben genannten Fragen, mit denen sich Philosophen bereits seit Jahrtausenden beschäftigen, zielen auf ein tieferes Verständnis ab als die rein technisch-maschinelle Umsetzung des Wissens (Mainzer, 2002, S. 15; Müller, 2020, S. 28) und den simplen Datenaustausch im Internet.

Für eine Wissensgesellschaft bedarf es der „subjektive[n] und kognitive[n] Anreicherung [von] Fakten [, welche] durch Algorithmen zu Wissen transformiert werden, die den persönlichen Zwecken von Individuen dienen und von diesen als ihr persönliches Wissen für ihren Zweck akzeptiert werden." (Müller, 2020, S. 28) Von diesem Zustand ist unsere Gesellschaft allerdings weit entfernt. Der Überfluss an Information und die Pluralität der Weltsichten, welche jederzeit im Internet abrufbar ist, produziert keineswegs eine kohärente übereinstimmende Realität mehr, sondern eine gespaltene Welt, welche sich durch fundamentalistisches Beharren auf vereinfachte Narrative, Verschwörungstheorien und postfaktische Politik auszeichnet. Dieser Gegensatz führt dazu, dass der Wert dem Wissen beigemessen und zerstört wird durch genau diesen Überfluss an Wissen (Bridle, 2018, S. 10 f.).

Müller kommt somit zu dem Schluss, dass unter keinen Umständen von einer „visionäre[n] Wissensgesellschaft [ausgegangen werden kann], sondern sehr viel profaner – eine ökonomisch motivierte Datengesellschaft“ (Müller, 2020, S. 29) die passendste Beschreibung der gegenwärtigen Gesellschaftsform ist.

3.1.3 Datafizierung

Das Internet, wie wir es heute können, wurde nicht primär für unternehmerische Zwecke entwickelt, sondern entstand aus der Grundlagen- und Militärforschung. Dennoch hat sich der Kapitalismus dieses Medium einverleibt und dient als mächtiger Produktions- und Reproduktionsfaktor (Rummler, 2020, S. 28). Als Kern der Digitalisierung, dem das Internet als Grundgerüst zur Verfügung steht, kann der Begriff der Datafizierung verstanden werden. Er steht für die Symbiose zwischen technischem und sozialem bzw. gesellschaftlichem Wandel. Datafizierung beschreibt die Infizierung sämtlicher Lebensbereiche mit Daten. Alles kann datenförmig erfasst werden und wird auch erfasst (Häußling et al., 2017, S. 2). Dabei wird Daten eine stetig wachsende Bedeutung zugeschrieben. Müller erinnert jedoch daran, dass Daten nicht zwangsläufig Wissen erzeugen:

> Immer zweifelhafter wird, ob die Daten der Wahrheit entsprechen, da allgemeine akzeptierte Wahrheiten und das Vertrauen in Autoritäten auf dem Rückzug sind. Den Fortschritten in den zivilisatorischen Errungenschaften wie freie Rede und Meinungsbildung stehen Lügen, Hassbeiträge, Filterblasen und Menschenverachtung ohne die gewohnten Möglichkeiten zur Verteidigung gegenüber. (Müller, 2020, S. 2)

Welche Rollen spielen Daten bei der Informationsgewinnung und Wissensgenerierung in einer Informations- bzw. Wissensgesellschaft und wie lässt sich der Begriff von anderen Begrifflichkeiten unterscheiden?

3.2 Die Wissenspyramide

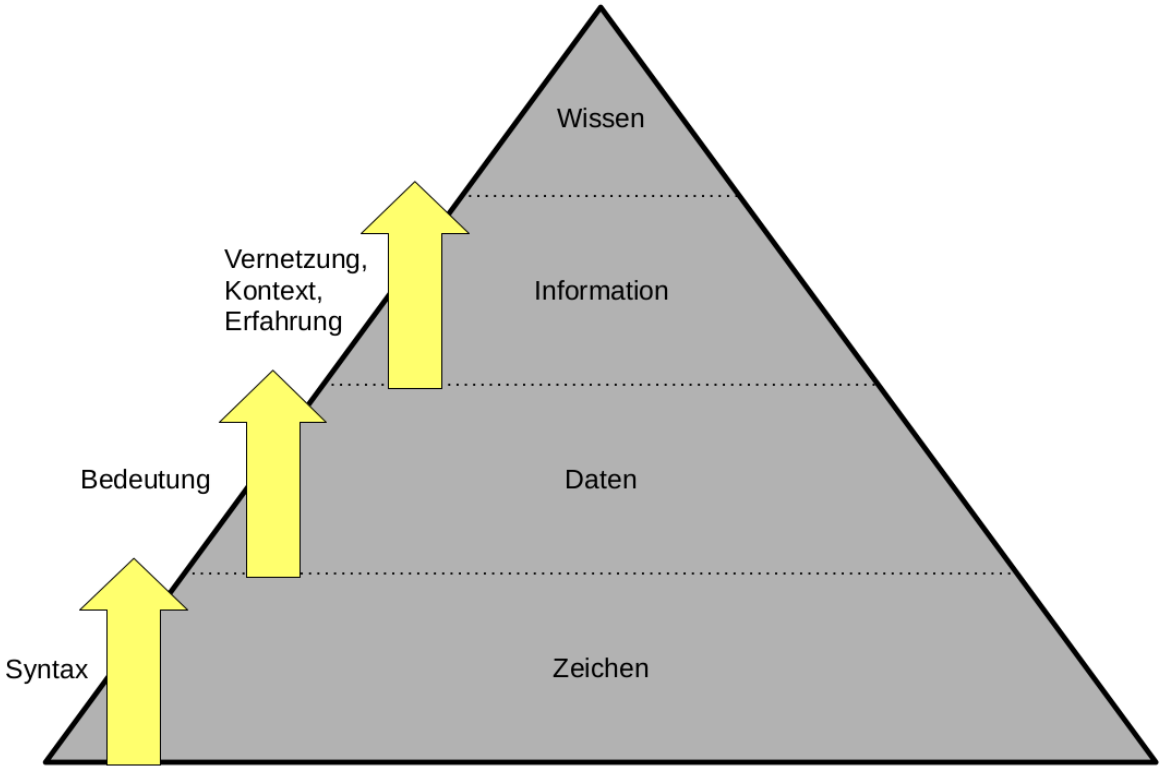

Abbildung 1:Wissenspyramide. Forst, 1999

Forst entwickelte 1999 ein deskriptives Modell, um Zeichen, Daten, Information und Wissen in Relation zu setzen. Ihre Wissenspyramide geht davon aus, dass Wissen an der Spitze einer Pyramide steht und sich aus den unterliegenden Ebenen zusammensetzt (Forst, 1999).

Prietl und Houben (2018) beschreiben Daten als „methodisch absichtsvoll reduzierte und technisch, medial oder materiell prozessierte Wirklichkeitsausschnitte." (Prietl & Houben, 2018, S. 18) Als Ausschnitte der Wirklichkeit zielen Daten somit stets darauf ab intersubjektiv anschlussfähig zu sein und bleiben trotz aller Bemühungen dennoch stets interpretationsbedürftig (Prietl & Houben, 2018, S. 18.).

Daten entstehen allerdings erst durch die Kombinationen von elementaren Zeichen zu zusammengesetzten Zeichen und können dabei als undifferenzierte Beobachtungen bezeichnet werden. Als zusammenhangslose Fakten ohne Kontext werden diese erst durch ihre Interpretation zu Informationen.

Kuneva, ehemalige Kommissarin für Verbraucherschutz in der Europäischen Union, verglich Daten mit Öl (Maydorn, 2014, zit. n. Müller, 2020, S. 29). Auch Palmer bediente sich demselben Vergleich und beschrieb Daten als Rohöl. Es ist wertvoll, allerdings bedarf es dem Raffinierungsprozess, um als Gas, Kunststoff oder andere Chemikalien genutzt zu werden (Palmer, 2006). Daten müssen dementsprechend erst kategorisiert und klassifiziert werden, um eine geordnete Struktur aufzuweisen, um daraus profitable Informationen ableiten zu können (Pfiffner & Stadelmann, 1999, S. 140).

Um aus Informationen wiederum Wissen generieren zu können, bedarf es einer Einordnung in einen Zweck- oder Zielzusammenhang (Müller, 2003, zit. n. Müller, 2020, S. 28). Folgendes Beispiel erläutert den Zusammenhang:

> So lassen sich aus einem Zeichenvorrat wie z. B. den Ziffern ‚1', ‚8', ‚1' nach syntaktischen Regeln Daten wie z. B. die Zahl 1,81 erzeugen, die im Kontext des Devisenkurses zu einer Information, wie z. B. $1 = DM 1,81, für einen Reisenden wird. Vernetzen wir diese Information mit den Gesetzen des Devisenmarkts, so erhalten wir ökonomisches Wissen, um z. B. bei einem Geschäftsabschluss in USA erfolgreich handeln zu können. (Mainzer, 2002, S. 15 f.)

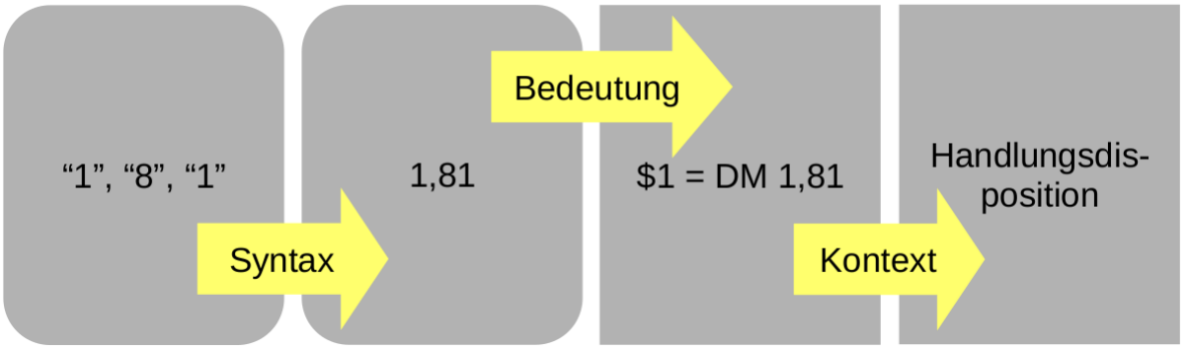

Abbildung 2: Wissensgenerierung aus Daten. Quelle: Eigene Darstellung des Verfassers angelehnt an Mainzer, 2002, S. 7

Aus Daten können somit kontextvarierend Informationen gewonnen werden, welche wiederum durch eine Vernetzung mit Erfahrungen zu Handlungsdispositionen werden und eingesetzt werden können, um Probleme zu lösen und Handlungen zu planen – Wissen entsteht (Mainzer, 2002, S. 15).

Bereits Thomas Hobbes schrieb in seinem Werk „Leviathan“ im Jahr 1651: „Scientia potentia est.“ In einer Wissensgesellschaft mag der Ausspruch seine Gültigkeit behalten, in einer Informations- bzw. Datengesellschaft sind es jedoch die Daten, welche denjenigen, die sie aufzeichnen und Informationen daraus gewinnen, eine enorme Macht in die Hand geben. So ist nicht der Leviathan das Unwesen in einer „ökonomisch motivierte[n] Datengesellschaft“ (Müller, 2020, S. 29), sondern eine Datenkrake, die ihre Tentakel über die Welt ausbreitet.

Daraus ergibt sich für Individuen, welche in einer „Datengesellschaft“ grundsätzlich auf der einen Seite als Nutzer und Nutzerinnen auftreten, die Problematik, auf der anderen Seite benutzt zu werden. Zwischen diesen zwei Modi tut sich ein schmaler Grat auf. Eine andere Beschreibung für diesen Umstand ist Missbrauch. Individuen „verwandeln (…) sich selbst zu digital repräsentierter, jederzeit abrufbarer und weiterverarbeitbarer Information.“ (Ribolits, 2011, S. 88)

Mit anderen Worten drückt es Zuboff (2018) aus. Demnach verwandeln wir uns in „Objekte einer technologisch fortgeschrittenen und zunehmend unentrinnbaren Operation zur Rohstoffgewinnung.“ (S. 25) Dies führt in Folge zu einer permanenten Sicht- und Kontrollierbarkeit von Individuen, oder auch Überwachung genannt, die die Entwicklungspotentiale von Individuen lediglich im Rahmen des gesellschaftlichen Systems entfalten lässt (Ribolits, 2011, S. 89). Mehr dazu in Kapitel 5.

3.3 Das Geschäft mit den Daten

Wenn Google beispielsweise nach einer E-Mail-Adresse oder Handynummer fragt, teilen die meisten Nutzer und Nutzerinnen diese bereitwillig mit. Sie tauschen ihre Daten für eine Dienstleistung. Teilweise benötigt Google diese Daten sogar, um Benachrichtigungen auf Nutzerkonten zu schicken.

Die Problematik entfaltet sich bei der anschließenden Wiederverwendung und Weiterverarbeitung dieser Informationen. Ob Google, Facebook, Mentimeter, der jö-Bonusclub oder das Fitnessstudio um die Ecke: Unternehmen verwenden, verarbeiten und verkaufen persönlichen Daten weiter (Corn, 2020). Daten werden damit zunehmend zur wertvollen Ware und sind – angelehnt an Marx – das neue „Kapital“.

Dieses lässt sich dank „Expropriation der Nutzer oder Datenquelle [vermehren]. Diesen wird ein Anteil des entstehenden Wertes als Naturalien – also kostenlosen Diensten [jö Bonuskarte, Gmail-Konto, etc.] – erstattet. Was darüber hinaus an Gewinn entsteht, verbleibt bei den Plattformen.“ (Müller, 2020, S. 29) Plattformen wie Google, Facebook und Co. profitieren dementsprechend von dem informationellen Ungleichgewicht zwischen ihnen und den Nutzern und Nutzerinnen (Beyvers, 2018, S. 227).

Umgangssprachlich hat sich der Ausspruch entwickelt: „Wenn es nichts kostet, bist du das Produkt.“ Doch hierbei sei noch einmal Zuboff angeführt, die uns daran erinnert, dass Menschen längst zu „Objekte[n] einer technologisch fortgeschrittenen und zunehmend unentrinnbaren Operation zur Rohstoffgewinnung“ (Zuboff, 2018, S. 25) geworden sind.

3.4 Big Data

Ohne eine vollständige Definition des schillernden Begriffes versuchen zu wollen, widmet sich der nächste Abschnitt dieser Arbeit dem Phänomen des stetig wachsenden Datenmeers. Die jüngste Entwicklung auf dem Gebiet der Datenerfassung und -speicherung ist das Aufkommen von Big Data, mit dem die exponentielle Zunahme und Verfügbarkeit von Daten beschrieben wird.

Schätzungen aus 2018 gehen davon aus, dass sich die Menge an gespeicherten Daten alle zwei Jahre verdoppelt. Sie ist durch die sogenannten „drei Vs“ gekennzeichnet: Volumen (*volume*), Geschwindigkeit (*velocity*) und Vielfalt *(variety)* (Mainzer, 2018, S. 123 f.; Wacks, 2015, S. 9).

„Volume“ bezeichnet die „Masse an Daten“, welche nicht mehr von handelsüblichem Rechner verarbeitet werden kann. „Velocity“ beschreibt „die Geschwindigkeit bzw. Beschleunigung“ des Datenverkehrs bis hin zur Analyse in Echtzeit. „Variety“ steht für die „Unterschiedlichkeit und Vielfalt“ von Daten. Von Text- und Bilddaten bis hin zu Positions-, Gesundheits- und oder Metadaten (mehr dazu in 3.4.2): Überall lassen sich Daten sammeln (Gapski, 2015, S. 10).

Aus diesem Grund trifft Schneiers Analogie zum Umweltschutz ins Schwarze: „Data is the pollution problem of the information age, and protecting privacy is the environmental challenge.“ (Schneier, 2016, S. 238)

3.4.1 Das blinde Vertrauen in Big Data

Befürworter behaupten, Big Data besitze das Potential, aus ausgewerteten Daten Informationen zu gewinnen, die wiederum dabei helfen können Verbrechen zu bekämpfen, Krankheiten vorzubeugen, Wettervorhersagen zu treffen, Geschäftstrends zu erkennen, aber auch Infektionsgeschehen zu prognostizieren und vor allem der Wirtschaft lukrative Gewinne zu versprechen (Mainzer, 2018, S. 127; Wacks, 2015, S. 10). Die Anwendungsmöglichkeiten von Big Data scheinen grenzenlos.

Vielerorts herrscht die Überzeugung, mit ausreichend Daten lasse sich jedes Problem lösen. Big Data wird die Fähigkeit zugeschrieben, bisher unentdeckte Erkenntnisse ans Licht zu bringen und Lösungen für Probleme zu liefern, die noch nicht einmal bekannt sind. Auf der anderen Seite ermöglichen moderne Technologien, riesige Mengen an Daten auszuwerten und auf Grundlage dieser Auswertung Vorhersagen über das künftige Verhalten von Einzelpersonen zu treffen.

In Bezug auf die eingangs gestellte Forschungsfrage ergibt sich daraus eine ernstzunehmende Herausforderung für die Erwachsenen- und Weiterbildung, die mit der Frage beginnt: Ist menschliches Verhalten vorhersehbar? Denn auch auf diese Frage verspricht Big Data eine Antwort. Durch die heterogene Beschaffenheit der Daten werden Vorhersagen noch präziser. Im Gegensatz zu früher beruhen diese Vorhersagen nicht auf einer Ausgangshypothese und sind folglich teleologisch und demzufolge, vom Willen und dem Ziel derer abhängig, die die Daten verarbeiten (PRESCIENT, 2011, S. 49).

3.4.2 Das Potential zur Vorhersagbarkeit von Big Data

Bereits 2000 warnte Froomkin vor diesem Szenario: „A further danger is that the government or others will attempt to use the ability to construct personal profiles in order to predict dangerous or antisocial activities before they happen.“ (Froomkin, 2000, S. 1471) Mit ausreichend Datenmaterial sollen sich terroristische Verhaltensmuster im Ansatz frühzeitig erkennen lassen. Nicht ohne Grund stellen Kritiker von Big Data die Zuverlässigkeit der Korrelationen und die Interpretation der Ergebnisse in Frage (Wacks, 2015, S. 10).

Philip K. Dick näherte sich 1956 literarisch an das Phänomen der Informatisierung an mit seinem Roman „The Minority Report“. Im Jahr 2002 brachte Steven Spielbergs Verfilmung die Thematik einem breiteren Publikum nahe und schilderte bildreich, wie sich im Jahre 2054 mithilfe von Big Data in Kombination mit Menschen mit hellseherischen Fähigkeiten Homizide voraussagen lassen (Mainzer, 2018, S. 128).

> Der Film endet mit der Erkenntnis, dass die ‚Precogs‘ [Personen, die eine übersinnliche Fähigkeit besitzen, Ereignisse in der Zukunft zu sehen] zwar jeden Mord vorhersehen können, gleichzeitig aber auch Visionen von Situationen haben, in denen ein Mord zwar wahrscheinlich ist, aber nicht stattfindet (Mainzer, 2018, S. 128 f.)

Mit Big Data verhält es sich in der Realität genauso. Der falsche Kontext, Integrationsprobleme oder fehlerhafte Algorithmen können dazu führen, dass aus Daten irreführende Schlüsse gezogen werden, welche wiederum reale Konsequenzen nach sich ziehen.

Das US-Northern Command (NORTHCOM) führte kürzlich eine Reihe von Tests durch, die als Global Information Dominance Experiments (GIDE) bekannt sind. Dabei wurden globale Sensornetzwerke, Systeme der Künstlichen Intelligenz und Cloud-Computing-Ressourcen in einem Versuch kombiniert mit dem Ziel, sogenannte „Informationsdominanz“ und „Entscheidungsüberlegenheit“ zu erreichen.

Damit wird dem Verteidigungsministerium der Vereinigten Staaten die Fähigkeit in die Hand gelegt, Ereignisse Tage im Voraus vorherzusagen. Basierend auf der Auswertung von Mustern, Anomalien und Trends in massiven Datensätzen könnte die Zukunft somit mit einer gewissen Zuverlässigkeit vorhergesagt werden. Auch wenn dies noch nach ferner Zukunft klingen mag, behauptetet General und Befehlsinhaber VanHerck von NORTHCOM 2021, dass diese Fähigkeit bereits durch Instrumente ermöglicht wird, die dem Pentagon zur Verfügung stehen (Fingas, 2021; Tingley, 2021; Tucker, 2021).

Predictive Analytics entsteht durch die Symbiose aus statistischen Methoden, Maschinenlernen und Data Mining. Es umfasst bereits unzählige Anwendungsbereiche. Von der Prognose von Konsumentscheidungen („Predictive Marketing“) zur vorausschauenden Polizeiarbeit („Predictive Policing“) bis hin zur Steuerung von Bildungsprozessen („Learning Analytics“) streifen die Anwendungsfelder von Big Data nahezu jeden Gesellschaftsbereich (Gapski et al., 2018, S. 11).

In lebensweltliche Erfahrungen von Individuen wird sich diese Entwicklung beispielsweise dadurch manifestieren, dass die Suchmaschine Google auf Grundlage prädiktiver Analysen Antworten liefert, noch bevor überhaupt eine Frage gestellt werden muss. Amazon ließ sich bereits 2013 das Verfahren des „pre-shipping“ patentieren. Dabei zielt der Onlineversandhändler darauf ab Produkte zum Kunden nach Hause oder in seine Nähe liefern zu lassen, ehe eine Bestellung überhaupt getätigt wurde (Spiegel et al., 2013). Im Gegensatz zum Film „The Minority Report“ bedarf es heutzutage also keiner Hellseherei, sondern lediglich ausgeklügelten Berechnungsmodellen, die aus der Unmenge an Daten Informationen gewinnen können, um Verhalten vorherzusehen und beeinflussen zu können.

Letztlich sind Daten und Personen, die auf Grundlage dieser Entscheidungen treffen, nicht vor Irrtümern gefeit. Aufgrund dessen werden die drei Vs bisweilen erweitert durch „Value“, der „monetären Verwertung“, und durch „Veracity“, der „Unsicherheit und Unschärfe“ der Daten und ihrer Analysen (Gapski, 2015, S. 10). Gapski stellt somit zu Recht Fragen nach der Sinnhaftigkeit und Vertrauenswürdigkeit von Big Data-Analysen (Gapski, 2015, S. 10). Ein weiterer entscheidender Unterschied zwischen Film und Realität ist folgender: Der Inhalt der einzelnen Daten muss nicht einmal bekannt sein, um dennoch „neue Einsichten und Erkenntnisse über Zusammenhänge sowie statistische Aussagen über zukünftige Ereignisse (...) formulieren zu können.“ (Gapski, 2015, S. 10.)

3.5 Metadaten

Metadaten sind Informationen über andere Daten: „[T]he accumulation of information about information, that is metadata.“ (Pasquinelli, 2015, S. 3) Die beiden Abbildungen dienen als Veranschaulichung, um den Unterschied zwischen Daten und Metadaten verstehen zu können.

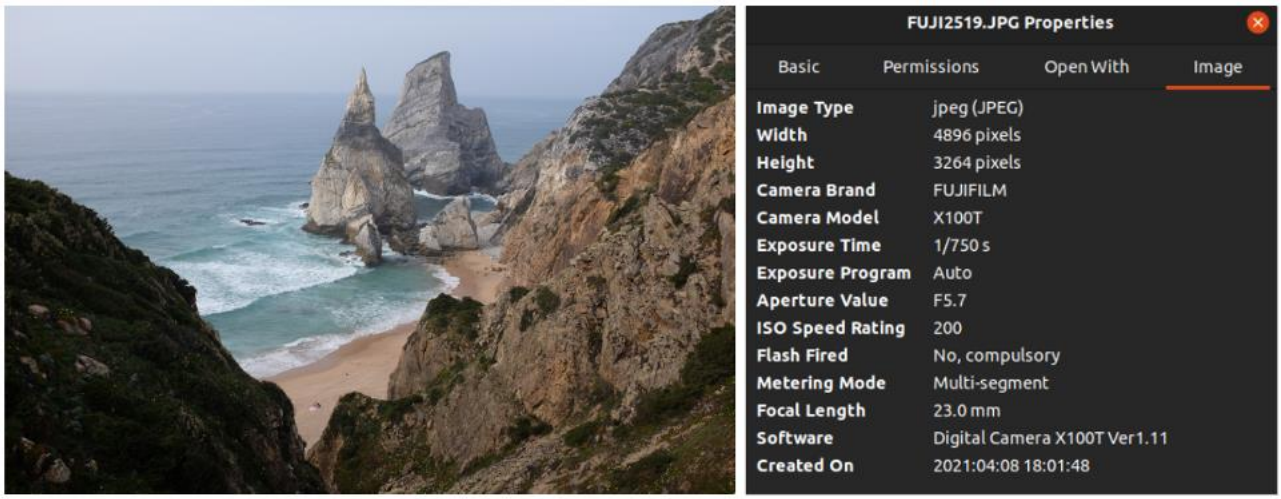

Abbildung 3: Daten und Metadaten. Quelle: Eigene Aufnahme des Verfassers, 2021.

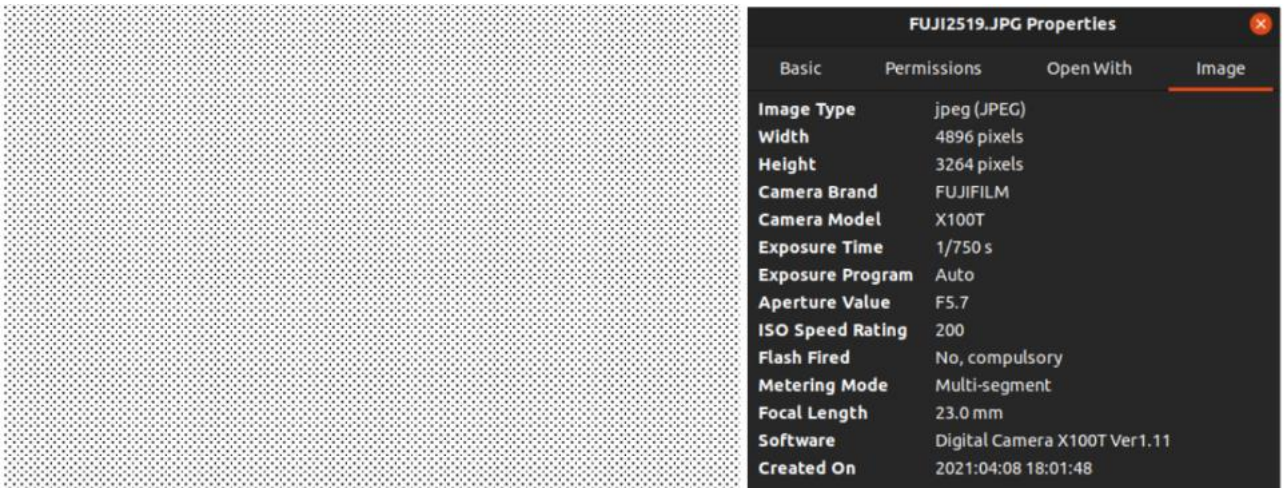

Abbildung 4: Verschlüsselte Daten und Metadaten. Quelle: Eigene Grafik des Verfassers, 2021.

Um den Bedeutungskontext von Metadaten zu verstehen, schildert Keber das illustrative Beispiel eines E-Book-Readers. Während ein gebundenes Buch keinerlei Informationen ins Internet sendet und lediglich den Titel beim Blick auf das Cover verrät, gibt es beim Lesen mit einem herkömmlichen E-Book-Readers eine Rückkopplung von Daten vom Empfänger zum Sender, welche Aufschluss über das Mediennutzungsverhalten der lesenden Person bringt (Keber, 2018, S. 262).

„Dabei verrät der Nutzer dem Anbieter nicht nur, was gelesen wird, sondern auch, wie schnell, [wie oft] und wann dies erfolgt.“ (Keber, 2018, S. 263) Unter dem Vorwand, dem Kunden und der Kundin ein optimales Nutzungserlebnis bereitstellen zu können, werden mitunter Büchersuchen und -käufe analysiert und kontextualisiert. Korrelationsmodelle werden berechnet und können politische Einstellungen, religiöse Überzeugungen, sexuelle Vorlieben, Freizeitaktivitäten etc. von Individuen bestimmen (Keber, 2018, S. 263).

Auf derselben Weise werden bei Nachrichtendiensten, wie beispielsweise WhatsApp, Facebook, Messenger, aber auch im E-Mail-Verkehr Daten abgesaugt. Erstere Anwendung basiert auf Ende-zu-Ende-Verschlüsselung und verschlüsselt somit übertragene Daten, welche ausschließlich von den Kommunikationspartnern entschlüsselt werden können und entgegen diversen Verschwörungstheorien nicht von Regierungen aufgebrochen werden, was im Falle von Metadaten längst nicht mehr notwendig ist.

Metadaten beinhalten Daten über die Art und Dauer der Kommunikation, die Häufigkeit, mit der ein Nutzer andere Nutzer kontaktiert, die Art der Kontaktaufnahme (Text- oder Bildform, Sprachnachricht, Audio- oder Videotelefonie), wer kontaktiert wird, wann die Nachricht empfangen und wann sie gelesen wird usw. Metadaten in anderen Anwendungsbereichen umfassen besuchte Internetseiten, IP-Adressen und geografische Positionen.

Auch wenn viele dieser Rohdaten in erster Hinsicht nicht als persönlich einzustufen sind und keine biografischen Daten beinhalten, ermöglichen Metadaten einem Datenverarbeiter den Nutzer zu verfolgen, zu identifizieren und erlauben präzise Rückschlüsse auf Details, wie z. B. soziale Beziehungen, Gewohnheiten, Interessen, Vorlieben usw. (PRESCIENT, 2011, S. 50).

Metadaten können somit personenbezogen sein, sind hochsensibler Natur und unterliegen den Fortschritten der Datenanalyse, die es ermöglicht, anonyme Metadaten zu deanonymisieren und auf bestimmte Personen zu beziehen (Müller, 2020, S. 132). Dementsprechend ist auch eine Ende-zu-Ende-Verschlüsselung allein kein ausreichender Schutz, um die Privatheit vor Datenkraken zu bewahren.

3.6 Big Data und Metadaten in der Erwachsenenbildung

Warum ist Big Data ein Thema für die Erwachsenen- und Weiterbildung?

> Da sich digitale Medienangebote als komplexe soziotechnische Handlungsumgebungen manifestieren, setzen sie meist ein sehr konkretes Wissen um Nutzungen und Nutzungspotentiale von Daten sowie ein technisch elaboriertes Wissen bezüglich ihrer Funktionsweise voraus – doch selbst wenn dieses vorliegt, so impliziert dies mitnichten einen adäquaten Umgang mit der eigenen Privatheit. (Piegsa & Trost, 2018, S. 19)

Hüther und Schorb bezeichnen die Geschichte der Medienpädagogik als „Geschichte der pädagogischen Reaktionen auf die jeweils „neuen Medien“ und die durch sie hervorgerufenen gesellschaftlichen Irritationen.“ (Hüther & Schorb, 1997, zit. n. Gapski, 2015, S. 13) Gesellschaftliche Irritationen aufgrund von technologischem Wandel werden von einer zeitverzögerten Anpassungsqualifikation gefolgt und führen zur Kompetenzentwicklung (Gapski, 2001, zit. n. Gapski, 2015, S. 13). Big Data ist mittlerweile längst zu einem lebensweltlich erfahrbaren Phänomen geworden und sollte mitsamt seinen gesellschaftlichen Konsequenzen in der Erwachsenenbildung vermittelt werden (Gapski, 2015, S. 13; Gapski et al., 2018, S. 130).

Globalisierung und Digitalisierung sind mittlerweile so eng miteinander verflochten, dass lediglich eine analytische Unterscheidung beider möglich ist (Thies, 2018, S. 139). Und eines ist gewiss: Der rasante technologische Wandel und die Digitalisierung warten nicht auf Medienbildung, Kritikfähigkeit und Selbstbestimmung. Es ist die Aufgabe der Erwachsenenbildung selbst, kritisch über Tendenzen und Entwicklungen zu informieren und die kritische Medienkompetenz zu fördern.

Dazu gehört Wissen über Big Data und Metadaten zu vermitteln und auf deren Bedeutung aufmerksam zu machen. Mehr dazu in 7.6. Allerdings steht dem kritisch kompetenten Wesen eines entgegen: Der Nutzer und die Nutzerin.

4 Das Paradox der Privatheit

„A paradox is merely truth standing on its head to attract attention.“

G. K. Chesterton[4]

Ehe ich mich dem für dieses Kapitel titelgebenden Phänomen widme, wird eine Abstraktion von Acquisti aus dem Jahre 2004 erläutert. Der Autor erstellte ein Modell, um Entscheidungen nachvollziehen zu können, in denen persönliche Informationen gegen diverse Dienstleistungen eingetauscht werden. Das Modell dient als erster Ansatz, um den Entscheidungsprozess bei der Datenfreigabe von Individuen verstehen zu können (Acquisti, 2004, S. 2).

4.1 Modell zur Entscheidungsfindung bei der Preisgabe von Daten

In seinem Modell der Entscheidungsfindung abstrahiert Acquisti den Entscheidungsprozess eines idealisierten rationalen Wirtschaftsakteurs, der bei der Durchführung einer bestimmten Handlung im Internet mit Kompromissen bezüglich seiner/ihrer Privatsphäre konfrontiert ist (Acquisti, 2004, S. 2).

$$\max_{d} U_t = \delta\left(v_E(a), p^d(a)\right) + \gamma\left(v_E(t), p^d(t)\right) - c_t^d \qquad (1)$$

δ und γ sind nicht näher spezifizierte Funktionen, die gewichtete Beziehungen zwischen erwartetem Nutzen aus einer Reihe von Ereignissen v und den Wahrscheinlichkeiten des Auftretens dieser Ereignisse p beschreiben (Acquisti, 2004, S. 2).

Genauer gesagt ist der Nutzen U bei Vollzug einer beliebigen Handlung t (die mit der Preisgabe persönlicher Informationen verbunden ist) gleich einer Funktion des erwarteten Nutzen $v_E(a)$, die sich aus der Geheimhaltung (bzw. der unterlassenen Preisgabe) bestimmter Informationen während dieser Handlung ergibt, und der Wahrscheinlichkeit der Geheimhaltung (bzw. der unterlassenen Preisgabe) dieser Informationen beim Einsatz der Technologie d, $p^d(a)\,[1 - p^d(a)]$ plus eine Funktion des erwarteten Nutzen $v_E(t)$ aus Vollzug (bzw. des unterlassenen Vollzuges) der Handlung (unter Preisgabe

[4] Chesterton, G. K. (1963). *The paradoxes of Mr. Pond* (1. publ.). Finlayson.

persönlicher Informationen) und der Wahrscheinlichkeit des Vollzuges [bzw. des unterlassenen Vollzuges] dieser Handlung mit einer bestimmten Technologie d, $p^d(t)\,[1 - p^d\,(t)]$ abzüglich der Risiken für den Einsatz der Technologie t: c_t^d (Acquisti, 2004, S. 2).

Dabei kann die Technologie d entweder vorteil- oder nachteilhaft für die Privatheit sein. Da der erwartete Nutzen in Gleichung (1) sowohl positiv als auch negativ sein kann, verkörpert Gleichung (1) sinnbildlich die Dualität, die in Datenschutzfragen impliziert ist: Es gibt sowohl Risiken als auch Nutzen, die durch die Preisgabe oder den Schutz persönlicher Informationen entstehen können (Acquisti, 2004, S. 2).

Risiken und Nutzen einer vollzogenen Handlung, $v_E\,(t)$ können sich von den Risiken und dem Nutzen der unterlassenen Preisgabe der damit verbundenen Informationen, $v_E\,(a)$, unterscheiden (Acquisti, 2004, S. 2).

So kann beispielsweise die Mitgliedschaft in einem Rabattclub und somit die Preisgabe der eigenen Identität und des Konsumverhaltens zu einem Rabatt führen. Umgekehrt kann Preisdiskriminierung dazu führen, dass ein höherer Preis gezahlt werden muss und ist eindeutig als Nachteil zu zählen (Acquisti, 2004, S. 2).

Um ein illustratives Beispiel aus der Erwachsenenbildung zu nennen, dient die Echtzeit-Feedback Anwendung Mentimeter. Mentimeter's Webseite bietet einen sogenannten Single-Sign-on-Service an, abgebildet in der folgenden Abbildung:

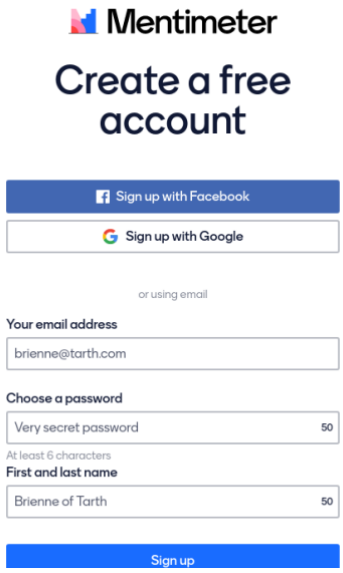

Abbildung 5: Login-Dialog auf mentimeter.com. Quelle: Screenshot des Verfassers vom 14.10.2021.

Weit verbreitet sind hierbei die Authentifizierungsdienste „Google Sign-In“ und „Facebook Login“.

> Das sind von den beiden Konkurrenten Google und Facebook angebotene Services, die sich in beliebige Android- und iPhone-Apps sowie auf Websites integrieren lassen und mithilfe derer die Entwickler_innen einer App oder Website es ihren Usern ermöglichen, sich mit ihrem Google- bzw. Facebook-Account bei der App oder Website zu registrieren, anstatt mit einem selbst gewählten Benutzernamen und Passwort für diesen Service einen neuen User-Account anzulegen. (Mühlhoff, 2019, S. 92)

Nicht nur Nutzer und Nutzerinnen profitieren von dem schnellen und bequemen Authentifizierungsprozess. Ohne den Besuch einer Google- oder Facebook-Internetseite werden bei einem Google bzw. Facebook Sign-In oder Log-In personenbezogene Daten an die beiden Betreiber gesendet „die auf dem Wege einer herkömmlichen Registrierung mit sehr viel mehr Aufwand den Nutzer_innen entlockt werden müssten.“ (Mühlhoff, 2019, S. 92)

Oftmals ohne Bewusstsein der Anwender und Anwenderinnen erhalten Google und Facebook somit Zugriff auf Klarnamen, E-Mail-Adressen, Fotos, Altersklasse, Geschlecht, Ortsangaben, Zeitzone und – im Falle von Facebook – eine Liste aller Facebook-Freunde, die ebenfalls Mentimeter benutzen (Mühlhoff, 2019, S. 92). Da viele Nutzer und Nutzerinnen sowieso permanent in ihren Konten angemeldet sind, ist der erwartete Nutzen somit Zeitersparnis und Bequemlichkeit. Die Risiken, die mit diesen Handlungen, welche oftmals aus einem einfachen Mausklick, der weniger als eine Sekunde dauert, einhergehen, sind vielen Nutzern und Nutzerinnen nicht bewusst.

Die Parameter δ und γ verkörpern die variablen Gewichtungen und Einstellungen, die ein Individuum in Bezug auf die unterlassene Preisgabe seiner Informationen (z. B. ihre Sensibilität für die Privatsphäre oder ihre Überzeugung, dass die Privatsphäre ein Recht ist, dessen Einhaltung von der Regierung durchgesetzt werden sollte) und den Vollzug bestimmter Handlungen haben kann. v_E () und p^d () können als multivariate Parameter betrachtet werden, in denen sich aufgrund der Komplexität der oben beschriebenen Thematik der Privatsphäre mehrere andere Variablen, Erwartungen und Funktionen verbergen. Im Laufe der Zeit hängt die Wahrscheinlichkeit, bestimmte Daten nicht

preiszugeben, nicht nur von der gewählten Technologie d ab, sondern auch von den Bemühungen anderer Parteien, sich diese Daten anzueignen (Acquisti, 2004, S. 3).

Die Wahrscheinlichkeit, Suchanfragen privat zu halten, ist sehr hoch bei der ausschließlichen Nutzung von Suchmaschinen, die Wert auf den Schutz personenbezogener Daten ihrer Nutzer und Nutzerinnen legen. Ein rationaler Wirtschaftsakteur und eine rationale Wirtschaftsakteurin entscheiden sich theoretisch für den Dienst bzw. für Technologie d, der den Nutzen U in Gleichung (1) maximiert. Er bzw. sie würde womöglich die Vorteile und die Risiken bei der Nutzung der Google Suchmaschine mit den Vorteilen und Risiken, die eine alternative Suchmaschine wie beispielsweise die relativ unbekannte privatsphärenrespektierende europäische Suchmaschine Qwant darstellt, vergleichen.

Die Größenordnung der Parameter in Gleichung (1) ändert sich mit der gewählten Technologie. Eine Nutzung von Qwant zur Suchanfrage kann dabei die erwarteten Eingriffe in die Privatsphäre verringern. Auf der anderen Seite bietet Googles Suchmaschine vermeintlich zuverlässigere und individualisierte Suchergebnisse.

Handeln Nutzer und Nutzerinnen somit rein rational und stets mit einer Abschätzung des erwarteten Nutzens bei der Verwendung von webbasierten Anwendungen?

4.2 Die Dichotomie zwischen Einstellung und Verhalten

Privatsphäre und Datenschutz im Internet sind – lange nachdem Acquisti sein Modell zur Entscheidungsfindung aufstellte – immer noch neue soziale Phänomene, die laut den beiden Autorinnen Oetzel und Gonja (2011) von Menschen noch nicht vollends verstanden werden können. Zweifellos ist das Konzept der Privatheit in der Offline-Welt Teil des gemeinsamen und allgemeinen Wissensbestandes. Aber dieses Verständnis von Privatheit lässt sich nicht ohne erhebliche Modifikation auf die digitale Welt übertragen. Die sozialen Repräsentationen, die es den Menschen ermöglichen würden, Privatsphäre und Datenschutz im Internet als Konzepte zu verstehen, haben sich noch nicht herausgebildet, wie eine empirische Studie mit österreichischen und deutschen Partizipierenden der beiden Autorinnen gezeigt hat. Zehn Jahre später scheint nichts auf ein verbessertes Verständnis hinzuweisen. Eine soziale Repräsentation ist ein konzeptionelles Schema, das Werte, Ideen, Metaphern, Überzeugungen und Praktiken umfasst, die von den Mitgliedern einer Gesellschaft geteilt werden. Die Theorie der sozialen Repräsentation legt nahe, dass Individuen neue Konzepte auf der Grundlage etablierter Schemata verstehen, und zwar durch die Prozesse der Objektivierung und Verankerung (Oetzel & Gonja, 2011, S. 2108).

Bei der Verankerung wird neuen Phänomenen eine Bedeutung zugeschrieben, indem sie in bestehende Begriffsschemata integriert werden, so dass sie interpretiert und mit vorhandenem Wissen (d.h. bereits Bekanntem) verglichen werden können. Im Prozess der Objektivierung werden abstrakte Konzepte durch das Entstehen neuer sozialer Repräsentationen konkret. Ergebnisse der obigen Studie zeigen: Der Wechsel von einer eindeutig positiven Bewertung von den Technologien Soziale Netzwerke, Google Dienstleistungen und Smartphone zu einer deutlich negativen Bewertung bei der Kombination von Technologie und Privatsphäre deutet darauf hin, dass Privatsphäre noch nicht in die gesellschaftliche Repräsentation dieser Technologien integriert ist. Lediglich bei der ausdrücklichen Erwähnung von Privatsphäre wird dieser Augenmerk geschenkt (Oetzel & Gonja, 2011, S. 2110).

Aufgrund einer fehlenden sozialen Repräsentation von Privatsphäre und Datenschutz im Internet, neue digitale Codes, Verhaltensweisen und Regeln, die mit bestehenden Normen nicht mehr übereinstimmen, gelingt es Individuen oft nicht, eine verlässliche Perspektive zu diesen Themenbereichen zu entwickeln (Kokolakis, 2017, S. 129; Müller, 2020, S. 4).

Und auch die Erwachsenenbildung als wissenschaftliche Disziplin hat noch keine differenzierte Perspektive hierfür. Ein Beispiel in der Auseinandersetzung mit Online-Privatsphäre hierzu ist das Paradox der Privatheit. Erstmalig von Norberg et al. 2007 erwähnt, bezeichnet das Privatheitsparadox eine gewisse Dichotomie zwischen der Einstellung zum Datenschutz und dem tatsächlichen Verhalten von Nutzern und Nutzerinnen (Kokolakis, 2017, S. 122; Norberg et al., 2007, S. 101).

Ein 2012 von Beresford et al. durchgeführtes Feldexperiment versuchte das bisweilen rein auf umfragenbasierte Paradox im Lebensalltag von Einzelpersonen zu bestätigen. Probanden und Probandinnen wurden gebeten, eine DVD in einem von zwei konkurrierenden Geschäften zu kaufen. Die beiden Geschäfte unterschieden sich lediglich im Hinblick auf die Datenabfrage. Das erste Geschäft erfasste das Einkommen und das Geburtsdatum ihrer Kunden und Kundinnen, während das zweite Geschäft die Lieblingsfarbe und das Geburtsjahr abfragte. Offensichtlich sind die vom ersten Geschäft abgefragten Daten wesentlich sensibler. Nichtsdestotrotz kauften Probanden und Probandinnen bei gleichem Preis im gleichen Ausmaß in beiden Geschäften. Als der Preis im ersten Geschäft um einen Euro niedriger angesetzt wurde, wählten fast alle Probanden das günstigere Geschäft, obwohl dort sensiblere Daten abgefragt wurden. Anschließend wurde mittels Umfragebögen untersucht, ob sich die Probanden und Probandinnen keine Sorgen um die abgefragten Daten machen. Dabei gaben 75 Prozent an, dass sie ein hohes Interesse am Datenschutz hätten, und 95 % seien am Schutz ihrer persönlichen Daten interessiert (Beresford et al., 2012, zit. n. Kokolakis, 2017, S. 124).

Die zivilgesellschaftliche Debatte rund um Datenschutz ist konfrontiert mit diesem Paradox, welches die „Dissonanz von Denken und Handeln der Subjekte im Medienumfeld“ (Piegsa & Trost, 2018, S. 19) adressiert. Während ein Großteil der Nutzer und Nutzerinnen webbasierter Anwendungen laut eigenen Angaben die Idee des Datenschutzes befürworten, so spiegelt sich dies in ihrem täglichen Handeln nicht wider und führt somit zur Ernüchterung und Ratlosigkeit von Datenschutzaktivisten (Müller, 2020, S. 119). Folgende Seiten widmen sich den Fragen nach der Existenz des Privatheitsparadox und wie sich die Dichotomie zwischen Einstellung zum Datenschutz und dem beobachteten Verhalten erklären lässt.

4.3 Institutionelle Datenerhebung

Hoffmann et al. (2016) zeigen anhand der Werke von Raynes-Goldie (2010) und Young & Quan-Haase (2013) auf, dass die Existenz des Privatheitsparadox am wahrscheinlichsten ist, wenn es sich um institutionelle Bedrohungen der Privatsphäre handelt (Hoffmann et al., 2016, S. 1). Nutzer und Nutzerinnen neigen sehr wohl dazu, sich an Bedrohungen der Privatheit, die von ihrem unmittelbaren sozialen Umfeld ausgehen – wie Stalking und Cybermobbing – anzupassen, reagieren aber weniger konsequent auf wahrgenommene Bedrohungen durch institutionelle Datensammlung (Boyd & Hargittai, 2010, zit. n. Hoffmann et al., 2016, S. 1).

Infolgedessen werden Verbrauchermärkte dominiert von Diensteanbietern, die regelmäßig für ihre Datenschutzpolitik kritisiert werden. Dies sind große, börsennotierte Unternehmen, die den Markt fest in ihrer Hand wissen.

Aufgrund der hohen Anzahl an Nutzern und Nutzerinnen einiger dieser Dienstleistungsanbieter erzeugen sie einen weitaus größeren Mehrwert als ihre Wettbewerber. Dementsprechend ist es nicht verwunderlich, dass auf der anderen Seite alternative Suchmaschinen, Webbrowser oder Nachrichtendienste, die kaum in die Privatsphäre der Nutzer und Nutzerinnen eingreifen, keinen nennenswerten Marktanteil erreichen. Nutzer und Nutzerinnen stehen vor dem Dilemma zwischen einer scheinbar freien Wahlmöglichkeit und den praktischen Grenzen der Handhabbarkeit zwischen unterschiedlichen Anbietern. Von einer echten Wahl kann aufgrund enorm höherer Netzwerkeffekte der großen Techkonzerne nicht mehr gesprochen werden (Beyvers, 2018, S. 183; Hug & Madritsch, 2020, S. 19).

Nicht nur die Nutzer und Nutzerinnen entscheiden sich für Big-Tech. Grob fahrlässige Nichtbeachtung von datenschutzrechtlichen Warnhinweisen und situationselastische Anpassung pädagogisch-ethischer Erwägungen waren im pandemiebedingten Digitalisierungsschub omnipräsent (Hug & Madritsch, 2020, S. 19). Nicht nur Erwachsenenbildner und Erwachsenenbildnerinnen, sondern auch die Nutznießer und Nutznießerinnen von erwachsenenpädagogischen Maßnahmen liefern sich somit der institutionellen Bedrohung der Privatheit aus.

Das Internet und der kompetente Umgang damit steht auf der einen Seite als Voraussetzung für soziale Teilhabe an der Gesellschaft, auf der anderen Seite für eine Realität, in der wir immanent „getrackt, geparst, ausgewrungen und modifiziert (...) werden." (Zuboff, 2018, S. 26) Eine ausbleibende Einwilligung, persönliche Daten preiszugeben, geht mit den Kosten einher, nicht in den Genuss der Vorteile zu kommen, die mit der Weitergabe personenbezogener Daten verbunden sind. Dies entspricht einer negativen Preisdiskriminierung, da Individuen nicht zur Gruppe der bevorzugten Kunden gehören, die in den Genuss von Rabatten kommen.

Datenschutz impliziert allerdings die Zurückhaltung bestimmter Informationen. Demnach könnten Personen, die bedacht darauf sind, ein Minimum an Daten im Internet preiszugeben, verdächtigt werden, etwas zu verbergen. In der Tat ist die Frage, warum Menschen Privatsphäre brauchen, wenn sie nichts (Bizarres oder Illegales) zu verbergen haben, eines der klassischen Argumente von Unternehmen, die versuchen, ihren Macht- und Gewinnzuwachs durch das Sammeln von Daten zu verbergen (PRESCIENT, 2011, S. 37).

4.4 Die Alltagsfloskel „Ich habe nichts zu verbergen"

Dieser Konflikt, so meint Zuboff, führt dazu, dass mit zynischer Resignation Aussagen wie „Ich habe nichts zu verbergen, demnach habe ich auch nichts zu befürchten" getroffen werden (Zuboff, 2018, S. 26). Dieses Argument durchdringt den öffentlichen Diskurs über Fragen der Privatsphäre (Solove, 2008, S. 748).

Das Argument ist in der Privatsphäre-Literatur gut dokumentiert (siehe Kokolakis, 2017) und fungiert als Hindernis für die Entwicklung von pragmatischen Privatsphären-Schutzstrategien (Viseu et al., 2004, S. 103). Die beiden Autorinnen und der Autor vergleichen das Dilemma mit der Privatheit damit, dass Personen, die von der globalen Erwärmung und den negativen Entwicklungen unseres Klimas wissen, die unmittelbaren Gewinne, mit dem Auto zur Arbeit zu fahren oder Kurzstreckenflüge zu buchen, dem oftmals unsichtbaren Verlust der Umweltverschmutzung bevorzugen (Viseu et al., 2004, S. 103).

Gleich wie Umweltschützer ständig Argumente von Klimawandelleugner widerlegen müssen, so müssen Verfechter der Privatheit dieses Argument ständig widerlegen. Konfrontiert mit dem drohenden Verlust der Privatheit wird das Risiko, welches damit einhergeht, oftmals heruntergespielt.

> The argument that no privacy problem exists if a person has nothing to hide is frequently made in connection with many privacy issues. When the government engages in surveillance, many people believe that there is no threat to privacy unless the government uncovers unlawful activity, in which case a person has no legitimate justification to claim that it remains private. Thus, if an individual engages only in legal activity, she has nothing to worry about. (Solove, 2008, S. 746 f.)

Die Auseinandersetzung mit dem Argument ist wichtig, spiegelt sie doch die Grundeinstellung eines großen Teils der Bevölkerung wider (Solove, 2008, S. 747) und ist eingebettet in eine bipolare Weltansicht, in der nur zwei Arten von Menschen existieren: Gute und böse Menschen. Dabei sind „böse" Menschen diejenigen, die Terrorattacken planen, in kriminelle Aktivitäten verwickelt sind, oder illegale Geschäftspraktiken tätigen. Diese Menschen sind daran interessiert, sich selbst und ihre Aktivitäten im Geheimen zu halten und somit ihre Privatsphäre bestmöglich zu schützen. Auf der anderen Seite existieren „gute" Menschen, die nach einem langen Arbeitstag nach Hause kommen, den Fernseher aufdrehen und das Internet nicht nutzen, um sich Bombenpläne herunterzuladen, sondern um Nachrichten zu lesen, Serien zu schauen oder ein neues Kochrezept zu suchen. Sie haben nichts zu verbergen und somit keine Angst davor „beobachtet" zu werden (Greenwald, 2014).

Möglicherweise haben sie nach den geltenden Gesetzen in ihrem Land momentan nichts zu verbergen. Allerdings trugen in den 1970er Jahren iranische Frauen Miniröcke, rauchten, tranken, gingen in Nachtclubs und hörten Musik der Beatles. Dies ist heutzutage anders. Ein Blick nach Afghanistan offenbart ähnliches. Und auch wenn sich die Europäische Union nicht mit Entwicklungsländern vergleichen lässt, so ist die politische Landschaft in 50 Jahren nicht vorhersehbar.

Edward Snowden, US-amerikanischer Whistleblower, ist davon überzeugt, dass wir mit obiger Weltansicht effektiv unsere Rechte abgeben (Snowden, 2014). Des Weiteren zeigt der ehemalige österreichische Präsident des Verfassungsgerichtshofs, Gerhart Holzinger, auf, dass oben genannte Behauptung einen fundamentalen Fehler in sich trägt.

> Dass die Menschen ein gewisses Maß an Freiheit genießen, zeichnet den liberalen Rechtsstaat aus. Damit verbunden ist, dass auch ein völlig unauffälliges Privatleben vor Überwachung geschützt werden muss. Ein Staat, der diese Freiheit nicht zugesteht, gleitet automatisch in eine Diktatur ab. (Holzinger, 2017)

Mit anderen Worten hat es wiederum Snowden (2014) formuliert: „Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.“ (Snowden, 2014)

Das Hauptmissverständnis besteht nach Solove (2008) darin, dass das Argument die Privatsphäre in ihrer gesamtgesellschaftlichen Bedeutung auf eine Form der Geheimhaltung, als das Recht, Dinge zu verbergen, reduziert. Dabei wird Privatheit kurzsichtig als eine Form des Verbergens oder der Geheimhaltung betrachtet, die nicht über die Preisgabe von Geheimnissen an den Staat hinausgeht. Es wird ein Großteil der weitreichenden, bereits ausführlich behandelten Folgen von Privatsphärenverlust ausgeblendet. Gerichte und Gesetzgeber suchen nach bestimmten Arten von Schäden, und ihr enger Fokus macht sie blind für andere Arten von gesamtgesellschaftlichen Schäden (Solove, 2008, S. 764-768).

Es ist gefährlich, Privatsphäre mit „etwas verbergen“ gleichzusetzen, denn es geht dabei um die Möglichkeit, um die Kontrolle, ob etwas verborgen werden kann. Gapski et al. (2018) zeigen auf, inwiefern bereits Kinder und Jugendliche mit einem gewissen Kontrollverlust konfrontiert werden:

> Fälle des Hackings und des Bekanntwerdens immer neuer Sicherheitslücken [zeigen] Effekte des Kontrollverlusts auf unternehmerischer und gesellschaftlicher Ebene. Dies befördert eine fatalistische Grundhaltung im Umgang mit Daten nicht nur bei Kindern und Jugendlichen. Die problematische Aussage ‚Ich habe doch nichts zu verbergen‘ wird zur Ergebung ‚Ich kann doch sowieso nichts verbergen.‘ (Gapski et al., 2018, S. 115)

Angesichts der Vielschichtigkeit von Problemen, die beim Schutz der Privatsphäre auftreten und durch die staatliche und institutionelle Datenerhebung und Weiterverarbeitung entstehen, hat das Argument, man habe nichts zu verbergen, letztlich nichts zu sagen (Solove, 2008, S. 772).

Im folgenden Abschnitt der Arbeit werden Erklärungsversuchen für das Privatheitsparadox vorgestellt und kritisch hinterfragt.

4.4.1 Datenschutzkalkül

Dieser Ansatz beruht auf der von Acquisti (2004) beschriebenen Dualität, die in Datenschutzfragen impliziert ist. Der Ansatz des sogenannten „Privacy Calculus“ beruht auf einer rationalen Entscheidung, die Individuen gegenüber der Preisgabe persönlicher Daten im Internet treffen, wenn sie die Vorteile gegenüber den Kosten und potenziellen Risiken einer Handlung im Internet abwägen (Lee et al., 2013, zit. n. Hoffmann et al., 2016, S. 2).

Bei diesem Ansatz hängt die Entscheidung, Informationen preiszugeben, stark von der individuellen Empfindlichkeit gegenüber dem ab, was als Eingriff in die Privatsphäre empfunden wird (Hurwitz, 2013, zit. n. Hoffmann et al., 2016, S. 2). Wie bereits behandelt, werden Eingriffe in die Privatsphäre oft nicht als solche erkannt und lassen sich aufgrund ihrer fehlenden Symptomatik nicht unmittelbar erkennen. Des weiteren hängt die Erklärung des Datenschutzkalküls stark davon ab, inwieweit sich Nutzer und Nutzerinnen der Vorteile und Risiken bewusst sind, die mit jeder Handlung online einhergehen (Hoffmann et al., 2016, S. 2).

Dieses Bewusstsein ist in vielen Fällen allerdings verständlicherweise schwach ausgeprägt, stehen Individuen tagtäglich einer enormen Komplexität von Datenerhebungsverfahren, Wirtschaftsmodellen, Käufer-Verkäuferbeziehungen und technologischen Anwendungen gegenüber, die oftmals die Fähigkeit oder Bereitschaft von Individuen, aktiv über die Verwendung und gemeinsame Nutzung ihrer Informationen zu entscheiden, übersteigt (Beyvers, 2018, S. 211; Art. 29-Datenschutzgruppe, WP 168, S. 20).

Auch Acquisti (2004) merkt an, dass die in seinem bereits behandelten Modell implizierten Kompromisse dazu führen, dass sich Individuen tagtäglich mit den Problematiken, unvollständige Informationen über alle Parameter zu haben und die begrenzte Fähigkeit besitzen, alle verfügbaren Informationen zu verarbeiten, auseinandersetzen müssen (Acquisti, 2004, S. 3).

4.4.2 Fehlendes Risikobewusstsein

Ein weiterer Erklärungsansatz bezeichnet eben dieses mangelnde Bewusstsein und fehlende Kenntnisse von Nutzern und Nutzerinnen über potenzielle Schäden, die mit der Datenpreisgabe im Internet verbunden sind. Nach dieser Ansicht fehlt es vielen Nutzern und Nutzerinnen an Verständnis und Bewusstsein für die Risiken der Online-Privatsphäre (Bartsch & Dienlin, 2016; Hoofnagle et al., 2010 & Trepte et al., 2015, zit. n. Hoffmann et al., 2016, S. 2 f.).

Es bedarf der Entwicklung eines Konzepts, welches die Problematik der Online-Privatsphäre umfasst. Öffentliche Diskussionen über Fragen des Datenschutzes sowie permanente Innovationen neuer Online-Dienste zeigen, dass sich dieses Konzept noch in der Entwicklung befindet und noch kein Stadium erreicht hat, das es Nutzern und Nutzerinnen erlauben würde, Risiken in Bezug auf ihre Datenpreisgabe zuverlässig einschätzen zu können (Oetzel & Gonja, 2011, S. 2108).

Mangelndes Verständnis und Bewusstsein kann einerseits auf die digitalen Fähigkeiten der Nutzer oder deren Mangel zurückführen (Dienlin & Trepte, 2015; Park, 2013, zit. n. Hoffmann et al., 2016, S. 3). Kapitel 7 widmet sich einigen Ansätzen, die dem entgegenwirken können.

4.4.3 Vertrauen der Nutzer und Nutzerinnen

Dieser theoretische Ansatz konzentriert sich auf das Vertrauen der Nutzer und Nutzerinnen in die Anbieter webbasierter Anwendungen. Dies kann beschrieben werden als „a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviors of another.“ (Rousseu et al., 1998, zit. n. Hoffmann et al. 2016, S. 2)

Ein Zustand der Vertraulichkeit führt dazu, dass Individuen bereitwilliger persönliche Informationen weitergeben (Gerber et al., 2017, S. 142). Nach dieser Auffassung berücksichtigen und bewerten Nutzer und Nutzerinnen nicht unbedingt die spezifischen Risiken und Vorteile einer Online-Transaktion. Vielmehr bilden sie verallgemeinerte Erwartungen gegenüber Transaktionspartnern (Bhattacharjee, 2002; McKnight et al., 2002, zit. n. Hoffmann et al., 2016, S. 2), die eine Art Heuristik darstellt und weniger Bedenken in Bezug auf Vertrauen des Transaktionspartners.

Dieser Ansatz ergänzt die Perspektive des Datenschutzkalküls, indem er sowohl kognitive als auch affektive Motive für die Preisgabe von Daten berücksichtigt (Krasnova et al., 2010, zit. n. Hoffmann et al., 2016, S. 2). Doch obwohl Vertrauen eine wichtige Voraussetzung für die Etablierung und das Wachstum von webbasierten Anwendungen darstellt (Hoffman et al., 1999; Jarvenpaa et al., 2000, zit. n. Hoffmann et al., 2016, S. 2), gibt es nur wenige Hinweise darauf, dass die Nutzer tatsächlich den Diensten vertrauen, auf denen oder denen sie persönliche Informationen preisgeben (Klara, 2016; Young & Quan-Haase, 2013, zit. n. Hoffmann et al. 2016, S. 2).

Tatsächlich würde die fragwürdige Reputation großer Internetdienste wie beispielsweise Facebook oder Google ein weit verbreitetes Misstrauen und institutionelle Bedenken hinsichtlich des Schutzes der Privatheit nach sich ziehen (Klara, 2016, zit. n. Hoffmann et al., 2016, S. 3).

4.4.4 Datenschutz-Zynismus und Möglichkeitsblindheit

Hoffmann et al. (2016) führen für den von Gapski et al. (2018) beschriebenen Kontrollverlust und für eine Situation des „Dauerstresses“ und der Überforderung den Begriff „privacy cynicism“ ein und beschreiben ihn als eine Haltung der Unsicherheit, der Machtlosigkeit und des Misstrauens gegenüber dem Umgang mit persönlichen Daten durch webbasierte Anwendungen, die ein Verhalten, welches auf den Schutz der Privatsphäre abzielt, subjektiv als aussichtslos erscheinen lässt (Hoffmann et al., 2016, S. 2).

Als kognitiver Bewältigungsmechanismus für Nutzer und Nutzerinnen, der es ermöglicht, Bedenken in Bezug auf den Schutz der Privatsphäre bei der Verwendung webbasierter Anwendungen beiseitezulegen, für den der Begriff steht, greift dieser Erklärungsversuch einige der bereits genannten Argumente auf (Hoffmann et al., 2016, S. 4). Dem zugrundeliegenden Kontrollverlust dieses Bewältigungsmechanismus können „unzureichende Medienkompetenz, das technische Unwissen und individuelle Fehler auf Seiten der Mediennutzerinnen und Mediennutzer“ gesehen werden (Hagendorff, 2019, S. 98).

Pörksen und Detel führen 2012 den Begriff der „Möglichkeitsblindheit“ ein, und bringen damit zum Ausdruck, „dass viele Nutzerinnen und Nutzer digitaler Informations- und Kommunikationstechnologien sich schlicht nicht vorstellen können, was mit den eigenen Daten passieren kann, in welchen Kontexten sie ‚zirkulieren‘ oder wie sie ‚geklaut‘ werden können.“ (Pörksen & Detel, 2012, zit. n. Hagendorff, 2019, S. 98) Der Begriff könnte des Weiteren für eine Blindheit gegenüber alternativen, weniger datenintensiven Diensten stehen, die jedoch aufgrund von Netzwerkeffekten nur schwer Marktmacht aufbauen können.

4.5 Die Lösung des Paradoxons

Müller argumentiert, dass der Schutz der eigenen Privatsphäre eine untergeordnete Rolle spiele, solange hinter der Freigabe von persönlichen Informationen ein kalkulierter Zweck stehe, bestimmte Ziele zu erreichen (Müller, 2020, S. 119 & 214). So „wandelt sich die Paradoxie in eine sinnvolle risikobewertete Handlung. Die Preisgabe von Daten ist dann nicht mehr irrational oder paradox, sondern dem Vorhaben liegt eine Risikoeinschätzung und damit eine Vorstellung zu den Kosten der Datenpreisgabe zugrunde.“ (Müller, 2020, S. 119) Auch Kokolakis attestiert, dass die Dichotomie zwischen dem theoretisch vorhandenen Problembewusstsein und dem widersprüchlichen Verhalten bei der Nutzung webbasierter Technologien nicht mehr als Paradoxon betrachtet werden sollte, da aktuelle Literatur mehrere logische Erklärungen hierfür liefert (Kokolakis, 2017, S. 130).

> Das Privatheitsparadox wird dadurch nur eine Metapher für einen Irrweg zahlreicher wertebelasteter Annahmen zu Verhaltensweisen von Nutzern, die ihre Rationalität bei der Preisgabe von persönlichen Daten aufgeben. Dies geschieht jedoch meist nicht bedingungslos, sondern im Rahmen eines expliziten oder impliziten Vertrages für bestimmte Zwecke und nur in bekannten Kontexten. Damit entfällt die Basis für das Privatheitsparadox (Müller, 2020, S. 120).

Unter der Annahme, das Privatheitsparadox existiere, wäre dies ein Ansporn für Betreiber von Online-Plattformen und webbasierten Anwendungen, mehr Daten zu sammeln. Politische Entscheidungsträger schieben dem aber einen Riegel durch beispielsweise die Europäische Datenschutzgrundverordnung vor – auf Grundlage der Bedenken von Nutzern und Nutzerinnen. Die Dichotomie des Privatheitsparadox schwächt wiederum die Existenzgrundlage getroffener Maßnahmen zum Schutz der Daten (Kokolakis, 2017, S. 122 f.).

Im Hinblick auf das zu Beginn des Kapitels genannte Zitat steht die Wahrheit somit wieder auf beiden Beinen, ist klar erkennbar, und das Paradox löst sich vorerst auf. Kann somit davon ausgegangen werden, dass Daten zu Großteilen auf gänzlich freiwilliger Basis preisgegeben werden?

4.6 Freiwilligkeit bei der Freigabe von Daten

Auch wenn es vor Jahren noch Gang und gäbe war, Nutzern und Nutzerinnen das Lesen von Nutzungsbedingungen und Datenschutzhinweisen ans Herz zu legen, so kann heutzutage zu Recht an der Sinnhaftigkeit dieser Empfehlung gezweifelt werden. Der in der Offline-Welt viel gegebene Ratschlag, das „Kleingedruckte“ zu lesen, lässt sich in der Online-Welt nur mit extremem Mehraufwand anwenden, wie folgend dargestellt wird (Čas et al., 2002, S. 18).

Die Anthropologin Barassi veranschaulicht mit folgendem Beispiel die Problematik – ein Szenario, das Nutzern und Nutzerinnen des Internets bekannt ist: Um die allgemeinen Datenschutzbestimmungen der EU einzuhalten (DSGVO), erscheint ein Pop-up-Fenster auf der Website, welches nach der Zustimmung zur personalisierten Seitennutzung fragt. Es bietet ebenfalls die Möglichkeit, dies zu verneinen und mehr über Dritte zu erfahren, mit denen die Daten bei Zustimmung geteilt werden.

Ein zustimmender Mausklick führte Barassi (2021) zu einer langen Liste von Unternehmen auf der ganzen Welt, die bei Zustimmung Zugriff auf ihre personenbezogenen Daten bekommen. Neben dem Namen jedes Unternehmens befand sich ein Link zu dessen jeweiligen Datenschutzbestimmungen. Barassi machte sich die Mühe und zählte, wie viele Datenschutzerklärungen sie lesen müsste, um herauszufinden, was mit ihren personenbezogenen Daten bei Besuch einer einzelnen Webseite geschieht. Es waren – nota bene – 439 (Barassi, 2021).

Bei dem Versuch, diese Ergebnisse zu reproduzieren, besuchte ich die Webseite erwachsenenbildung.at. Prompt erscheint das Cookie-Banner, welches nach einem Klick die Schaltfläche „Show details“ Verlinkungen zu zehn unterschiedlichen Datenschutzbestimmungen offenbart, angefangen von Firmen wie Microsoft, Google, TED usw. Folgt man diesen Links, können seitenlange Datenschutzbestimmungen oftmals nicht gelesen werden, weil ein weiteres Cookie-Banner nach der Zustimmung zur personalisierten Seitennutzung fragt.

Während die Webseite erwachsenenbildung.at auch ohne Zustimmung zum personalisierten Zugriff einwandfrei nutzbar ist, wird Nutzern und Nutzerinnen oftmals keine Wahl gelassen. Seien es eine Zeitersparnis, der falsche Moment, oder – wie bereits erwähnt – seitenlange juristische Klauseln, die bei Menschen ein Gefühl der Ohnmacht oder gar des Kontrollverlustes hervorrufen können. In extremen Fällen gibt es keine Möglichkeit, der Personalisierung und damit der Weitergabe von personenbezogenen Daten an Dritte zu widersprechen mit Ausnahme eines gänzlichen Verzichts auf den jeweiligen Dienst (Mühlhoff, 2019, S. 82).

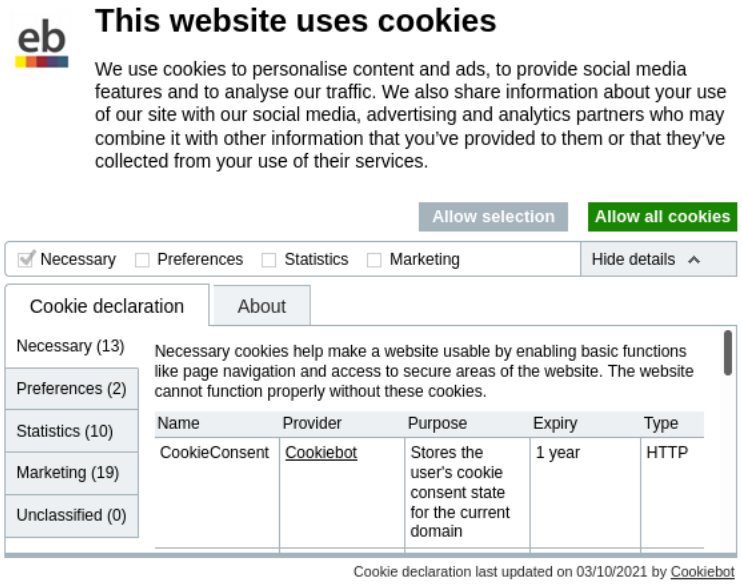

Abbildung 6: Cookie-Banner auf erwachsenenbildung.at. Quelle: Screenshot des Verfassers vom 14.10.2021.

Für die vorliegende Arbeit relevant, unterscheidet Mühlhoff zwischen zwei Formen von Unfreiwilligkeit, die im Folgenden jeweils in den zwei konkreten Fallstudien illustriert werden. Das erste Fallbeispiel illustriert, welche Rolle Cookies beim Arbeiten mit dem World Wide Web spielen.

4.6.1 Cookies

Kaum einem Mensch gelingt es heutzutage, sich dem breiten Repertoire an Google Dienstleistungen zu entziehen. Bei der Nutzung dieses umfassenden Portfolios an Angeboten entstehen viele Daten, welche unfreiwillig und unbemerkt von Google erhoben werden. Eingeloggt in eine der zahlreichen Google-Dienstleistungen, beispielsweise Gmail, Google Drive oder YouTube, erzeugt Google ein Cookie, das Nutzer und Nutzerinnen durch ihr Google Konto eindeutig identifiziert. Dies ermöglicht, den detaillierten Suchverlauf, das Klickverhalten und weitere Informationen einem bestimmten Benutzerkonto zuzuordnen.

Diese unbemerkte, aber nicht heimliche Erhebung von Daten führt dazu, dass Nutzer über einen unbegrenzten Zeitraum hinweg verfolgt werden können (Mühlhoff, 2019, S. 90). Denn Cookies werden standardmäßig beim Schließen des Browsers nicht gelöscht, auch nicht beim Neustart des Endgerätes.

Dies ermöglicht Google sogar, verschiedene Nutzungssessions, die „auf verschiedenen Geräten erfolgen, miteinander zu verknüpfen und auf diese Weise lebenslange und geräteübergreifende Suchhistorien anzulegen“ (Mühlhoff, 2019, S. 91) – von E-Mail-Inhalten und Dokumenten aus Google Drive zum Standort des Android-Smartphones, gespeicherten Orten in Google Maps, Telefonnummern von Freunden, Telefonanrufe und SMS-Nachrichten. Es gibt kaum Daten, auf die Google keinen Zugriff hat (Mühlhoff, 2019, S. 91). In der gleichen Art und Weise operieren beispielsweise Facebook, Amazon oder Apple.

4.6.2 Einloggen mit nur einem Klick

Als weiteres Beispiel für die vorgesetzte Freiwilligkeit der Preisgage von Daten nennt Mühlhoff Single Sign-on Services, wie von Google und Facebook betrieben und am Beispiel von Mentimeter in 4.1 von mir beschrieben. Im Gegensatz zur unbemerkten, aber nicht heimlichen Erhebung von Daten aus dem ersten Fallbeispiel, in denen technischen Einrichtungen verdeckt operieren, handelt es sich hierbei um eine subjektiv freiwillige und wissentliche, aber nicht voll informierte Weitergabe von Daten.

Vor allem Googles und Facebooks Authentifizierungsschnittstellen sind sehr verbreitet. Aber vor allem im Bereich der Wissenschaft und Lehre dürfte die dezentralisierte Lösung Shibboleth vielen ein Begriff sein. Es steht allerdings in Bezug auf datenschutzrechtliche Bedenken in keinem Vergleich zu Google und Facebook. Zur Veranschaulichung von Single Sign-on-Services skizziert Mühlhoff (2019) folgendes Beispiel:

> Der Verwendung des Facebook Log-ins würde in der ‚realen Welt‘ entsprechen, wenn man stets beim Betreten eines Shops die Liste seiner Interessen, Freunde, Likes, Statusposts, Sprachfähigkeiten, Schulabschlüsse, Berufserfahrungen etc. am Eingang abgeben würde. Der Shop könnte dann ganz schnell die räumliche Anordnung seiner Produktregale, die Anordnung der Produkte in diesen Regalen, sowie die Preise der Produkte und mögliche Sonderangebote auf diesen einen Benutzer abstimmen. Das gleiche gilt auch, wenn man ein Versicherungsbüro betritt oder sich um einen Job bewirbt – um nur wenige Felder zu nennen, in denen diese Daten verwertet werden (Mühlhoff, 2019, S. 93).

Sobald ein Single-Sign-In-Service verwendet wird, erhält nicht nur der verwendete Dienst, sondern ebenfalls der Betreiber des Single-Sign-In-Service wertvolle Echtzeit-Information, dass dieser Nutzer oder die Nutzerin soeben diesen bestimmten Service nutzt (Mühlhoff, 2019, S. 96).

Eine detaillierte Auseinandersetzung mit diesen für die Erwachsenenbildung vermeintlich lediglich peripher interessanten, alltäglichen Hintergrundprozessen muss umso mehr von Bedeutung sein. Denn „Sachen zu verkomplizieren, ihre Details und Ambivalenzen sichtbar zu machen, ist im kulturellen und subjektiven Verhältnis zu Technik verpönter denn je – und in diesem Punkt liegt eine unbemerkte Komplizenschaft einer über politische, soziale und Klassengrenzen hinweg weit verbreiteten subjektiven Einstellung mit den ökonomischen Interessen von“ Big Tech (Mühlhoff, 2019, S. 97).

Denn eine Kombination aus „Resignations- und Ohnmachtshaltung gegenüber Technik“ und eine „subjektiv empfundene (...) Unverzichtbarkeit“ (Mühlhoff, 2019, S. 82 & 105) von etlichen webbasierten Anwendungen von nur wenigen Anbietern gibt diesen ein riesiges Meer an Daten. Dies führt zu noch nie dagewesener Machtkonzentration von wenigen Technologiekonzernen in unserer Gesellschaft.

> Dazu kommt, dass die technologische Entwicklung es zunehmend ermöglicht, auch im Bildungssektor die regionalen Grenzen der Vermarktung zu sprengen (…). Konsequenterweise wird ja heute auch von allen Seiten das Lernen mit Hilfe von Informations- und Kommunikationstechnologien als riesiger Fortschritt gepriesen (…). Und die notwendigen Investitionsmittel, um Lernangebote zu entwickeln, die die Möglichkeiten der Informations- und Kommunikationstechnologien wirklich perfekt ausnützen, bringt ein großer internationaler Konzern allemal noch leichter auf, als irgendeine nationale Bildungsagentur. (Ribolits, 2010, S. 235)

Infolgedessen sehen wir uns konfrontiert mit wenigen Unternehmen, welche mit dem Zugang zu persönlichen Daten und Informationen einen Wettbewerbsvorteil errungen haben, der noch nie zuvor dagewesene Gefahren mit sich bringt.

5 Machtverhältnisse

„Those who do not move, do not notice their chains.“

Rosa Luxemburg[5]

Seit dem 11. September 2001 wird der Diskurs um öffentliche Sicherheit dominiert von unterschiedlichen staatlichen Überwachungsprojekten (Ganz, 2018, S. 235). Globaler Terrorismus wird dabei maßgeblich als Grund genannt.

> Die Anlässe für diese Entwicklungen liegen auf der Hand: Berechtigte Furcht und das Bedürfnis nach Sicherheit kann sich paranoid verselbstständigen, in das Gegenteil umschlagen und den autoritären Überwachungsstaat erzeugen, der sich wie eine Krake mit seinen Informationsnetzen über die Welt ausbreitet. Die Glasfaserkabel und Internetknoten des World Wide Web sind die Krakenarme, die das Programm Upstream des britischen Dienstes GCHQ (Government Communication Headquarters) nutzt. Der amerikanische Partnerdienst NSA greift mit dem Programm Prism auf die Daten von Firmen wie Microsoft, Google, Facebook, Yahoo und Apple. Landesgrenzen werden bei dieser Ausspähung unterlaufen und Landesgesetze formal noch nicht einmal verletzt (Mainzer, 2018, S. 130 f.).

5.1 Überwachungsgesellschaft

Moderne Gesellschaften sind als Überwachungsgesellschaften definiert worden, weil sie strukturell darauf angewiesen sind, persönliche und organisatorische Daten zu sammeln, um effizient arbeiten zu können. Die Toleranz gegenüber einer verstärkten Überwachung zu Sicherheitszwecken nimmt ebenfalls zu und ergibt sich hauptsächlich aus der geringeren Bereitschaft moderner Gesellschaften, jede Art von Risiko zu akzeptieren sowie das Auftreten neuer globaler und weniger vorhersehbarer Bedrohungen (Chandler, 2009, zit. n. PRESCIENT, 2011, S. 46).

[5] Dieser allgemein bekannte Ausspruch wird oft Rosa Luxemburg zugeschrieben, da sie oft Metaphern über das Zerbrechen oder Sprengen von Ketten verwendete. Der wahre/die wahre Verfasser/in des Zitats bleibt unbekannt.

Die Macht und Fähigkeit von Regierungen und privaten Organisationen, private Informationen zu sammeln und zu analysieren, nimmt zu. Die Privatsphäre der Menschen wird oft der Bequemlichkeit oder Sicherheit geopfert (Chandler, 2009, zit. n. PRESCIENT, 2011, S. 46). Eine Evaluierung von Überwachungspraktiken seit 9/11 bleibt aus. Die Aussage, mehr Überwachung führe zu mehr Sicherheit, wurde nie belegt.

Die überwiegende Mehrheit der Bürgerinnen und Bürger geht durch ihr tägliches Leben in dem Glauben, dass sich Überwachungsprozesse nicht gegen sie selbst richten, sondern gegen Übel- und Unrechtstäter, siehe hierzu 4.3. Trotz aller Anzeichen dafür, dass die Überwachung des individuellen Verhaltens zur Routine und zum Alltag geworden ist, herrscht die Ansicht vor, dass Überwachungsmechanismen stets auf andere und nicht auf das eigene ich gerichtet sind (Bennett, 2008, S. 97 f.).

Viele Autoren und Autorinnen sind sich einig: Die Überwachung stellt uns vor ständige ethische Paradoxien, denn sie ist nützlich, aber schädlich, willkommen, aber anstößig, ein notwendiges Übel, aber eine üble Notwendigkeit (PRESCIENT, 2011, S. 47). Der Schutz der Privatsphäre ist dabei ein wichtiger Aspekt, durch den viele neue Technologien, insbesondere neue Überwachungstechnologien, kritisch betrachtet werden (Finn et al., 2013, S. 7).

Neben dem profitorientierten Geschäft mit den Daten in der Privatwirtschaft ist der zweite große Nutznießer in einer ökonomisch motivierten Datengesellschaft der Staat. Zu viel Überwachung führt zu Verletzungen der Privatheit und kann zu schleichendem Autoritarismus führen.

> Berechtigte Furcht und das Bedürfnis nach Sicherheit kann sich paranoid verselbstständigen, in das Gegenteil umschlagen und den autoritären Überwachungsstaat erzeugen, der sich wie ein Krake mit seinen Informationsnetzen über die Welt ausbreitet. (Mainzer, 2018, S. 130 f.)

In der Mitte des 20. Jahrhunderts entwarf George Orwell die Vorstellung des Big Brothers, in der die Regierung als Überwachungsorgan fungiert und praktisch jedes Individuum jederzeit überwacht. Dies mag dystopisch klingen, und bereits im Jahr 2000 hat Froomkin davor gewarnt, dass – sofern keine sozialen, rechtlichen oder technischen Kräfte eingreifen –, es vorstellbar ist, dass kein Ort auf der Erde existieren wird, an dem sich ein normaler Mensch der Überwachung entziehen kann.

Als Science-Fiction beschreibt Froomkin (2020) Technologien der Gesichtserkennung, Spracherkennung und die Möglichkeit, Echtzeit-Informationen über den Standort eines jeden Menschen liefern zu können. 72 Jahre nach Erscheinen von Orwells Bestseller „1984“ sind diese Technologien längst in den Alltag eines jeden Individuums in westlichen Industriestaaten eingezogen. Weiter prophezeit Froomkin (2020), die gesamte Kommunikation – mit Ausnahme einiger verschlüsselter Nachrichten – wird durchsuchbar und sortierbar sein und trifft auch hiermit genau ins Schwarze (2020, S. 1475).

5.2 Dataveillance

Angesichts der rasanten Zunahme von Technologien, die die Privatheit bedrohen, ist mehr und mehr unklar, ob die informationelle Privatsphäre zu erträglichen Kosten geschützt werden kann oder ob wir uns einer Ära ohne informationelle Privatheit nähern, einer Welt, die Clarke (1988) als „Data Surveillance“ bezeichnet (Clarke, 1988, zit. n. Froomkin, 2000, S. 1465; Froomkin, 2000, S. 1465).

Der Neologismus setzt sich aus den zwei englischen Begriffen „data“ für Daten und „surveillance“ für Überwachung zusammen und lässt sich in der deutschen Sprache als „Überwachung der Daten“ verstehen. Dataveillance beschreibt den rapiden Wandel von der (teuren) physischen und elektronischen Überwachung durch Kameras und Mikrofone von Personen hin zur (kostengünstigeren) Überwachung des Verhaltens von Menschen durch die stetig steigende Flut an Daten, welche Individuen tagtäglich erzeugen (Clarke, 1997).

Clarke vertritt die Ansicht, dass das „Big Brother“-Szenario – eine Welt, in der ein einziger, staatlicher „Big Brother“ über die Schulter schaut – nicht eingetreten ist, weil es unnötig ist, denn Technologiekonzerne haben eine Welt aufgebaut, die Individuen aus freien Stücken dazu bewegt, mehr von sich selbst online zu stellen, mehr Daten preiszuegben, um deren Gewinnspannen zu erhöhen (Clarke, 1997).

Diese ständige Überwachung wird von Individuen selbst durchgeführt, und zwar aus freien Stücken. Sie wird uns nicht von einer böswilligen Bürokratie, gesichtslosen Unternehmen oder einzelnen Personen oder Parteien aufgezwungen. Big Data, Metadaten und automatisierte Prozesse der modernen Datenverarbeitung liefern die Voraussetzung für totalitäre Regime, schleichend Einzug ins 21. Jahrhundert zu halten. Grundlage hierfür ist die bewusste Einwilligung von Bürgern und Bürgerinnen, permanent Daten über sie zu erheben (Mainzer, 2018, S. 130 f.).

Dataveillance ist somit effizienter als die Personifizierung einer Kollektivherrschaft, sei es vom technischen, wirtschaftlichen oder politischen Standpunkt aus (Clarke, 1988, zit. n. Bennett, 2008, S. 15). Es geht allerdings nicht nur darum, dass Individuen weniger Privatsphäre haben, sondern dass diese neuen Überwachungspraktiken zu qualitativen Veränderungen in der Art und Weise geführt haben, wie Individuen deren Interaktionen mit Institutionen und Technologien subjektiv erleben (Bennett, 2008, S. 17).

5.3 Surveillance Capitalism

30 Jahre nach Clarkes neologistischer Schöpfung von dataveillance versucht die Autorin Zuboff in ihrem Buch „Das Zeitalter des Überwachungskapitalismus“ ein Terra incognita zu vermessen (Zuboff, 2018, S. 33). Sie spricht dabei gar von der „Verfinsterung des digitalen Traums und dessen rapide Mutation zu einem ganz und gar neuen gefräßigen kommerziell orientierten Projekt.“ (Zuboff, 2018, S. 22) Der Überwachungskapitalismus hat unsere Politik und Kultur in einer Weise geprägt, die viele Menschen nicht wahrnehmen.

> Überwachungskapitalismus beansprucht einseitig menschliche Erfahrung als Rohstoff zur Umwandlung in Verhaltensdaten. Ein Teil dieser Daten dient der Verbesserung von Produkten und Diensten, den Rest erklärt man zu proprietärem Verhaltensüberschuss, aus dem man mithilfe fortgeschrittener Fabrikationsprozesse, die wir unter der Bezeichnung ‚Maschinen- oder künstliche Intelligenz‘ zusammenfassen, Vorhersageprodukte fertigt, die erahnen, was sie jetzt, in Kürze oder irgendwann tun (Zuboff, 2018, S. 22).

5.3.1 Informationelle Asymmetrie

Dabei sind Zugang und Art der Auswertungsmethode dem Individuum gänzlich verwehrt und liegen in den Händen von wenigen privaten Unternehmen. Individuen können somit weder nachvollziehen, auf welchen Datengrundlagen Entscheidungen über ihr Leben getroffen werden, noch haben sie einen Kontrollmechanismus an der Hand, um Einfluss darauf nehmen zu können (Westermann et al., 2018, S. 40).

> Überwachungskapitalisten wissen alles über uns, während ihre Operationen so gestaltet sind, uns gegenüber unkenntlich zu sein. Überwachungskapitalisten entziehen *uns* unermessliche Mengen neuen Wissens, aber nicht *für* uns; sie sagen unsere Zukunft nicht zu unserem, sondern zu anderer Leute Vorteil voraus (Zuboff, 2018, S. 26).

Somit entsteht eine zunehmende informationelle Asymmetrie, die es einigen wenigen Unternehmen ermöglicht hat, eine bislang unbekannte informationelle Überlegenheit aufzubauen (Müller, 2020, S. V; Westermann et al., 2018, S. 40). Müller zählt zu diesen Hegemonen die US-amerikanischen Unternehmen Amazon, Apple, Facebook, Google und Microsoft. Er ergänzt diese fünf mit den chinesischen Unternehmen mit Alibaba, Baidu und Tencent.

5.3.2 Informationsmacht

Digitalisierung und ihre Durchdringung in den Alltag eines jeden und jeder Einzelnen haben den Aufbau von territorial nicht verhafteten, ökonomisch als auch politischen Megakonzernen, welche ihren Wert aus unseren Daten schöpfen, enorm erleichtert. Diese nutzen ihre Informationsmacht, indem sie das Zurückgreifen auf Datenbestände, Handlungen von Dritten so beeinflussen, „dass diese nicht mehr allein durch die von einer Person selbst gewählten Präferenzen bestimmt sind.“ (Müller, 2020, S. 81)

Das bekannteste Beispiel hierfür ist wohl der Fall von Cambridge-Analytica. Durch die Auswertung von Massen an persönlichen Daten durch das britische Unternehmen Cambridge-Analytica wurde erstmals die Bandbreite des Einflussspektrums von Big Tech Unternehmen wie Facebook aufgezeigt.

Dank der von Facebook erhobenen Daten konnte das britische Unternehmen das Wahlverhalten einer großen Anzahl an Einzelpersonen beim BREXIT-Referendum und bei der amerikanischen Präsidentschaftswahl 2016 beeinflussen, indem alle Wähler und Wählerinnen kategorisiert wurden. Lediglich unentschlossene Wähler und Wählerinnen wurden unter besonderer Rücksichtnahme gezielt kontaktiert. Dadurch konnte kosteneffizienter und fokussierter Wahlkampf auf die Gruppe von Wählern, deren Entscheidungsfindung am empfänglichsten für Beeinflussung war, betrieben werden (Doward & Gibbs, 2017).

Die Auswirkungen dieser großangelegten Verhaltensmanipulation sind von globaler Bedeutung, doch es lässt sich die berechtigte Frage stellen, ob eine Einwilligung oder informierte Zustimmung der Betroffenen noch eine Rolle spielt (Müller, 2020, S. 6). „Die bittere Erkenntnis, dass der Fall Cambridge-Analytica kein Vergehen gegen den Datenschutz war, zeigt die Dichotomie von Erwartung und Wirklichkeit.“ (Müller, 2020, S. 66)

Fragen, die nicht oft genug gestellt, geschweige denn beantwortet werden, sind hierbei: Welche politischen Veränderungen von Macht- und Herrschaftsverhältnissen gehen mit dem monopolisierten Besitz von Daten und deren Zugang einher? (Iske et al., 2020, S. 3). Ob das Ziel nun „Informationsmacht“, „Informationsdominanz“ oder „Entscheidungsüberlegenheit“ heißt: Alle Begriffe zielen auf die Maximierung der Datenerhebung und Datenanalyse ab. Diese wird wiederum durch den manipulativen Eingriff in Handlungen von Individuen verstärkt, wodurch ein Teufelskreis entsteht, der den „gläsernen Menschen“ am Ende sieht.

Kontrollverlust, Überforderung und Dauerstress könnten am Ende dazu führen, dass keinerlei Gewalt von Nöten ist, um das deutsche Grundgesetz Art. 1 einzuschränken: Die Würde des Menschen ist unantastbar. Doch unsere eigene Bequemlichkeit lässt uns eine schleichende Veränderung dulden und somit unsere Würde angreifbar machen (Mainzer, 2018, S. 130 f.).

Čas et al. bringen es in einer Studie im Auftrag der ehemaligen Bundeskammer für Arbeiter und Angestellte auf den Punkt:

> Natürlich kann und soll niemand gezwungen werden, aus seinem Privatleben ein gut gehütetes Geheimnis zu machen, ebenso wenig darf aber Unkenntnis oder Sorglosigkeit zu einem Verlust von Grundrechten verbunden sein. Unwissenheit schützt nicht vor Strafe, darf aber auch nicht dazu führen, dass Rechtsverletzungen ungehindert und ungestraft möglich werden. (Čas et al., 2002, S. 35)

Eine grundlegende Veränderung des Machtungleichgewichts zwischen Unternehmen und Einzelpersonen bei der Erhebung, Verarbeitung und Speicherung personenbezogener Daten scheint die Datenschutzgrundverordnung der Europäischen Union zu sein. Sie zielt darauf ab, das Recht des Einzelnen auf Zugang und Kontrolle der Verwendung seiner personenbezogenen Daten zu stärken (Goddard, 2017, S. 3).

Im nächsten Abschnitt der Arbeit werden Gesetzesgrundlagen, die vermeintlich zum Schutz von Individuen geschrieben wurden, kritisch beleuchtet und untersucht, inwiefern diese wirklich zum Schutz der Privatheit von Einzelpersonen beitragen.

6 Das Recht auf Datenschutz

„Relying on the government to protect your privacy is like asking a peeping tom to install your window blinds.“

John Perry Barlow[6]

Der Schutz der Privatheit, der Privatsphäre und der eigenen Daten ist in einer hoch digitalisierten Welt ohne rechtliche Regeln nicht vorstellbar. Ziel dieser Regeln sind ein Schutz der Interessen der Bürger und Bürgerinnen sowie die Verhinderung von nachteiligen gesamtgesellschaftlichen Auswirkungen.

Der schmale Grat, den Justitia dabei zu gehen hat, ist dabei, das Recht des Einzelnen und der Einzelnen zu wahren, ohne dabei Potenziale neuer Technologien und damit einhergehendes Wirtschaftswachstum einzuschränken (Westermann et al., 2018, S. 7).

> In einem technisch-rechtlichen Sinne, liegt das Dilemma der Digitalisierung im Widerspruch um den Schutz von Personen und der Förderung von Innovationen. Die digitale Transformation hat in Europa den Schutz nur der primären Daten in der Datenschutzgrundverordnung (DSGVO) reguliert, wobei ein Rückblick auf die Sozialgesetzgebung vor ca. 150 Jahren und die heftige Kritik an der DSGVO den Verdacht aufkommen lässt, dass mit den Daten ein nachrangiger Gegenstand reguliert wurde, da der Schutz von Menschen hätte gemeint sein müssen. (Müller, 2020, S. 2)

Das Recht auf Privatsphäre findet sich in der „Allgemeinen Erklärung der Menschenrechte“.

[6] Barlow, J. P. (2018, 8. Februar). The Guardian view on internet privacy: it’s the psychology, stupid. The Guardian. Abgerufen 16. November 2021, von https://www.theguardian.com/global/commentisfree/2018/feb/08/the-guardian-view-on-internet-privacy-its-the-psychology-stupid.

In Artikel 12 heißt es:

> Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen. (A/RES/217, UN-Doc. 217/A-(III))

Daraus ist ersichtlich, dass zwar das Recht auf Privatsphäre im Sinne des Örtlichen ein Menschenrecht darstellt, die informationelle Dimension des Privaten verständlicherweise noch keine Erwähnung findet. Privatheit und Datenschutz werden aus den 1948 verkündeten Menschenrechten abgeleitet. Die „Charta der Grundrechte der Europäischen Union“ (EU-Grundrechtecharta) widmet sich in Artikel 8 dem „Schutz personenbezogener Daten“:

Artikel 8

Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht. (ABI. C 2012/326, S. 391)

Des Weiteren zielen Artikel 7, 9 und 15 auf den Schutz der Privatheit ab:

Artikel 7

Achtung des Privat- und Familienlebens

Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation. (ABI. C 2012/326, S. 391)

Artikel 9

Recht, eine Ehe einzugehen und eine Familie zu gründen

Das Recht, eine Ehe einzugehen, und das Recht, eine Familie zu gründen, werden nach den einzelstaatlichen Gesetzen gewährleistet, welche die Ausübung dieser Rechte regeln. (ABI. C 2012/326, S. 391)

Artikel 15

Berufsfreiheit und Recht zu arbeiten

(1) Jede Person hat das Recht, zu arbeiten und einen frei gewählten oder angenommenen Beruf auszuüben.

(2) Alle Unionsbürgerinnen und Unionsbürger haben die Freiheit, in jedem Mitgliedstaat Arbeit zu suchen, zu arbeiten, sich niederzulassen oder Dienstleistungen zu erbringen.

(3) Die Staatsangehörigen dritter Länder, die im Hoheitsgebiet der Mitgliedstaaten arbeiten dürfen, haben Anspruch auf Arbeitsbedingungen, die denen der Unionsbürgerinnen und Unionsbürger entsprechen. (ABI. C 2012/326, S. 391)

Recht als tragender Bewältigungsmechanismus der immanenten Datensammlung war bisweilen bedingt erfolgreich darin mithilfe von Grenzziehungen den Auswirkungen auf Individuum und Gesellschaft Einhalt zu gebieten, denn die Digitalisierung ist inhärent entgrenzend.

> So sind die digitalen Technologien und deren Infrastrukturen sowie die eingesetzten Geschäftsmodelle nicht oder nur ausnahmsweise regional, etwa national, begrenzt. Vielmehr sind sie häufig transnational oder auch global verfügbar. Gleiches gilt für die mit digitalisierter Technik erbrachten Dienste. Auch verschwimmen im IT-Bereich die Grenzen zwischen Hardware und Software und zwischen Dienstleistungen und den genutzten IT-Infrastrukturen als ihrem Medium. (Westermann et al., 2018, S. 20)

Erstmalig schaffte es die Europäische Union mit der „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG“ ein grenzübergreifendes Regelwerk zur Verarbeitung von personenbezogenen Daten einzuführen.

6.1 Datenschutz-Grundverordnung

Nach langen und intensiven Verhandlungen trat am 25. Mai 2018 die EU-Datenschutz-Grundverordnung (DSGVO) in Kraft und lieferte der Europäischen Union einen neuen europaweiten Rahmen für den Datenschutz (Westermann et al., 2018, S. 41). Angetrieben von einem philosophischen Ansatz für den Datenschutz, der auf dem Konzept des Schutzes der Privatsphäre als grundlegendes Menschenrecht (wie in der EU-Grunderchtcharta verankert) beruht, wurde die Verordnung zwar in der Europäischen Union eingeführt, entfaltet ihre Wirkung jedoch de facto auf die ganze Welt (Goddard, 2017, S. 1).

Ihre Rechtsvorschriften umfassen einen extraterritorialen Geltungsbereich, d. h. sie gelten für Einrichtungen außerhalb der EU, die personenbezogene Daten von in der EU ansässigen Personen verarbeiten, indem sie ihnen Waren und Dienstleistungen anbieten oder ihr Verhalten überwachen bzw. beeinflussen, unabhängig davon, ob die Verarbeitung in der EU erfolgt oder nicht.

Die DSGVO muss nicht erst von den Mitgliedsstaaten der Europäischen Union interpretiert werden, sondern entfaltet ihre Wirkung direkt (Müller, 2020, S. 60). Sie löst eine Richtlinie aus dem Jahr 1994 ab, welche datenverarbeitende Stellen grundsätzlich nur dann zur Rechenschaft ziehen konnte, wenn diese im Hoheitsgebiet von Europa niedergelassen waren.

Damit kann das europäische Datenschutzrecht seinen Einfluss auf Auslandssachverhalte erstrecken, bei denen ihm bisher die Hände gebunden waren (Djeffal, 2019, S. 177 & 180 f.). Die DSGVO ist der wichtigste Beitrag zur Regulierung der Digitalisierung (Müller, 2020, S. VI).

6.1.1 Einwilligung

Eine der wichtigsten Neuerungen, die mit Einführung der DSGVO einhergeht, ist die Geheimhaltung mit informierter Zustimmung zur Datenfreigabe. Dies beschreibt das Prinzip des Datenschutzes, wie er heute für Europa gültig ist und mit der DSGVO in Gesetzesform vorliegt (Müller, 2020, S. 114).

Die Einwilligung muss hierbei freiwillig, spezifisch und in Kenntnis der Sachlage gegeben und durch eine eindeutige bestätigende Handlung nachgewiesen werden. Des

Weiteren muss nachvollziehbar sein, zu welchen Zwecken die Daten weiterverarbeitet werden (Goddard, 2017, S. 2).

Erst durch diese informierte Einwilligung bzw. Zustimmung der Nutzer und Nutzerinnen (Data Subject) wird dem Auftragsverarbeiter (Data Processor) im Auftrag des Verantwortlichen (Data Controller) gestattet, personenbezogene Daten weiterzuverarbeiten. Dabei entscheidet stets der Verantwortliche über die Zwecke und Mittel der Verarbeitung. Der Auftragsverarbeiter ist zumeist ein Dritter, der vertraglich an den Verantwortlichen gebunden ist (Müller, 2020, S. 60).

Um was es sich bei einer Einwilligung handelt, definiert Art. 4 Nr. 11 der EU-DSGVO:

> [J]ede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

In Kapitel 4 wurde bereits aufgezeigt, inwieweit Individuen wirklich freiwillig handeln und inwiefern sie oftmals die Freiwilligkeit vorgesetzt bekommen, denn:

> [s]ind bestimmte Dienste für die Nutzerinnen und Nutzer allerdings aus gewichtigen beruflichen und persönlichen Gründen, etwa für das Handeln in der Arbeitswelt oder für die gesellschaftliche Teilhabe an Kommunikation, praktisch unverzichtbar und gibt es, wie es insbesondere in den oligopolisierten Märkten häufig der Fall ist, keine Konkurrenzangebote vergleichbarer Qualität, bleibt den Nutzerinnen und Nutzern praktisch nichts anderes übrig, als die Einwilligung zu erteilen (Westermann et al., 2018, S. 43)

Im Zuge der Digitalisierung und ihrer Durchdringungstiefe in den Lebensalltag von Individuen wird das Sammeln von Daten immer weniger eine Frage der freiwilligen vertraglichen Einwilligung sein.

Einerseits steht die Teilhabe an der digitalen Öffentlichkeit, welche für immer weniger Personen ein reines Freizeitvergnügen darstellt, sondern vor allem aufgrund des pandemiebedingten Digitalisierungsschubs für viele Menschen Bedingung ihres

Einkommenserwerbs ist. Andererseits werden Personen, die aus diesen Gründen auf ihre Rechte aus der DSGVO verzichten, nicht geschützt (Müller, 2020, S. 60).

Der Anteil der Personen, die zur Teilhabe an der digitalen Öffentlichkeit bewusst auf Datenschutz verzichten, beläuft sich laut Acquisti (2017) auf beeindruckende 75 Prozent.

„Die DSGVO hindert 75 % der Datensubjekte nicht daran, persönliche oder sogar für sie nachteilige Daten im Netz bekannt zu geben (…), wenn sie sich davon Vorteile versprechen." (Acquisti, 2017, zit. n. Müller 2020, S. 66)

Welche Daten versucht die DSGVO demnach zu schützen?

6.1.2 Personenbezogene Daten

Personenbezogene Daten sind Informationen, die eine Person direkt oder indirekt identifizieren können, und umfassen insbesondere Online-Kennungen wie IP-Adressen, Cookies und digitale Fingerabdrücke sowie Standortdaten, die Personen identifizieren können (Goddard, 2017, S. 1).

Nach Art. 4 Nr. 1 der EU-DSGVO sind personenbezogene Daten:

> alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (…) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Damit verschließt die DSGVO ihren achtsamen Blick bewusst vor Metadaten. Während Datensparsamkeit und Datenminimierung als wünschenswerte Prinzipien von der DSGVO geregelt werden, wird die Datensparsamkeit dennoch aufgrund der Fortschritte der Datenanalyse und Big Data als „Auslaufmodell" angesehen, da in Kapitel 3 darauf hingewiesen wurde, wie einfach es ist Metadaten, welche von der DSGVO als anonyme Daten verstanden werden, zu personalisieren und somit bestimmten Personengruppen zuzuordnen (Müller, 2020, S. 114).

6.1.3 Kritik an der DSGVO

Anonymisierte Daten sind somit nicht mehr personenbezogenen im Sinne der DSGVO, obwohl sie de-anonymisiert und zur Re-Identifizierung von Personen verwendet werden können.

> Die Begrenzung der DSGVO auf persönliche Daten ist eine der gravierendsten Defizite des europäischen Datenschutzes, da dadurch die anonymen Daten, also ohne direkten Personenbezug, ungehindert von der DSGVO den Datensammlern überlassen werden, obwohl solche Daten leicht personalisiert werden können (Müller, 2020, S. VI).

Die DSGVO schützt somit die Preisgabe von personenbezogenen Daten, nicht jedoch die Preisgabe von Metadaten, welche in erster Instanz nicht als personenbezogen einzustufen sind. Datenverarbeiter allerdings erlauben, gezielte Rückschlüsse auf soziale Beziehungen, Gewohnheiten, Hobbies etc. zu ziehen, die in weiteren Verarbeitungsschritten sogar einzelnen Personen zugeordnet werden können (PRESCIENT, 2011, S. 50).

Der europäische Datenschutz bietet somit keinen vollständigen Schutz von Menschen, da auf der einen Seite die Datenpreisgabe von personenbezogenen Daten geschützt ist, auf der anderen Seite allerdings keine Regelungen bezüglich der Verwendung und Verarbeitung der Daten existieren.

Die DSGVO mag in diesem Sinne zwar ihren Teil dazu beitragen aufzudecken, wie sich die Datenverarbeitung im Verborgenen gestaltet. Dennoch spielt das, was sich hinter den geschlossenen Türen von datengierigen Unternehmen durch die angewendeten Datenanalysen aus den Daten ableiten lässt, welches Wissen sich daraus gewinnen lässt, und welche Schlussfolgerungen zu womöglich manipulativen Zwecken sich daraus ergeben, lediglich eine untergeordnete Rolle (Müller, 2020, S. 55).

Die DSGVO ist somit primär eine passive Regulierung, die versucht, Möglichkeiten des Missbrauches zu minimieren und infolgedessen einen Schutz „Wovor“ festschreibt. Andererseits schenkt sie dem Schutz „Wozu“ kaum Bedeutung und ahndet Eingriffe in die Privatheit von Einzelpersonen generell erst, nachdem diese stattgefunden haben (Müller, 2020, S. VI & 66). In Kapitel 2 wurde aufgezeigt, inwiefern es schwierig ist,

Eingriffe in die Privatheit als solche aufgrund ihrer indirekten Auswirkungen zu erkennen.

Der regulatorische Ansatz zum Schutz personenbezogener Daten der DSGVO ist somit ein wünschenswerter Schritt in die richtige Richtung, schafft es allerdings kaum, die Sammlung, Verarbeitung und Auswertung von Nutzerdaten, welche zur Informationsmacht weniger internationaler Unternehmen führt, zu unterbinden (Müller, 2020, S. 59).

Ein prädestiniertes Beispiel für die enorme Macht, welche aus Daten und deren Verarbeitung entspringt, ist der Fall von Cambridge Analytica und dem Brexit-Referendum. Uneingeschränkte Informationsmacht durch den Zugriff auf personenbezogene als auch Metadaten führt zu einer Bedrohung von Freiheitsrechten, gesellschaftlichen Werten und der Rechtsstaatlichkeit. Die beiden Fälle zeigen auf, inwiefern die DSGVO einerseits „zum Schrecken für den Mittelstand, sogar für Schulen und Sportvereine wird, jedoch das Problem des Datenmissbrauchs bis hin zur Manipulation nicht regelt." (Müller, 2020, S. 70)

Nichtsdestotrotz ist es der DSGVO zu verdanken, dass die Beeinflussung der US-amerikanischen Präsidentschaftswahl durch die Ergebnisse aus der Auswertung von Nutzerdaten von Facebook durch Cambridge Analytica eine weitreichende Diskussion angestoßen hat, da die Daten im Gegensatz zum Brexit-Referendum zwar nicht von Unionsbürgern und -bürgerinnen stammen, Cambridge Analytica jedoch ein britisches Unternehmen ist und zum damaligen Zeitpunkt noch ein Unternehmen der Europäischen Union war und demzufolge der europäischen DSGVO unterlag (Müller, 2020, S. 70).

6.1.4 Ein erster Schritt

Zusammenfassend lässt sich sagen, dass sich die DSGVO nicht als wirksam erwiesen hat, die Informationsmacht von Facebook, Google und Co. zu begrenzen (Müller, 2020, S. 71). Trotz Unzulänglichkeiten, Enttäuschungen und verpasster Chancen kann sie als Instrument eine solide Infrastruktur für den Schutz der Rechte von Unionsbürgern und -bürgerinnen bieten.

Müller (2020) attestiert, dass mit den Daten in der DSGVO „ein nachrangiger Gegenstand reguliert wurde, da der Schutz von Menschen hätte gemeint sein müssen." (Müller, 2020, S. 2) Ohne die vernetzte Zusammenarbeit von Regulierungsbehörden, Zivilgesellschaft und Bildungsträgern bleibt ein wirksamer Schutz von Daten und Menschen illusorisch.

Müller stellt die Frage, ob der Datenschutz ein Recht geworden ist, welches man sich leisten können muss (Müller, 2020, S. 58). Er gesteht sich seine saloppe Ausdrucksweise ein und konstatiert, die DSGVO schütze Daten ebenso wenig, wie ein Regenschirm den Regen schützt (Müller, 2020, S. VI). Geschützt werden müssen nicht die Daten, sondern die Menschen in einer digital veränderten Zeit (Müller, 2020, S. 70 f.).

Zahlreiche Beispiele in der vorliegenden Arbeit illustrieren das Dilemma, dem sich Nutzer und Nutzerinnen jeden Tag ausgesetzt sehen, wenn sie sich für bzw. gegen die Datenpreisgabe entscheiden müssen (siehe hierzu Kapitel 4). Als vermeintliche Hilfe zur Entscheidungsfindung ist die DSGVO nur bedingt geeignet.

Es sind nicht mehr rechtlich-regulative Rahmensetzungen, die den Schutz personenbezogener und Metadaten sicherstellen, sondern informierte Entscheidungen bei der Nutzung von webbasierten Anwendungen (Schrape, 2019, S. 223). Zwei Dinge sind dabei essenziell: Aufklärung und Kompetenzen.

7 Auswege für die Erwachsenenbildung

„We should all be working to maintain a sense of liberty and freedom, not working even harder to ensure that every single source of information regarding one's life is subject to surveillance by default, and indiscriminately so."

Gus Hosein[7]

Der kompetente Umgang im Internet und vor allem im Rahmen der Arbeit mit webbasierten Anwendungen wird zunehmend als Voraussetzung zur gesellschaftlichen Teilhabe gesehen. Längst ist der kritische Umgang mit Internettechnologien zum Bildungskanon zu zählen (Schön, 2015, S. 09–06). Dabei erzeugt die Technologie sowohl die Krankheit als auch einen Teil der Heilung (Wacks, 2015, S. 135 f.).

Unsere Lebenswelten wurden in die Welt der digitalen Daten überführt und machen somit unser aller Leben messbar, auswertbar und beeinflussbar (Westermann et al., 2018, S. 8). Aus diesem Grund ist die kritische Betrachtungsweise der Erfassung und Auswertung von Daten eine Aufgabe der Erwachsenen- und Weiterbildung.

> In der digitalen Weiterbildung selbst hat die Erwachsenenbildung Verantwortung zu übernehmen, indem sie AnwenderInnen dabei unterstützt, digitale Medien in möglichst sicherer Form zu nutzen, ihre Privatsphäre zu schützen und einen bewussten selektiven Umgang mit Medien zu pflegen. Dazu gehört anbieterseitig das Einhalten der Datenschutzgrundverordnung im Umgang mit personenbezogenen Daten, aber auch der möglichst weitgehende Verzicht auf unsichere bzw. datenhungrige Tools. (Aschemann, 2018, S. 69)

Bei der Nutzung von webbasierten Anwendungen kann zwischen drei Systemebenen unterschieden werden. Die Benutzeroberfläche der genutzten Anwendung ist dabei die Ebene des Sichtbaren und wird von dem jeweiligen Anbieter den Nutzern und Nutzerinnen zur Verfügung gestellt. Dahinter verbirgt sich die Ebene der Rechenprozesse

[7] Hosein, G. (2006). *Privacy as freedom*. MIT Press. Abgerufen 16. November 2021, von http://mitpress.mit.edu/main/home/default.asp. S. 145.

und Algorithmen, die beispielsweise beim Login auf der Webseite von Mentimeter oder beim Tätigen einer einfachen Suchanfrage im Hintergrund arbeitet.

Die Rechenleistung und physische Infrastruktur, die dafür benötigt wird, wird einerseits von Endgeräten der Nutzer und Nutzerinnen und andererseits von Großrechnern auf der ganzen Welt zur Verfügung gestellt. Jede einzelne dieser Systemebenen bietet den Nutzern und Nutzerinnen die Möglichkeit Einstellungen vorzunehmen, welche Einfluss nehmen darauf, wie die jeweilige Anwendung Daten nutzen darf (Datenschutz), inwiefern die Nutzer und Nutzerinnen darüber informiert (Transparenz), und inwiefern die Daten weiterverarbeitet werden (Datensicherheit) (Westermann et al., 2018, S. 7).

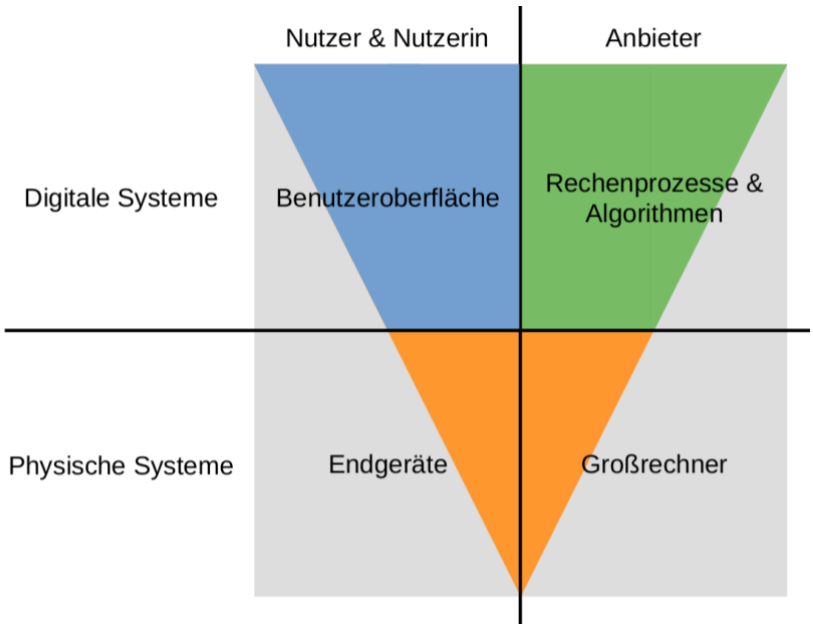

Abbildung 7 Die drei Systemebenen der Digitalisierung. Quelle: Eigene Darstellung des Verfassers angelehnt an Westermann et al., 2018, S. 7.

Bei der Auseinandersetzung mit den Herausforderungen einer kontinuierlichen Datensammlung und immanenten elektronischen Überwachung von Individuen ist es wesentlich, die einzelnen Quadranten innerhalb der drei Systemebenen und deren jeweilige Verknüpfungen stets zu berücksichtigen (Westermann et al., 2018, S. 7).

Der folgende Abschnitt untersucht eine Reihe von aktuellen Maßnahmengruppen, um die Beziehung zwischen Individuum und kommerzieller und/oder staatlich kontrollierter Organisationen, die Daten erheben, zu verstehen und normative Interventionen zu ermöglichen.

7.1 Regulatorische Maßnahmen

Die am häufigsten verwendete Linse, durch die die Problematiken, die mit der immanenten Datenerfassung einhergehen, ist die der Rechtssprache. Regulierungsmaßnahmen sind insofern politisch, als dass sie versuchen, ungerechte und ungleiche Machtverhältnisse zu verhindern, die das Individuum in eine verletzliche Beziehung bringen. Regulierungsmaßnahmen basieren somit auf einer Heuristik, die versucht, die Beziehung zwischen dem Einzelnen und der Gesellschaft zu rechtfertigen, zu rationalisieren und zu legitimieren, und die ihre Autorität daraus ableitet, dass das Kollektiv von Rechtsgrundsätzen reguliert wird, die im Interesse des Einzelnen wirken. Im Gegensatz dazu muss der Grundsatz der Rechte vom Gemeinwesen ebenso geschützt werden, wie er vom Einzelnen geltend gemacht werden muss (Pangrazio & Sefton-Green, 2020, S. 210 f.).

Dabei hat das vorherige Kapitel aufgezeigt, inwiefern sich regulatorische Schritte als unwirksam erwiesen haben, um die informationelle Asymmetrie auszugleichen und die enorme Informationsmacht von wenigen Unternehmen zu beschränken. Privatheit kann nicht ausschließlich von Regulierungsmaßnahmen geschützt werden.

7.2 Technische Hilfsmittel

Es gibt eine Reihe von technischen und gestalterischen Lösungen, um sich den Prozessen der Datenerfassung zu widersetzen oder um sie anzupassen. Während regulatorische Maßnahmen versuchen, Datenschutzprobleme und Informationsasymmetrien zu beheben, wirken technische Lösungen diesen entgegen, indem sie den reibungslosen Fluss von Daten in der digitalen Wirtschaft unterbrechen. Dies wird von Vertretern der orthodoxen neoklassischen Theorie als unerwünschte Marktstörung verstanden - siehe hierzu Kapitel 3 (Pangrazio & Sefton-Green, 2020, S. 210).

Technische Hilfsmittel können dabei helfen, den Einzelnen und die Einzelne auf die Datenverarbeitung aufmerksam zu machen und rüsten sie dabei gleichzeitig mit einer Reihe von Strategien zum Schutz ihrer Daten aus. In vielerlei Hinsicht entstehen technische Lösungen als Reaktion auf die fehlende Regulierung der Medien und basieren auf der Vorstellung, dass eine größere Transparenz die Bürger und Bürgerinnen dazu motivieren wird, eine Reihe von DIY-Tools und Technologien zum Schutz ihrer Daten auszuprobieren. Anstatt zu lernen, sich als gefügiges Datensubjekt dem

Überwachungskapitalismus zu unterwerfen, geht eine Zuhilfenahme von technischen Hilfsmitteln davon aus, dass der und die Einzelne die politische Bedeutungsbreite seiner bzw. ihrer Teilnahme versteht und animiert ist, aktiv zu werden (Pangrazio & Sefton-Green, 2020, S. 210).

Technische Hilfsmittel, um die Datenerhebung zu unterbinden, und webbasierte Anwendungen, die kaum Daten erheben, waren in der Vergangenheit Nischenprodukte, die ein spezielles Verständnis der zugrundeliegenden Sicherheitsmechanismen bedurften, um sie bedienen zu können. Dennoch sind viele der grundlegenden Konzepte, um die individuelle Privatheit zu schützen, einfach.

Mit Verschlüsselungstechnologien lässt sich zum Beispiel der Inhalt einer Nachricht vor Dritten verbergen. Nutzern und Nutzerinnen wird der Verschlüsselungsschlüssel anvertraut, der ähnlich wie ein langes, komplexes Passwort dazu dient, die Daten zu verschlüsseln, und einen Entschlüsselungsschlüssel, um sie wieder zu entschlüsseln. Facebook hat vor einigen Jahren genau diese Funktion für seinen Nachrichtendienst WhatsApp eingeführt, ohne dabei die Nutzererfahrung zu gefährden (Brody, 2016, S. 1 & 3).

Allerdings betrifft dies in keiner Weise die Erhebung von Metadaten (siehe hierzu in Kapitel 3.5). Alternativen zum datenhungrigen WhatsApp existieren. Leider ist die Akzeptanz von Alternativangeboten gering, was oftmals daran liegt, dass sie in der Bedienung komplexer und vor allem die Netzwerkeffekte bei konkurrierenden Diensten ungleich stärker ausgeprägt sind (Beyvers, 2018, S. 183).

Vielmehr lässt sich eine Blindheit gegenüber alternativen, weniger datenhungrigen Anwendungen feststellen. Dass alternative Anwendungen immer komplexer sind, muss nicht so sein. Der Nachrichtendienst „Signal“ oder der Browser „Brave“ zeigen als Open-Source-Projekte auf, dass Softwareentwickler und Softwareentwicklerinnen in der Open-Source-Gemeinschaft, die in der Regel die ersten sind, die Verschlüsselungs- und andere technische Hilfsmittel zum Schutz der Privatheit entwickeln, vermehrt das Design ihrer Anwendungen verbessern, um sie benutzerfreundlicher und zugänglicher für weniger versierte Nutzer und Nutzerinnen zu machen (Brody, 2016, S. 1).

Allerdings sei bei der Zuhilfenahme von technischen Hilfsmitteln und alternativen Anwendungen stets anzumerken:

> One fundamental challenge to both the usability and adoption of privacy-preserving tools is that privacy is considered a secondary task, as demonstrated through user-experience research. A secondary task is always subservient in users' minds to the primary task, which is whatever core activity the software is meant to enable: sending emails in an email client, exchanging instant messages in a chat program, or collaborating on documents in a file-sharing application. (Brody, 2016, S. 2)

Nutzer und Nutzerinnen können somit ihre Privatheit zu einem gewissen Maße mit technischen Hilfsmitteln und durch die Verwendung von alternativen Anwendungen schützen.

Während regulatorische Maßnahmen voraussetzen, dass Individuen in der Lage sind, sich über den bloßen Schutz durch das Gesetz und andere soziale Konventionen hinaus zu behaupten und sich auf Formen des Schutzes durch die Gesellschaft zu verlassen, betonen technische Hilfsmittel und die Zuhilfenahme von alternativen Anwendungen den Schutz durch ein gewisses Maß an Wissen und Kompetenz (Pangrazio & Sefton-Green, 2020, S. 211).

7.3 Pädagogische Maßnahmen

Die Idee, dass Menschen Wissen und Kompetenz über die Funktionsweise der Datenverarbeitung verfügen sollten, wird häufig als die vielversprechendste Lösung dargestellt. Wie dieses Wissen erworben und Kompetenzen diesbezüglich aufgebaut werden könnten, ist oft vage (Pangrazio & Sefton-Green, 2020, S. 211).

Die Anzeichen mehren sich dafür, dass weder regulatorische Maßnahmen noch technische Hilfsmittel messbaren Erfolg gebracht haben. Als Antwort darauf haben sich bisher pädagogische Maßnahmen als erfolgreichste Strategie zur Bekämpfung der Herausforderungen der Datenerfassung erwiesen.

Das Einfordern von Rechten und der Einsatz technischer Hilfsmittel zum Schutz personenbezogener Daten erfordert zweifelsohne ein gewisses Maß an Bewusstsein und Verständnis für Datenverarbeitungsprozesse. Datenkompetenz stellt somit einen wichtigen ersten Schritt zur Durchsetzung der Rechte und Strategien zum Schutz und zur Verwaltung persönlicher Daten und der Privatheit dar (Pangrazio & Sefton-Green, 2020, S. 211 f.).

7.4 Digitale Selbstverteidigung

Aus einer zweistufigen, schriftlichen Befragung von 16 Expertinnen und Experten aus unterschiedlichen Bildungs- und Arbeitsbereichen resultiert, dass „Praktische Schutzmaßnahmen für die eigene Privatsphäre im Umgang mit Daten“ und die Anwendung von „digitaler Selbstverteidigung“ einheitlich stark nachgefragt werden (Gapski et al., 2018, S. 117 f.).

Trotz vermeintlich datenschutzfreundlicher Voreinstellungen – ein Beispiel hierfür findet sich in Kapitel 4 – wird die Privatheit in vielen webbasierten Anwendungen grundsätzlich nicht geschützt und erfordert täglich das proaktive Handeln von Nutzern und Nutzerinnen. Zwischen nicht standardisierten, sich stetig ändernden Kontrollmechanismen sieht sich das Individuen bei der Wahl einer informierten Entscheidung ständig aufs Neue konfrontiert (Gapski et al., 2018, S. 153).

Hierbei kommt das Konzept der digitalen Selbstverteidigung und des Selbstdatenschutzes zur Anwendung. Digitale Selbstverteidigung beschreibt die Nutzung unterschiedlicher Methoden von Nutzer und Nutzerinnen mit dem Ziel, die intrusiven Eingriffe allgegenwärtiger Datenkraken abzuwehren. Von Verschlüsselungstechnologien, siehe Kapitel 4, bis hin zur Anonymisierung, ebenfalls behandelt in Kapitel 4, reichen die angewandten Werkzeuge. Zahlreiche Unterwanderdungseffekte beeinflussen den Erfolg dieser Handlungsstrategien.

> Der Einsatz dieser Verteidigungstechniken setzt nicht nur stets aktualisierte, fachliche und methodische Kenntnisse, sondern auch ein Vertrauen in die Werkzeuge selbst voraus, das nicht selten schon grundsätzlich erschüttert oder durch Sicherheitslücken gestört wurde. Bei konsequenter digitaler Selbstverteidigung kann es zur kommunikativen Abkapselung von der Peer-Group und zum Ausstieg aus den komfortablen digitalen Ökosystemen der Internet-Konzerne führen. (Gapski et al., 2018, S. 114)

Die beiden Autoren und die Autorin werfen die Frage in den Raum, ob eine kritische Medienbildung einen Verlust der kommunikativen Komfortzone herbeiführen soll oder sie durch alternative Sinn- und Kommunikationsangebote kompensieren soll (Gapski et al., 2018, S. 114).

Eine Auseinandersetzung mit dem Schutz der Privatheit und Fragen zum Datenschutz dürfen weder zum Kontrollverlust noch zum Verlust der kommunikativen Komfortzone führen.

Die Erwachsenenbildung muss Nutzern und Nutzerinnen in einer hochdigitalisierten Welt Werkzeuge für den Schutz der Daten und somit zum Schutz der Menschen an die Hand geben. Im Folgenden wird skizziert, wie Aufklärung einerseits und andererseits ein stärkeres Augenmerk auf das Konzept der Datenkompetenz dazu beitragen kann, negativen Auswirkungen des Überwachungskapitalismus entgegenzuwirken.

7.5 Datenkompetenz (Data literacy)

Weder am Arbeitsplatz noch zu Hause können Individuen davon ausgehen, dass deren webbasierte Anwendungen sicher sind. Sowohl auf die Technologie als auch auf das Gesetz muss ein differenzierter Blick zum Schutz von personenbezogenen Daten geworfen werden.

Ein Großteil dieser Daten, die erhoben und weiterverarbeitet werden, betrifft sensible Informationen: wo wir wohnen, wo wir arbeiten, wohin wir gehen; wen wir lieben, wen nicht, und mit wem wir unsere Zeit verbringen; was wir zu Mittag gegessen haben, wie viel wir Sport treiben, und welche Medikamente wir einnehmen; welche Geräte wir in unseren Häusern benutzen, und welche Themen unsere Emotionen anregen (Wacks, 2015, S. 135 f.; Weigend, 2017, S. 11).

> Welche Auswirkungen das Sammeln dieser Daten hat, ist nicht immer sofort klar ersichtlich. Wer sich im Internet bewegt, benötigt Wissen über die technischen Vorgänge (z.B. der Algorithmen) sowie die Tragweite des eigenen Handelns im Internet. Bei vielen Menschen muss ein neues Bewusstsein für den Wert ihrer Daten und den Schutz ihrer Privatsphäre geschaffen werden. Nur wer sich mit Fragen zu diesen Themen beschäftigt hat, wer sich Wissen über die neuen Medien angeeignet hat, ist in der Lage ein kritisch-reflektiertes Medienhandeln, und damit kritische Medienkompetenz auszubilden. (Lyß & Witt, 2018, S. 4)

Der bewusste Umgang mit eingesetzten Technologien in der Erwachsenenbildung kann dazu beitragen, Privatheit, Daten und somit Menschen zu schützen. Der Einsatz von webbasierten Anwendungen, technischen Hilfsmitteln und Technologie in der Erwachsenenbildung im Allgemeinen bedarf von Anfang an einer strengen Überprüfung

in Bezug auf seine Konsequenzen auf das Individuum und die Gesellschaft. Es muss kritisch reflektiert werden, aufgrund welcher Interessen digitale Technologien in Bezug auf ihren gesellschaftlichen Nutzen zu bewerten sind. Erwachsenenbildner und Erwachsenenbildnerinnen werden zu oft „mit scheinbar fertigen Ergebnissen konfrontiert." (Faulstich, 2018, S. 966)

Viel zu selten wird dabei kritisch über Auswirkungen diverser webbasierter Anwendungen reflektiert. Denn erst in der Rolle als aktive Nutzer und Nutzerinnen kann auf die Entwicklung von technischen Hilfsmitteln und webbasierten Anwendungen rückgewirkt werden.

Faulstich (2018) kommt zu dem Schluss, dass es unabdingbar ist, für eine verstärkte Verbraucheraufklärung über die Gestaltungsmöglichkeiten und über alternative Anwendungen zu sorgen (Faulstich, 2018, S. 966).

Bridle (2018) argumentiert, dass technologische Systeme auch dann verstanden werden sollten, ohne zuerst die Kunst der Softwareentwicklung zu erlernen oder eine Ausbildung zum Datenanalysten zu absolvieren. „[J]ust as one should not need to be a plumber to take a shit." (Bridle, 2018, S. 4)

Allerdings setzt bewusstes Nutzerverhalten voraus, dass Nutzer und Nutzerinnen informiert darüber sind, welche Daten sie erzeugen, wie diese gesammelt und verwertet werden. Es bedarf eines Grundwissens und einer kritischen Auseinandersetzung über potenzielle Gefahren und Risiken, die bei der Nutzung von webbasierten Anwendungen auftreten (Čas et al., 2002, S. 15).

Wie wäre auch anders eine Partizipation in der zivilgesellschaftlichen Debatte rund um digitale Technologien möglich, wenn es nur den Ingenieuren und Technikern vorbehalten wäre, an diesen zu partizipieren?

Deshalb hängt die Fähigkeit der Menschen, fundierte Entscheidungen über ihre Kommunikation zu treffen, nicht nur davon ab, wie die Technologie funktioniert, sondern auch davon, wie sie in der Gesellschaft funktioniert. Es geht zum Beispiel nicht nur darum zu wissen, wie man seine Privatsphäre-Einstellungen im Griff hat, sondern auch darum zu wissen, welche Folgen es haben kann, wenn man sich für eine Einstellung entscheidet (Seargeant & Tagg, 2018, S. 182).

Unabdingbar für die Erwachsenenbildung und alle, die im Spannungsfeld zwischen digitaler und analoger Welt ihre Profession ausüben, ist somit die sogenannte „Data literacy“ geworden (Weigend, 2017, S. 15). Der Ansatz der Datenkompetenz ist problem- und risikoorientiert.

Datenkompetenz sieht sich als Sammelbegriff „mit unklaren Bedeutungszuschreibungen aufgeladen.“ (Ortner, 2014, S. 124) Daher ist es unumgänglich zu definieren welche Fähigkeiten und Kenntnisse Datenkompetenz umfasst (Ortner, 2014, S. 126). Auf der einen Seite versteht sich Datenkompetenz als der verantwortungsbewusste Umgang mit Daten aus Sicht von Verwaltungspersonal und Statistikern, usw. Fragen nach der Aussagekraft von Daten und Fragen nach den Grenzen ihrer Verwertbarkeit werden impliziert (Romeike & Hager, 2020, S. X). Auf der anderen Seite zielt der Begriff Datenkompetenz auf Datenschutz und Privatsphäre ab.

Dabei lässt sich feststellen, dass das Modell der Datenkompetenz noch nicht in die theoretischen Zusammenhänge der Medienpädagogik überführt wurde und somit ebenfalls „nicht in Relation zu Media Literacy bzw. Medienkompetenz und -bildung gesetzt“ (Ortner, 2014, S. 124) wurde.

> Digital- und Datenkompetenz stellen somit eine Grundbedingung für Teilhabe aller Akteur*innen dar, sowohl der Lehr- und Forschungsverantwortlichen als auch der Studierenden. Digital und Data Literacy müssen nicht als abstraktes Wissen, sondern als Teil der Hochschulausbildung aktiv vermittelt werden, um dieses Ziel zu erreichen. Gleichzeitig bedarf es der erweiterten Kompetenzen, um Studierende in die Lage zu versetzen, sich selbständig weiterzubilden und ihre aktive Advokat*innenrolle in einer vom digitalem Kapitalismus geprägten hybriden und datenzentrierten Sozialstruktur auch künftig kritisch-reflexiv wahrnehmen zu können. (Rennstich, 2021, S. 211)

Da die Integration von kognitiven und emotionalen Aspekten für privatheitssensibles Handeln unumgänglich ist, sollen Nutzer und Nutzerinnen im Internet darin unterstützt werden, eine Datenkompetenz zum Schutz ihrer Privatheit zu entwickeln (Piegsa & Trost, 2018, S. 21). Die Menschen müssen wissen, wie ihre Datenrechte verletzt werden, um Rechtsmittel einlegen zu können. Sie müssen sich der Datafizierung bewusst sein, um im digitalen Kontext taktisch zu handeln oder zu intervenieren. Datenkompetenz könnte den

Einzelnen davor schützen, durch Datenverarbeitungsprozesse manipuliert zu werden, was bedeutet, dass die Konzeptualisierung von Datenkompetenz für demokratische Prozesse von zentraler Bedeutung zu sein scheint, so wie das Erlernen von Lesen und Schreiben für die Definition von demokratischen Freiheiten von zentraler Bedeutung war (Pangrazio & Sefton-Green, 2020, S. 218).

Die beiden Autoren streichen die Bedeutung heraus, inwiefern Datenkompetenz ein wichtiger Teil einer Strategie in demokratischen Gesellschaften ist, um mit dem Leben in einer digitalen Welt zurechtzukommen. Denn „[z]ur Würde des Menschen gehört die Möglichkeit, in seine Zukunft einzugreifen und sie gestalten zu können." (Mainzer, 2018, S. 132)

Es geht nicht nur um die individuelle Bedeutung von Datenkompetenz. Die vermeintlich freiwillige Preisgabe von Daten – für Nutzer und Nutzerinnen kaum noch abschätzbar, ob relevant und welche Bedeutung diesen in der Gegenwart bis in die Zukunft zugeschrieben wird – kann zur informationellen Selbstgefährdung führen. Da aber auch aus den Daten anderer, Wahrscheinlichkeitsaussagen über die eigene Person getroffen werden können bedroht die Preisgabe von Daten infolgedessen ebenso die informationelle Freiheit Dritter (Gapski et al., 2018, S. 113).

Somit bedarf es gesamtgesellschaftlicher Verantwortung, sich den Problematiken der immanenten Datensammlung entgegenzustellen. Vor allem der große Teil der Nutzer und Nutzerinnen, die den Einfluss auf deren Entscheidungsfindungen und den mangelnden Schutz an personenbezogenen sowie Metadaten nicht als problematisch empfinden, siehe Kapitel 4.4, sind eine Herausforderung, welche weitaus größerer Investitionen und eines stärkeren Engagements in der formalen und informellen Bildung bedarf, um das Konzept der Datenkompetenz in Gang zu setzen (Pangrazio & Sefton-Green, 2020, S. 209).

Im Folgenden werden zwei Beispiele illustriert, wie gesamtgesellschaftliche Verantwortung ausschauen und die erfolgreiche Vermittlung von Datenkompetenz als Aufgabe der Erwachsenenbildung funktionieren kann.

7.6 Stadt, Land, Datenfluss

Gefördert vom Deutschen Bundesministerium für Bildung und Forschung (BMBF), hat der Deutsche Volkshochschul-Verband (DVV) eine Applikation entwickelt, welche die treibenden Technologien der Digitalisierung mit zentralen Lebensfeldern, in denen sie zum Tragen kommen, verknüpft.

In einer ersten Version der App sind dies die Lebensbereiche Arbeit, Gesundheit und Mobilität. Geplant sind Erweiterungen der Handlungsfelder wie Leben und Freizeit, Energie und Umwelt sowie für die Erwachsenenbildung von Interesse, Bildung und Teilhabe.

Die App wurde entwickelt, um die Datenkompetenz der Bürger und Bürgerinnen zu fördern, indem sie die Funktionsweise neuer datengestützter Technologien spielerisch erklärt. Ziel ist es, die Nutzer und Nutzerinnen dahingehend aufzuklären, verantwortungsbewusst mit Daten umzugehen.

Um Bürger und Bürgerinnen zu befähigen, in einer digitalisierten und datafizierten Welt souverän mit Daten umzugehen und sie auf die Potenziale und Gefahren datengestützter Technologien aufmerksam zu machen, wollen die deutschen Volkshochschulen das Thema bundesweit aufnehmen. Eine österreichweite Alternative ist dem Autor der vorliegenden Arbeit nicht bekannt.

Der KI-Campus ist ein vom Bundesministerium für Bildung und Forschung (BMBF) gefördertes Pilotprojekt, welches sich auf den prototypischen Aufbau einer auf das Thema „Künstliche Intelligenz“ spezialisierten digitalen Lernplattform fokussiert. KI-Campus beschreibt den auf ihrer Webseite verfügbaren Kurs wie folgt:

> Der Kurs ‚Stadt | Land | DatenFluss‘ sensibilisiert für einen souveränen Umgang mit Daten in einer digitalisierten Welt und weckt das Interesse an neuen datengestützten Technologien. Er ist kostenlos unter der Lizenz CC BY-SA 4.0 verfügbar und basiert auf der gleichnamigen App, die der Deutsche Volkshochschul-Verband (DVV) entwickelt hat. Schirmherrin der App ist die deutsche Bundeskanzlerin Dr. Angela Merkel. (KI-Campus, o. D.)

Abbildung 8: Applikation „Stadt | Land | DatenFluss“. Quelle: Screenshots des Verfassers vom 25.10.2021.

7.7 Data Detox Kit

Eine weitere Ressource für die Vermittlung von Datenkompetenz ist das sogenannte Daten-Detox-Kit. Entwickelt für den Glas Room London im Jahr 2017, eine Pop-up-Ausstellung mit dem Ziel, Themen rund um Daten und Privatsphäre in sinnliche und greifbare Erfahrungen zu verwandeln, wird das Kit seitdem von der Berliner Organisation Tactical Tech kuratiert.

Das Daten-Detox-Kit vermittelt auf der interaktiven Webseite alltägliche Schritte, um die Privatheit, Sicherheit und das Wohlbefinden von Nutzern und Nutzerinnen in der digitalen Welt zu kontrollieren. Weiters bietet es Arbeitsmaterialien für Pädagogen und Pädagoginnen an, um Datenkompetenz in die Lehre zu integrieren.

Es existiert ebenfalls als gedrucktes Kit in Form einer PDF-Datei und ist in insgesamt 35 Sprachen verfügbar. Das Daten-Detox-Kit ist lizenziert unter der Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Lizenz und ist somit für Erwachsenenbildner und Erwachsenenbildnerinnen in nicht abänderbarer und nicht kommerzieller Form nutzbar.

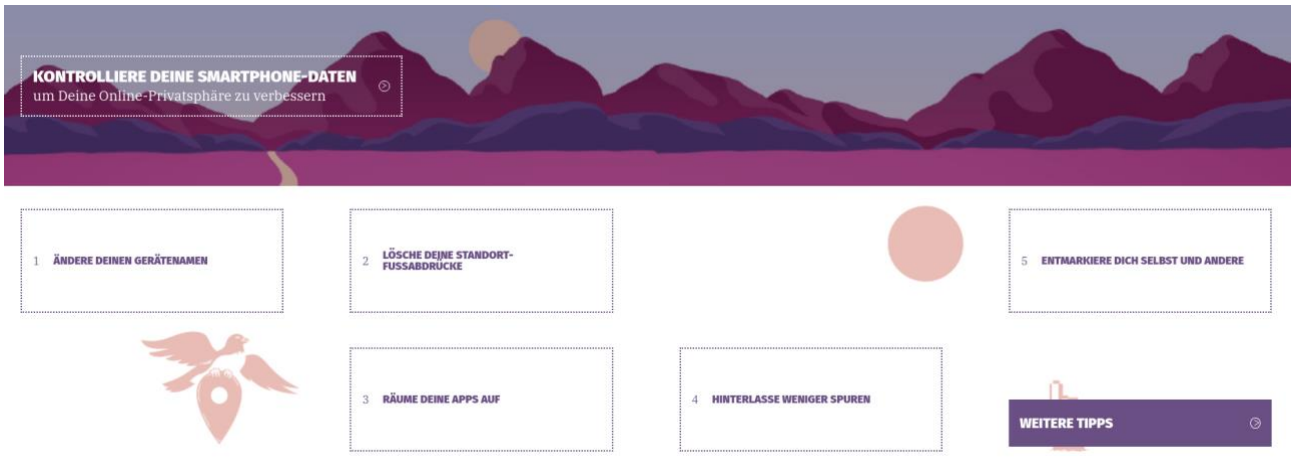

Abbildung 9: Webseite „Daten-Detox-Kit“. datadetoxkit.org/de. Quelle: Screenshot des Verfassers vom 25.10.2021

7.8 Ausblick in eine ungewisse Zukunft

Digitale Selbstverteidigung bietet einen gewissen Schutz, kann aber nicht verhindern, dass Daten verarbeitet werden, die als „nicht personenbezogen“ eingestuft werden (Mansell, 2012, S. 188). Ebensowenig schaffen es rein regulatorische Maßnahmen, Menschen und ihre Daten in ausreichendem Maße zu schützen.

Dementsprechend ist kritische Aufklärung über Daten und die Schaffung von Datenkompetenz der Schlüssel zur Optimierung sowohl regulatorischer Maßnahmen als auch der Zuhilfenahme von technischen Hilfsmitteln.

Die Menschen müssen wissen, wie ihre Rechte verletzt werden, um Rechtsmittel einlegen zu können. Sie müssen sich der Probleme der Datenerhebung bewusst sein, um dieser gezielt einen Riegel vorzulegen. Sie müssen wissen, „Wozu“, „Wovor“ und „Warum“ sie sich schützen müssen. Datenkompetenz könnte dabei den Einzelnen und die Einzelne davor schützen, durch Datenverarbeitungsprozesse manipuliert zu werden. So wie das Erlernen des Lesens und Schreibens für die Definition des demokratischen Wahlrechts zentral war, scheint Konzeptualisierung von Datenkompetenz für demokratische Prozesse zentral zu sein. Wenn die Kenntnis über die Datenverarbeitung dem Einzelnen die Wahl, die Meinung, den Widerstand oder die Akzeptanz gegenüber der Art und Weise, wie seine Daten verwendet werden, ermöglicht, wird ein solches Modell der Datenkompetenz eine gewisse Beruhigung in Bezug auf die Wahrnehmung des Rückgangs der Erosion des Grundwertes Privatheit in der digitalen Zukunft bringen (Pangrazio & Sefton-Green, 2020, S. 218).

Aus diesen Gründen kann nur eine Kombination aus regulatorischen und pädagogischen Maßnahmen dazu beitragen, der breiten Bevölkerung die ungebrochene Bedeutung von Datenschutz und Privatheit näherzubringen. Durch Aufklärung und den Einzug von Datenkompetenz in Instiutionen der Erwachsenenbildung als auch in die eigenen vier Wände können Datenkraken die „Krakenarme gestutzt werden“.

8 Conclusio

„We should not be comfortable or content in a society where the only way to remain free of surveillance and repression is if we make ourselves as unthreatening, passive, and compliant as possible.“

Glenn Greenwald[8]

In der vorliegenden Arbeit wurde analysiert, mit welchen Herausforderungen die Gesellschaft allgemein und die Erwachsenenbildung im Speziellen konfrontiert ist – in einer Welt, in der persönliche Information die Form von Bits und Bytes annimmt, und ihre Ausbeutung und Anfälligkeit für Missbrauch omnipräsent ist (Wacks, 2015, S. 120).

Betroffene haben keine Vorstellung davon, was mit Daten, die im Jetzt oder in der Vergangenheit erhoben wurden, in Zukunft passieren wird. Es ist unmöglich abzuschätzen, was in zehn Jahren mit den heutigen Datenbeständen über Einzelpersonen herausgefunden werden kann. Ein weitverbreiteter Irrglaube ist, dass die Europäische Datenschutzgrundverordnung in geeignetem Ausmaß die Privatheit schützt. Sie bezieht ihre Wirkung allerdings lediglich auf personenbezogene Daten und schließt somit Metadaten gänzlich aus.

Die vorliegenden Kapitel haben aufgezeigt, mit welchen Herausforderungen sich die Erwachsenenbildung im digitalen Kontext in den nächsten Jahren konfrontiert sieht. Privatheit schließt dezisionale und informationelle Bereiche mit ein und unterscheidet sich zur Privatsphäre darin, dass sie metaphorisch gesehen an keinen Ort gebunden ist. Als pluralistisches Konzept ist es schwierig, den Begriff der Privatheit zu definieren. Beide Begrifflichkeiten stellen eine entscheidende Grundlage für zwischenmenschliche

[8] Greenwald war einer der ersten Journalisten, der die Edward-Snowden-Akten mit ihren Enthüllungen über die umfassende Überwachung von Privatpersonen durch die Vereinigten Staaten zu Gesicht bekam und darüber berichtete.
Greenwald, G. (2014, Oktober). *Why privacy matters* [Video]. TED Konferenzen. https://www.ted.com/talks/glenn_greenwald_why_privacy_matters.

Beziehungen, für die Gesellschaft selbst und ihre Gruppen und Kategorien von Personen, sowie für die Funktionsweise demokratischer politischer Systeme dar (Raab, 2017, S. 87).

Der Datenschutz zielt auf die Kontrolle, ob und wie personenbezogene Daten erhoben, gespeichert und verarbeitet werden. Datenschutzvergehen bleiben oft unbemerkt, da sie erst in Jahren nachteilige Effekte für Individuen und auch die Gesellschaft nach sich ziehen können. Als ausschlaggebend für die Problematiken, die der Datenschutz mit sich bringt, ist die Wandlung einer güterproduzierenden Gesellschaft zur Informationsgesellschaft.

Einhergehend ist der Tatbestand, dass Privatheit im wirtschaftstheoretischen Verständnis ein Stein auf dem Weg zur Profitmaximierung darstellt. Daten haben mittlerweile sämtliche Lebensbereiche infiziert und lassen sich mit Bedeutungszuschreibungen und der Vernetzung von Erfahrungen im entsprechenden Kontext zu Wissen verarbeiten.

Die enorme Menge an Daten, die mittlerweile darauf warten, verwertet zu werden, erzeugte das Phänomen Big Data. Menschliches Verhalten wird somit zunehmend vorhersehbar und für wirtschaftliche Zwecke beeinflusst bzw. manipuliert. Nicht nur personenbezogene Daten, sondern auch sogenannte Metadaten, die oftmals keine Bedeutung in Rechtsschutzmechanismen finden, können detaillierte Auskünfte über soziale Beziehungen, Gewohnheiten, Interessen, Vorlieben usw. geben, welche wiederum kapitalisierbare Informationen für Wirtschaftstreibende darstellen.

Während Nutzer und Nutzerinnen zwar angeben, ihre Privatheit hochzuschätzen, steht ihr beobachtbares Verhalten dieser Einstellung allerdings diametral entgegen. Nutzer und Nutzerinnen entwickeln mit der Zeit fatalistische Grundhaltungen in Bezug auf ihre eigenen Daten und scheuen nicht davor zurück, diese vermeintlich willkürlich preiszugeben, um entsprechende Dienstleistungen in Anspruch zu nehmen und um webbasierte Anwendungen in erster Instanz überhaupt erst nutzen zu können. Freiwilligkeit ist hierbei ein Vorwand der eigenen Bequemlichkeit. Oftmals bleibt Nutzern und Nutzerinnen keine Wahl. Sie werden zu Entscheidungen gedrängt.

Zu Beginn noch der Staat als Hauptakteur, so ist es mittlerweile eine institutionelle Bedrohung der Privatheit, mit der sich Individuen konfrontiert sehen.

Der Überwachungskapitalismus beschreibt den Umstand, dass die mit technischen Mitteln erhobenen Daten analysiert werden, um das Verhalten von Nutzern und Nutzerinnen zu prognostizieren und zu manipulieren. Individuen können sich dagegen kaum wehren, unterliegen sie doch der Informationsmacht der großen Datensammler wie Facebook, Google und Co. und können weder nachvollziehen, auf welchen Datengrundlagen Entscheidungen über ihr Leben getroffen werden, noch können sie gezielt Einfluss darauf nehmen.

Diese Big Player bauen aufgrund der Daten, die sie tagtäglich von Menschen abschöpfen, ihre Machtpositionen aus und erreichen bisher ungesehenen politischen Einfluss. Privatheit und Privatsphäre werden geschützt von den Menschenrechten, der europäischen Grundrechtecharta und von der Europäischen Datenschutzgrundverordnung. Dabei besteht die Schwierigkeit darin, Menschen, und nicht Daten, in ausreichendem Maße zu schützen und gleichzeitig den Weg für technische Innovationen zu ebnen. Defizite sind hierbei eine fehlende Beachtung von nicht personenbezogenen Daten und der Umstand, dass eine freiwillige Einwilligung selten gegeben ist, denn ohne Zustimmung bleiben viele Dienstleistungen und Anwendungen verwehrt, die zur Teilhabe an der digitalen Öffentlichkeit unumgänglich sind. Nutzer und Nutzerinnen verzichten demnach bewusst auf Datenschutz.

Die Erwachsenenbildung hat dabei die Verantwortung zu übernehmen, Nutzer und Nutzerinnen dabei zu unterstützten und sie aufzuklären darüber, wie sich Privatheit schützen lässt und welche Bedeutung der Datenschutz im 21. Jahrhundert hat. Pädagogische Maßnahmen in Kombination mit regulatorischen Maßnahmen und der Zuhilfenahme von technischen Hilfsmitteln und alternativen Anwendungen sind die vielversprechendste Lösung, um die genannten Herausforderungen zu bewältigen.Wissen und Kompetenz über die Funktionsweise der Datenverarbeitung und der bewusste Umgang mit eingesetzten Technologien kann dazu beitragen, Privatheit, Daten und somit Menschen zu schützen.

Es geht nicht nur darum, Einstellungen zum Datenschutz zu ändern, sondern auch darum, die gesamtgesellschaftlichen Folgen von Entscheidungen im Blick zu behalten. Datenkompetenz lässt sich auf unterschiedlichste Weise vermitteln. Beispiele hierfür sind die beiden vorgestellten Pilotprojekte „Stadt, Land, Datenfluss“ und das „Daten-Detox-Kit“.

Auf das eingangs genannte Zitat: „*Software will eat the world“* bezogen, so attestiert Andreessen, dass wir uns mitten in einem dramatischen und weitreichenden technologischen und wirtschaftlichen Wandel befinden, in dem Softwareunternehmen große Teile der Wirtschaft übernehmen werden (Andreessen, 2011). Auch wenn der US-amerikanische Softwareentwickler und Unternehmer nicht die überwachungskapitalistischen Züge gemeint hat, die Big Tech längst aufzeigt, so hat er durchaus Recht mit der Behauptung, dass es zu verstehen gilt, wie die neue Generation von Technologieunternehmen das tut, was sie tut, und welche weiterreichenden Folgen dies für die Einzelpersonen als auch die Gesellschaft hat (Andreessen, 2011).

Um zu verhindern, dass die Welt von Software und den dahinterliegenden Tech-Riesen „aufgefressen“ wird und unsere Daten als „Mastfutter“ dafür dienen, ist es wichtig, sich die zahlreichen Risiken für die Privatheit des Individuums und für die Gesellschaft als Ganzes bewusst zu machen (Sixt, 2018, S. 313).

Weder Überwachung noch der Schutz der Privatheit von Individuum und Gesellschaft sind nationale Phänomene (Bennett, 2008, S. 224). Rein regulatorische Ansätze zum Schutz der Privatheit reichen nicht aus. Datenkompetenz ist ein relativ neuer Zugang in die unzähligen Kompetenzbereiche, die ein Individuum in der schnelllebigen Zeit, in der wir leben, sich anzueignen hat, um handlungsfähig bleiben zu können. Ein neues Interesse an der Privatsphäre jenseits des Datenschutzes ist daher unerlässlich. Den Nutzern und Nutzerinnen kommt hierbei eine zentrale Rolle zugute. Indem sie Alternativen erkunden und anwenden, fördern sie auch deren Weiterentwicklung und Verbreitung im Allgemeinen, indem sie ihre Rechte einfordern, welche ihnen die Europäische Datenschutzgrundverordnung in die Hand legt und Datenschutzpraktiken der Anbieter bei ihren Entscheidungsfindungen berücksichtigen:

> Die Aufklärung und Schaffung von datenschutzbewussten KonsumentInnen ist daher ein wesentliches Element einer umfassenden Strategie zur Wahrung des Grundrechts auf Privatsphäre, ohne aber dabei zu vergessen, dass gerade die unbedachten NutzerInnen eines besonderen Schutzes bedürfen. (Čas et al., 2002, S. 35)

Viele Herausforderungen in Bezug auf unterschiedlichste Aspekte der Digitalisierung warten noch darauf, von Erwachsenenbildnern und Erwachsenenbildungsforschern bearbeitet zu werden. Ich hoffe, dass diese Arbeit dazu anregt, kreative Antworten und Lösungsschritte auf die Herausforderungen und Problematik, die behandelt wurden, zu finden.

Die Zukunft der Privatheit und deren Schutz liegt nicht darin, anderen sozialen Bewegungen nachzueifern oder auf das große Datenschutz-Armageddon zu warten. Sie liegt in der beharrlichen, unnachgiebigen und sachkundigen Artikulation des sehr einfachen Satzes, dass der Einzelne und die Einzelne ein Recht darauf haben, die Informationen und Daten zu kontrollieren, die ihn und sie betreffen. Nur wenige würden dieses Recht leugnen. Jeder will es für sich selbst. Das Anliegen ist gerecht. Das Thema wird nicht verschwinden, und die Menschen, die dafür eintreten, werden es auch nicht (Bennett, 2008, S. 225).

Literaturverzeichnis

Acquisti, A. (2004). Privacy in Electronic Commerce and the Economics of Immediate Gratification. *Proceedings of the ACM Conference on Electronic Commerce*, *5*. https://doi.org/10.1145/988772.988777

Andreessen, M. (2011). *Why Software Is Eating The World*. Genius. Abgerufen 16. November 2021, von https://genius.com/Marc-andreessen-why-software-is-eating-the-world-annotated

Aschemann, B. (2018). *Digitalisierung, Didaktik, Internettechnologien*. Berufsförderungsinstitut Oberösterreich.

Barassi, V. (2021). Tech Companies Are Profiling Us From Before Birth. *The MIT Press Reader*. Abgerufen 16. November 2021, von https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth/

Behrendt, H., Loh, W., Matzner, T., & Misselhorn, C. (2019). Einleitung: Neuverortungen des Privaten. In H. Behrendt, W. Loh, T. Matzner, & C. Misselhorn (Hrsg.), *Privatsphäre 4.0: Eine Neuverortung des Privaten im Zeitalter der Digitalisierung* (S. 1–10). J.B. Metzler. https://doi.org/10.1007/978-3-476-04860-8_1

Bennett, C. J. (2008). *The Privacy Advocates: Resisting the spread of surveillance*. The MIT Press. Abgerufen 16. November 2021, von https://mitpress.mit.edu/books/privacy-advocates

Bentham, J. (1791). *The Works of Jeremy Bentham.* Online Library of Liberty. Abgerufen 16. November 2021, von https://oll.libertyfund.org/title/bowring-the-works-of-jeremy-bentham-vol-4

Beyvers, E. (2018). *Privatheit in der Waagschale: Instrumente des datenschutzrechtlichen Interessenausgleichs im Kontext sozialer Online-Netzwerke*.

Bridle, J. (2018). *New dark age: Technology and the end of the future*. Universitätsbibliothek. Abgerufen 16. November 2021, von https://permalink.obvsg.at/wuw/AC15060592

Brody, S. (2016). *Protecting Data Privacy With User-Friendly Software*. CFR. Abgerufen 16. November 2021, von https://cdn.cfr.org/sites/default/files/pdf/2016/02/CyberBrief_Brody_Privacy_OR.pdf

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) (2011). *Datenschutz im Internet. Eine repräsentative Untersuchung zum Thema Daten im Internet aus Nutzersicht*. Bitkom. Abgerufen 16. November 2021, von https://www.bitkom.org/sites/default/files/file/import/BITKOM-Publikation-Datenschutz-im-Internet.pdf.

Calo, R. (2010). *The Boundaries of Privacy Harm.* Abgerufen 16. November 2021, von Social Science Research Network. https://papers.ssrn.com/abstract=1641487

Čas, J., Strohmaier, Th., & Peissl, W. (2002). Datenvermeidung in der Praxis – Individuelle und gesellschaftliche Verantwortung. Studie im Auftrag der Bundeskammer für Arbeiter und Angestellte. In I. für Technikfolgen-Abschätzung, *ITA - Elektronische Publikationen* (S. ITA-pb-a29). Verlag der Österreichischen Akademie der Wissenschaften. https://doi.org/10.1553/ITA-pb-a29

Cascio, J. (2005). *The Rise of the Participatory Panopticon*. Open the future. Abgerufen 16. November 2021, von http://www.openthefuture.com/wcarchive/2005/05/the_rise_of_the_participatory.html

Christl, W., & Spiekermann, S. (2016). *Networks of control: A report on corporate surveillance, digital tracking, big data & privacy* (1. Aufl.). Facultas.

Clarke, R. (1997). *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*. Roger Clark. Abgerufen 16. November 2021, von http://www.rogerclarke.com/DV/Intro.html

Corn, M. (2020, Juni 20). *We're losing the war against surveillance capitalism because we let Big Tech frame the debate*. Salon. Abgerufen 16. November 2021, von https://www.salon.com/2020/06/20/were-losing-the-war-against-surveillance-capitalism-because-we-let-big-tech-frame-the-debate/

Djeffal, C. (2019). „Privatheit 4.0“ im Spiegel von Recht und künstlicher Intelligenz. Das Recht als (Re)aktion und der status activus technicus. In H. Behrendt, W. Loh, T. Matzner, & C. Misselhorn (Hrsg.), *Privatsphäre 4.0: Eine Neuverortung des Privaten im Zeitalter der Digitalisierung* (S. 177–197). J.B. Metzler. https://doi.org/10.1007/978-3-476-04860-8_11

Lerch., S., Iller., C., von Felden., H., Dörner., O., & Schüßler., I. (2020). *Erwachsenenbildung und Lernen in Zeiten von Globalisierung, Transformation und Entgrenzung*. Verlag Barbara Budrich.

Doward, J., & Gibbs, A. (2017, März 4). Did Cambridge Analytica influence the Brexit vote and the US election? The Guardian. Abgerufen 16. November 2021, von https://www.theguardian.com/politics/2017/mar/04/nigel-oakes-cambridge-analytica-what-role-brexit-trump

Duhigg, C. (2012, Februar 16). *How Companies Learn Your Secrets.* The New York Times. Abgerufen 16. November 2021, von https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

Eichenhofer, J. (2019). Rechtswissenschaftliche Perspektiven auf Privatheit. In H. Behrendt, W. Loh, T. Matzner, & C. Misselhorn (Hrsg.), *Privatsphäre 4.0: Eine Neuverortung des Privaten im Zeitalter der Digitalisierung* (S. 155–175). J.B. Metzler. https://doi.org/10.1007/978-3-476-04860-8_10

Faulstich, P. (2018). Weiterbildung und Technik. In R. Tippelt & A. von Hippel (Hrsg.), *Handbuch Erwachsenenbildung/Weiterbildung* (S. 947–971). Springer Fachmedien. https://doi.org/10.1007/978-3-531-19979-5_47

Fingas, J. (2021). *Pentagon believes its precognitive AI can predict events „days in advance“*. Engadget. Abgerufen 16. November 2021, von https://www.engadget.com/pentagon-ai-predicts-days-in-advance-135509604.html

Finn, R. L., Wright, D., & Friedewald, M. (2013). Seven Types of Privacy. In S. Gutwirth, R. Leenes, P. de Hert, & Y. Poullet (Hrsg.), *European Data Protection: Coming of Age* (S. 3–32). Springer Netherlands. https://doi.org/10.1007/978-94-007-5170-5_1

Fried, C. (1968). Privacy. *Yale Law Journal, 77*(3), 475–493. https://digitalcommons.law.yale.edu/ylj/vol77/iss3/3

Froomkin, A. (2000). The Death of Privacy? *Stanford Law Review*, *52*. https://doi.org/10.2307/1229519

Ganz, K. (2018). Die Post-Privacy-Debatte. In *Die Netzbewegung* (1. Aufl., S. 235–268). Verlag Barbara Budrich; JSTOR. https://doi.org/10.2307/j.ctvbkjvtj.11

Gapski, H. (Hrsg.). (2015). *Big Data und Medienbildung: Zwischen Kontrollverlust, Selbstverteidigung und Souveränität in der digitalen Welt*. kopaed.

Gapski, H., Tekster, T., & Elias, M. (2018). *Bildung für und über Big Data. Status quo; Möglichkeiten und Grenzen der Medienbildung; flankierende Handlungsempfehlungen. Gutachten im Rahmen von ABIDA – Assessing Big Data*. https://doi.org/10.25656/01:17187

Gerber, P., Volkamer, M., & Gerber, N. (2017). *Dialogmarketing Perspektiven 2016/2017: Tagungsband 11. wissenschaftlicher interdisziplinärer Kongress für Dialogmarketing*. Springer Fachmedien Wiesbaden. http://dx.doi.org/10.1007/978-3-658-16835-3

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International Journal of Market Research*, *59*(6), 703–705. https://doi.org/10.2501/IJMR-2017-050

Greenwald, G. (2014, Oktober). *Why privacy matters*. Ted. Abgerufen 16. November 2021, von https://www.ted.com/talks/glenn_greenwald_why_privacy_matters

Grunwald, A. (2018). Abschied vom Individuum – werden wir zu Endgeräten eines global-digitalen Netzes? In S. Burk, M. Hennig, B. Heurich, T. Klepikova, M. Piegsa, M. Sixt, & K. E. Trost (Hrsg.), *Privatheit in der digitalen Gesellschaft.* (Bd. 10, S. 35–48). Duncker & Humblot GmbH; JSTOR. http://www.jstor.org/stable/j.ctv1q69v1n.4

Gugitscher, K., & Schlögl, P. (2021). *Existenzsicherung, Professionalisierung, Innovation und Digitalisierung in der österreichischen Erwachsenenbildung im Kontext der COVID-19-Pandemie*. 69.

Gutwirth, S. (2002). *Privacy and the information age*. Rowman & Littlefield Publishers.

Hagendorff, T. (2019). Post-Privacy oder der Verlust der Informationskontrolle. In H. Behrendt, W. Loh, T. Matzner, & C. Misselhorn (Hrsg.), *Privatsphäre 4.0: Eine Neuverortung des Privaten im Zeitalter der Digitalisierung* (S. 91–106). J.B. Metzler. https://doi.org/10.1007/978-3-476-04860-8_6

Häußling, R. A. M., Eggert, M., Kerpen, D., Lemm, J., Strüver, N., & Ziesen, N. K. (2017). *Schlaglichter der Digitalisierung: Virtureale(r) Körper - Arbeit - Alltag: Ein Vorstoß zum Kern der Digitalisierung aus einer techniksoziologisch-relationalen Perspektive: Working Paper des Lehrstuhls für Technik- und Organisationssoziologie* [Online]. Lehrstuhl für Technik- und Organisationssoziologie, Institut für Soziologie, RWTH Aachen.

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(4). https://doi.org/10.5817/CP2016-4-7

Holzinger, G. (2017, 17. Februar). *VfGH-Präsident kritisiert Überwachungspläne der Regierung*. Der Standard. Abgerufen 16. November 2021, von https://www.derstandard.at/story/2000052786527/vfgh-praesident-holzinger-kritisiert-ueberwachungsplaene-der-regierung.

Hosein, G. (2006). *Privacy as freedom*. MIT Press. Abgerufen 16. November 2021, von http://mitpress.mit.edu/main/home/default.asp

Hug, T., & Madritsch, R. (2020). Globale Bildungsindustrie – Erkundungen zum Stand der Dinge in Österreich. *Medienimpulse*, 55. https://doi.org/10.21243/MI-04-20-03

Kade, J., Seitter, W., & Dinkelaker, J. (2018). Wissen(stheorie) und Erwachsenenbildung/Weiterbildung. In R. Tippelt & A. von Hippel (Hrsg.), *Handbuch Erwachsenenbildung/Weiterbildung* (S. 275–294). Springer Fachmedien. https://doi.org/10.1007/978-3-531-19979-5_14

Keber, T. O. (2018). Stützen der Informationsgesellschaft – zur Rolle von Datenschutz und Datensicherheit im Mediensystem. In S. Burk, M. Hennig, B. Heurich, T. Klepikova, M. Piegsa, M. Sixt, & K. E. Trost (Hrsg.), *Privatheit in der digitalen Gesellschaft.* (Bd. 10, S. 261–288). Duncker & Humblot GmbH; JSTOR. http://www.jstor.org/stable/j.ctv1q69v1n.15.

KI-Campus (o. D.). *Stadt | Land | DatenFluss*. KI-Campus. Abgerufen 16. November 2021, von https://ki-campus.org/datenfluss.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Lyß, J., Witt, S. (2018). *Kritische Medienkompetenz und Erwachsenenbildung*. EPALE. Abgerufen 16. November 2021, von https://epale.ec.europa.eu/sites/default/files/20181130_dossier_kritische_medien kompetenz_und_erwachsenenbildung_final.pdf

Magi, T. J. (2011). Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature. *The Library Quarterly*, *81*(2), 187–209. https://doi.org/10.1086/658870

Mainzer, K. (2002). *Leben in der Wissensgesellschaft*. pedocs. Abgerufen 16. November 2021, von http://nbn-resolving.de/urn:nbn:de:0111-opus-90708

Mainzer, K. (2018). Digitale Würde? In S. Burk, M. Hennig, B. Heurich, T. Klepikova, M. Piegsa, M. Sixt, & K. E. Trost (Hrsg.), *Privatheit in der digitalen Gesellschaft.* (Bd. 10, S. 115–136). Duncker & Humblot GmbH; JSTOR. http://www.jstor.org/stable/j.ctv1q69v1n.8

Mansell, R. (2012). Imagining the Internet: Communication, innovation, and governance. In *Imagining the Internet: Communication, innovation, and governance* (1. publ..). Oxford Univ. Press. https://permalink.obvsg.at/wuw/AC09425679

Mühlhoff, R. (2019). Big Data Is Watching You Digitale Entmündigung am Beispiel von Facebook und Google. In R. Mühlhoff, A. Breljak, & J. Slaby (Hrsg.), *Affekt Macht Netz* (S. 81–106). transcript Verlag. https://doi.org/10.14361/9783839444399-004

Müller, G. (2020). *Protektion 4.0: Das Digitalisierungsdilemma* (1st ed. 2020.). Heidelberg. https://doi.org/10.1007/978-3-662-56262-8

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Ochs, C. (2019). Teilhabebeschränkungen und Erfahrungsspielräume: Eine negative Akteur-Netzwerk-Theorie der Privatheit. In H. Behrendt, W. Loh, T. Matzner, & C. Misselhorn (Hrsg.), *Privatsphäre 4.0: Eine Neuverortung des Privaten im Zeitalter der Digitalisierung* (S. 13–31). J.B. Metzler. https://doi.org/10.1007/978-3-476-04860-8_2

Ortner, H. (2014). *Datenflut und Informationskanäle* (1. Aufl..). UnivPress. https://resolver.obvsg.at/urn:nbn:at:at-ubi:3-385

Oetzel, M. C., & Gonja, T. (2011). The online privacy paradox: A social representations perspective. *Proceedings of the 2011 Annual Conference Extended Abstracts on Human Factors in Computing Systems - CHI EA '11*, 2107. https://doi.org/10.1145/1979742.1979887

Palmer, M. (2006). *Data is the New Oil*. ANA Marketing Maestros. Abgerufen 16. November 2021, von https://ana.blogs.com/maestros/2006/11/data_is_the_new.html

Pangrazio, L., & Sefton-Green, J. (2020). The social utility of 'data literacy'. *Learning, Media and Technology*, *45*(2), 208–220. https://doi.org/10.1080/17439884.2020.1707223

Pasquinelli, M. (2015). *Anomaly Detection: The Mathematization of the Abnormal in the Metadata Society*. Abgerufen 16. November 2021, von http://matteopasquinelli.com/anomaly-detection/

Pfiffner, M., & Stadelmann, P. (1999). *Wissen wirksam machen: Wie Kopfarbeiter produktiv werden* (2., unveränd. Aufl). Haupt.

Piegsa, M., & Trost, K. E. (2018). Privatheit in der digitalen Gesellschaft. In M. Piegsa, K. E. Trost, S. Burk, M. Hennig, B. Heurich, T. Klepikova, & M. Sixt (Hrsg.), *Privatheit in der digitalen Gesellschaft.* (Bd. 10, S. 7–32). Duncker & Humblot GmbH; JSTOR. http://www.jstor.org/stable/j.ctv1q69v1n.3

Prietl, B., & Houben, D. (2018). Datengesellschaft: Einsichten in die Datafizierung des Sozialen. In *Datengesellschaft*. transcript Verlag. https://doi.org/10.14361/9783839439579

Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment (PRESCIENT) (2011). *Deliverable D1. Legal, social, economic and ethical conceptualisations of privacy and data protection*. https://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT-D1---final.pdf.

Raab, C. D. (2017). Security, Privacy and Oversight. In A. W. Neal (Hrsg.), *Security in a Small Nation: Scotland, Democracy, Politics* (S. 77–102). Open Book Publishers. https://doi.org/10.11647/OBP.0078.03

Regan, P. (1995). *Legislating Privacy: Technology, Social Values and Public Policy*.ChapelHill: University of North Carolina Press.

Rennstich, J. K. (2021). Neue Tricks für alte Hunde? Digitalisierung als Herausforderung in Lehrvermittlung und Forschung. In M. Wunder (Hrsg.), *Digitalisierung und Soziale Arbeit. Transformationen und Herausforderungen* (S. 201–214). Verlag Julius Klinkhardt. https://doi.org/10.35468/5909-14

Ribolits, E. (2010). *Bildung ohne Wert: Wider die Humankapitalisierung des Menschen*. Löcker.

Ribolits, E. (2011). *Bildung - Kampfbegriff oder Pathosformel: Über die revolutionären Wurzeln und die bürgerliche Geschichte des Bildungsbegriffs*. Löcker.

Romeike, F., & Hager, P. (2020). *Erfolgsfaktor Risiko-Management 4.0: Methoden, Beispiele, Checklisten Praxishandbuch für Industrie und Handel*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-29446-5

Rummler, K. (2020). *Digitalisierung – Subjekt – Bildung* (V. Dander, P. Bettinger, E. Ferraro, & C. Leineweber, Hrsg.). Verlag Barbara Budrich. https://doi.org/10.3224/84742350

Schneier, B. (2016). *Data and Goliath: The hidden battles to collect your data and control your world* (First published as a Norton paperback). W.W. Norton & Company.

Schön, S. (2015). Neue Inhalte, neue Räume und neue Organisationsformen. Wie entwickelt sich Erwachsenenbildung in Hinblick auf Technologien?. *Magazin erwachsenenbildung.at, 25*(12). https://doi.org/10.25656/01:10956

Schrape, J.-F. (2019). Big Data und Privatheit – eine prozesssoziologische Perspektive. In H. Behrendt, W. Loh, T. Matzner, & C. Misselhorn (Hrsg.), *Privatsphäre 4.0: Eine Neuverortung des Privaten im Zeitalter der Digitalisierung* (S. 213–229). J.B. Metzler. https://doi.org/10.1007/978-3-476-04860-8_13

Seargeant, P., & Tagg, C. (2018). Critical Digital Literacy Education in the 'Fake News' Era. In K. Reedy & J. Parker (Hrsg.), *Digital Literacy Unpacked* (1. Aufl., S. 179–190). Facet. https://doi.org/10.29085/9781783301997.015

Spiegel, J. R., McKenna, M. T., Lakshman, G. S., Nordstrom P. G. (2013). *Method and system for anticipatory package shipping*. U.S. Patent Nr. 8,615,473. Washington, DC: Vereinigte Staaten.

Snowden, E. (2014). *Here's how we take back the Internet*. Ted. Abgerufen 16. November 2021, von https://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3), 477–564. https://doi.org/10.2307/40041279

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

Stang, R., & Schüller-Zwierlein, A. (2018). Bibliotheken und Erwachsenenbildung. In R. Tippelt & A. von Hippel (Hrsg.), *Handbuch Erwachsenenbildung/Weiterbildung* (S. 857–871). Springer Fachmedien. https://doi.org/10.1007/978-3-531-19979-5_40

Thies, C. (2018). Verantwortung im digitalen Weltsystem. In S. Burk, M. Hennig, B. Heurich, T. Klepikova, M. Piegsa, M. Sixt, & K. E. Trost (Hrsg.), *Privatheit in der digitalen Gesellschaft.* (Bd. 10, S. 137–152). Duncker & Humblot GmbH; JSTOR. http://www.jstor.org/stable/j.ctv1q69v1n.9

Tingley, B. (2021). *The Pentagon Is Experimenting With Using Artificial Intelligence To „See Days In Advance"*. The Drive. Abgerufen 16. November 2021, von https://www.thedrive.com/the-war-zone/41771/the-pentagon-is-experimenting-with-using-artificial-intelligence-to-see-days-in-advance

Tucker, P. (2021). *AI Gives 'Days of Advanced' Warning in Recent NORTHCOM Networked Warfare Experiment*. Defense One. Abgerufen 16. November 2021, von https://www.defenseone.com/technology/2021/07/ai-gives-days-advanced-warning-recent-northcom-networked-warfare-experiment/184163/

Viseu, A., Clement, A., & Aspinall, J. (2004). Situating Privacy Online. *Information*, *7*. https://doi.org/10.1080/1369118042000208924

Wacks, R. (2015). *Privacy: A very short introduction* (Second edition.).

Warren, S., & Brandeis, L. (1890). *The Right to Privacy*. Harvard Law Review. Abgerufen 16. November 2021, von https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

Weigend, A. S. (2017). Data for the people: How to make our post-privacy economy work for you. In *Data for the people: How to make our post-privacy economy work for you*. Basic Books. https://permalink.obvsg.at/wuw/AC13474043

Westermann, S., Witt, E., Deutsche Akademie der Naturforscher Leopoldina, Union der Deutschen Akademien der Wissenschaften, & Deutsche Akademie der Technikwissenschaften (Hrsg.). (2018). *Privatheit in Zeiten der Digitalisierung: Stellungnahme*. Deutsche Akademie der Naturforscher Leopoldina e.V.

Zuboff, S. (2018). *Das Zeitalter des Überwachungskapitalismus*. Content select. Abgerufen 16. November 2021, von https://content-select.com/de/portal/media/view/5aa3a6f9-1fbc-4f76-bc73-27e2b0dd2d03