universität wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

„Smart Control

Eine transdisziplinäre Analyse der privaten Datenverarbeitung im Internet der Dinge“

verfasst von / submitted by

Patricia Eva Groll, B.A.

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Arts (MA)

Wien, 2017 / Vienna 2017

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	066 581
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Theater-, Film- und Mediengeschichte
Betreut von / Supervisor:	Mag. Dr. habil. Ramón Reichert

Danksagung

Eine universitäre Ausbildung erfordert viel Arbeit, starke Nerven, Selbstdisziplin und Durchhaltevermögen. Während ich an manchen Nachmittagen, an denen ich eigentlich an dieser Masterarbeit schreiben wollte, abschweifte und der Tag damit endete, dass ich Wikipedia Einträge und YouTube Videos zu *Kony 2012* sah, kamen mir leider oft Zweifel, ob ich diese Tugenden wirklich besitze.
Zum Glück gibt es noch einen weiteren Grundpfeiler, ohne den so eine Arbeit nicht zu meistern wäre – Menschen die hinter einem stehen, an einen glauben und einen daran erinnern, dass 34 Seiten Text leider noch nicht genug sind.
An dieser Stelle möchte ich mich bei allen bedanken, die durch ihre fachliche und persönliche Unterstützung zum Gelingen dieser Arbeit beigetragen haben.

Dieser Dank gilt vor allem Mag. Dr. habil. Ramón Reichert, der meine Arbeit und mich betreut hat. Neben fachlicher Hilfestellung möchte ich mich auch für die moralische Unterstützung bedanken, die mir letztendlich doch die Angst vor „zu wenig Eigenanteil“ genommen hat.
Vielen Dank, für die Zeit und Mühe, die Sie in meine Arbeit investiert haben.

Daneben gilt mein Dank Lisa, Tessa und Florian, die in zahlreichen Stunden Korrektur gelesen haben. Ich weiß, es war furchtbar.
Danke, dass Ihr mir so geholfen habt.

Ganz besonderer Dank gilt abschließend meinen Eltern Lilly und Pit. Sie haben mir nie gesagt, ich könne nicht tun was ich mir wünsche, oder nicht werden, was ich werden möchte. Auch wenn ich manchmal selbst nicht genau weiß, wohin der Weg mit diesem Studium führt, haben sie mir nie das Gefühl gegeben, dass es der falsche ist und mich dabei stets unterstützt.
Dafür danke ich Euch sehr.

Eidesstattliche Erklärung

Ich versichere, dass

- ich diese Masterarbeit selbstständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.
- ich dieses Masterarbeitsthema bisher weder im Inland noch im Ausland einem/einer BegutachterIn zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.
- diese Arbeit mit der vom/von der BegutachterIn beurteilten Arbeit übereinstimmt.

Die Studierende/Absolventin räumt der Universität Wien das Recht ein, die Masterarbeit für Lehre- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei die Studierende/Absolventin als Urheberin zu nennen ist. Die Studierende/Absolventin räumt weiter ein, dass die Masterarbeit in der Universitätsbibliothek und im Institut für Theater-, Film- und Medienwissenschaften aufgestellt und allgemein zugänglich gemacht werden darf. Von der erschienen, d.h. beurteilten Masterarbeit, darf die Bibliothek für den eigenen Gebrauch Kopien in beliebiger Zahl anfertigen. Für den Gebrauch durch andere Personen dürfen Kopien von der Bibliothek bzw. ihren BenutzerInnen nur mit Genehmigung der Autorin hergestellt werden. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen der Studierenden/Absolventin und der Universität Wien.

_____ _____

Ort, Datum *Unterschrift*

für meine Eltern

Inhaltsverzeichnis

1 Einleitung: *I'll be watching you*

„Every breath you take and
every move you make
every bond you break,
every step you take […]
Every single day and
every word you say
I'll be watching you“[1]

Jeder Atemzug kann durch CO_2 Detektoren und Alkoholtester, jede Bewegung durch GPS-Satellitenortung und Bewegungsmelder, jede übertretene Grenze durch Alarmsysteme, jeder Schritt durch Bewegungsprofile und jedes gesprochene Wort durch Wanzen, Lauschangriffe und Stimmenanalyse überwacht, kontrolliert und ausgewertet werden.[2] Sicher war es 1982 nicht Gordon Sumners Absicht, mit dem Welthit *Every breath you take* das ubiquitäre Überwachungssystem des 21. Jahrhunderts zu beschreiben, aber dennoch gelang es ihm treffsicher.

»Big Brother is watching you« - diese in der Medienlandschaft omnipräsente Aussage ließe sich problemlos in den Liedtext des *The Police* Songs integrieren. Auch auf der Suche nach der Erzählperson der Geschichte, liegt die Idee des »großen Bruders« nahe. Spätestens, seit Ende der 90er Jahre die Fernsehindustrie das Motiv der ubiquitären Überwachung für sich entdeckte, ist der »Big Brother« den Mediennutzenden ein feststehender Begriff. Dieser Bruder ist aber keineswegs ein gedanklicher Auswuchs des Realitätsfernsehens, sondern vielmehr die Schöpfung des englischen Schriftstellers George Orwell, der den überwachenden Bruder 1949 zum ersten Mal in seinem fiktiven Roman *1984* erwähnte. Die dystopische Erzählung beschreibt einen totalitären Überwachungsstaat, in dem der »Big Brother« die Personifikation der ubiquitären Kontrolle darstellt; erfunden von einer Partei, die ihrem Staatssystem nicht nur Fakten und Gesetze, sondern sogar ein eigenes, reales Gesicht geben wollte. Bezweckt wird damit, dass die Idee einer gottähnlichen, überwachenden Gestalt in den Köpfen der

---

1 Sumner, Gordon M. (1983): „Every Breath You Take“.

2 Vgl. Nogala, Detlef, „Der Frosch im heißen Wasser. Wie in der informatisierten Gesellschaft des 21. Jahrhunderts Überwachung trivialisiert wird.“, in: *Vom Ende der Anonymität. Die Globalisierung der Überwachung*, Hg. Christiane Schulzki Haddouti, Hannover: Verlag Heinz Heise GmbH & Co KG 2000, S. 144.

Bevölkerung existiert, auch wenn diese sich nicht der etwaigen Existenz der Figur sicher sein kann.

Diese schier wahnsinnige Vorstellung der totalen Überwachung, die wie ein Damoklesschwert über den Überwachten schwebt, ist, wie bereits erwähnt, nicht nur im Privatfernsehen zur Wirklichkeit, sondern auch im realen Leben ein Teil unseres Alltags geworden. Seit sich dieses reale Leben außerdem von der offline- in die online-Welt überträgt, sind für Datensammelnde vollkommen neue Möglichkeiten der Überwachung von Individuen entstanden. Diese Überwachungsmöglichkeiten stehen aber keineswegs nur dem »großen Bruder« oder anderen übergeordneten Instanzen zur Verfügung, sondern auch den Nutzenden selbst. Vor allem seit der flächendeckenden Verbreitung des Internets und der kontinuierlichen Ausbreitung des *Internet der Dinge*[3], spielen die Themen der Fremd- und Selbstüberwachung eine deutlich größere Rolle, als es noch im analogen Zeitalter der Fall war. Hatte Orwell diese Entwicklungen möglicherweise im Jahre 1949 bereits vorausgesehen?

1.1 Vorgehen

Nun stellt sich die Frage, wieso die technisch strukturierte Kontrolle im Bereich des Internet der Dinge analysiert und hinterfragt werden sollte.

Wie bereits erwähnt, ist Überwachung kein Novum des 21. Jahrhunderts. Bei beinahe jeder großen technischen oder medialen Neuerung in der Geschichte der Menschheit veränderte sich die Anordnung der Kontrolle grundlegend. Hierbei sind das Abfangen und Lesen von fremden Briefen, das Abhören von Gesprächen und Telefonaten, oder die optische Kontrolle von Handlungen durch eine Videokamera oder mit dem bloßen Auge nur einige wenige von vielen nennenswerten Beispielen, die zur Überwachung genutzt werden. Seit der flächendeckenden Verbreitung des Internets durchlaufen die *Surveillance Studies* allerdings eine grundlegende Veränderung, die zuletzt von der Kontrolldebatte bezüglich des *Social Webs* ihren Höhepunkt fand. Nun entwickelt sich diese Diskussion über das „Mitmach-Internet“[4] durch ein technisches Novum weiter. Das Internet der Dinge wird bereits seit Längerem als „the next big thing“[5] gehandelt

---

[3] In der folgenden wissenschaftlichen Arbeit werden die Begriffe „Internet der Dinge“, „Internet of Things“ und die Abkürzung „IoT“ synonym füreinander verwendet.

[4] Werner, Hendrik, „Das Web 2.0 hat seine besten Tage hinter sich“, *Welt.de*, 02.12.2009, http://www.welt.de/wirtschaft/webwelt/article5400784/Das-Web-2-0-hat-seine-besten-Tage-hinter-sich.html, Zugriff: 06.07.2016.

[5] Burrus, Daniel, „The Internet of Things Is Far Bigger Than Anyone Realizes“, *Wired*, 19.11.2014, http://www.wired.com/insights/2014/11/the-internet-of-things-bigger/, Zugriff: 06.07.2016.

und spielt ebenfalls seit geraumer Zeit (vielleicht auch unbemerkt), eine unterschwellige Rolle in vielen Lebensbereichen der Nutzenden.
Was aber bedeutet diese Integration der technisch strukturierten Überwachung in das Privatleben für die Nutzenden? Was passiert mit der Privatsphäre wenn die Nutzenden das Internet der Dinge ohne große weiterführende Überlegungen in ihr Privatleben und ihr Zuhause integrieren? Wie entwickelt sich der private Überwachungsraum im Vergleich zum öffentlichen Überwachungsraum und gibt es diese Unterscheidung überhaupt noch oder ist sie nur eine Reliquie aus dem Erinnerungsvermögen, welches die Nutzenden aus dem 20. Jahrhundert mitgebracht haben?

An dieser Stelle wird die These aufgestellt, dass durch die Verarbeitung privater Daten, die die Integration des Internet der Dinge in das private Zuhause mit sich bringt, die letzten noch vorhandenen Grenzen zwischen öffentlichem und privatem Leben aufgehoben werden. Durch die Eingliederung der intelligenten, technischen Gadgets in das Heim der Benutzenden findet eine vollkommene Eliminierung der Privatheit statt, ausgelöst durch die personenbezogene Datenüberwachung, die wissentlich und freiwillig geschieht.
Diese These gilt es im Folgenden anhand bereits bestehender Medien- und Sozialwissenschaftlicher Theorien zu hinterfragen und anschließend durch eine Analyse des Beispiels *Smart Home* zu belegen oder zu widerlegen. Hierfür müssen als erstes, grundlegende, aktuelle Überwachungstheorien miteinander verglichen und gegeneinander aufgewogen werde. Dabei steht das Motiv von Jeremy Benthams Modell des Panoptikums[6], das seit der Wiederentdeckung durch Foucault als Inbegriff der Surveillance Studies gilt, im Mittelpunkt. Die Analyse der Theorie lässt sich anhand dieses Motivs gut einteilen, da sich die Forschung bezüglich der Aktualität des Panoptikums in zwei Lager spaltet.

Nach der Abhandlung der theoretischen Grundlagen wird eine Methode zur Analyse des praktischen Beispiels entwickelt. Diese Analysemethode setzt sich aus einem soziologischen, einem medialen und einem biopolitischen Bestandteil zur *Post-Privacy* Debatte zusammen. Anhand der herausgestellten Punkte wird dann das Smart Home als neues Dispositiv der vollkommenen Überwachung untersucht. Vor der Analyse

[6] Der englische Begriff „Panopticon“ und die deutsche Übersetzung „Panoptikum“ werden im Folgenden synonym füreinander verwendet.

wird zusätzlich noch auf Mark Weisers theoretische Vorüberlegungen zum *Ubiquitous Computing* eingegangen, um historisch an das Thema Internet der Dinge heranzuführen. Anschließend soll auf dessen aktuelle Bedeutung für die Gesellschaft eingegangen werden. Daraufhin wird mithilfe der zuvor bereits erarbeiteten Forschungsmethode das Beispiel des privaten Raumes im Zusammenhang mit dem Internet der Dinge, verkörpert durch das Smart Home, analysiert. Abschließend bleibt in einem Resümee festzustellen, inwieweit sich die vorangestellte These bewahrheitet.

2 Forschungsstand und Methoden

Um eine genaue Forschungsmethode festzulegen, ist es zunächst relevant, einen groben Überblick über den aktuellen Forschungsstand zu erhalten. Außerdem werden im Vorfeld Fragen nach Geschichte, Hintergründen sowie aktuellen Motiven der Überwachung erörtert.

2.1 Relevanz des Themas »Überwachung«

Die Relevanz des Themas Überwachung von Individuen, egal ob durch simples optisches Beobachten, elektronische Abhörgeräte oder in dem hier signifikanten Beispiel, dem Internet der Dinge, ist vor allem durch grundlegende Definitionen zu erläutern. Es ist zu klären, was Überwachung einerseits für das Subjekt der Überwachung und andererseits für deren ausführende Instanz bedeutet und wie die Machtverhältnisse in verschiedenen Überwachungsräumen verteilt sind. Außerdem ist eine historische Heranführung an das Thema von entscheidender Bedeutung, um dessen gesamtes Ausmaß zu verstehen.

> „Überwachung ist das gezielte Beobachten eines bestimmten Raums, Objekts oder des Verhaltens einer Person(engruppe) mit dem Ziel, Informationen zu sammeln, Verhalten zu kontrollieren, zu beeinflussen oder zu steuern und gegebenenfalls sanktionierbar zu machen.“[7]

Definitionen wie diese finden sich zu Hunderten in soziologischer Fachliteratur. Zwar sind sie teilweise voneinander abweichend, trotzdem aber größtenteils allesamt zutreffend. Überwachung findet in den unterschiedlichsten Formen statt und ist keinesfalls ein Produkt des modernen Verwaltungsstaats, wie es teilweise erscheinen mag. Auch wenn es in manchen Momenten wirkt, als wäre ein Großteil der Überwachungsformen im Zuge von Industrialisierung und Urbanisierung als städtisches Phänomen etabliert worden und findet größtenteils im öffentlichen Raum statt,[8] so ist das nur oberflächlich richtig. Die Idee der Überwachung sitzt tiefer in den Köpfen der Gesellschaft fest und ist erwiesenermaßen kein neues Ereignis der Moderne oder Postmoderne. Um nun die genaue Bedeutung der Begrifflichkeit zu ergründen, ist es hilfreich, sich zu Beginn der etymologischen Herkunft des Wortes zu widmen. Das Grimmsche Wörterbuch gibt

---

7 Eick, Volker, „Überwachung“, in: *Handbuch kritische Stadtgeographie*, Hg. Bernd Belina, Matthias Naumann, Anke Strüver, Münster: Westfälisches Dampfboot [2]2016, S. 163.

8 Vgl. Ebd., S. 164.

beispielsweise als Erklärung für das Verb »überwachen« die kontrollierte Handlung als Bedeutung an, die gemeinhin eher negativ konnotiert ist. Des Weiteren wird hier allerdings auch eine positiv zu deutende Semantik erklärt. Während beispielsweise das Kind bereits schläft, bleiben Erwachsene länger wach und beschützen somit den Schlaf des besagten Kindes. Dadurch, dass die überwachende Instanz länger wach bleibt, ist für die Sicherheit des Schützlings gesorgt.[9] Diese Erklärung zeigt, dass Überwachung keineswegs nur negativ konnotiert sein muss und greift beispielsweise auch beim *Ambient Assisted Living,* auf das später noch genauer eingegangen wird.

Ferner ist auch der geschichtliche Hintergrund interessant. Der Glaube an den allwissenden, allesüberwachenden großen Bruder wurde nicht erst von George Orwell mit *1984* geprägt, sondern entspringt viel mehr dem christlichen Glauben an einen allwissenden Gott, dem nichts vorenthalten werden kann und der im Falle einer Übertretung der gesellschaftlichen Regeln auch zum strafenden Gott werden kann.[10] Bis heute ist diese religiöse Variante der Beobachtung im christlichen Glauben verankert. Aus ihr lässt sich auch der Plan der Gefängnisanstalt ableiten, die im 18. Jahrhundert vom englischen Philosophen Jeremy Bentham entworfen wurde und den Grundstein für die von da an folgenden philosophischen und soziologischen Betrachtungen auf die Überwachung legte.

Während bis zum Ende des 18. Jahrhunderts von der Justiz vorgesehen wurde, VerbrecherInnen und Gefangene in Kerker zu werfen, zu foltern und/oder öffentlich zu demütigen,[11] befand sich die ausführende Staatsgewalt bereits ein Jahrhundert später im Umbruch und der Umgang mit Kontrolle und Bestrafung von Verurteilten hatte sich merklich verändert. „Die Strafe soll, wenn ich so sagen darf, eher die Seele treffen als den Körper“[12], formulierte der französische Philosoph Gabriel Bonnot de Mably 1789 das damals neu definierte Prinzip der Bestrafung. Diese Auffassung teilte auch der britische Philosoph Jeremy Bentham, der das Prinzip des *Panoptismus* 1787 als Gedankenexperiment entwickelte. Dem Gelehrten gelang damit seiner Zeit der Durchbruch in der Sozialpragmatik. In seiner 1791 erschienenen Publikation *Panopticon:*

---

9 Vgl. Nogala, Detlef, „Der Frosch im heißen Wasser. Wie in der informatisierten Gesellschaft des 21. Jahrhunderts Überwachung trivialisiert wird.“, in: *Vom Ende der Anonymität. Die Globalisierung der Überwachung*, Hg. Christiane Schulzki-Haddouti, Hannover: Verlag Heinz Heise GmbH & Co KG 2000, S. 142.

10 Vgl. Ebd., S. 143.

11 Vgl. Foucault, Michel, *Überwachen und Strafen. Die Geburt des Gefängnisses*, Frankfurt a. Main: Suhrkamp 1994, S. 9; (Orig. *Surveiller et punir – la naissance de la prison*, Paris: Gallimard 1975).

12 Mably, Gabriel Bennot de, *De la legislation, Œvres completes*, Bd. IX, Paris: 1789, S. 326, zit. Nach Michel Foucault, *Überwachen und Strafen. Die Geburt des Gefängnisses*, Frankfurt a. Main: Suhrkamp 1994, S. 26; (Orig. *Surveiller et punir – la naissance de la prison*, Paris: Gallimard 1975).

or, the Inspection-House[13] beschrieb Bentham das Prinzip eines effizienten Gefängnisses, das die bisher dagewesene Idee von Überwachung und Bestrafung ablösen und verbessern sollte. Die Architektur dieses runden Gebäudes erlaubt es dem Überwacher, der seinen Platz in einem Turm in der Mitte hat, alle Gefangenen, die sich in sternförmig um ihn herum angeordneten Räumen befinden, jederzeit und ohne deren Wissen und Bemerken zu sehen und zu kontrollieren. Bentham kehrt in seiner panoptischen Anlage also die bisherigen Prinzipien um. Von den ursprünglichen Eigenschaften einsperren, verdunkeln, verbergen und vergessen, wurde allein die erste beibehalten. Die drei übrigen werden durch ständige Sichtbarkeit ersetzt, da diese viel allumfassendere Möglichkeiten der Überwachung bietet als die Unsichtbarkeit. Des Weiteren lässt sich auch der Utilitarismus, der von Bentham mitbegründet wurde, im Modell des Panoptikums deutlich wiedererkennen. Ein wichtiger Punkt der utilitaristischen Denkweise ist die Wirtschaftlichkeit. Überwachung soll möglichst effizient und beispielsweise ohne die Verschwendung menschlicher Ressourcen vonstattengehen. Außerdem sollten die Gefangenen, wie bereits beschrieben, keine körperlichen Leiden von der Bestrafung davontragen, sondern nur psychischem Druck unterstellt sein.[14]
Der französische Philosoph Michel Foucault beschreibt Benthams Modell, das er Ende der 70er Jahre wiederentdeckte, als Paradebeispiel der Überwachungslogik und brachte es durch seine Schrift *Überwachen und Strafen*[15] einer breiten Masse zur Kenntnis. Die Hauptaufgabe des Panoptikums sieht Foucault in der Schaffung eines bewussten und permanenten Sichtbarkeitszustandes beim Gefangenen, durch den die Einhaltung des Machtverhältnisses sichergestellt ist. Dieses Machtverhältnis besteht vor allem darin, dass die Überwachten zwar ständig unter Beobachtung stehen könnten, aber es nicht zwingend müssen.[16] Diese Ungewissheit über den eigenen Status der Überwachung löst dann in den Gefangenen die seelischen Qualen aus, von denen de Mably bereits im 18. Jahrhundert spricht. Im Zuge dessen erwähnt Foucault die Disziplinarmacht, die seinen Aufzeichnungen nach charakteristisch für das 19. und 20.

---

13 Bentham, Jeremy, *The Works of Jeremy Bentham*, Bd. IV, Hg. John Bowring, Edinburgh: William Tait 1843, S. 37-173.

14 Vgl. Jespersen, Julie Leth/Anders Albrechtslund/Peter Øhrstrøm/Per Hasle/Jørgen Albretsen, *Surveillance, Persuasion, and Panopticon*, 2007, https://www.researchgate.net/publication/229031001_Surveillance_Persuasion_and_Panopticon, Zugriff: 07.06.2015, S. 3f.

15 Foucault, Michel, *Überwachen und Strafen. Die Geburt des Gefängnisses*, Frankfurt a. Main: Suhrkamp 1994; (Orig. *Surveiller et punir – la naissance de la prison*, Paris: Gallimard 1975).

16 Vgl. Ebd., S. 258.

Jahrhundert ist und die sich um die Dressur von menschlichen Körpern dreht.[17] Aufgrund der Disziplinarmacht, die durch Ungewissheit und Angst vor der ständigen Überwachung auf die Gefangenen wirkt, setzen diese sich selbst unter Druck. Nicht der Wärter im Turm ist die treibende Kraft bei der Unterdrückung des Geisteszustandes, sondern die Gefangenen führen sich diese seelischen Qualen unterbewusst selbst zu.[18] Foucault sagt über die Gefangenen: „The inmates should be caught up in a power situation of which they are themselves the bearers"[19]. In einer Studie der Technischen Universität von Tennessee wird dieses Phänomen mit dem Namen *Little Brother* betitelt. Anders als beim orwellschen Prinzip des *Big Brother*, der alles überwacht, ist der kleine Bruder weniger eine übergeordnete Instanz sondern mehr die eigene Persönlichkeit der Gefangenen, die sich die Überwachung und Kontrolle selbst zufügt.[20]

Nun ist es aber nicht nur von akuter Wichtigkeit, sich mit der Vergangenheit und Geschichte der Überwachung auseinanderzusetzen, sondern auch mit ihrer aktuellen Bedeutung in der Gegenwart. Überwachung von Individuen oder der ganzen Gesellschaft bekam bereits mit der flächendeckenden Verbreitung von E-Mails und dem World Wide Web eine völlig neue Bedeutung. Durch ein Novum des technischen Fortschrittes, das Internet der Dinge, steigert sich die bereits vorhandene Beobachtung und dadurch entstehende Informationssammlung und Kontrolle ins Unermessliche. Überwachung findet auch heute in den unterschiedlichsten Formen statt und ist, wie bereits durch die geschichtlichen Hintergründe belegt, keinesfalls ein Produkt des modernen Verwaltungsstaats, obwohl es teilweise bei aktuellen Vorkommnissen durchaus so erscheinen mag. Überwachung und Kontrolle ist nicht erst im Zuge von Industrialisierung und Urbanisierung als städtisches Phänomen etabliert worden.

---

17 Selbstverständlich ist die genaue Definition der Disziplinarmacht deutlich komplexer als diese kurze Aussage, allerdings würde eine detailliertere Beschreibung den Rahmen dieser Arbeit deutlich sprengen. Daher wird aus Platzgründen darauf verzichtet.

18 Vgl. Ruoff, Michael, *Foucault-Lexikon: Entwicklung, Kernbegriffe, Zusammenhänge*, Stuttgart: UTB 2009, S. 45f.

19 Foucault, Michel, *Discipline and punish: The birth of the prison*, New York: Vintage Books 1979, S. 201; (Orig. *Surveiller et punir – la naissance de la prison*, Paris: Gallimard 1975).

20 Vgl. Brignall, Tom III, „The New Panopticon: The Internet Viewed as a Structure of Social Control", *Theory & Science* 3/1, 2002, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.5894&rep=rep1&type=pdf, Zugriff: 08.06.2016.

2.2 Forschungsstand im Überblick

Um eine Theorie und eine daraus folgende Methode zur anschließenden Analyse des Beispiels Smart Home zu finden, ist es zuerst notwendig, einen Blick auf den aktuellen Forschungsstand der Surveillance Studies zu werfen. Bis heute spielt das Motiv von Benthams Panoptikum eine wichtige Rolle in beinahe allen Theorien zur Überwachung – sei es um das Prinzip zu bestätigen, ein anderes Motiv daraus abzuleiten, oder, um sich dagegen auszusprechen und es zu widerlegen. Daher ist der folgende Überblick in zwei Kategorien aufgeteilt. Begonnen wird in dieser Abhandlung mit der Riege der Wissenschaftler, die sich für das Panoptikum aussprechen, Benthams Ansätze immer noch als aktuell empfinden, sie gegebenenfalls den neuen, technologischen Gegebenheiten anpassen und dann eine fortschrittliche Überwachungsideologie daraus entwickeln. Anschließend soll eine Reihe von Forschern angeführt werden, die in ihren Theorien gegen die Aktualität das panoptischen Prinzips vorgehen und versuchen, mit ihren Ideen die imaginären Mauern des Panoptikums einzureißen.

2.2.1 Pro Panoptikum

Die Begrifflichkeit Panoptikum setzt sich etymologisch aus den beiden griechischen Wörtern »pan«, deutsch *alle* und dem Begriff »opticon«, deutsch *optisch* zusammen. Zusammengesetzt lässt sich Panopticon also inhaltlich so übersetzen, dass alle gesehen werden.[21] Das Motiv des Panoptikums kann in mehrere Richtungen interpretiert und der neuesten Technik entsprechend aktualisiert werden. Im Folgenden werden vier unterschiedliche Adaptionsansätze vorgestellt.

2.2.1.1 Diana R. Gordon – *The Electronic Panopticon* (1987)

Diana R. Gordon beschreibt in ihrer Abhandlung *The Electronic Panopticon: A Case Study of the Development of the National Criminal Records System*[22] bereits 1987 die Verwandlung des Panoptikums, weg von Benthams architektonischem Modell, hin zu einer elektronischen Version dessen. Als Analysebeispiel dient ihr hierbei das Aufzeichnungssystem für Kriminalität in den Vereinigten Staaten von Amerika. Gordon

---

21 Vgl. Mathiesen, Thomas, *Silently Silenced. Essays on the Creation of Acquiescence in Modern Society*, Winchester: Waterside Press 2004, S. 98.

22 Gordon, Diana R., „The Electronic Panopticon: A Case Study of the Development of the National Criminal Record System“, in: *Surveillance, Crime & Social Control*, Hg. Clive Norris, Dean Wilson, Aldershot: Ashgate 2006, S. 383-411; (Orig. *Politics & Society* 15, 4, 1986-87, S. 483-511).

beschreibt die Weiterentwicklung des amerikanischen Justizsystems und welche Folgen diese auf das alltägliche Leben der BürgerInnen hat, die diesem System unterstellt sind.

Während in den Anfängen der polizeilichen Akten analoge Aufzeichnungen dominieren, beginnt das amerikanische Justizsystem bereits Anfang der 1970er Jahre damit, sein Strafjustizregister zu digitalisieren. Wo schon 1971 fast 2,5 Millionen Einträge zu finden waren, stieg die Zahl der Verzeichnungen im System bis zum Erscheinen der Abhandlung auf 17 Millionen Einträge. Gordon nahm weiter an, dass bereits zwei Jahre später jeden Tag eine Million neuer Strafdelikte im System verzeichnet werden sollten.[23] Bei solchen immens hohen Zahlen, die bereits vor mehr als 25 Jahren Realität waren, ist es daher kaum verwunderlich, dass normale BürgerInnen mittlerweile seit dem Jahr 2008 über ein kostenloses Online-Portal Zugang zum US-amerikanischen Strafregister haben.[24] Durch diese Funktion wird es Privatpersonen möglich, Einblick in die kriminelle Vergangenheit ihrer Nachbarn, Bekannten, schlicht jeder erdenklichen Person, sei sie nun fremd oder bekannt, zu erhalten. Auch wenn Gordon diese Entwicklung 1987 noch nicht voraussehen konnte, so ging ihre Vorstellung eines „elektronischen Panoptikums“ entschieden in die gleiche Richtung.

> „Bentham’s Panopticon was a circular prison with individual cells around a central tower so that a single warden could observe the movements of all inmates at all times. With the national computerized system, the entire function of crime control, not just the prison, becomes a “panoptic schema”, with the record surrogate for the inmate and all of law enforcement as warden. Such an image has no boundaries; the warden becomes boss and landlord and banker, too.“[25]

Gordon beschreibt hier, wie die US-amerikanische Gesellschaft durch die Einführung der computerbasierten Datenbank für Straftaten und polizeiliche Vermerke ein panoptisches Schema entwickelt. Durch diese elektronische Zugänglichkeit von jedem Ort aus werden die Grenzen von Benthams architektonischem Modell aufgehoben und auch die Person des Wärters kann nicht auf einen einzelnen Menschen festgemacht werden. Viel mehr wird das gesamte alltägliche Leben zu einem Überwachungsraum, in dem alle Menschen potentiell zu Überwachenden gemacht werden. Während in Gordons Realität der 1980er Jahre »nur« Bankangestellte, Vermietende und Vorgesetzte Zugriff auf diese Daten hatten (und dieser Zugriff noch dazu zahlungspflichtig war),

---

23 Vgl. Ebd., S. 383.
24 Vgl. O.N., „CriminalSearches“, http://www.criminalsearches.com/, Zugriff: 25.08.2015.
25 Gordon, „The Electronic Panopticon“, S. 387.

so hat sich die Zahl der Zugriffsberechtigten bis heute, ausgelöst durch die bereits erwähnte Online-Plattform *CriminalSearches.com,* auf alle US-amerikanischen BürgerInnen mit Internetzugriff erhöht.[26] Erschwerend hinzu kommt auch, dass auf Aktualität und Vollständigkeit dieses elektronischen Systems nur teilweise Rücksicht genommen wird – veraltete oder schlicht falsche Einträge können nur durch eine direkte Kontaktaufnahme mit der Polizei korrigiert werden.[27] Unkontrollierter Zugriff auf vertrauliche Daten, deren Richtigkeit nicht unbedingt bestätigt ist, kann schwerwiegende Folgen haben. Allgemein lassen sich die Auswirkungen der Überwachung und Kontrolle und deren Folgen durch das von Gordon beschriebene elektronische Panoptikum gut mit ihren eigenen Worten zusammenfassen: „In an age where information is power and more is almost always better, the dynamic of system expansion is very powerful.“[28] Information ist Macht. Macht, die Überwachende über die Überwachten gewinnen und die große gesellschaftliche Auswirkungen mit sich bringen kann.

2.2.1.2 Mark Poster - *Superpanopticon* (1990)

Auch mehr als zehn Jahre später spielt in den Theorien von Film- und Medienwissenschaftler Mark Poster die Unabdingbarkeit der Kontrolle anhand der Datenbanktechnologie eine vergleichbar große Rolle, wie zuvor bei Diana R. Gordon. Auch Jeremy Benthams Motiv des Panoptikums erhält in seiner Theorie einen ähnlich großen Stellenwert. In seiner Abhandlung *Databases as Discourse; or Electronic Interpellations*[29] beschreibt Mark Poster seine Idee eines „Superpanopticons“[30].

> „My argument is that with the advent of computerized databases, a new discourse/practice operates in the social field, a superpanopticon if you will, that reconfigures the constitution of the subject.“[31]

---

26 Stone, Brad, „If You Run a Red Light, Will Everyone Know?“, *nytimes.com*, 03.08.2008, http://www.nytimes.com/2008/08/03/technology/03essay.html?ref=technology, Zugriff: 27.08.2016.

27 O.N., (Anonym: pte), „Webseite macht US-Strafregister kostenlos zugänglich“, *derStandard.at*, 04.08.2008, http://derstandard.at/1216918474464/Webseite-macht-US-Strafregister-kostenlos-zugaenglich, Zugriff: 27.08.2016.

28 Gordon, „The Electronic Panopticon“, S. 396.

29 Poster, Mark, „Database as Discourse; or, Electronic Interpellations“, in: *Computers, Surveillance and Privacy*, Hg. David Lyon, Elia Zureik, Minneapolis: University of Minnesota 1996, S. 175-192; (Orig. Mark Poster, *The Second Media Age*, Cambridge: Polity Press 1995).

30 Ebd., S. 182.

31 Ebd..

Marc Poster erläutert in dieser Passage, dass durch die Einführung der computerbasierten Datenbanken eine vollkommene Neuorientierung und Neuordnung des sozialen Umfeldes der Kontrolle für das Wesen des Subjektes stattfindet. Darüber hinaus weist er ergänzend auf weitere wichtige Zusatzinformationen hin, welchen sowohl von Kritikern, als auch von Befürwortern der Technologie, oft zu wenig Beachtung geschenkt wird. Elektronisch basierte Datenbanken haben kein biologisches oder technisches Ablaufdatum und können daher im besten Fall für immer bestehen bleiben. Außerdem können sie sich ohne besonderen Aufwand verbreiten und es kann von jedem erdenklichen Standpunkt aus darauf zugegriffen werden. Durch diese Möglichkeit des Zugriffs ist nicht nur die Gelegenheit gegeben, Information einzusehen, sondern auch die Datenbanken zu bearbeiten. Poster spricht in diesem Zusammenhang davon, dass die ursprüngliche Autorität, die der Autor für gewöhnlich inne hat, vom System der elektronischen Datenbank untergraben und verspottet wird, da jeder zum Autor werden kann.[32] „The database is no one's and everyone's.“[33]

Mark Poster beschreibt seine Idee des Superpanoptikums im Vergleich zu Benthams Panoptikum vor allem mit der Eigenschaft des geringen Aufwandes. Die Möglichkeiten der absoluten Überwachung im Superpanoptikum wurden von den Menschen selbst geschaffen.

> „The phone cables and electric circuitry that minutely crisscross and envelop our world are the extremities of the superpanopticon, transforming our acts into an extensive discourse of surveillance, our private behaviors into public announcements, our individual deeds into collective language.“[34]

Diese Idee der »Extremitäten des Superpanoptikums« lässt sich problemlos in das 21. Jahrhundert übertragen. Telefonleitungen, Glasfaserkabel, drahtlose Verbindungen, das Internet und auch das Internet der Dinge sind ursprüngliche Ideen des Menschen, die als Extremitäten des Überwachungsapparates kategorisiert werden können, falls sie sich dieser zu eigen macht. Unterschiede zwischen der älteren Idee des Panoptikums und dem von Poster angedachten Superpanoptikum finden sich hingegen vor allem in der Subjektbildung. Während die vom Panoptikum betroffenen Subjekte sich ihrer Umgebung und der Möglichkeit der (nicht mehr vorhandenen) Selbstbestimmung

---

32 Vgl. Ebd., S. 183.
33 Ebd., S. 182.
34 Ebd., S. 184.

bewusst sind, verhält sich das überwachte Subjekt im Superpanoptikum deutlich verändert. Die Individuen sind sich hier ihrer Umgebung und ihrer Selbst nicht wirklich bewusst.[35] „The scandal, perhaps, of the superpanopticon is its flagrant violation of the great principle of the modern individual, of its centered "subjectified" interiority."[36] Poster spricht hier davon, dass der eigentliche Skandal um das Superpanoptikum vielleicht in seiner eklatanten Missachtung des modernen Individuums und im Zuge der Verletzung seines zentrierten Innenlebens, seiner Seele die zum Subjekt wird, liegt. Während allgemein angenommen werden könnte, dass der moderne oder auch der postmoderne Mensch eigentlich als freie Subjekte leben und sich frei entfalten könnten, so ist dem nach Poster nicht so. Das Superpanoptikum agiert im Verborgenen, gibt den Menschen das Gefühl, dass eine Subjektifikation stattfinden kann und beraubt sie dann anschließend unbemerkt wieder dieser Möglichkeit der Subjektwerdung.
Poster beschreibt in seiner Theorie den postmodernen Überwachungsapparat nach psychologischer Sicht als eine Einschränkung der Persönlichkeitsentwicklung für jeden einzelnen von uns. Auf diese dem sozialwissenschaftlichen Sektor zuzuordnende Theorie folgt nun Thomas Mathiesens vorwiegend mediale Perspektive auf das panoptische Prinzip der Überwachung.

2.2.1.3 Thomas Mathiesen - *Internet as a silencing Synopticon* (2004)

Der norwegische Rechtssoziologe Thomas Mathiesen beschreibt in seinem Aufsatz *Panopticon and Synopticon as Silencing System*[37] das Internet als Teil eines wie er es nennt *silent silencing* Systems. Er bezeichnet es in diesem Kontext außerdem als *Synopticon*[38]. Diese Begrifflichkeit entsteht für Mathiesen etymologisch im Zusammenhang mit der Geschichte der Überwachung. Während in ferner Vergangenheit beispielsweise durch an den Pranger stellen Viele die Wenigen beobachteten, änderte sich diese Anordnung mit Benthams Modell des Panoptikums grundlegend. In dieser neueren Anordnung, die auch von Foucault aufgegriffen wurde, beobachteten nun stattdessen Wenige die Vielen. Diese räumliche Anordnung wurde anschließend durch die Verbreitung der Massenmedien wieder umgekehrt. Beispielsweise beim Fernsehen be-

35 Vgl. Ebd., S. 190.
36 Ebd..
37 Mathiesen, Thomas, *Silently Silenced. Essays on the Creation of Acquiescence in Modern Society*, Winchester: Waterside Press 2004, S. 98-102.
38 Der englische Begriff „Synopticon" und die deutsche Übersetzung „Synoptikum" werden im Folgenden synonym füreinander verwendet.

obachten Viele, oft sogar zur gleichen Zeit, einige Wenige. Vor allem an dieser Synchronität setzt Mathiesens Begriff des Synoptikums an, der sich etymologisch vom griechischen *syn* ableitet, das *gemeinsam*, oder *zur gleichen Zeit* bedeutet. Seine Bedeutung umfasst also viele Individuen, die zusammen ihren Fokus auf etwas richten.[39] Wie ist aber nun das Internet in die Reihe dieser Begrifflichkeiten einzuordnen, da es kein Synoptikum im klassischen Sinn darstellt? Anfänglich wirkt das Internet für viele wie eine demokratische Plattform, auf der sich alle Teilnehmenden ebenbürtig gegenüber treten können. Mathiesen blickt hier tiefer in das System:

> „[…] in actual practice, the Internet becomes to a considerable extent a part of the synoptical system, in as much as it is, to a substantial degree, dominated by powerful economic agents […]. To the same degree, the structure becomes characterized by a one-way flow, from the relatively few in control of economic capital, symbolic capital and technical know-how, to the many who are entertained or who by the products.“[40]

Auch wenn im Internet nicht alle Zuschauenden gleichzeitig ihre Aufmerksamkeit auf ein und denselben Kanal, sondern teilweise auf unterschiedliche, richten, so findet dennoch eine klassische, einseitige Sender-Empfänger Situation statt.[41] Obwohl diese Interaktion auf eine Seite beschränkt ist, gibt es dennoch eine weitere Verbindung zwischen Sender und Empfänger. Der Aspekt der Überwachung darf nicht außer Acht gelassen werden und genau dieser ist es auch, den Mathiesen als *silently silenced* bezeichnet. Die Kontrolle findet unbemerkt statt und die Überwachten werden leise zum Schweigen gebracht. Während die Nutzenden vermeidlich nur konsumieren und Input von großen Sendern bekommen, so geschieht dies von Senderseite nicht aus reiner Nächstenliebe und dem Drang zu Mitteilungsbedürfnis und Unterhaltung der Gesellschaft, sondern vor allem aus einem wirtschaftlichen Blickwinkel heraus. „Media must sell“[42] – Dieser Verkaufsprozess findet im Fall des Internets vor allem durch die Überwachung und das Sammeln von Nutzendendaten statt. Mathiesen betrachtet das Internet also als eine wechselseitige Abhängigkeit von panoptischem und synoptischem System, die ohneeinander nicht funktionieren kann. Wichtigster Aspekt hierbei ist für ihn, dass die panoptischen und synoptischen Prozesse für Zusehende und Überwachte *silently silenced* geschehen.

---

39 Vgl. Mathiesen, *Silently Silenced*, S. 98f.
40 Ebd., S. 100.
41 Vgl. Ebd..
42 Ebd., S. 102.

2.2.1.4 Hans Rämö & Mats Edenius - *Mobile panopticon* (2008)

Auch die schwedischen Wirtschaftswissenschaftler Hans Rämö und Mats Edenius griffen im Jahr 2008 die Idee von Jeremy Benthams Panoptikum auf und setzten sie gedanklich so um, dass sie sich den technischen Gegebenheiten des 21. Jahrhunderts anpasst. In ihrer Abhandlung *Time Constraints in New Mobile Communication*[43] unterbreiten Rämö und Edenius den Lesenden die Idee eines „mobile Panopticon“[44]. Erklärt wird dieses Konzept anhand der Verbreitung und Nutzung von Smartphones unter ManagerInnen in arbeitsintensiven Positionen.[45]

Durch die Einführung von Smartphones als zusätzliche Arbeitsgeräte neben Standrechner, Laptop, Festnetztelefon und Mobiltelefon verändern sich die Arbeitsumgebung und die allgemeine Arbeitsweise grundlegend. Während das traditionelle Büro an einen festen Ort gebunden ist, werden diese Grenzen beim Arbeiten mit einem Smartphone fast gänzlich aufgehoben – einzig und allein unterschiedliche Zeitzonen halten Geschäftsleute möglicherweise davon ab, miteinander zu kommunizieren. Aus Angst, Mitarbeitenden oder Konkurrierenden in Leistung nachzustehen, eignen sich die beschriebenen ManagerInnen eine „24/7/365“ Erreichbarkeit an.[46]

> „In an electronically nomadicized world I have become a two legged terminal, an ambulatory IP address, maybe even a wireless router in an ad-hoc mobile network. I am inscribed not within a single Vitruvian circle, but within radiating electromagnetic wavefronts.“[47]

Neben Vorteilen wie verbessertem Zeitmanagement, da ManagerInnen beispielsweise viel Arbeit von unterwegs aus erledigen können und mehr Zeit für Kommunikation im Allgemeinen, gibt es aber auch eine Kehrseite, welche die Umstellung mit sich

---

43 Rämö, Hans/Mats Edenius, „Time Constraints in New Mobile Communication: Practices among Senior Managers“, *KronoScope* 8/2, 2008, S. 147-157.

44 Ebd., S. 155.

45 Der Artikel erschien im Jahr 2008, als sich die allgemeine Nutzung und Verbreitung von Smartphones noch in der Entwicklung befand. Daher handelt es sich bei den Smartphones, von denen im Folgenden die Rede ist, weitgehend um Smartphones der ersten und zweiten Generation des Herstellers *Blackberry*. *Blackberry* brachte 2006 die ersten Smartphones auf den Markt, Konkurrent *Apple* starte den Verkauf des ersten *IPhone* 2007.

46 Vgl. Rämö/Edenius, „Time Constraints in New Mobile Communication“, S. 148f.

47 Mitchell, William J., *Me++: The Cyborg Self and the Networked City*, Cambridge: MIT Press 2003, S. 57.

bringt.[48] Ein großer Nachteil ist beispielsweise ein vermeintlicher Vorteil: Wo zu Beginn die aufgehobenen, räumlichen Grenzen des Büros und die Abschaffung der festgelegten Anfangs- und Feierabendzeiten eine schier nicht enden wollende Freiheit darstellen, ergeben sich bald eine Büroatmosphäre und Arbeitszeiten, die sich auf das komplette Leben ausweiten. Die Möglichkeit der ständigen Erreichbarkeit und auch der Zwang, diese Verfügbarkeit nicht einstellen zu dürfen, lösen in den Nutzenden ein Gefühl der Überwachung aus. Das Smartphone wird in diesem Zusammenhang zum bereits erwähnten mobilen Panoptikum, mit dem die ManagerInnen sich selbst, die Community in der sie sich befinden und beispielsweise ihre Nachbarn, überwachen.
Auch wenn in der Theorie durch das mobile Panoptikum von Rämö und Edenius keine offensichtliche Dauerüberwachung stattfindet, so ist die Art der Kontrolle durchaus mit der des Panoptikums von Jeremy Bentham zu vergleichen. Besitzende eines Smartphones können sich durch die dauerhafte Erreichbarkeit nie in Sicherheit der Ruhe und der Singularität wägen. Wie den Insassen des architektonischen Panoptikums, ist auch den Gefangenen der mobilen Version niemals klar, wann der tatsächliche Akt der Kontrolle stattfindet.[49]
In diesem Zusammenhang ist es außerdem wichtig, nicht ausschließlich die technischen Gegebenheiten der nahen Vergangenheit zu betrachten, sondern auch aktuelle Geschehnisse und Entwicklungen zu analysieren. Während in der Abhandlung von Rämö und Edenius nur ManagerInnen und wichtige Geschäftsleute Smartphones in Gebrauch hatten, so besitzen heute – beinahe zehn Jahre später – über 60 Prozent der Bewohnenden im deutschsprachigen Raum ein Smartphone.[50] Somit wurde in den vergangenen Jahren auch die Zahl der »Insassen« des mobilen Panoptikums auf fast zwei Drittel der Bevölkerung erhöht. Durch die allgegenwärtige Erreichbarkeit überwachen wir sowohl uns selbst, als auch andere.

---

48 Vgl. Gant, Diana/Kiesler Sara, „Blurring the boundaries: cell phones, mobility and the line between work and personal life.“, in: *Wireless world: social and interactional aspects of the mobile age*, London: Springer-Verlag 2001, S. 121.

49 Vgl. Rämö/Edenius, „Time Constraints in New Mobile Communication“, S. 154f.

50 Laut *statista.com* besitzen im Jahr 2016, 49 Millionen Menschen ein Smartphone (Vgl. *statista.com*, „Anzahl der Smartphone-Nutzer in Deutschland in den Jahren 2009 bis 2016 (in Millionen)“, http://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/, Zugriff: 03.09.2016), in Österreich 61% (Vgl. *statista.com*, „Anteil der Smartphone-Besitzer sowie Nutzung von Mobile Commerce in Österreich von 2013 bis 2016“, http://de.statista.com/statistik/daten/studie/568185/umfrage/smartphone-besitz-und-smartphone-nutzung-in-oesterreich/, Zugriff: 03.09.2016) und in der Schweiz 78% der Bevölkerung (Vgl. *statista.com*, „Anteil der Smartphone- und Tablet-Besitzer in der Schweiz in den Jahren 2012 bis 2016“, http://de.statista.com/statistik/daten/studie/297293/umfrage/smartphone-und-tablet-besitzer-in-der-schweiz/, Zugriff: 03.09.2016).

2.2.2 Contra Panoptikum

„[…] it still seems that writing and talking about going beyond the Panopticon – rather than actually doing it – is the case […]“[51]. Der dänische Kommunikationswissenschaftler Anders Albrechtslund beschreibt mit dieser Aussage einen aktuellen Trend im Bereich der Surveillance Studies. Das Grundprinzip von Jeremy Benthams elektronischem Panoptikum wird schon seit einiger Zeit von beinahe allen Forschenden im Bereich der Überwachungsstudien nicht mehr als aktuell angesehen. In einigen Theorien wird es stattdessen seit mehreren Jahren zwar als überholt, veraltet und nicht mehr zeitgemäß bewertet, aber dennoch immer wieder für Vergleiche herangezogen. Im Folgenden werden vier unterschiedliche Überwachungsansätze des späten 20. und frühen 21. Jahrhunderts erläutert, die sich von der Idee des architektonischen Panoptikums weitgehend distanzieren und sie dennoch, oder möglicherweise auch gerade deswegen, immer wieder reflektieren und für Analogien heranziehen.

2.2.2.1 David Lyon - *Postpanoptisches Zeitalter* (2006/2013)

Der amerikanische Forscher und Soziologe David Lyon beschäftigt sich in seinen Abhandlungen neben Themen wie Globalisierung und Säkularisierung größtenteils mit Überwachung in den Bereichen Postmoderne, Informationstechnologie und Konsum. Lyon ist Direktor des *Surveillance Study Centre*[52] in Kingston und Mitherausgeber der in dieser Arbeit viel zitierten Zeitschrift *Surveillance & Society*[53].
Lyon distanziert sich in vielen seiner Schriften ganz offen von der Aktualität des Panoptikums nach Bentham und Foucault.[54] Dennoch bildet das kritisierte Dispositiv der Überwachung einen wichtigen Bestandteil seiner Studien, da auch Lyon immer wieder Vergleiche herstellt und Parallelen mit neueren Formen der Überwachung zieht oder wiederlegt – „[…] the panopticon refuses to go away“[55] – so erklärt Lyon dieses Phänomen in der Einleitung seines Sammelbandes *Theorizing surveillance: The panopti-*

---

51 Albrechtslund, Anders, „Online social networking as participatory surveillance“, *first monday – pre-reviewed journal on the internet* 13, 03.03.2008, http://firstmonday.org/ojs/index.php/fm/article/view/2142/1949, Zugriff: 28.09.2016.
52 O.N., „Surveillance Study Center“, http://www.sscqueens.org/about, Zugriff: 07.09.2016.
53 O.N., „Surveillance & Society“, http://surveillance-and-society.org/, Zugriff: 07.09.2016.
54 Vgl. Bauman, Zygmunt/David Lyon, *Daten, Drohnen, Disziplin: Ein Gespräch über flüchtige Überwachung*, Berlin: Suhrkamp 2013, S. 79; (Orig. *Liquid Surveillance. A Conversation*, Cambridge: Polity Press 2013).
55 Lyon, David, *Theorizing surveillance. The panopticon and beyond*, Portland: Willan Publishing 2006, S. 4.

con and beyond. Die Erwähnung von Jeremy Bentham und Michel Foucault in Überwachungsdiskursen beschreibt Lyon als beinahe routinemäßig notwendig und auch in seinen eigenen Theorien kommt er nicht umhin, dem Panoptikum Beachtung zu schenken. Während er sich im Jahr 1991 noch mit der Aktualität der Idee des Hochsicherheitsgefängnissees als Metapher für unsere Gesellschaft identifizieren konnte, so ist dieser Vergleich heute, nach der flächendeckende Verbreitung von elektronischer Kontrolle, nicht mehr ebenso leicht zu ziehen.

> „Today, the influential idea of Panopticon lives on, but in a new context. Electronic technologies monitor our everyday lives so intimately, it is said, that society itself is like a panoptic prison. A disturbing thought, indeed. But is it true?“[56]

Bereits 1991 hinterfragte Lyon in dieser Aussage, ob die damalige Gesellschaft selbst als panoptisches Gefängnis angesehen werden kann. Schon zu diesem Zeitpunkt ist ihm klar, dass das panoptische Prinzip nicht mehr in die allgemeine Beschreibung der westlichen Gesellschaft passt. „If pain was once the instrument for achieving social order, which Bentham and his cadre replaced with (panoptic) discipline, then today the key principle is pleasure.“[57] Lyon beschreibt hier, wie sich im Laufe der Jahrzehnte und Jahrhunderte die gesellschaftlichen Konventionen verändert haben. Während Bentham Ende des 18. Jahrhunderts mit seiner Idee der Aufhebung der körperlichen Bestrafung für Aufsehen sorgte, geht die heutige Gesellschaft noch einen entscheidenden Schritt weiter. Kontrolle und Überwachung sollen nicht nur keinen physischen Schmerz für das Objekt der Überwachung bedeuten, sondern viel mehr noch, sie sollen Vergnügen bereiten. Dem Menschen, welcher in der westlichen Konsumgesellschaft des 21. Jahrhunderts lebt, wird Freude in Form von elektronischen Hilfsmitteln und Spielereien geboten. Im Gegenzug dazu setzen sich die Menschen dann der Kontrolle durch übergeordnete Instanzen aus. Das Modell eines gesellschaftlichen Panoptikums bezeichnet David Lyon in diesem Zusammenhang bereits 1991 als Hirngespinst.[58]
An dieser Aussage hält Lyon auch noch mehr als 20 Jahre später fest. Hierbei stützt er sich auf Aussagen des polnischen Soziologen Zygmunt Bauman und kooperiert mit ihm. Im Jahr 2013 veröffentlichten die beiden Soziologen *Daten, Drohnen, Disziplin*,

---

56 Lyon, David, „Bentham's Panopticon: From Moral Architexture to Electronic Surveillance“, in: *Surveillance, Crime & Social Control*, Hg. Clive Norris, Dean Wilson, Aldershot: Ashgate 2006, S. 13; (Orig. *Queen's Quarterly* 98, 3, 1991, S. 596–617).
57 Ebd., S. 29.
58 Vgl. Ebd., S. 31.

ein Gespräch über flüchtige Überwachung[59], in dem sie sich (erneut) gemeinsam gegen die Aktualität des panoptischen Prinzips nach Bentham in der gesellschaftlichen Überwachung aussprechen. Vielmehr betitelt Bauman die westliche Gesellschaft und die in ihr stattfindende Entwicklung von Überwachung als „post-panoptisch“[60]. In ihr kann sich die Instanz der Überwachung ihrer Verantwortung entziehen. Sie muss nicht mehr an ein und demselben Ort verharren, da es in unserer heutigen Gesellschaft keine wechselseitigen Verpflichtungen zwischen Instanz und Objekt der Überwachung mehr gibt.[61] Das beinhaltet Freiheit für beide Parteien, denn im Panoptikum sind nicht nur die Gefangenen an eine feste Zelle gebunden, sondern auch der Wärter an den Turm, den er nicht verlassen darf. Im post-panoptischen 21. Jahrhundert verschiebt sich dieses Machtverhältnis, wie bereits erwähnt. Es „[…] können die, die unter den heutigen Verhältnissen an den Hebeln der Macht sitzen, sich jederzeit »in die absolute Unzulänglichkeit zurückziehen«“[62].

David Lyon verweist weiter in seinen Abhandlungen auf Gilles Delleuze und die Rhizomartigkeit[63] der post-panoptischen Überwachung, sowie auf die „Adiaphorisierung“[64], die im Zuge der Überwachungsprinzipien mehr und mehr vonstattengeht. Auf diese Haltung, den Menschen als simple Ansammlung von Daten zu sehen, geht auch die folgende Theorie von Kevin D. Haggerty und Richard V. Ericson genauer ein.

2.2.2.2 Kevin D. Haggerty & Richard V. Ericson - *The Surveillant Assemblage* (2000/2007)

Kevin D. Haggerty und Richard V. Ericson beschreiben in ihrer Abhandlung *The Surveillant Assemblage*[65] ein neuartiges Überwachungsdispositiv, das zwar foucaultsche Ideen aufgreift und berücksichtigt, aber sich grundlegend neu verortet und von veralteten Prinzipien lossagt. Während Überwachung in der Vergangenheit weitgehend diskret ablief, beschreibt die Theorie von Haggerty und Ericson eine neue, radikalere, offensichtlichere Form, die sie *Surveillant Assemblage* nennen.

---

59 Bauman,/Lyon, *Daten, Drohnen, Disziplin*.
60 Bauman, Zygmunt, *Flüchtige Moderne*, Frankfurt am Main: Suhrkamp 2003, S. 18; (Orig. *Liquid Modernity*, Cambridge: Polity Press 2000).
61 Vgl. Bauman/Lyon, *Daten, Drohnen, Disziplin*, S. 15.
62 Ebd., S. 24.
63 Vgl. Ebd., S. 14.
64 Ebd., S. 18.
65 Haggerty, Kevin D./Richard V. Ericson, „The Surveillant Assemblage“, in: *Surveillance, Crime & Social Control*, Hg. Clive Norris, Dean Wilson, Aldershot: Ashgate 2006, S. 61-78; (Orig. *The British Journal of Sociology* 51, 4, S. 605-622).

> „This assemblage operates by abstracting human bodies from their territorial settings and separating them into a series of discrete flows. These flows are then reassembled into distinct ‘data doubles’ which can be scrutinized and targeted for intervention.“[66]

Diese Assemblage funktioniert also, indem sie den Gegenstand der Überwachung – im Fall dieser Arbeit den menschlichen Körper – von seinem bekannten territorialen Umfeld trennt und ihn anschließend in einer Folge aus eigenständigen, unabhängigen Überwachungsabläufen separiert. Die Informationen, die aus diesen Vorgängen gewonnen werden, speichert ein System anschließend als sogenannte *data doubles* ab. Bei eventuellen Ermittlungen können diese Datenpakete dann anvisiert und verwertet werden.

Was sind nun aber die Eigenschaften, die diese beschriebene Art der Überwachung neu und einzigartig machen und sie vom bisher Dagewesenen unterscheiden? Besonders wichtig ist der Aspekt, dass nicht nur einzelne, bereits auffällig gewordene Individuen der Überwachung unterzogen werden. Jeder wird zum Überwachungsziel dieses Systems. Gesellschaftsgruppen die vormals ausgenommen waren, stehen jetzt ebenso im Fokus der Aufmerksamkeit, wie Menschen, die bereits straffällig geworden sind.[67] Dies ist ebenfalls ein Unterschied zum Prinzip des Panoptikums. Auch hier wird nicht jedes Mitglied der Gesellschaft überwacht, sondern nur, wer sich bereits strafbar gemacht hat. Ein weiterer wichtiger Aspekt ist die beobachtende Instanz selbst, ihre Verortung im Dispositiv und die räumliche Begrenzung des Überwachungsraumes. In Benthams architektonischem Modell ist nur ein einzelner Wärter angedacht. Dieser überwacht den runden Raum von einem Turm in der Mitte, also von einem immer gleich bleibenden, fixen Punkt aus. Neben dem Überwachenden wird auch den Überwachten ein fester Platz zugewiesen. Jede/r Gefangene hat seine eigene, in sich abgeschlossene Zelle, in der die Überwachung stattfindet. Ein Ausbrechen aus diesem Überwachungsraum ist nicht vorgesehen.

Ganz anders verhält es sich nun bei der *Surveillant Assemblage*. In diesem rhizomartig angelegten Dispositiv gibt es weder eine gleichbleibende Personifikation, die beobachtet, noch einen fixierten Punkt, von dem aus beobachtet wird. Vielmehr handelt es sich um ein komplexes System, bestehend aus mehreren Personen, das ein Überwachungsprotokoll herstellt, welches dann bei Bedarf vom potentiellen Überwachenden eingesehen werden kann. Ebenso gibt es in der *Surveillant Assemblage* keine begrenzten

---

66 Ebd., S. 62.
67 Vgl. Ebd..

Räume. Indem der Gegenstand der Überwachung von seinem territorialen Umfeld getrennt betrachtet wird, werden jegliche räumliche Grenzen aufgehoben, die den Überwachungsraum einschränken könnten.

Als Exempel für die *Surveillant Assemblage* lässt sich beispielsweise das soziale Netzwerk *facebook*[68] anführen. Nutzen Handelnde die Plattform in der Form, in der sie konzipiert wurde, füllen sie also regelmäßig mit privaten Daten wie Fotos, Freunden, Standorten und dortige Aufenthaltszeiten, dann werden vom Netzwerk virtuelle Datendoubles der Benutzenden erstellt. Auf dieses Doubles können dann die Personen oder Firmen zugreifen, die das Soziale Netzwerk für diesen Service bezahlen. Dieses System funktioniert, obwohl, oder gerade weil, weder der Gegenstand der Überwachung, noch die überwachende Instanz, sich in einem physischen Überwachungsraum aufhalten. Der Raum ist nur virtuell vorhanden. Diese scheinbare Abwesenheit des greifbaren Raumes trügt allerdings. Vielmehr wird jeder physische Raum zum potentiellen Überwachungsraum.

2.2.2.3 William Bogard - *Deterritorialized System of Control* (2006)

Der amerikanische Soziologieprofessor William Bogard beschreibt in seiner Abhandlung *Surveillance assemblages and lines of flight*[69] wie das System der Kontrolle mehr und mehr „deterritorialized“[70] wird. Wie Haggerty und Ericson betitelt auch Bogard die von ihm beschriebene enträumlichte Überwachung als eine Überwachungs-Assemblage[71]. Diese Enträumlichung[72] ist für Bogard der Grundstein der post-panoptischen Überwachung und liegt vor allem in der Rhizomartigkeit der Informationsnetzwerke begründet, die gleichzeitig zu Netzwerken der Überwachung werden. Hierbei ist der ungewöhnliche räumliche Aufbau des Netzwerkes von besonderem Interesse. Dieses Netzwerk kennt keinen nachvollziehbaren Ursprung, sondern setzt sich aus einzelnen Knotenpunkten zusammen, die jeweils miteinander verbunden sind. Jeder Knoten muss mit den anderen Knoten in einer offen gehaltenen Struktur verbunden sein,

---

68 O.N., „facebook“, https://www.facebook.com/, Zugriff: 07.09.2016.

69 Bogard, William, „Surveillance assemblage and lines of flight“, in: *Theorizing surveillance. The panopticon and beyond*, Hg. David Lyon, Portland: Willan Publishing 2006, S. 97–122.

70 Ebd., S. 97.

71 Die freie deutsche Übersetzung „Überwachungs-Assemblage“ wird im Folgenden als Synonym für den originalen, englischen Begriff „Surveillant Assemblage“ verwendet.

72 Der englische Begriff „deterritorialization“ wird im Folgenden mit dem deutschen „Enträumlichung“ übersetzt.

damit eine geöffnete Netzwerkstruktur entstehen kann.[73] Genau in dieser Struktur liegen sowohl die Stärken, als auch die Schwächen dieses Netzwerks verankert.

> „Deterritorialized controls are far from perfect, however; they produce deterritorialized forms of resistance as a function of their own organization. Networked information is hard to secure and easy to reproduce. This fact of the digital age explains both the power of surveillance assemblages today (the ease with which they gather and share information on us) and their potential weakness or vulnerability.“[74]

Anders als beispielsweise ein baumartig aufgebautes Netzwerk, also eines, das einem Grundstamm entspringt, aus dem die einzelnen (Informations-)Verästelungen entstehen, kann das rhizomartige Netzwerk nicht einfach zerstört oder durchbrochen werden. Während der Baum durch das Vernichten des ursprünglichen Anfangs, des Stammes, zerstört werden kann, so ist dies beim Rhizom nicht möglich. Auch wenn hier der erste Knoten, in dem das Netzwerk seinen Grundstein findet, gelöscht wird, so bleibt das Netz als Ganzes dennoch bestehen. Grund dafür ist, dass nicht alle Verbindungen nur an einem Punkt, wie vergleichsweise einem Stamm, zusammenlaufen, sondern sich in einer offenen Struktur befinden.[75] Daher ist es beinahe unmöglich, eine Information, die einmal in das Netzwerk eingespeist wurde, nachzuverfolgen, zu kontrollieren oder wieder vollständig zu entfernen.

> „Ultimately no police power is capable of controlling the deterritorialization of surveillance, because the number of virtual connections in a rhizomatic network always exceeds the number that can acutually be monitored (if one path is blocked, another can be found).“[76]

Übergeordnete Instanzen der Überwachung oder Kontrolle sind in diesen Fällen weitestgehend machtlos, da es nicht eine einzige zuständige Behörde gibt, die im System Verantwortung trägt. Auch die Polizei ist nach Aussage von Bogard hilflos, da die Kraft der Enträumlichung unkontrollierbar ist. An dieser Stelle zeichnet sich ein deutlicher Unterschied zwischen der Funktionsweise der Überwachungs-Assemblage hin zum Prinzip des Panoptikums ab. Jede Person mit Zugriff zur Assemblage wird zum potentiellen Objekt, aber auch gleichzeitig zum potentiellen Subjekt der Überwachung. Im panoptischen Prinzip ist es hingegen nicht möglich, beide Rollen inne zu

---

73 Vgl. Bogard, „Surveillance assemblage and lines of flight“, S. 97.
74 Ebd., S. 97.
75 Vgl. Ebd., S. 103.
76 Ebd., S. 101.

haben. Teilnehmende des Dispositivs sind in diesem Zusammenhang entweder Überwachende oder werden selbst überwacht.
Darüber hinaus verweist Bogard im Hinblick auf die Informationalisierung der Überwachung in der Postmoderne auf Deleuze. Statt einer hierarchischen Ordnung im Dispositiv der Überwachung besteht das System in der Postmoderne größtenteils nur aus Daten, die entschlüsselt, verschlüsselt und aufgenommen werden.[77] Deleuze beschreibt diese Veränderung mit der Entstehung von *dividuals* anstatt der Aufrechterhaltung von *individuals.*[78] Die Individualität geht verloren. Dieses Phänomen beschreiben bereits Haggerty und Ericson in Form der sogenannten *data doubles.* Als Teil des Netzwerks sind Nutzende nur noch eine kleine oder große Ansammlungen von Daten, die sich in der postpanoptischen, postmodernen *Surveillance Assemblage* uneingeschränkt bewegen.

2.2.2.4 Anders Albrechtslund - *Participatory Surveillance* (2008)

Der dänische Kommunikations- und Informationswissenschaftler Anders Albrechtslund fokussiert sich in seinen Studien und Abhandlungen auf das Thema der Überwachung, die online in sozialen Netzwerken stattfindet. In seinem Aufsatz *Online social networking as participatory surveillance*[79] erklärt Albrechtslund die sozialen Netzwerke als Praxis und Schauplatz für eine partizipatorische Art der Überwachung, die größtenteils durch die User selbst initiiert wird.[80] Das soziale Netzwerk gilt als Inbegriff des Web 2.0. Es zieht seine Daseinsberechtigung aus dem Drang des Nutzers, ein Teil des Netzwerks zu sein. Nach persönlichen Interessen, Gedanken und Vorlieben, sind geografische Informationen wie beispielsweise Wohn-, Geburts- oder aktueller Standort nur eine weitere private Angelegenheit, die von Nutzenden freiwillig, ja meist sogar gerne, preisgegeben wird.

> „Whereas cyberspace is an abstract, virtual space, the geographical places are not. Even though the relations and practices are similar, geo-based social networking changes the rules for shared personal information.“[81]

Statt konstruierter Realität, die sonst so oft in der Onlinewelt zu finden ist, stellt Geotagging wieder einen Bezug zur realen Welt her. Jedes Profil, das in einem sozialen

---

77 Vgl. Ebd., S. 106.
78 Delleuze, Gilles, „Postscript on the Societies of Control“, *October* 59, Winter, 1992, S. 4.
79 Albrechtslund, „Online social networking as participatory surveillance“.
80 Vgl. Ebd..
81 Ebd..

Netzwerk angelegt ist, ist an eine physische, real existierende Person gekoppelt. Diese Person möchte, dass alle ihre Daten online zu finden sind.[82] Vor allem deshalb stellt diese Art der Onlineüberwachung einen Unterschied zur regulären offline-Form dar. Dennoch folgt sie den vier Eigenschaften des sozialen Onlinenetzwerks, die Albrechtslund nach Danah Boyd definiert: „persistency, searchability, replicability and invisible audiences“[83]. Anhand dieser Charakterisierung kann nur eine kleine Parallele zur Überwachung durch das Panoptikum hergestellt werden. Sowohl Ausdauer, Beharrlichkeit, Wiederauffindbarkeit als auch die Nachvollziehbarkeit und die Möglichkeit des Wiederherstellens sind Eigenschaften, die sich nicht in Benthams Idee wiederfinden lassen. Einzig das unsichtbare Publikum, vor dem sich die Szenerie abspielt, stellt hier eine Parallele dar. Allerdings weist auch dieser Vergleich Lücken auf. Dort wo das Objekt der Beobachtung im Panoptikum gezwungen wird, sich dem unsichtbaren Publikum zu stellen, gibt es diesen Zwang beim Onlinenetzwerk nicht.

Abgesehen von diesen vier Eigenschaften ist der Überwachung in sozialen Netzwerken im Cyberspace noch eine weitere Parallele zum Panoptikum eingeschrieben. In beiden Vorstellungen ist das Dispositiv der Überwachung negativ konnotiert. Diesen Vergleich sieht Albrechtslund allerdings als falsch an, da die Überwachung im sozialen Netzwerk für ihn nicht nur negative Seiten hat. Vielmehr stellt er heraus, dass die Nutzenden sich im Vorfeld zu wenig über die Hierarchien der Überwachung im Netzwerk informieren und daher nicht ahnen können, welche möglichen Gefahren durch Überwachung online auf sie warten könnten.[84] Er führt deshalb den Begriff der partizipatorischen Überwachung an, an der die Nutzenden offensichtlich selbst Teil haben. Diese Begrifflichkeit setzt sich für Albrechtslund aus zwei spezifischen Eigenschaften zusammen. Zum einen sollen die Bevollmächtigung der Handelnden und der Aufbau von Subjektivität im Vordergrund stehen. Zum anderen ist es von Nöten, die Nutzung von sozialen Onlinenetzwerken als eine Möglichkeit zu sehen, um sich anderen mitzuteilen, anstatt Handel mit persönlichen Informationen zu betreiben. Grundsätzlich ruft Albrechtslund mit seinem Ideen zu bewussterem Handeln auf und dazu, nicht überall nur Ängste und Gefahren wahrzunehmen. Er ist vielmehr der Meinung, dass in

---

82 Vgl. Ebd..

83 Boyd, Danah, „We googled you: Should Fred hire Mimi despite her online history? “, *Harvard Business Review*, Juni 2007, http://www.danah.org/papers/HBRJune2007.html, Zugriff: 29.09.2016.

84 Vgl. Albrechtslund, Anders, „Online social networking as participatory surveillance“.

technischen Nova, wie beispielsweise dem sozialen Onlinenetzwerk, eine Chance gesehen werden sollte, das grundlegende Konzept der Überwachung nochmals zu überdenken.[85]

2.3 Forschungsmethode

Nach diesem Überblick über den aktuellen Forschungsstand im Bereich Überwachung und Surveillance Studies ist es notwendig, eine oder gegebenenfalls mehrere Forschungsmethoden zur später folgenden Analyse hervorzuheben. Die bisher erläuterten Theorien stammen aus unterschiedlichen wissenschaftlichen Bereichen, weshalb sich auch kein einheitlicher Schwerpunkt für die Analyse festlegen lässt. Stattdessen kristallisieren sich aber drei Ansätze heraus, auf die im Folgenden anhand einer transdisziplinären Analyse näher eingegangen wird. Den Anfang gestaltet die soziologische Perspektive, die sich im bisher Erörterten bereits bei dem Panoptikum-Gegner David Lyon wiederfinden lässt. Des Weiteren darf jene medientechnische Sicht nicht außer Acht gelassen werden, die vor allem in den technisch orientierten Theorien verortet werden kann. Den Abschluss bildet das große biopolitische Feld der Post-Privacy Debatte.

2.3.1 Soziologischer Ansatz

Die soziologische Perspektive, auf der die folgende Analyse fußt, basiert größtenteils auf den Aussagen, Theorien und Überlegungen des polnischen Soziologen Zygmunt Bauman und seines amerikanischen Kollegen David Lyon zur post-panoptischen Überwachung. Miteinbezogen wird im Zuge dessen außerdem Marc Andrejevics Begriff der lateralen Überwachung.

In seinem zur Jahrtausendwende erschienenen Werk *Flüchtige Moderne*, betitelt Zygmunt Bauman das anbrechende 21. Jahrhundert als gleichnamige Epoche, in der wir uns seiner Aussage nach auch heute, im Jahr 2017, noch befinden. Sie folgt laut Bauman auf das vorangegangene Zeitalter des späten 20. Jahrhunderts, das von ihm selbst als „solide Moderne“[86] bezeichnet wird. Bauman sieht die westliche Gesellschaft des 21. Jahrhunderts als, wie der Name schon sagt, flüchtig an. Die Menschen verhalten sich radikal und schnell. Soziale Beziehungen verflüchtigen sich. Die Beständigkeit, welche in der Vergangenheit bekannt war, wurde gegen eine fragile

---

85 Vgl. Ebd..

86 Bauman/Lyon, *Daten, Drohnen, Disziplin*, S. 21.

Schnelllebigkeit getauscht. In dieses Konzept einer alltäglichen Gesellschaft fügt sich die Vorstellung eines panoptischen Überwachungsapparates nach Benthams Modell nicht problemlos ein. Allein in eingeschränkten Bereichen der Gesellschaft lässt sich das Modell der panoptischen Kontrolle für ihn wiederfinden:

> „So wie ich es sehe, erfreut sich das Panoptikum bester Gesundheit, es bedient sich elektronisch optimierter, »cyborgisierter« Muskeln, die ihm mehr Macht verleihen, als es sich Foucault oder gar Bentham je hätten vorstellen können oder wollen – aber es ist jetzt nicht mehr das universelle Muster beziehungsweise die universelle Strategie der Herrschaft, wie zur jeweiligen Zeit dieser beiden Autoren, und nicht einmal mehr ihr vornehmstes oder am häufigsten praktiziertes Mittel. Man hat das Panoptikum verlagert und seine Verwendung auf die »unbeherrschbaren« Teile der Gesellschaft beschränkt, die sich in Gefängnissen, Lagern, psychoiatrischen Kliniken und andren »totalen Institutionen« im Sinne Erving Goffmans wiederfinden.“[87]

Im alltäglichen Leben sieht diese Art der Überwachung für Bauman allerdings anders aus. Ein gleichbleibender Punkt von dem aus überwacht wird, ist im fließenden, flüchtigen Modell der Überwachung unvorstellbar. Vielmehr setzt Baumans Idee, für den Großteil der westlichen Welt an einem Überwachungsmodell an, das ebenfalls fließend ist und ohne verorteten Fixpunkt überwacht.[88] Mit kleineren Adaptionen technischer Neuerungen, wie beispielsweise der alltäglichen Nutzung von Smartphones und Tablet-PCs außerhalb der häuslichen Umgebung oder des Arbeitsplatzes, lässt sich für Bauman Aktualität in das panoptische Prinzip bringen:

> „Wie die Schnecke, die ihr Haus immerzu bei sich trägt, so müssen die Beschäftigten in der schönen neuen flüchtig-modernen Welt ihr jeweils persönliches Panoptikum selbst hervorbringen und auf dem eigenen Buckel mitschleppen. Sie sind uneingeschränkt verantwortlich dafür, sich selbst in gebrauchsfähigem Zustand zu erhalten und ihren störungsfreien Betrieb zu gewährleisten.“[89]

Bauman macht hier deutlich, dass das Prinzip der lückenlosen Dauerüberwachung durchaus Aktualität besitzt, auch wenn dazu buchstäblich einige grundlegende Mauern eingerissen werden müssen.

Einen weiteren wichtigen Punkt machen Lyon und Bauman in der Freiwilligkeit der Überwachung fest. Diesbezüglich ist es wichtig, festzustellen, dass der Mensch von

---

87 Ebd., S. 74.
88 Vgl. Ebd., S. 22ff.
89 Ebd., S. 78.

der Privatwirtschaft bereits seit Langem weniger als fühlende Person und mehr als Ansammlung von Daten angesehen wird, die dann als Ware weiter verwertet werden kann.[90] Diese Daten, von denen Lyon spricht, sind dem Menschen eingeschrieben und können durch Überwachungsmethoden von höheren Instanzen gesammelt werden. »Können« deshalb, weil dies nicht unbedingt die Art und Weise sein muss, wie Daten in den Umlauf geraten. Oft gibt der Mensch seine persönlichen Daten „routinemäßig, achtlos und freiwillig“[91], sogar gerne, an fremde Dritte weiter, die zum großen Teil Profit daraus schlagen. Dies ist allerdings kein Novum seit der Einführung des Internets. Beispielhaft sind an dieser Stelle analoge Gewinnspielkarten anzuführen. Verlosende verfolgen dabei meist nicht nur das Ziel, Gewinne zu verteilen, sondern vor allem Kontaktdaten zu sammeln und diese dann später gewinnbringend weiter zu verwerten bzw. verkaufen. In diesem Zusammenhang sind zudem beispielsweise Kundenkarten zu erwähnen. Auch hier steht es für das Gewerbe ebenfalls nicht im Vordergrund, potentielle Rabatte an Kunden zu verteilen, sondern das Einkaufsverhalten und die Kundendaten zu sammeln und zu speichern. Dieser Punkt der Freiwilligkeit muss auch in der folgenden Analyse, im Bezug auf das Smart Home hinterfragt werden.
Eine weitere wichtige Rolle im soziologischen Teil der Analyse spielt die Gefühlswelt der Bewohnenden des Smart Home. Sie befinden sich 24 Stunden am Tag, sieben Tage die Woche unter der Beobachtung des Hauses. Die Frage, welche sich in diesem Zusammenhang stellt, ist, ob bei den Nutzenden durch diese kontinuierlich anhaltende Überwachung ein Gefühl von Geborgenheit und Sicherheit oder eher eines von Angst und Verfolgung ausgelöst wird.[92] Im Zusammenhang mit der Gefühlswelt spielt auch die Frage nach der inneren Sicherheit der Bewohnenden eine ausschlaggebende Rolle in der Analyse. Lyon beschreibt, dass seit frühesten Erzählungen Wachen beinahe immer mit einer Art des Schutzes konnotiert werden und daher „Überwachen als Fürsorge“[93] ein weitverbreiteter Grundsatz war.

> „Verhalf einem einst das Wissen um die Nachtwache am Stadttor zu einem ruhigen Schlaf, so leisten heutige »Sicherheitsmaßnahmen« nicht mehr dasselbe. Vielmehr gehen sie ironischerweise mit Formen von Unsicherheit einher – oder führen diese in manchen Fällen gar absichtlich herbei?; eine Unsicherheit, die gerade jene Menschen

90 Vgl. Ebd., S. 48.
91 Ebd., S. 25.
92 Vgl. Ebd., S. 37.
93 Ebd., S. 126.

> zu spüren bekommen, die die Sicherheitseinrichtungen angeblich beschützen sollen."[94]

Lyon stellt hier den Aspekt der Überwachung als Fürsorge aus heutiger Sicht in Frage. Auch dieser Vermutung, dass Unsicherheit in der Gefühlswelt der Überwachten absichtlich herbeigeführt wird, muss in der folgenden Analyse nachgegangen werden. Passend zur Frage, welche Intentionen Überwachung eigentlich verfolgt, ist es hilfreich, den von Marc Andrejevic verwendeten Begriff der lateralen Überwachung anzuführen, denn auch in diesem Zusammenhang ist es möglich, Überwachung als Fürsorge, vor allem innerhalb einer Gruppe, zu deuten.

> „Lateral surveillance, or peer–to–peer monitoring, understood as the use of surveillance tools by individuals, rather than by agents of institutions public or private, to keep track of one another, covers (but is not limited to) three main categories: romantic interests, family, and friends or acquaintances."[95]

Mark Andrejevic beschreibt mit dem Begriff der lateralen Überwachung das Phänomen der Überwachung unter mehreren Personen oder innerhalb einer Gruppe, beispielsweise innerhalb eines sozialen Onlinenetzwerkes oder auch simpel in einer offline Gruppenkonstellation. Wichtig ist dabei vor allem, dass ausführende Instanz und Objekt der Überwachung gleichgestellt sind und ebenbürtig agieren können. In der folgenden Analyse wird versucht, herauszustellen, ob und wenn ja wie, diese Art der lateralen Überwachung im Smart Home durch dessen Bewohnende stattfinden kann.
Den abschließenden Punkt des soziologischen Theorieteils bildet Didier Bigo mit seinem Begriff des „Ban-opticon"[96]. Auch er stellt klar, dass es in unserer heutigen Gesellschaft kein Panoptikum mehr gibt, sondern „nur mehr jenes fragmentarische und heterogene Dispositiv"[97]. Durch diese Art der Überwachung von staatlicher und privatwirtschaftlicher Seite entsteht, so Bigo, ein Raum transnationaler Unsicherheit[98],

---

94 Ebd., S. 126f.

95 Andrejevic, Mark, „The work of watching one another: Lateral surveillance, risk, and governace.", *Surveillance & Society* 2/4, 2005, S. 479-497; http://www.surveillance-and-society.org/articles2(4)/lateral.pdf, Zugriff: 30.09.2016, S. 488.

96 Bigo, Didier, „Globalized (in)Security: the Field and the Ban-opticon", in: *traces 4. Translation, Biopolitics, Colonial Difference*, Hg. Naoki Sakai, Jon Solomon, Hong Kong: Hong Kong University Press 2006, S. 109-156.

97 Bauman/Lyon, *Daten, Drohnen, Disziplin*, S. 81.

98 Vgl. Bigo, „Globalized (in)Security: the Field and the Ban-opticon", S. 144f.

der keineswegs der Idee eines Panoptikums entspricht. Verallgemeinert lässt sich diesbezüglich feststellen, dass das Ziel des Bannoptikum[99] darin besteht, „bestimmte Minderheiten als »unerwünscht« zu identifizieren“[100] und sie dadurch aus einem räumlich abgegrenzten Bereich fernzuhalten. Auch wenn sich Bigo in seiner Abhandlung auf eine transnationale Ebene bezieht, lässt sich seine Idee des Fernhaltens von Externen, statt nur des Einsperrens von Insassen, auf interessante Weise auf das Modell des Smart Home übertragen. Aus diesem Grund wird auch dieser Aspekt in die folgende Analyse mit einbezogen.

2.3.2 Medialer Ansatz

Da die Forschungsmethode der folgenden Analyse auf drei unterschiedlichen Ansätzen basiert, folgt nun auf die soziologische Perspektive die Heranführung an den medialen Ansatz.

Spätestens seit den Enthüllungen von Edward Snowden sollte dem Großteil der Weltbevölkerung bewusst sein, dass staatliche Instanzen Individuen überwachen, daraus generierte Daten sammeln, speichern und aus ihnen nutzbares Wissen ziehen. Weniger bekannt ist hingegen, dass auch Mimen der privaten Wirtschaft sich ähnlicher Überwachungsmethoden bedienen, um an Daten von Handelnden zu gelangen. Auch wenn die Umsetzung sich in diesen beiden Punkten ähnelt, so sind die Beweggründe doch meist unterschiedlicher Natur. Vor allem soziale Onlinenetzwerke und mein späteres Analysebeispiel, das Internet der Dinge, sind nur zwei von unzähligen medialen Abläufen, in denen beinahe automatische Messungen von Daten der Nutzenden stattfinden.[101] In den genannten Beispielen werden „mediale Prozesse, Ereignisse und Kommunikationen automatisierten Vermessungen unterzogen, werden Daten zu Treib- und Rohstoff anonymer Entscheidungsprozesse, die Verfahren der Kontrolle etablieren“[102]. Die hier beschriebenen, gesammelten Daten, bilden allerdings nicht nur den Treibstoff für die Entscheidungsprozesse, von welchen Kammerer und Waitz sprechen, sondern sie lassen sich ebenso gut anderweitig einsetzen. Lyon stellt diesbezüglich hinsichtlich der bereits definierten flüchtigen Überwachung fest, dass diese sich

---

99 Im Folgenden wird Bigos englischer Begriff des *Ban-opticon* mit dem deutschen *Bannoptikum* übersetzt.

100 Bauman/Lyon, *Daten, Drohnen, Disziplin*, S. 81.

101 Vgl. Kammerer, Dietmar/Thomas Waitz, „Überwachung und Kontrolle. Einleitung in den Schwerpunkt“, *Zeitschrift Für Medienwissenschaft* 13, 2016, S. 11.

102 Ebd., S. 11.

„[…] löst aus ihren alten Verankerungen, da sich für einen bestimmten Zweck erhobene Daten immer leichter anderen Zwecken zuführen lassen“[103]. Auch die bereits angeführten *data doubles*, die von Haggerty und Ericson eingeführt wurden, lassen sich problemlos in diesem Zusammenhang sehen. Die Handelnden werden auf eine simple Ansammlung von Daten reduziert, die dann zu beliebigen Zwecken, beispielsweise der Privatwirtschaft, weitergenutzt werden können. Negativ gesehen, wird der Mensch in Form seiner Daten somit zur Ware.

Der Vorgang der sogenannten „Verdatung“[104] stellt in diesem Zusammenhang ein essentielles Schlagwort dar. Der österreichische Kultur- und Medienwissenschaftler Ramón Reichert definiert mit diesem Begriff „mediale Verfahren und Praktiken, die für die Speicherung und Verarbeitung personenbezogener Wissensbestände eingesetzt werden“[105]. In seiner Abhandlung zum Thema der digitalen Selbstvermessung stellt Reichert Fitness-Tracker als Schnittstelle zur medialen Verdatung des menschlichen Körpers heraus.[106] Genauer beschäftigt er sich mit unterschiedlichen „[…] Gadgets, die individuelle Körperpraktiken in ein dichtes Netzwerk quantifizierender Verdatung überführen“[107]. Dadurch soll aus dem ursprünglichen handelnden Menschen aus Fleisch und Blut ein individuelles Paket aus Daten entstehen, „that becomes a knowable, calculable and administrable object“[108].

Die Soziologin und Medienwissenschaftlerin Deborah Lupton stellt fest, dass Selbstvermessung kein neues Phänomen seit der digitalen Revolution darstellt. Vielmehr versucht der Mensch schon seit Langem, Überwachungsprotokolle über sich selbst anzulegen und diese anschließend zu reflektieren, damit eine Selbstoptimierung stattfinden kann. Dieser Vorgang funktioniert auch ohne digitale Gadgets, mit Stift und Papier – sei es nun in Form eines Diätplans oder eines Haushaltsbuches, in dem Ausgaben festgehalten werden.[109] Reichert bringt mit dem Schlagwort der „Gamifizierung“[110] einen weiteren wichtigen Punkt an die Tagesordnung. Auch wenn die Selbstkontrolle durch die meisten technischen Hilfsmitteln eine simple Ansammlung von personenbe-

---

103 Bauman/Lyon, *Daten, Drohnen, Disziplin*, S. 12f.

104 Reichert, Ramón, „Digitale Selbstvermessung. Verdatung und soziale Kontrolle“, *Zeitschrift Für Medienwissenschaft* 13, 2016, S. 66.

105 Ebd..

106 Vgl. Kammerer/Waitz, „Überwachung und Kontrolle“, S. 19.

107 Reichert, „Digitale Selbstvernetzung“, S. 66.

108 Shove, Elizabeth/Mike Pantzar/Matt Watson, *The Dynamics of Social Practice. Everydady Life and How it Changes*, London: SAGE Publications 2012, S. 17.

109 Lupton, Deborah, *Self-Tracking Modes: Reflexive Self-Monitoring and Data Practices*, 27.08.2014, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2483549, Zugriff: 15.10.2016.

110 Reichert, „Digitale Selbstvernetzung“, S. 68.

zogenen Daten bedeutet, so spielt sich deren anschließende Auswertung meist auf einer spielerisch anmutenden Benutzeroberfläche ab. In den von Reichert beschriebenen Fitness-Gadgets erhalten die Handelnden beispielsweise verschiedene Abzeichen oder es können neue Übungen eingesehen werden, sobald ein bestimmter Grad an Fitness erreicht wurde.[111] Diese Art des Belohnungssystems erinnert sehr stark an Spiele, in denen neue Level durch das Erreichen bestimmter Ziele freigeschalten werden können. In diesem Zusammenhang ist es außerdem interessant auf die fünf unterschiedlichen Arten der Selbstkontrolle einzugehen, die von Lupton vorgeschlagen werden. Lupton differenziert zwischen *private, pushed, communal, imposed* und *exploited* Self-Tracking. Bei der folgenden Erläuterung wird die von Lupton angeführte Reihenfolge jedoch außer Acht gelassen und stattdessen mit *private* und *communal* begonnen, da diese selbstterminiert sind und nicht durch ein fremdbestimmtes Machtgefüge produziert werden. *Private self-tracking* stellt dabei noch die wohl simpelste Form der Selbstkontrolle dar. Die Handelnden entscheiden sich in diesem Modus aus freien Stücken für die Kontrolle, führen diese allein mithilfe von technischen Hilfsmitteln durch und entscheiden anschließend auch frei darüber, was mit den ausgewerteten Daten geschehen soll - sei es eine simple Steigerung des Selbstbewusstseins, oder eine Veränderung der Lebensweise.[112] Lupton stellt des Weiteren fest, dass der Großteil der analysierten Daten sich mit gesundheitsbezogenen Themen befasst.[113] Das liegt vermutlich vor allem daran, dass die Überwachenden auf diese Faktoren des Lebens selbst am meisten Einfluss besitzen. Das *communale self-tracking* unterscheidet sich in der Art der Überwachung nicht grundlegend vom Modus des *private self-tracking*. Obwohl sich das *tracking* ausschließlich auf die eigene Person bezieht, stellt Lupton dennoch fest, dass sich einige Nutzende als Teil einer Gemeinschaft sehen.[114] Auf sozialen Onlineplattformen, die gemeinsam mit den technischen Gadgets entwickelt wurden, ist es für die Nutzenden möglich, ihre gesammelten Daten und Leistungen mit anderen zu teilen und sich auszutauschen.[115] Dies muss allerdings nicht immer nur in exklusiven Netzwerken stattfinden. Die Fitness-App *Runtastic*[116] lässt sich beispielsweise mit dem bereits bestehenden sozialen Netzwerk *facebook* verbinden, um den Sporttreibenden so

---

111 Vgl. Ebd., S. 67f.
112 Vgl. Lupton, *Self-Tracking Modes*, S. 5f.
113 Vgl. Ebd., S. 6.
114 Vgl. Lupton, Deborah, „Understanding the Human Machine“, IEEE Technology & Society Magazine, 32/4, Dezember 2013, S. 28f, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6679313, Zugriff: 16.10.2016.
115 Vgl. Lupton, *Self-Tracking Modes*, S. 8.
116 O.N., „runtastic“, https://www.runtastic.com/de/apps/runtastic, Zugriff: 18.01.2017.

die Möglichkeit zu geben, ihre Leistungen mit einer bereits bestehenden Community zu teilen und sich positives Feedback oder »Anfeuerungen« zu generieren.[117] Diese Form der Bestätigung erfolgt in beide Richtungen. Wer gerade noch selbst Feedback zu seiner Leistung bekommen hat, gibt möglicherweise einem anderen Mitglied der Community bald darauf Hilfestellung bezüglich einer potentiellen Laufstrecke. Mitglieder lassen sich also als sogenannte „prosumer“[118] bezeichnen. Sie sind demnach sowohl Konsumenten und gleichzeitig auch Produzenten von Information.

Die folgenden Modi des Self-Tracking unterscheiden sich von den ersten beiden in der Hinsicht, dass sie nicht selbst-, sondern fremdterminiert sind. Das *pushed self-tracking* ist bereits seit einiger Zeit beispielgebend in den „Anwendungsbereichen der Präventivmedizin und der Patientenüberwachung“[119] verankert. Der Mensch wird hierbei von Ärzten oder medizinischen Einrichtungen dazu aufgefordert sein körperliches Befinden zu Überwachen und dieses mit Ihnen zu teilen. Grundsätzlich unterscheidet sich diese Art des Self-Tracking in der Ausführung nicht von der *personal* Version. Die Intention, die hinter der Umsetzung steht, ist allerdings eine andere.[120] Bereits 2014 machte beispielsweise die italienische Versicherungsgruppe Generali bekannt, dass sie in Zukunft bei ihren Lebens- und Krankenversicherungen auf „die elektronische Kontrolle von Fitness, Ernährung und Lebensstil“[121] setzen. Mithilfe einer App sollen sportliche Aktivität und das Wahrnehmen von Vorsorgeterminen dokumentiert und an den Versicherungsagenten übertragen werden. Neben Anreizen wie Gutscheinen für Reisen oder Sportangebote wirbt Generali auch mit vergünstigten Versicherungsprämien.[122] Das bietet neben der finanziellen Seite auch noch andere Vorteile. So ist es beispielsweise Patienten, die an chronischen Krankheiten leiden, möglich, ihren Kontakt mit medizinischem Personal und den Krankenkassen auf ein Minimales zu reduzieren, da man durch die digitale Selbstkontrolle ohnehin unentwegt unter medizinischer Beobachtung steht. Lupton beschreibt diesen Status der Patienten als „digitally engaged“[123].

---

117 Vgl. O.N., „15 Runtastic-Features, die Du ausprobieren solltest“, https://www.runtastic.com/blog/de/technologie/runtastic-features-2015/, Zugriff: 16.10.2016.

118 Lupton, „Understanding the Human Machine“, 29.

119 Reichert, „Digitale Selbstvernetzung“, S. 75.

120 Vgl. Lupton, *Self-Tracking Modes*, S. 7.

121 Gröger, Anne-Christin, „Generali erfindet den elektronischen Patienten“, *sueddeutsche.de*, 21.11.2014, http://www.sueddeutsche.de/geld/neues-krankenversicherungsmodell-generali-erfindet-den-elektronischen-patienten-1.2229667, Zugriff: 16.10.2016.

122 Vgl. Ebd..

123 Lupton, Deborah, „The digitally engaged patient: Self-monitoring and self-care in the digital health era“, *Social Theory & Health* 11/3, 2013, S. 256-270, http://link.springer.com/article/10.1057/sth.2013.10, Zugriff: 15.10.2016.

Wo das *pushed self-tracking* noch weitgehend freiwillig terminiert ist, so dringt das *imposed self-tracking* noch weiter in die Privatsphäre der Nutzenden ein. In diesem Fall wird, wie bereits durch den Namen erkennbar, beispielsweise Mitarbeitern einer Firma die Selbstkontrolle von ihren Vorgesetzten aufgezwungen.

> „One example is the productivity self-tracking devices that are becoming a feature of many workplaces as employers seek to identify the habits of staff members in the interests of collecting data that will assist in maximising worker efficiency or reduce costs. Some companies, including those in the banking, technology, pharmaceutical and healthcare industries, require their employees to wear badges equipped with RFID chips and other sensors that can record sound, geo-location and physical movement to monitor such aspects of the wearers as tone of voice, posture and who they speak to and for how long.“[124]

Lupton macht an dieser Stelle deutlich, welche starke Form der Überwachung in diesem Zusammenhang stattfindet. Allerdings ist es wichtig festzustellen, dass diese Art der Überwachung für die Überwachten durchaus positive Folgen nach sich zieht. Bei Auswertungen von Mitarbeiterdaten aus einem Call Center der *Bank of America* wurde beispielsweise festgestellt, dass die Belegschaft mit einer kurzen Kaffeepause produktiver an die Arbeit geht und insgesamt weniger Kündigungen eingehen. Auf diese Auswertung hin wurde eine 15 Minütige Kaffeepause fest in den Arbeitstag integriert, um die Zufriedenheit des Personals zu gewährleisten.[125]

Abschließend nennt Lupton das *exploited self-tracking* als fünfte mögliche Art der Selbstkontrolle. Reichert bezeichnet diese als „Ökonomisierung von Biodaten“[126]. Hierbei sammeln die Benutzenden ihre persönlichen Daten (mithilfe elektronischer Gadgets); dies kann sowohl als *personal* als auch als *pushed, communal oder imposed self-tracking* von statten gehen. Anschließend geben die Handelnden ihre gesammelten Daten an Dritte weiter, die die Informationen für Ihre Zwecke weiterverwenden und sich meist finanziell daran bereichern. Die größte amerikanische Apothekenkette Walgreens setzt beispielsweise bereits seit 2013 *exploited self-tracking* als Teil ihres

---

124 Lupton, *Self-Tracking Modes*, S. 9.

125 Vgl. Lohr, Steve, „Unblinking Eyes Track Employees. Workplace Surveillance Sees Good and Bad“, *nytimes.com*, 21.06.2014, http://www.nytimes.com/2014/06/22/technology/workplace-surveillance-sees-good-and-bad.html?_r=0, Zugriff: 16.10.2016.

126 Reichert, „Digitale Selbstvernetzung“, S. 76.

Treuepunktesystems ein.[127] Hierbei lässt sich die Überwachung mittlerweile sowohl durch spezielle tragbare Geräte durchführen, als auch durch diverse Gesundheits-Apps, die online, mithilfe der kostenlosen Walgreens App, mit dem jeweiligen Kundenkonto verbunden werden können. Diese Apps sind im Gegensatz zu den technischen Gadgets größtenteils kostenlos. Beispielhaft ist hier die *HealthKit*[128] App von Apple anzuführen, die sogar beim Kauf eines i*Phones* bereits vorinstalliert ist. Nach der erfolgreichen Installation der App muss nur noch eine Meile zu Fuß oder mit dem Fahrrad zurückgelegt werden und schon befinden sich 20 zusätzliche Treuepunkte auf dem Kundenkonto.[129] Auch wenn die meisten Kunden nur ihren eigenen Vorteil, in Form von Gutscheinen und Rabatten bei dieser Art der Selbstkontrolle sehen, so findet hier tatsächlich nur ein Marketingprozess durch Überwachung statt.
Durch welche genauen Methoden die beschriebene mediale Kontrolle stattfindet, wird unter Punkt 3.3 dieser Arbeit genauer definiert. Wie weit sich die beschriebenen Arten des Self-Tracking im Überwachungsdispositiv des Smart Home wiederfinden lassen, bleibt in der anschließend folgenden Analyse herauszustellen.
Abschließend bleibt des Weiteren festzustellen, dass auch aus medialer Sichtweise das Panoptikum immer noch ein gewisses Restinteresse innehat. Hierbei dreht sich die Aufmerksamkeit vor allem um kleine mobile Gegenstände der Überwachung, wie das Smartphone oder die beschriebenen Gadgets zur Überwachung des Körpers.

> „Die Macht bewegt sich mit der Geschwindigkeit elektronischer Signale, so daß die Zeit ihrer Übermittlung auf eine momenthafte Gegenwart schrumpft. Damit ist die Macht in jeder Hinsicht *exterritorial* geworden. Sie ist weder an den Raum gebunden, noch hindert dieser ihre Verbreitung. Man kann die Einführung des Handys als den symbolischen »K.-o.-Schlag« gegen die Raumgebundenheit interpretieren. Für die Übermittlung von Befehlen und die Überwachung ihrer Ausführung ist heute nicht einmal mehr ein Telefonanschluss erforderlich.“[130]

Während Zygmunt Bauman hier nur auf Mobiltelefone eingeht, lässt sich diese Theorie der exterritorial gewordenen Überwachung auch auf beliebige andere mobile Gadgets, wie beispielsweise die von Reichert erwähnten Fitnesstracker ausdehnen. Die

---

127 Vgl. O.N. (Anonym: gshwach), „Walgreens Incentivizes Self-Tracking“, http://networkedmedicine.tumblr.com/post/47422186125/walgreens-incentivizes-self-tracking, *Medicine in the Age of Networked Intelligence*, Zugriff: 17.10.2016.

128 Vgl. O.N., „Health Apps & Devices“, *Walgreens*, https://www.walgreens.com/steps/appmarket.jsp?ban=BRHC_DMI_earnban, Zugriff: 17.10.2016.

129 Vgl. O.N., „Balance Rewards for healthy choices“, *Walgreens*, https://www.walgreens.com/steps/brhc-loggedout.jsp, Zugriff: 17.10.2016.

130 Bauman, *Flüchtige Moderne*, S.18.

Handelnden binden sich an ihr »kleines Gefängnis«, vertrauen ihm Daten an, geben Einblick in das private Leben und nehmen es freiwillig überall hin mit. Auch in der folgenden Analyse soll diese Idee des portablen Gefängnisses berücksichtigt werden.

2.3.3 Post-Privacy Debatte

„You have no privacy anyway, Get over it.“[131] antwortete Scott McNeal, Vorstand des amerikanischen IT-Unternehmens Sun, bereits 1999 auf die Frage nach den Ängsten der Gesellschaft vor der allgegenwärtigen Überwachung durch technologischen Fortschritt. Die Tatsache zu glauben, dass wir keine Privatsphäre mehr haben und einfach »darüber hinwegkommen« sollen, schien 1999 utopisch und auch heute, in einer Zeit, in der das Thema Post-Privacy an der Tagesordnung liegt, ist es für viele Menschen immer noch schwer, das zu realisieren. Eric Schmidt, der ehemalige CEO von Google, ging zehn Jahre später mit seiner Aussage noch einen Schritt weiter: „If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place.“[132] Schmidt weist die Menschen nicht nur darauf hin, »sich nicht so anzustellen«, wie Scott McNeal es getan hat, sondern gibt ihnen noch den gut gemeinten Rat, alles, von dem sie nicht wollen, dass es jemand erfahren könnte, am besten sowieso von vornherein zu unterlassen. Schmidts Idee wirkt einfach, doch die Realisierung scheint schier unmöglich. Der Blogger und Filmkritiker Christian Heller definiert das Szenario 2011 mit den Worten:

> „Die Privatsphäre ist ein Auslaufmodell. Unser Sein und Handeln, egal wie persönlich oder geheimniskrämerisch, ist zunehmend für andere einsehbar. Wir müssen lernen, damit klarzukommen. Wir treten ein in das Zeitalter der »Post-Privacy«: in ein Leben nach der Privatsphäre.“[133]

Die Aussage von Heller behält auch heute immer noch Gültigkeit. Bereits seit der Einführung und flächendeckenden Verbreitung der ersten sozialen Netzwerke ist die Post-Privacy Debatte ein gesellschaftspolitisches Thema, das alle Nutzenden angeht. Laut Christan Heller lässt sich dieses Verschwinden der Privatheit auch nicht mehr aufhalten. Um nicht in Orwellsche Verhältnisse abzurutschen, ist es demnach von größter Wichtigkeit, dass die Macht über die Überwachung nicht in die Hände einiger weniger

---

131 Sprenger, Polly, „Sun on Privacy: »Get over it«“, *Wired*, 26.01.1999, http://archive.wired.com/politics/law/news/1999/01/17538, Zugriff: 19.10.2016.

132 Tate, Ryan, „Google CEO: Secrets Are for Filthy People“, *Gawker*, 04.12.2009, http://gawker.com/5419271/google-ceo-secrets-are-for-filthy-people, Zugriff: 19.10.2016.

133 Heller, Christian, *Prima leben ohne Privatsphäre*, München: Verlag C.H.Beck oHG 2011, S. 7.

Privilegierter fällt, sondern bei den Menschen, also den ursprünglichen Besitzern der Daten, bleibt.[134] Einen Kontrollverlust gilt es unbedingt zu verhindern. „Wir müssen lernen, dass Daten nicht schlimm sind. Es sind die Menschen, die Schlimmes damit tun“[135], stellt Netzaktivist und Telecomix-Vertreter Stephan Urbach treffend fest. Der Kulturwissenschaftler Michael Seemann weist jedoch darauf hin, dass die Post-Privacy nicht nur positiv oder negativ konnotiert ist und es keine einheitliche Idee für ihre Definition gibt. Vielmehr stellt sie für ihn eine Einladung zum Diskurs dar.[136] Einen möglichen positiven Aspekt spiegelt die Hilfe wieder, die Nutzende im World Wide Web erhalten können.[137] Bereits Kinder lernen, dass sie die bestmögliche Hilfe erhalten, wenn sie klar und deutlich ausdrücken, was ihnen fehlt. Stehen Handelnde also vor einem Problem und stellen es online zur Diskussion, beispielsweise in einem Forum zum passenden Thema, so wird der Sachverhalt einerseits öffentlich gemacht und verliert seine Privatheit. Andererseits ist die/der UserIn dadurch in der Lage, schnellstmöglich die bestmögliche Antwort auf das Problem zu erhalten. Jedoch hat Post-Privacy im Netz, wie bereits angedeutet, nicht nur positive Seiten.

> „Das Netz als Post-Privacy-Maschine entblößt und stellt alle an den öffentlichen Pranger – auch die Großen und Mächtigen, wie zum Beispiel die Fälle WikiLeaks und zu Guttenberg zeigen, aber auch die Kleinen und Schwachen, die oftmals viel weniger Fluchträume oder Mittel zur Gegenwehr besitzen.“[138]

Christian Heller stellt hier Negativbeispiele des Kontrollverlustes heraus. Durch lockeren Umgang mit (den falschen) Daten kann jeder Mensch und jede Institution zu jeder Zeit Spott und Hohn auf sich ziehen oder möglicherweise auch einen Skandal auslösen. Öffentliche Demütigung ist jedoch kein neues Konzept. Jahrhundertelang wurden Menschen an den Pranger gestellt um ein scheinbares Gefühl von Gerechtigkeit wieder herzustellen. Dieser Pranger wurde nun durch den Verlust der Privatheit im Internet remediatisiert und vom Hauptplatz des mittelalterlichen Dorfes auf die Facebook Pinnwände und in die Twitter-Feeds des 21. Jahrhunderts katapultiert. Durch

---

134 Vgl. Heller, Christian, „Post-Privacy – Vom Ende der Privatheit“, in: *»Wir nennen es Wirklichkeit« Denkanstöße zur Netzkultur*, Hg. Peter Kemper, Alf Mentzer, Julika Tillmanns, Stuttgart: Philipp Reclam jun. 2014, S. 27.

135 Ebd., S. 32.

136 Vgl. Seemann, Michael, „Was ist Postprivacy (für mich)?“, *ctrl+verlust*, 23. März 2011, http://www.ctrl-verlust.net/was-ist-postprivacy-fur-mich/, Zugriff am 19.10.2016.

137 Vgl. Heller, „Post-Privacy – Vom Ende der Privatheit“, S. 28.

138 Ebd., S. 29f.

diese Remediatisierung ist es beispielsweise möglich geworden aufgrund eines rassistischen Kommentars im sozialen Online-Netzwerk *Twitter*[139], das Leben einer einzelnen Frau innerhalb von nur elf Stunden komplett zu zerstören. Nachdem ihr Tweet „Going to Africa. Hope I don't get AIDS. Just kidding. I'm White!"[140] sich viral über das World Wide Web verbreitet hatte, verlor die US-Amerikanerin Justine Sacco in kürzester Zeit ihren Arbeitsplatz, ihre Unterkunft und ihr Gesicht in der Öffentlichkeit, ohne dies selbst überhaupt zu merken. Sacco veröffentlichte den Tweet kurz bevor sie ins Flugzeug nach Afrika stieg und das *Online Shaming*[141] fand bereits während des Langstreckenflugs statt.[142] Auch wenn Justine Sacco mit diesem (ihrer Meinung nach) ironischen Post nur ihre rund 170 Follower unterhalten wollte, verließen die 64 Zeichen ihr vermeintlich privates Umfeld schnell.
Diese Beispiele haben herausgestellt, dass die Post-Privacy Debatte einen offenen Diskurs darstellt und nicht ausschließlich negativ oder positiv einzuordnen ist.

> „Postprivacy ist auch – so ist jedenfalls meine Meinung – der Zustand auf den unsere Gesellschaft unweigerlich zusteuert. Der Kontrollverlust führt aber nicht zur totalen Transparenz – das wird oft falsch verstanden. Der Kontrollverlust führt aber zwangsläufig in den Zustand, dass die Grenze zwischen öffentlich/nichtöffentlich keine selbstbestimmte mehr sein kann. So dass ich nicht mehr weiß, was andere von mir wissen, dass ich mich in Zweifel auch nicht darauf verlassen kann, unbeobachtet zu sein, meine Identität und/oder meine Eigenschaften zu verbergen. Nicht alles ist öffentlich, aber ich bestimme nicht mehr, was öffentlich ist, oder nicht. Es gibt einen großen Unterschied zwischen totaler Transparenz und Kontrollverlust. Beides könnte man als Postprivacy beschreiben, aber ich glaube nur an zweiteres."[143]

Michael Seemann wirft offen die Frage auf, ob Post-Privacy die bloße Transparenz des privaten Lebens ist, oder ob diese noch zu weit davon entfernt ist und der Zustand der Post-Privacy erst durch den Zustand des Kontrollverlustes eintritt. Auch wenn Seemann sich an dieser Stelle bereits für Letzteres ausspricht, gilt es, diese Frage in Bezug auf das Smart Home in der folgenden Analyse erneut aufzurollen.

---

139 O.N., „Twitter", https://twitter.com/, Zugriff: 19.10.2016.
140 Ronson, Jon, „How One Stupid Tweet Blew Up Justine Sacco's Life", *nytimes.com*, http://www.nytimes.com/2015/02/15/magazine/how-one-stupid-tweet-ruined-justine-saccos-life.html, Zugriff: 19.10.2016.
141 Vgl. Ebd..
142 Vgl. Stephan, Felix, „Der Schwarm als Meute", *zeit.de*, 26.09.2016, http://www.zeit.de/kultur/literatur/2016-09/in-shitgewittern-jon-ronson-soziale-netzwerke, Zugriff: 19.10.2016.
143 Seemann, „Was ist Postprivacy (für mich)?".

Auch das omnipräsente Schlagwort *Big Data* ist in diesem Zusammenhang nicht außer Acht zu lassen. Big Data wird oft als Überbegriff für neue, digitale Technologien verwendet. Es steht allerdings nicht nur als Bezeichnung für die Technologie an sich, sondern auch für die Datenmengen, die durch die Nutzungen dieser Technologien gesammelt werden und außerdem für deren Auswertung, Sammlung, Analyse und Nutzung.[144] Hierbei unterscheidet Ramón Reichert zwischen transaktionalen Daten und nutzergenerierten Daten. Erstgenannte, die Nutzende durch das Einloggen in Onlinenetzwerke, Cookies und Bezahlvorgänge im Internet hinterlassen, lassen sich im wissenschaftlichen Sinne als Big Data bezeichnen. Daten, die von Nutzenden selbst generiert werden, sind nicht objektiv genug, um wissenschaftlich ausgewertet zu werden.[145]

Für Chris Anderson, den Herausgeber des in dieser Arbeit bereits zitierten Magazins *Wired*, bedeutet Big Data „das Ende der Theorie“[146]. Laut seiner Feststellung müssen durch Big Data keinerlei Hypothesen mehr aufgestellt werden, da stattdessen die riesigen gesammelten Daten direkt ausgewertet und befragt werden können. Welchen Teil zur Sammlung dieser riesigen Datenmengen das Smart Home beiträgt und in welchem Zusammenhang diese noch mit dem Schlagwort Big Data steht, soll in der Analyse des genannten Beispiels auf den Grund gegangen werden.

2.3.4 Forschungsmethode zur transdisziplinären Analyse

Nach diesen ausführlichen Erläuterungen lässt sich eine dreiteilige Forschungsmethode formulieren, die es in der Analyse auf ein reales, theoretisches Beispiel anzuwenden gilt.

Im ersten Teil werden die soziologischen Aspekte der Überwachung anhand des Beispiels Smart Home analysiert, die bereits theoretisch herausgestellt wurden. Hierbei bilden die Schlagworte flüchtige Moderne/flüchtige Überwachung, Freiwilligkeit und Selbsttermination, die Gefühlswelt der Überwachten und die Begrifflichkeit der lateralen Überwachung das Grundgerüst der Analyse. Passende literarische Grundlage

---

144 Vgl. Reichert, Ramón, *Big Data: Analysen zum digitalen Wandel von Wissen, Macht und Ökonomie*, Bielefeld: transcript Verlag 2014, S. 9f.

145 Vgl. Krichmayr, Karin, „Wir sind noch nicht am Ende des Zufalls“, *derStandard.at*, 28.10.2014, http://derstandard.at/2000007420701/Wir-sind-noch-nicht-am-Ende-des-Zufalls, Zugriff: 24.10.2016.

146 Anderson, Chris, „The End of Theory: The Data Deluge Makes the Scientific Mehtod Obsoltete“, *Wired*, 23.06.2008, https://www.wired.com/2008/06/pb-theory/, Zugriff: 24.10.2016.

dazu bieten Zygmunt Bauman und David Lyon. Neben diesen theoretischen Grundpfeilern bergen Abhandlungen von Marc Andrejevic und Bigo Didier interessante Ansätze, die Denkanstöße für die Abhandlung liefern.

Nach Behandlung der soziologischen Fragen an das Smart Home ist es an der Zeit, genauer auf die medial geprägten Fragestellungen einzugehen. Hierbei sind Verdatung, Gamifizierung und Self-Tracking die großen Schlagworte die es zu hinterfragen gilt. Es wird versucht, anhand des theoretischen Beispiels zu klären, in welcher Form die mediale Überwachung im eigenen Zuhause stattfinden kann und wie viel Privatsphäre dadurch noch im privaten Raum vorhanden bleibt. Literarisches Hauptaugenmerk wird in diesem Abschnitt auf Debora Lupton und ihre Studien im Bereich der Self-Tracking Kultur gelegt. Außerdem gibt Ramón Reicherts Abhandlung zur digitalen Selbstvernetzung interessante Denkanstöße für diesen Teil der Analyse.

Nach dem soziologischen und dem medialen Teil der Methode, macht der dritte und letzte Teil auf den ersten Blick möglicherweise den Eindruck einer „losen Thesensammlung über die Gesellschaft und de[n] Zusammenhang von Transparenz und Toleranz“[147], wie Michael Seemann den aktuellen Forschungsstand über die Post-Privacy beschreibt. In diesem letzten Teil wird das bereits genannte Beispiel Smart Home hinsichtlich der Post-Privacy Debatte beleuchtet. Auch wenn diese beim Überblick über Literatur und aktuelle Berichterstattung den Eindruck einer lockeren Stichwortsammlung erweckt, muss dennoch analytisch an das Thema herangegangen werden. Nach einer kurzen Erläuterung des »Privaten« wird unter der Berücksichtigung von Nicholas Negropontes Literatur zum Thema, auf die Postdigitalität eingegangen. Weiter bietet Michael Seemanns Abhandlung „Das Neue Spiel“[148] an dieser Stelle Literatur, die sich mit Theorien zum Kontrollverlust durch digitale Medien auseinandersetzt. Außerdem liefern Christian Heller und Peter Schaar interessante Ansätze zum Thema Post-Privacy. Neben dem von Seemann angeführten Punkt des Kontrollverlustes, spielt in der Analyse auch der Hinweis auf das bereits erwähnte Schlagwort Big Data eine interessante Rolle. Das Smart Home wird im Folgenden hinsichtlich dieser Aspekte untersucht. Welche Daten produzieren die Bewohnenden des intelligenten Hauses und was passiert mit den erzeugten Datenmengen? Bis zu welchem Punkt haben die Nutzenden selbst die Kontrolle über gesammelte Daten und wann geben sie diese an die

147 Seemann, „Was ist Postprivacy (für mich)?“.

148 Seemann, Michael, *Das Neue Spiel. Strategien für die Welt nach dem digitalen Kontrollverlust,* Freiburg: orange-press 2014.

Überwachenden ab oder verlieren sie gar? Profitieren die Handelnden von der den Folgen des Datenverlustes und wer zieht neben ihnen noch seine Vorteile daraus?
All diese Fragen gilt es, in der folgenden Analyse hinsichtlich des Beispiels Smart Home zu klären und zu hinterfragen.
Um davor allerdings noch näher an die Themen Smart Home im Speziellen und Internet der Dinge im Allgemeinen heranzuführen, folgt nun neben einer historischen Heranführung an das Thema auch eine Übersicht, über die unterschiedlichsten technischen Methoden, mit deren Hilfe überwacht werden kann, um einen Realitätsbezug herzustellen.

3 Historische Heranführung

In den 1990er Jahren gelang es Douglas Coupland mit seinem Episodenroman *Generation X*[149] das Lebensgefühl, die Sorgen und die Ängste einer ganzen Generation einzufangen und so literarisch für die Nachwelt festzuhalten. Dies ist ein Phänomen, das nur wenigen Autoren zuteil wird. Der US-amerikanische Autor Dave Eggers gilt seit Längerem als neuer „Zeitgeist-Autor, dessen Literatur die Gegenwart seismografisch abbildet“[150] und tritt damit in Couplands literarische Fußstapfen. Mit seinem dystopischen Roman *Der Circle*[151], der 2014 in deutscher Übersetzung erschien, gelang ihm die Abbildung einer fremden, furchteinflößenden Welt, die mehr über ihre Bewohnenden zu wissen scheint, als diese es selbst tun. Eggers beschreibt eine fiktive Welt, in der Privatheit mit Geheimnissen und Lügen gleichgesetzt wird und in der Kinder wie Hunde mit Chips versehen werden, um sie vor Entführungen zu schützen. Diese Welt erinnert auf den ersten Blick an Orwells *1984*, mit technologischer Ergänzung durch das Internet. Eggers eröffnet den Lesenden die uneingeschränkte Welt des Internet der Dinge, das sich auf alle Lebensbereiche auswirkt und die mit unserer realen Welt bereits mehr Parallelen aufweist, als es vielleicht anfänglich scheinen mag. Diese Parallelen werfen einige Fragen auf, welche vor der anschließenden Analyse geklärt werden müssen.

Im Folgenden wird versucht, zu erläutern, was genau das Internet der Dinge eigentlich ist, wie es sich entwickelt hat und in welcher Art und Weise es sich in unserer heutigen Gesellschaft verbreitet. Außerdem wird darauf einzugehen versucht, wie sich die eigene Privatheit bezüglich einzelner Anwendungen des Internet der Dinge verhält. Treten Nutzende mit dem Akzeptieren der allgemeinen Geschäftsbedingungen ihr Recht auf Privatsphäre an große Technikhersteller ab?

---

149 Coupland, Douglas, *Generation X. Geschichten für eine immer schneller werdende Kultur*, München: Goldmann Verlag [8]1995; (Orig. *Generation X. Tales for an Accelerated Culture*, New York: St. Martin’s Press 1995).

150 Andre, Thomas, „Die Tyrannei des Internets. Diskussion um US-Bestseller »The Circle«“, *spiegel.de*, 04.08.2014, http://www.spiegel.de/kultur/literatur/dave-eggers-roman-dystopie-the-circle-a-982663.html, Zugriff: 18.10.2016.

151 Eggers, Dave, *Der Circle*, Köln: Verlag Kiepenheuer & Witsch [5]2014; (Orig. *The Circle*, New York: Alfred A. Knopf 2013).

3.1 Mark Weiser - *Ubiquitous Computing*

Um zu verstehen wie genau das Internet der Dinge definiert ist, liegt es auf der Hand, sich der Begrifflichkeit historisch zu nähern. Wegweisend war in diesem Feld Mark Weiser, der mit seiner Theorie über den „Computer for the 21st Century“[152] bereits in den 1990er Jahren im Xerox Parc, in Silicon Valley, Visionen für die digitale Zukunft der Gesellschaft hatte. Während Weiser gedanklich an seiner Vision des unsichtbaren Internets feilte, das sich überall um die Nutzenden herum befinden sollte, war der Personal Computer bereits weit verbreitet und die Entwicklung von Laptops und Tablet PCs schien in erreichbarer Nähe. Diese Phase sah Weiser allerdings nur als einen Zwischenschritt, hin zur vollkommenen Unsichtbarkeit der Technik.

> „The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are distinguishable from it.“[153]

Dieses Verschwinden ist für Weiser keine Konsequenz des technologischen Fortschrittes, sondern vielmehr eine Ausgeburt der menschlichen Psyche. Hat der Mensch etwas ausreichend konsumiert, macht er sich bewusst keine Gedanken mehr dazu und nimmt den Sachverhalt anschließend nur noch unterbewusst war. Weiser führt hier exemplarisch das Beispiel der Schrift an. Ein Kind, das gerade erst die Fähigkeit des Lesens erlernt, nimmt alle Buchstaben und jegliche Form der Schrift in seinem Umfeld bewusst war. Besitzen Lesende allerdings schon seit einiger Zeit die Qualifikation, Geschriebenes zu erkennen, findet die Wahrnehmung auf einer anderen Ebene statt. Beispielsweise lesen Betreffende auf einem Straßenschild nicht die einzelnen Buchstaben des Wortes »STOP« und setzt sie dann in ihrem Kopf zusammen. Stattdessen greifen sie auf Erfahrungen zurück und ordnen die Botschaft des Schildes so anders ein, wie es jemand tun würde, der gerade erst mit dem Lesen lernen beginnt. Weiser beschreibt diese Eigenschaft der Schrift als „constant background presence“[154], die bereits aus der Gesellschaft der 90er Jahre nicht wegzudenken gewesen wäre. Diese Eigenschaft der Präsenz im Hintergrund war für Mark Weiser auch für das Internet vorstellbar und hat sich mit der Verbreitung des *Ubiquitous Computing* bereits weitgehend in Realität verwandelt. Diese Allgegenwärtigkeit bestand für Weiser allerdings nicht aus einer

---

[152] Weiser, Marc, „The Computer for the 21st Century“, *ACM SIGMOBILE. Mobile Comuputing and Communications Review* 3/3, 1999; (Orig. *Scientific American* 265/3, September 1991, S. 94-104).
[153] Ebd., S. 3.
[154] Ebd..

Vision davon, dass jeder Mensch seinen tragbaren Personal Computer überall mithinnehmen kann, sondern vielmehr in einer „embodied virtuality“[155], in der der altbewährte Computer seine Schale und seinen elektronischen Motor verlässt und sich ein neues Zuhause in Alltagsgegenständen sucht. Als entscheidende Kriterien, die erfüllt werden müssen, weist Weiser auf „location and scale“[156] hin. Die Kenntnis über den Einsatzort hilft dem Computer dabei sich auch ohne künstliche Intelligenz entsprechend notwendiges Verhalten anzueignen. Des Weiteren soll die Größe des Computers an die Aufgabe angepasst werden, zu deren Erfüllung er eingebaut wird.[157] Vor allem deshalb können Internet der Dinge und Ubiquitous Computing nicht mit einem gewöhnlichen Personal Computer gleichgesetzt werden, der sich lediglich in einer anderen, ungewöhnlicheren Verpackung befindet. Ein Intelligenter Gegenstand, der sich unter den Überbegriff Internet der Dinge einordnen lässt, besitzt deutlich weniger Fähigkeiten als ein PC oder Laptop. Grundsätzlich erfüllt er nur genau die eine oder mehrere wenige Aufgaben, für die er konstruiert und eingebaut wurde.
Neben Einsatzort und Größe des Miniaturcomputers spielen drei weitere wichtige Grundlagen eine entscheidende Rolle für die Nutzung des Internets der Dinge: Die günstigen Kosten, Computer, welche die von ihnen geforderte Aufgabe mit geringer Leistung durchführen können und ein Netzwerk, das sie alle zusammenhält.[158]

3.2 Internet der Dinge - Heute

„Im *Internet der Dinge* kommuniziert alles mit allem. Bloß ohne Menschen“[159], titelte die Onlineausgabe der Frankfurter Allgemeinen Zeitung, anlässlich der CeBIT 2015. Mark Weiser hatte eine klare Vision davon vor Augen, wie sich die Technik rund um Computer und Internet weiterentwickeln sollte. In seiner Vorstellung war klar, dass der Computer seine ursprüngliche Form und sein altes Gehäuse verlassen und ein neues Zuhause in Alltagsgegenständen finden sollte. Nun ist beispielsweise aber nicht die Rede davon, einem Kugelschreiber auf einem Chip Daten über seinen Herstellungsort einzuspeichern, sondern davon, ihn tatsächlich intelligent zu machen. Intelligenz bedeutet hierbei das eigenständige Durchführen einer vordefinierten Aufgabe.

---

155 Ebd., S. 5.
156 Ebd. S. 5.
157 Vgl. Ebd., S. 5.
158 Vgl. Ebd., S. 7.
159 Schipper, Lena, „Was eigentlich ist das Internet der Dinge? Ein Schlagwort macht Karriere: Im „Internet der Dinge“ kommuniziert alles mit allem. Bloß ohne Menschen.“, *faz.net*, 17.03.2015, http://www.faz.net/aktuell/wirtschaft/cebit/cebit-was-eigentlich-ist-das-internet-der-dinge-13483592.html, Zugriff: 07.08.2016.

„Das Ziel ist es allen Dingen die bisher auf die Steuerung durch ihre menschlichen Besitzer angewiesen sind, mit Hilfe des Internets eine Art Eigenleben einzuhauchen.“[160] Außerdem soll der Gegenstand „adressierbar gemacht werden“[161]. Technische Grundlage für das intelligente Handeln und die Adressierbarkeit bilden hierbei drei Grundvoraussetzungen, die Florian Spenger und Christoph Engemann in der Einleitung zu ihrem Sammelband *Im Netz der Dinge* beschreiben. Im »Ding« müssen Sensordaten integriert sein, die auf die jeweilige Umgebung bezogen sind, in der sich der Gegenstand befindet. Die Vernetzung einzelner, verteilter Bestandteile, die als Internet der Dinge bezeichnet werden kann, muss gewährleistet sein. Außerdem muss die Rechenkraft ausgelagert sein, was den Sensoren und Transistoren die Reduzierung auf ein Minimales ihrer potentiellen physischen Größe ermöglicht.[162]

Neben den technischen Aspekten eines wissenschaftlichen Phänomens, spielt auch die Benennung dessen eine wichtige Rolle. Die Namensgebung *Internet der Dinge* ist möglicherweise auf konzeptueller Ebene für Nutzende irreführend. Was macht ein Ding zu einem Ding? Und bleibt es mit Eigenschaften wie Intelligenz und der Möglichkeit der Vernetzung und Kommunikation immer noch ein solches? Und ist das im Namen verwendete Internet immer noch das Internet, das wir kennen und täglich nutzen?

Die intelligenten Gegenstände müssen nicht notwendigerweise über das von uns allgemein verwendete Internet miteinander kommunizieren. Vielmehr können sie auch in eigenen, kleineren, extra angelegten Netzen und Clouds Verbindungen zueinander aufbauen, die dann möglicherweise mit dem Internet (wie es uns als Nutzenden bekannt ist), verknüpft werden. Diesbezüglich ist es auch interessant, den Namensvorreitern des IoT[163] genauere Beachtung zu schenken. Angefangen mit Mark Weisers bereits beschriebenen Version des Ubiquitous Computing, entwickelten sich weitere Bezeichnungen wie beispielsweise „Things That Think“[164] oder „Everyware“[165], die sich allesamt nicht als allgemeingültig durchsetzen konnten.

---

160 Ebd..

161 Sprenger, Florian/Christoph Engemann**,** „Im Netz der Dinge: Zur Einleitung“, in: *Internet der Dinge: Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt*, Hg. Christoph Engemann, Florian Sprenger, Bielefeld: transcript (Digitale Gesellschaft) 2015, S. 16.

162 Vgl. Ebd., S. 8.

163 Der Terminus *Internet der Dinge* und die verbreitete, englische Abkürung *IoT* werden im Folgenden als Synonyme füreinander verwendet.

164 O.N., „Things That Think Consortium: MIT Media Lab“, *MIT Media Lab*, http://ttt.media.mit.edu/, Zugriff: 08.06.2016.

165 Greenfield, Adam, *Everyware. The dawning age of ubiquitous computing*, Berkley: New Riders 2006.

Neben der Begrifflichkeit ist es an diesem Punkt ebenfalls wichtig, den Mehrwert des Novums zu betrachten. Es ist notwendig festzuhalten, dass diese Technologie für den Menschen als Nutzenden keineswegs lebensnotwendig, sondern in den meisten Fällen schlicht lebenserleichternd und/oder vereinfachend ist. Der amerikanische Literaturwissenschaftler und Videospieldesigner Ian Bogost beschreibt in seiner Publikation *Das Internet der Dinge, die wir nicht brauchen*[166] genau dieses Phänomen. Hierbei ist meist die Rede von Gegenständen, die den Nutzenden eine bisher zeitaufwändige Aufgabe abnimmt und ihnen dadurch scheinbar das Leben erleichtert. Ein aktuelles Beispiel, das hier anzuführen ist, greift da, wo die Entwicklung des IoT ihren größten Anklang findet: im Bereich Wertschöpfungs- und Lieferketten. Das folgende Beispiel greift zeigt die Position des Endverbrauchers auf. Gillette, der Marktführer in der Herstellung für Rasierapparate[167], versucht seit mehr als einem Jahr das Internet der Dinge in die Badezimmer der deutschen[168] Männer zu bringen. Geplant ist das in Form eines vernetzten Nassrasierers. Potentieller Kunde ist der vergessliche Bartträger, der erst bei der morgendlichen Nassrasur merkt, dass er keine Ersatzklingen mehr zuhause hat und dann, am Abend im Supermarkt oder in der Drogerie bereits wieder vergessen hat, dass die besagten Klingen auf seiner Einkaufsliste stehen. Gillette gibt dem Nutzer hierfür als Ablage für seinen Nassrasierer eine kleine Box mit einer simplen Taste, durch deren gedrückt Halten für einige Sekunden die gewünschten Klingen einfach nachbestellt und am nächsten Tag (außer Sonntag) automatisch über den Postweg zugestellt werden. Der letzte Schritt zur neuen Klinge ist die Bestätigung der Bestellung in einer E-Mail, die ebenfalls automatisch beim Drücken der Bestelltaste an die hinterlegte E-Mailadresse gesendet wird. Diese erneute Bestätigung ist allerdings nicht aus technischer Notwendigkeit eingebaut, sondern soll den Nutzer vielmehr vor unüberlegten Bestellungen – beispielsweise durch ein Kind, das unabsichtlich den Knopf betätigt – schützen. Der Bestellvorgang funktioniert durch eine vorherige Online-Anmeldung mit Adresse und Bankverbindung, woraufhin der Verbraucher das entsprechend personalisierte Gerät mit Mobilfunk-Terminal und passender SIM-Karte auf dem Versandweg durch die Post erhält. Durch Drücken des Knopfes wird die SIM-

---

166 Bogost, Ian, „Das Internet der Dinge, die wir nicht brauchen“, in: *Internet der Dinge: Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt*, Hg. Christoph Engemann, Florian Sprenger, Bielefeld: tran-script (Digitale Gesellschaft) 2015, S. 89–100.

167 Vgl. O.N., „Gillette – Über Gillette“, http://gillette.de/de-de/ueber-gillette, Zugriff: 10.08.2016.

168 Im bisherigen Testlauf liefert Gillette ausschließlich innerhalb Deutschlands (siehe: O.N., „The Perfect Shave – Lieferbedingungen“, *The Perfect Shave*, https://www.perfect-shave.de/zahlungsarten-lieferbeschraenkungen, Zugriff: 10.08.2016.).

Karte für einige Augenblicke aktiviert und sendet über das Mobilfunknetz die entsprechenden Bestelldaten an das Logistikunternehmen. Das Gerät bezieht seine Energie zwar über eine eingelegte Batterie, aber dadurch, dass deren Leistung nur während des Drückens des Knopfes beansprucht wird, bleibt der Stromverbrauch minimal und die Nutzungsdauer der Batterie verlängert sich auf ein Maximales.[169] Der Internethändler *Amazon*[170] griff kürzlich das Prinzip von Gillette in Form des *Dash Buttons* auf, auf den ich in der späteren Analyse noch genauer eingehen werde.

Dies ist nur eines von unzähligen Beispielen, wie das Internet der Dinge bereits in das tägliche Leben der Nutzenden eingreift und es scheinbar erleichtert. Neben diesen Erleichterungen fällt das Augenmerk allerdings auch auf einen weiteren wichtigen Punkt, der für diese wissenschaftliche Arbeit relevant ist und auf den ersten Blick negativ konnotiert ist: Die Sammlung von Daten und die daraus folgende personenbezogene Überwachung und Kontrolle der Nutzenden.

3.3 Überwachungsmethoden des Internet der Dinge

Wie bereits erläutert, ist das Internet der Dinge ein weit gefächerter Begriff, der den Nutzenden bereits heute in allen erdenklichen Bereichen des täglichen Lebens gegenübertreten kann und auch in Zukunft wird. In den unterschiedlichen Ansätzen der Forschungsmethode wurde bereits detailliert beschrieben, welche inneren Intentionen die Handelnden zur Selbstüberwachung bewegen und auch die Zielsetzungen der Fremdüberwachung wurden in dem erwähnten Abschnitt genauer erläutert.

Im Folgenden wird nun versucht, die einzelnen technischen Grundgegebenheiten zu nennen und zu erklären. Ziel ist es, zu verdeutlichen, welche speziellen Formen der Überwachung durch technische Neuerungen der vergangenen Jahre möglich geworden sind. Eine große Rolle spielt hier vor allem die Überwachung durch sogenannte Bewegungsprofile. Diese entstehen dann, wenn ortsgebundene Daten gespeichert und ausgewertet werden.[171] Diese Art der Datengewinnung stellt eine radikale Veränderung im Bereich der Überwachung dar.

---

169 Vgl. O.N., „The Perfect Shave – The Gillette Box“, *The Perfect Shave*, https://www.perfect-shave.de/gillette-box, Zugriff: 10.08.2016.

170 O.N., „Amazon“, https://www.amazon.de/, Zugriff: 18.12.2016.

171 Vgl. Simon, Anne-Catherine/Thomas Simon, *Ausgespäht und abgespeichert. Warum uns die totale Kontrolle droht und was wir dagegen tun können*, München: Herbig Verlag 2008, S. 21f.

> „[…] allein die Möglichkeit, dass Bewegungsdaten aufgezeichnet, gespeichert und ausgewertet werden können, [*stellt*] eine sehr schwerwiegende Veränderung im Überwachungspotential einzelner Menschen dar.“[172]

Möglichkeiten zur Erstellung solcher Bewegungsprofile bieten unter anderem die RFID-Technologie und GPS, die im Folgenden erläutert werden. Des Weiteren wird zusätzlich auf biometrische Daten und persönliche Kundenprofile eingegangen.

3.3.1 RFID

Der russische Wissenschaftler Léon Theremin ist dem Großteil der Weltbevölkerung bis heute nur als Entwickler des ersten und bis heute beinahe einzigen elektronischen Musikinstruments bekannt, das vom Menschen ohne die kleinste Berührung gespielt werden kann. Viel interessanter als diese Entdeckung ist jedoch die Tatsache, dass Theremin mit seinen Forschungen und Erfindungen nicht nur zum Entdecker der elektronischen Musik wurde, sondern auch den Grundstein für *Radio Frequncy Identification* legte, wie wir sie heute nutzen. RFID-Technologie steht für die Möglichkeit der Identifizierung eines Sensors, mit Hilfe von elektromagnetischen Wellen. Dieser Sensor ist im Fall von RFID-Chips ein flacher, kleiner Transponder, in dessen Mitte sich ein winziger Mikroprozessor befindet, der von einer spiralförmig darum gelegten Antenne umgeben wird. Dieser Transponder ist zumeist passiv, was bedeutet, dass er sich nicht selbst mit Strom versorgt, sondern kabellos durch Induktion aufgeladen werden kann. Sobald der Chip durch die elektromagnetischen Wellen mit Strom versorgt wird, schaltet er sich also an und sendet anschließend das ihm eingeschriebene Signal an Empfangende.[173]

Wie aber wird diese Technologie nun im Bereich Internet der Dinge eingesetzt und anschließend zur Überwachung genutzt?

Ein Großteil der deutschsprachigen Bevölkerung ist bereits mit RFID-Technologie in Berührung gekommen – sei es nun bewusst oder unbewusst. Als Exempel für den alltäglichen Einsatz ist beispielsweise das Bibliothekswesen anzuführen. Während bis heute in vielen Bibliotheken immer noch das Prinzip des Barcodes an der Tagesordnung ist, erprobte die *Stadtbibliothek Wien* am Urban Loritz Platz bereits vor 14 Jahren

---

[172] Čas, Johann/Walter Peissl, *Beeinträchtigung der Privatsphäre in Österreich. Teil 1 Bestandsaufnahme: Datensammlungen über ÖstereicherInnen*, Wien: Institut für Technisfolgen-Abschätzung der Österreichischen Akademie für Wissenschaften 2000, http://epub.oeaw.ac.at/ita/ita-projektberichte/d2-2a24.pdf, Zugriff: 29.10.2016, S. 19.

[173] Vgl. Simon/Simon, *Ausgespäht und abgespeichert*, S. 86f.

das Prinzip von RFID. „Als erste Großbibliothek des deutschen Sprachraums testet die Hauptbücherei das Selbstverbuchungssystem über Transponder-Geräte“[174], schrieb die österreichische Tageszeitung *der Standard* im April 2003. Hierbei wurden beim Umzug in den Neubau alle Medien mit Transpondern versehen, wodurch es den Benutzenden nun möglich ist, mehrere Medien gleichzeitig an Selbstbedienungsterminals zu verbuchen und auch wieder zurückzugeben – sogar außerhalb der Öffnungszeiten.[175] Ein weiterer wichtiger Faktor ist die Bestandspflege durch das Personal. Durch die Transponder in den Medien ist es beispielsweise möglich, verschollene Werke wiederzufinden, die sonst oft jahrelang an fehlerhaften Standorten gelagert und möglicherweise nie wieder gefunden worden wären.[176] Neben der Wiener Stadtbibliothek führte außerdem drei Jahre später die Münchner Zentralbibliothek, als erste Bibliothek in Europa, für ihr gesamtes Ausleihsystem ein RFID-Bibliothekssystem ein.[177]

Als weiteres Beispiel für die alltägliche Nutzung von RFID-Technologie sind Autos anzuführen, deren Schlüssel nicht mehr im Zündschloss umgedreht werden müssen. In ihrem Inneren befindet sich ein Transponder, wodurch das Vorhandensein des Schlüssels im Auto bereits ausreicht, um den Motor zu starten. Auch wenn viele Nutzende noch nicht selbst mit Autos dieser Art in Berührung gekommen sind, so ist ihnen aber möglicherweise die Berichterstattung über Weltfußballer David Beckham ein Begriff, da ihm bereits zwei Fahrzeuge mit RFID-Schlüssel entwendet wurden. Den HackerInnen war es möglich, während seines Restaurantbesuchs aus einiger Entfernung den RFID-Chip im Autoschlüssel zu klonen.[178]

Dies sind nur zwei von unzähligen Beispielen, wie RFID-Technologie bereits heute in das alltägliche Leben von Nutzenden integriert ist und zugleich technische Herausforderungen mit sich bringt. Wie aber kann diese Technologie noch weiter verbreitet und im Bereich Überwachung eingesetzt werden?

> „Johannes K. kauft ab und zu im Omni-Center ein, besitzt aber keine Kundenkarte. Als er sich dem Verkaufsschalter der Herrenabteilung nähert, registriert das System,

---

174 Niedermeier, Cornelia, „Der Bauch des Wals“, *derStandard.at*, 07.04.2003, http://derstandard.at/1264666/Der-Bauch-des-Wals, Zugriff: 07.08.2016.

175 Vgl. Wenzel, Bernhard, „RFID in der Hauptbücherei Wien“, *Vortrag im Rahmen von ODOK 2007 (12. Österreichisches Online-Informationstreffen, 13. Österreichi-scher Dokumentartag)*, Graz: 20. September 2007, https://www.uibk.ac.at/odok/ppt/wenzl.pdf, Zugriff: 07.08.2016, S. 6.

176 Vgl. Ebd., S. 5.

177 Vgl. Ziegler, Peter-Michael, „München stellt Bibliotheken auf RFID-Technik um“, *heise online*, 24.01.2006, http://www.heise.de/newsticker/meldung/Muenchen-stellt-Bibliotheken-auf-RFID-Technik-um-168454.html, Zugriff: 07.08.2016.

178 Vgl. Holl, John, „High-tech thieves use laptops to steal cars“, *ForbesAUTOS.com*, 26.06.2006, http://www.nbcnews.com/id/13507939/ns/business-autos/t/high-tech-thieves-use-laptops-steal-cars/#.V6WOhvmLQdU, Zugriff: 07.08.2016.

> dass ein Unterhemd in den Empfangsbereich geraten ist, das vor 18 Monaten hier gekauft worden ist und in drei weitere Einkäufe involviert war. Die Verkäuferin liest diskret von ihrem Display ab, dass dieser Kunde eine Vorliebe für Billigsocken und preisreduzierte Jacketts besitzt, und lässt ihn vorerst allein herumirren, während sie mit ihrem charmantesten Lächeln Herrn Müller-Lüdenscheid namentlich begrüßt, den das System aufgrund seiner Kundenkarte und der vergangenen Umsätze als finanzstarken Premiumkunden ankündigt.“[179]

Diese Geschichte über Johannes K. ist nur eine von vielen, wie sie mit dem technischen Einsatz von RFID-Chips denkbar wäre. Durch den Einbau eines der besagten Chips in einen regulären Gegenstand ohne eigentliche technische Bestandteile wird dieser Gegenstand zu einem intelligenten »Ding« gemacht. Im Fall von Johannes K. ist es das Unterhemd, das er beim Einkauf trägt. Der im Unterhemd integrierte Transponder schaltet sich durch die elektromagnetischen Wellen im Eingangsbereich des betretenen Kaufhauses ein und sendet die gespeicherten Kundendaten an das Display der Verkäuferin. Auch wenn Johannes K. keine Kundenkarte besitzt, so sind beispielsweise elektronisch getätigten Einkäufe im System des Kaufhauses gespeichert und das Unterhemd kann somit zu einem bestimmten Einkauf der Vergangenheit zugeordnet werden. Selbst wenn K. das Unterhemd mit Bargeld bezahlt haben sollte, so können dennoch die anderen Artikel eingesehen werden, die gemeinsam bezahlt wurden – im genannten Beispiel sind das „billige Socken“ und „preisreduzierte Jacketts“. Ab dem Zeitpunkt, an dem Dinge mit RFID-Technologie in den persönlichen Besitz übergehen, ist es also kaum mehr möglich, unbeobachtet zu sein, sofern es Beobachtende wollen.

3.3.2 GPS

Als im Jahr 2007 ein Bus voller Pilger in Südostfrankreich von einer Bergstraße abkam, auf tragische Weise in eine Schlucht stürzte und 26 Menschen starben, wurde die Schuld von vielen Seiten auf ein technisches Hilfsmittel des Fahrers gelenkt. Das GPS-Navigationssystem hatte die kleine gefährliche Bergstraße als kürzeste Route zum Ziel angezeigt und der Fahrer verließ sich – trotz zahlreicher Verbotsschilder entlang der Strecke – auf sein intelligentes Gerät, dass ihm die schnellste Verbindung vorschlug.[180]

---

[179] Simon/Simon, *Ausgespäht und abgespeichert*, S. 92.

[180] Vgl. O.N., „Wenn sich das Navi verfährt“, *AugsburgerAllgemeine.de*, 26.07.2007, http://www.augsburger-allgemeine.de/panorama/Wenn-sich-das-Navi-verfaehrt-id2814791.html, Zugriff: 29.10.2016.

Dies ist nur eines von unzähligen Beispielen, bei denen sich Nutzende auf das scheinbar allwissende Gerät verlassen und keine eigenen, weiterführenden Überlegungen anstellen. Wie aber funktioniert die GPS-Technologie? Und weiter: Ist sie fehlbar? Oder liegt das Versagen bei Fehlern auf menschlicher Seite?

GPS[181], ein globales Positionierungssystem, ermöglicht es den Menschen über Satelliten, welche im Weltall die Erde umkreisen, die genaue Position eines Gegenstandes festzustellen, der entsprechende Signale an das Satellitensystem aussendet. Dieser Gegenstand kann beispielsweise das bereits erwähnte Navigationssystem, ein Mobiltelefon, ein Smartphone oder eine Smartwatch sein. Die erwähnten Satelliten umkreisen die Erde in einem Orbit mit einem Radius von mehr als 20.000 Kilometern und senden während ihrer Umrundungen unentwegt Daten, die nach einer Reise mit Lichtgeschwindigkeit von den Endgeräten auf der Erde empfangen werden und dadurch mit diesen in den Dialog treten. Durch diesen Dialog, den das mobile Endgerät als GPS-Empfänger mit mehreren Satelliten innerhalb von Tausendstelsekunden führt, lassen sich Standort und zurückgelegte Strecken exakt berechnen.[182]

Neben dieser Möglichkeit der Navigation ist GPS vielseitig einsetzbar. Gebrauchsgegenstände lassen sich unter anderem mit GPS-Sensoren versehen, die die Position selbiger messen und im Falle eines Diebstahls geortet und wiedergefunden werden könnten. Beispielsweise bietet das amerikanische Unternehmen *Spreon* mit *SkyLINK* seit 2012 eine eingebaute GPS-Überwachung für Autos und Motorräder an, die mit der staatlichen Polizei zusammenarbeitet und verspricht, gestohlene Fahrzeuge innerhalb weniger Minuten wieder aufzufinden.[183]

> „K. ist auf dieser Strecke noch nie gefahren, aber ihre Eintönigkeit sprengt ihn an. Auf der transparenten Lärmschutzwand begleitet ihn ein mobiler Werbespot, er läuft K.s Wagen im konstanten Abstand von zehn Metern voraus. K. fragt sich, warum das nicht längst verboten ist, man hört doch immer wieder von den Unfällen. Aber ohne Sponsoring wäre der Straßenbau längst nicht mehr zu finanzieren. K. geht vom Gas, der Spot passt sich an. K. beschleunigt stark – ein unangenehmer Brummton. Sofort bremst K., doch zu spät. Der zweite Ton ist bereits ertönt. Noch während K. flucht,

---

181 GPS ist die internationale Abkürzung für “global positioning system“. Vgl. Hardens, Immo, *Die elektronische Überwachung von Straffälligen. Entwicklungen, Anwendungsbereiche und Erfahrungen in Deutschland und im europäischen Verlgeich*. Mönchengladbach: Forum Verlag Godesberg 2014.

182 Vgl. Simon/Simon, *Ausgespäht und abgespeichert,* S. 191.

183 Vgl. O.N., „SkyLINK: The Next Generation in Theft Recovery.“, http://www.myskylink.com/, Zugriff: 29.10.2016.

> übermittelt sein GPS-Logger per Mobilfunk die Meldung der Übertretung an die Behörde. Unverzüglich und automatisch ergeht eine Zahlungsaufforderung an K.s Postfach. Sollte eine andere Person sein Fahrzeug gelenkt haben, solle er diese angeben. Eine zweite Mail ergeht an die Versicherung, die K. tags darauf einen Minuspunkt einträgt und seine Prämie »anpasst«.“[184]

Dieses Beispiel von Simon und Simon lässt erkennen, dass die Möglichkeit der GPS-Überwachung allein im automobilen Bereich unzählige Nutzungsmöglichkeiten mit sich bringt. Sicherheitsrisikos durch Geschwindigkeitsübertretungen oder zu nahes Auffahren an das voranfahrende Fahrzeug könnten so durch nachfolgende Strafen möglicherweise noch besser als bisher unterbunden werden. Hierbei steht jedoch nicht nur die Sicherheit der Beteiligten im Vordergrund. Im genannten Beispiel nutzen auch die Werbe- und die Versicherungsindustrie die Daten, die durch die GPS-Überwachung gewonnen werden – hier rückt allerdings die Sicherheit des Fahrers in den Hintergrund und der kommerzielle Anreiz drängt sich in den Vordergrund. Wo beispielsweise bisher Policen nur im Falle eines tatsächlichen Unfalls erhöht wurden, wird der Betrag im Beispiel bei K. bereits präventiv angepasst.

Auch wenn die Nutzenden durch unterschiedliche Privatsphäreeinstellungen an Smartphones oder ähnlichen mobilen Endgeräten die Verdatung ihres Standortes und Bewegungsprofils meist unbewusst zulassen, so können Standorte auch bewusst freiwillig verdatet werden. Anders Albrechtslund beschreibt 2008 das Phänomen des *Geographical Tagging*[185] als einen einfachen Weg, um Medien geografische Information hinzuzufügen. Soziale Netzwerke und damit verbundene Formen der Online-Dienstleistung, die Geotagging unterstützen, legen den Grundstein für eine ortsbasierte Folksonomie.[186] Als aktuelles Beispiel lässt sich hierfür unter anderem das Geotagging auf dem sozialen Netzwerk *facebook.com* erläutern. Durch Hilfe von GPS ortet das Smartphone den aktuellen Standort von Personen, die diesen Dienst nutzen wollen. Diese Information kann dann direkt mit dem Umfeld im sozialen Online-Netzwerk geteilt werden. Abgesehen von Diensten wie *facebook.com*, bei welchen geographische Informationen nicht zwangsläufig die Nutzung des Services beeinflussen, beschreibt Albrechtslund auch sogenannte „MoSoSo – Mobile Social Software“[187], die in der

---

184 Simon/Simon, *Ausgespäht und abgespeichert*, S. 195.

185 *Geographical Tagging* wird im Folgenden auch mit der von Albrechtslund verwendeten Abkürung *Geotagging* synonym gesetzt.

186 Vgl. Albrechtslund, „Online social networking as participatory surveillance“.

187 Ebd..

Verwendung des persönlichen Standortes eine Grundbedingung sieht. Hierzu gehören vor allem Netzwerke und Programme, die sich mit Dingen aus dem räumlichen Umfeld einer Person befassen - etwa Online-Dating- oder Sharing-Portale. So zeigt die Dating-App *Tinder*[188] den Nutzenden beispielsweise an, wie weit entfernt sich ein potentieller Partner aufhält. Die Dating-App *happn*[189] geht hier noch einen Schritt weiter und zeigt den Suchenden ohnehin nur mögliche Personen an, die sich in einem Umkreis von 250 Metern aufhalten.[190] Möglichkeiten wie diese wären ohne metergenaue Standortbestimmung durch GPS nicht denkbar.

3.3.3 Biometrische Daten

Als der amerikanische Fotograf Steve McCurry 2002 nach Pakistan reiste, um das Mädchen wiederzufinden, das er fast 20 Jahre zuvor als »Afghan Girl« für das Titelbild von *National Geographic* fotografiert hatte, schien die Suche aussichtslos. Doch die junge Frau konnte tatsächlich wiedergefunden werden. Mithilfe des Vergleichs von Irismerkmalen war es möglich, das Mädchen nach der vergangenen Zeit zu identifizieren.[191] Da die Technologie in den 2000ern bereits so weit entwickelt war, stellt sich die Frage, welche technischen Möglichkeiten diesbezüglich heute gegeben sind und welche Merkmale die biometrischen Verfahren erkennen können.

> „Unter biometrischen Verfahren sind alle technischen Methoden zu verstehen, die geeignet sein können, aufgrund biologischer Merkmale Personen zu identifizieren oder die Identifikation erheblich zu erleichtern (Biometrie). Insbesondere sind Fingerabdrucke, DNA-Spuren, Iris-Muster, sonstige Gesichtsmerkmale, Zusammensetzung der Stimme darunter zu verstehen.“[192]

Mit diesen Worten definierte die Österreichische Organisation für Datenschutz bereits 2002 biometrische Verfahren zu Identifikation von Personen. Schon seit der Erfindung

---

188 O.N., „Tinder“, https://www.gotinder.com/, Zugriff: 12.01.2017.
189 O.N., „happn“, https://www.happn.com/de/, Zugriff: 12.01.2017.
190 Britz, Paul-Christian, „Ich will jetzt sofort einen Flirt“, *zeit.de*, 22.08.2014, http://www.zeit.de/digital/mobil/2014-08/app-test-happn-dating-tinder, Zugriff: 29.10.2016.
191 Vgl. Daugman, John, „How the Afghan Girl was Identified by Her Iris Pattern“, *University of Cambridge Computer Laboratory*, http://www.cl.cam.ac.uk/~jgd1000/afghan.html, Zugriff: 30.10.2016.
192 O.N., „Schaffung geeigneter Regelungen zur Videoverwendung (Aufzeichnung/Überwachung) und zur Biometrie“, *ARGE DATEN Privacy Service*, 02.11.2002, http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=11563vpp, Zugriff: 17.10.2016.

der Fotografie werden ähnliche genannte Verfahren eingesetzt, um Personen wiederzuerkennen.[193]

Heutzutage werden die biometrischen Verfahren beispielsweise an Flughäfen vor allem zur Bekämpfung des internationalen Terrorismus[194] eingesetzt. Hierbei werden aktuelle Momentaufnahmen mit Inhalten einer Referenzdatenbank verglichen, um Ähnlichkeiten oder Übereinstimmungen festzustellen. Allerdings sind Messfehler oder Veränderungen am Körper der beobachteten Person nicht auszuschließen und bilden ein hohes Risiko der fehlerhaften Erkennung.[195] Diese Art der Überwachung lässt sich gut mit den in 2.2.2.2 erwähnten *data doubles,* die von Haggerty und Ericson beschrieben wurden, in Verbindung bringen. Auch Diana Gordons Idee einer Datenbank, in der sich alle bereits gesammelten Informationen über eine Person bei Bedarf einfach abrufen lassen (vgl. 2.2.1.1), liegt bei der Sammlung von biometrischen Daten nahe. Die gesammelten Daten lassen sich in Bezug auf die Post-Privacy Debatte auch in den großen Pool von Big Data eingliedern.

Praktische Verwendung von biometrischen Personenerkennungsverfahren findet im alltäglichen Leben aktuell vor allem der Fingerabdruck. Nicht nur für Fahndungslisten oder biometrische Reisepässe finden Fingerabdrücke Fürsprache. Der Trend geht bereits seit einigen Jahren zur Nutzung des Fingers als personalisierter Schlüssel für Smartphones, Laptops und Schlösser von beispielsweise Türen und Autos. Zwar stellt ein Fingerabdruck eine gewisse Einmaligkeit dar, aber auch ein einmaliges Objekt kann täuschend echt kopiert werden. Daher bieten auch scheinbar einbruchsichere, biometrische Schlösser keine absolute Sicherheit vor unwillkommenen Eindringlingen. Der britische Autor Richard Austin Freeman beschrieb bereits 1907 in einem Detektivroman[196] eine Methode zum Kopieren von Fingerabdrücken, mithilfe von Gelatinefolie. Bei Untersuchungen ließen sich im Jahre 2008 drei viertel der handelsüblichen elektronischen Geräte mit kopierten Fingerabdrücken aus Gelatine täuschen.[197] Welche Auswirkungen diese Tatsache auf das Smart Home hat, in dem der Fingerabdruck möglicherweise als Schlüssel verwendet werden kann, wird in der folgenden Analyse herausgestellt.

---

193 Vgl. Schaar, Peter, *Das Ende der Privatsphäre: Der Weg in die Überwachungsgesellschaft*, München: Bertelsmann 2007, S. 81.

194 Die Daten des biometrischen Reisepasses, der nach den Terroranschlägen des 11. Septembers 2001 von amerikanischen Behörden gefordert und durchgesetzt wurde, können von ausländischen Behörden ausgelesen werden.

195 Vgl. Schaar, *Das Ende der Privatsphäre*, S. 76f.

196 „The Red Thumb Mark (Dr. Thorndyke Mysteries #1)".

197 Vgl. Simon/Simon, *Ausgespäht und abgespeichert*, S. 203.

3.3.4 Persönliches Kundenprofil

Kundendatenbanken oder Kundenkarten stellen kein Novum dar, das durch das Internet der Dinge eingeführt wurde. Viel mehr speichern Unternehmen seit Jahrzehnten Kontaktdaten und Informationen über das Kaufverhalten ihrer treuen Kunden und machen mit Hilfe von angepassten Rabattaktionen aus Kunden Stammkunden.[198] Auch wenn die Grundidee nicht neu ist, so bringen vor allem elektronische Kundenkarten einige entscheidende Neuerungen mit sich. Für scheinbare Rabatte bezahlen die Einkaufenden mit ihren persönlichen Daten, die vom verkaufenden Unternehmen ausgewertet und marketingtechnisch weiterverwendet werden.[199]

> „Jedes Mal, wenn Sie fortan Ihre Kundendaten in einer Filiale vorweisen oder mit Ihrer registrierten Geld- oder Kreditkarte zahlen, wird gespeichert, wann, wo und was sie gekauft haben.“[200]

Ähnlich wie mit elektronischen Kundenkarten verhält es sich beim Einkaufen im Internet. Einkaufende sind zwangsläufig gezwungen, ein persönliches Kundenprofil mit allen vom Unternehmen geforderten Daten anzulegen. Nur so können sie das gewünschte Produkt kaufen. Während sich die Preisgabe von persönlichen Kundendaten beim Einkauf im Einzelhandel beim Verweigern einer Kundenkarte und unter der Verwendung von Bargeld scheinbar noch vermeiden lässt, so ist diese Möglichkeit des anonymen Einkaufens im World Wide Web nie gegeben. Name, E-Mailadresse, Lieferadresse, Alter und Bankverbindung sind Daten, deren Angabe sich in keinem Online-Shop umgehen lässt.[201] Durch die, sei es durch Kundenkarten oder Kundenprofile in Online-Shops, freiwillig bereitgestellten Daten, lassen sich sogenannte persönliche Kundenprofile erstellen, die sich immer mehr der Kontrolle der einzelnen Einkaufenden entziehen.[202] Beispielsweise kann personalisierte Werbung nun anhand der Kundendaten und des Kaufverhaltens an die angegeben Kontaktdaten versendet werden. Neben einer größtenteils unerwünschten Flut an Werbung kann die Verwendung von Kundenkarten oder Online-Kundenprofilen aber auch weit größere Folgen nach sich

198 Vgl. Ebd., S. 266.
199 Vgl. Ebd., S. 267.
200 Ebd., S. 266.
201 Auch wenn die Möglichkeit der elektronischen Bezahlung umgangen wird und stattdessen beispielsweise eine Zahlung per Nachnahme erfolgt, ist ein anonymisierter Bestellvorgang aus Gründen der persönlichen Zustellung meist unmöglich.
202 Vgl. Schaar, *Das Ende der Privatsphäre,* S. 188.

ziehen. Auch wenn die Weitergabe der persönlichen Daten der Kunden und Kundinnen an Dritte vertraglich verboten ist, so beklagen Verbraucherschützer dennoch immer öfter Datenmissbrauch. Beispielsweise verwenden Behörden bereits seit längerer Zeit personenbezogene Konsumentendaten, zum Teil aus Supermärkten oder Online-Shops, um verdächtige Personen zu beobachten und ihr Handeln zu hinterfragen. Über diese Form der Überwachung und Kontrolle berichtete zum Beispiel die Organisation *FoeBuD e.V.* im Jahr 2007 anhand eines Falles aus der Schweiz. Hier wurden 139 Inhaber der Kundenkarte eines Supermarktes persönlich von der Polizei aufgesucht, da alle von ihnen das gleiche Werkzeug gekauft hatten, mit dem kurze Zeit später ein Einbruch verübt wurde.[203]

Auch durch technologische Neuerungen des Internet der Dinge fanden und finden im Bereich der persönlichen Kundenprofile signifikante Veränderungen statt. Auf einige dieser Neuerungen im Bereich des Smart Home wird in der folgenden Analyse genauer eingegangen.

[203] Vgl. O.N., „Geschäfte mit dem gläsernen Kunden“, *FoeBuD e.V.*, 07.06.2005, https://archiv.foebud.org/pc/docs/pc_sz050607_geschaefteMitDemGlaesernenKunden.html, Zugriff: 29.10.2016.

4 Analyse

> „Since these devices are smart and communicate with each other mainly via wireless links, security must be ensured. Otherwise the smart devices deployed around us would come back to hurt us and the result would be catastrophic.“[204]

Eine Studie, die im Dezember 2014 von der Organisation Bitkom[205] durchgeführt wurde, ergab, dass 51 % der befragten Personen wissen, was der Begriff des Smart Homes zu bedeuten hat.[206] Außerdem stellte sich heraus, dass jede siebte befragte Person bereits wissentlich NutzerIn einer Smart-Home-Anwendung ist[207] und wiederrum fast 80 % dieser Nutzenden in keinem Fall mehr bereit sind, auf das Internet der Dinge in ihrem Zuhause zu verzichten.[208]

Was aber nun ist das Smart Home, das mittlerweile zum Buzzword des 21. Jahrhunderts geworden ist? Zunächst lässt sich feststellen, dass trotz allgemeiner Verbreitung noch immer keine einheitliche Begrifflichkeit zur Nennung der neuartigen Technologie festgelegt werden kann – Connected Home, Intelligentes Wohnen, Smart House, Elektronisches Haus und Smart Home[209]. Dies sind nur einige von unzähligen Bezeichnungen, die für das vernetzte Heim im Umlauf sind; eine Vereinheitlichung gibt es noch nicht. Obwohl das Smart Home bereits als „Wohnform des 21. Jahrhunderts“[210] betitelt wird und laut Hochrechnungen bereits 2020, also in weniger als drei Jahren, weltweit mehr als 50 Milliarden Geräte miteinander vernetzt sein sollen, ist der deutschsprachige Raum von einer Durchdringung des Marktes mit Lösungen für ein intelligentes Zuhause jedoch noch weit entfernt.[211] Die Gründe dafür stellte die Organisation Bitkom bereits 2014 durch eine Umfrage heraus. Als häufigsten Grund

---

204 Wang, Jun/Yaling Yang/William Yurcik, *Secure Smart Environments: Security Requirements, Challenges and Experiences in Pervasive Computing*, 2005, http://citeseer.ist.psu.edu/viewdoc/download?doi=10.1.1.60.4730&rep=rep1&type=pdf, Zugriff: 13.07.2016, S. 1.

205 Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

206 Vgl. Illek, Christian P., „Smart Home in Deutschland“, *BITKOM – Bundesverband für Informationswirtschaft, Telekommunikation und neue Medien e.V.*, 18.12.2014, https://www.bitkom.org/Publikationen/2014/Studien/Smart-Home-in-Deutschland-Praesentation/Praesentation-Smart-Home.pdf, Zugriff: 13.07.2016, S. 2.

207 Vgl. Ebd., S. 4.

208 Vgl. Ebd., S. 6.

209 Vgl. Glasberg, Ronald, „Studienreihe zur Heimvernetzung. Konstumennutzen und persönlicher Komfort“, *BITKOM - Bundesverband für Informationswirtschaft, Telekommunikation und neue Medien e.V.*, Oktober 2008, https://www.bitkom.org/Publikationen/2008/Leitfaden/BITKOM-Studie-Konsumentennutzen-und-persoenlicher-Komfort/Studie-Konsumentennutzen.pdf, Zugriff: 02.11.2016, S. 8.

210 Kulick, Christian, „Wohnform des 21. Jahrhunderts – neue Smart-Home-Studie“, *BITKOM - Bundesverband für Informationswirtschaft, Telekommunikation und neue Medien e.V.*, 2015, https://www.bitkom.org/Themen/Internet-Telekommunikation-Netze/Smart-Home/SmartHome-Studie15.html, Zugriff: 02.11.2016.

211 Vgl. Ebd..

für ein Ablehnen der neuen Technologie, gaben die Befragten an, dass ihnen der Einbau zu aufwändig, die Bedienung der Geräte zu kompliziert und die smarten Geräte im Allgemeinen zu teuer sind. Neben diesen materiellen und praktischen Gründen gaben rund ein Viertel der befragten Smart Home-Gegner an, dass sie das Smart Home aus Angst um ihre Privatsphäre ablehnen.[212] Mit der Frage nach der Privatsphäre im Smart Home befasst sich die folgende Analyse.

4.1 Ausgangslage – Internet der Dinge

> „Das Internet der Dinge, so seine Konstrukteure/Architekten/Ingenieure, werde einer Revolution gleichen. Es stehe in einer Reihe mit dem Faustkeil, dem Rad und dem Verbrennungsmotor und werde uns mit einem enormen Zuwachs an Sicherheit und Lebensqualität beeindrucken. Endlich sei es möglich, von der Waschmaschine im Keller zu erfahren, wann sie fertig sei, vom Kühlschrank über die Haltbarkeit der Milch informiert zu werden und von der Barbiepuppe über die geheimen Wünsche des Nachwuchses auf dem Laufen gehalten zu werden.“[213]

Die deutsche Kulturwissenschaftlerin Natascha Adamowsky bringt hier zum Ausdruck, welche Bedeutung dem Internet der Dinge zugemessen wird. Was auf den ersten Blick »nur« wie eine Reihe von technischen Alltagserleichterungen erscheinen mag, wird von Adamowsky in eine Riege mit der Entwicklung des Rades und des Feuers gestellt – zwei der Entdeckungen, die das menschliche Leben wie nur wenige andere beeinflusst und geprägt haben. Aus den bisherigen Darstellungen und Definitionen über das Internet der Dinge in dieser und anderen Abhandlungen ergeben sich mehrere grundlegende Eigenschaften die das IoT innehaben muss.

Ein sehr häufig genannter Begriff in diesem Zusammenhang ist das Netz oder Netzwerk. Daher spielt der Terminus der Konnektivität bei der Definition des Internet der Dinge die vielleicht wichtigste Rolle. Das Internet der Dinge lässt sich als hybrides „Netz aus Netzwerken“[214] beschreiben, das erst durch diese Struktur einzigartig wird. Allgegenwertige Kommunikation wird in diesem Netz ermöglicht. Des Weiteren stellen diese Netzwerke nicht nur Verbindungen untereinander her, sondern nähern sich

---

212 Vgl. Illek, „Smart Home in Deutschland“, S. 6.

213 Adamowsky, Natascha, „Vom Internet zum Internet der Dinge. Die neue Episteme und wir“, in: *Internet der Dinge: Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt*, Hg. Christoph Engemann, Florian Sprenger, Bielefeld: transcript (Digitale Gesellschaft) 2015, S. 121.

214 Evans, Dave, „Das Internet der Dinge. So verändert die nächste Dimension des Internet die Welt“, *Cisco*, April 2011, http://www.cisco.com/c/dam/global/de_de/assets/executives/pdf/Internet_of_Things_IoT_IBSG_0411FINAL.pdf, Zugriff: 04.11.2016, S. 4.

einander auch immer mehr an. Konvergenz[215] der einzelnen technischen Neuerungen untereinander ist daher wichtig. Neben diesen grundlegenden Softwareeigenschaften spielt auch die Hardware eine wichtige Rolle bei der Definition. Bereits Mark Weiser wies darauf hin, wie wichtig die kleine Größe der technischen Gadgets ist.[216] Daher ist die Miniaturisierung[217] der Technik ein wichtiger Punkt, der erfüllt sein muss. Des Weiteren spielt nach Weiser die Positionierung des IoT-Netzwerkteils eine wichtige Rolle.[218] Vor allem sollte die Technik eine gewisse Mobilität aufweisen, um sich den unterschiedlichsten räumlichen Gegebenheiten anpassen zu können. Das Internet der Dinge ist ubiquitär[219] und daher nicht zwingend an einen festen Standort gebunden. Vor allem diese Allgegenwärtigkeit wirkt zu Beginn auf (potentielle) Nutzende möglicherweise einschüchternd. Die Hardware muss jedoch nicht nur mobil, klein, handlich und allgegenwärtig sein sondern auch für Laien benutzbar bleiben. Consumer Hardware muss leicht verständlich und einfach bedienbar sein. Aus diesem Grund sollte die technische Neuerung auch eine innovative, intuitive Benutzungsschnittstelle[220] aufweisen, die problemlos in den Alltag der Nutzenden integriert und deren Bedienung unauffällig in den alltäglichen Rhythmus und Gewohnheiten eingegliedert werden kann. Zu dieser innovativen Benutzungsschnittstelle ist auch die Tatsache zu rechnen, dass das Internet der Dinge in manchen Fällen nicht wirklich vom Nutzenden selbst und wissentlich bedient werden muss. Die automatische Erfassung von Kontexten und anschließende Selbstorganisation[221] spielt in diesem Zusammenhang eine einschneidende Rolle in der Nutzung. Oft verfügen die technischen Gadgets des IoT über eine ausgeprägte Sensorik, die durch zuvor vorgenommene Programmierung eigenständig Informationen aufnimmt, sammelt, auswertet und dann anschließend dementsprechend dem intelligenten Gegenstand ein eigenständiges Handlungsmuster vorgibt,

---

215 Vgl. Botthof, Alfons/Marc Bovenschulte (Hg.), „Das »Internet der Dinge«. Die Informatisierung der Arbeitswelt und des Alltags“, *Hans Böckler Stiftung*, Juli 2009, http://ernaehrungsdenkwerkstatt.de/fileadmin/user_upload/EDWText/TextElemente/Medien/RFID_Internet_der_Dinge_Arbeit_Alltag_Boeckler_2009.pdf, Zugriff: 08.11.2016, S. 11.

216 Vgl. Weiser, „The Computer for the 21st Century“, S. 5.

217 Vgl. Botthof/Bovenschulte (Hg.), „Das »Internet der Dinge«“, S. 11.

218 Vgl. Weiser, „The Computer for the 21st Century“, S. 5.

219 Vgl. Dworschak, Bernd/Helmut Zaiser/Leif Brand/Lars Windelband, „Qualifikationsentwicklung durch das Internet der Dinge und dessen Umsetzung in der Praxis“, in: *Qualifikationsentwicklungen durch das Internet der Dinge. Trends in Logistik, Industrie und „Smart House“,* Hg. Lothar Abicht, Georg Spöttl, Bielefeld: W. Bertelsmann Verlag 2012, S. 7.

220 Vgl. Wende, Jörg, „Die fünf Dimensionen des Internets der Dinge (Internet of Things – IoT)“, *IBM advertorial – Online Themenspecial IT-Trends 2014: BigData/Hadoop und Internet der Dinge*, 2014, https://www-935.ibm.com/services/multimedia/Die_5_dimensionen_von_IoT_WUO12360DEDE.pdf, Zugriff: 08.11.2016, S. 3.

221 Vgl. Botthof/Bovenschulte (Hg.), „Das »Internet der Dinge«“, S. 11.

dem dieser dann folgen kann. Auch die Möglichkeit der Personalisierung[222] spielt in allen Bereichen des IoT eine ausschlaggebende Rolle. Durch individuelle Programmierung und automatische Kontexterfassung können und sollen Nutzende die technischen Hilfsmittel an ihr persönliches Umfeld und Leben anpassen.

4.1.1 Vorgehen

Im Folgenden findet nun die Analyse des Gegenstandes Smart Home anhand der in Punkt 2.3 herausgestellten Methoden statt. Nach einem kurzen Definitionsversuch des zu analysierenden Sujets wird genauer auf die soziologischen Aspekte eingegangen. Es wird versucht, die Theorien von David Lyon und Zygmunt Bauman auf das Smart Home zu projizieren. Schlagworte, die es diesbezüglich zu thematisieren gilt, sind wie bereits erwähnt, moderne/flüchtige Überwachung, Freiwilligkeit, Selbsttermination, die Gefühlswelt der Überwachten und die Begrifflichkeit der lateralen Überwachung. Darauffolgend beginnt die Analyse des medialen Überwachungsansatzes im Smart Home. Hierbei wird anhand von Anwendungsbeispielen, die im Smart Home zu finden sind, auf die bereits erarbeiteten Aspekte aus 2.3.2 eingegangen. Hauptaugenmerkt liegt auf der Überwachung durch biometrische Daten, GPS-Tracking, RFID-Technologie und dem Dasein des Menschen als Kunde in Zeiten von gespeicherten Kundenprofilen und Big Data. Nach den ersten beiden Teilen der Analyse, die größtenteils sachlich gegliedert auf literarischen, geordneten Quellen aufbauen, macht der letzte Teil der Forschungsmethode eher den Eindruck einer „losen Themensammlung“ [223], was dem aktuellen Forschungsstand der Post-Privacy geschuldet ist. Ausschlaggebendes Thema dieses Analyseteils stellt daher neben dem Begriff der Privatheit und der zeitlichen Einordnung das Schlagwort des Kontrollverlustes dar. Angefangen mit der Frage, welche Daten die Bewohnenden des intelligenten Hauses produzieren, bis hin zur Überlegung was mit den erzeugten Datenmengen passiert und wo der Kontrollverlust über besagte Daten beginnt.

---

[222] Vgl. Jeschke, Sabina/Tammo Andersch/Karsten Schulze/Dorothée Fritsch/Katherina Marquardt/Tobias Meisen/Anja Richert/Max Hoffmann/Christian Tummel, „Industrie 4.0 *ante Portas.* Praradigmenwechsel im deutschen Maschienen- und Anlagebau“, in: *Internet der Dinge: Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt*, Hg. Christoph Engemann, Florian Sprenger, Bielefeld: transcript (Digitale Gesellschaft) 2015, S. 268f.

[223] Seemann, „Was ist Postprivacy (für mich)?“.

4.1.2 Smart Home

Eine der wohl ältesten bekannten Definitionen für das Smart Home äußerte R. Lutolf bereits im Jahr 1992:

> „The Smart Home concept is the integration of different services within a home by using a common communication system. It assures an economic, secure and comfortable operation of the home and includes a high degree of intelligent functionality and flexibility.“[224]

Seit dieser Äußerung wird von den unterschiedlichsten Seiten versucht eine passende Definition für das Smart Home zu finden. Da diese Definitionsversuche alle gewisse Ähnlichkeit miteinander aufweisen und sich nicht grundlegend unterscheiden, ist es sinnvoll, keine Liste von Definitionen anzuhäufen, sondern sie durch ihre wichtigsten Schlagworte zusammenzufassen. Lutolf beginnt durch seine Definition diese Aufzählung bereits mit den Stichwörtern *Intelligenz, Vernetzung/Vereinigung, Kommunikation, Wirtschaftlichkeit, Sicherheit, Lebensqualität* und *Funktionalität.* Erwähnenswerte Punkte sind außerdem die *Automatisierung von Arbeitsabläufen* und *effizientere Energienutzung*.[225]

> „Auch die Wohnung als Inbegriff eines lokalen Privatbereichs verändert im Zeitalter allgegenwärtiger Informationstechnik ihren Charakter. Die intelligente Haustechnik verbindet das Zuhause mit dem weltweiten Netz wie auch dem Supermarkt um die Ecke. Smart-Home-Szenarien konzipieren den privaten Wohnbereich als Ort der Integration in den *außer*häuslichen Bereich, hier gilt das Heim als Integrationszentrum.“[226]

Jessica Heesen beschreibt, wie privater Wohnraum im Informationszeitalter seinen Charakter ändert. Um festzulegen, welche einzelnen Bereiche sich genau verändern, bieten Changmin Lee et al. in ihrer Abhandlung von 2014 eine mögliche Ordnung an.

---

[224] Lutolf, R., „Smart Home Concept and the Integration of Energy Meters into a Home Based System,“ in: *Proceedings of the Seventh International Conference on Metering Apparatus and Tariffs for Electricity Supply* 367, November 1992, S. 277.

[225] Vgl. Kulick, Christian, „Vor dem Boom – Marktaussichten für Smart Home“, *BITKOM - Bundesverband für Informationswirtschaft, Telekommunikation und neue Medien e.V.,* 23.10.2014, https://www.bitkom.org/Publikationen/2014/Studien/Marktaussichten-fuer-Smart-Home/141023-Marktaussichten-SmartHome.pdf, Zugriff: 02.11.2016, S. 8.

[226] Heesen, Jessica, „Keine Freiheit ohne Privatsphäre. Wandel und Wahrung des Privaten in informationstechnisch bestimmten Lebenswelten“, in: *1984.exe – Gesellschaftliche und juristische Aspekte moderner Überwachungstechnologien*, Hg. Sandro Gaycken, Constanze Kurz, Bielefeld: transcript Verlag 2008, S. 238.

Erster genannter Punkt ist hierbei die automatische, intelligente Steuerung der Beleuchtung im Wohnraum, die sich an das Tageslicht, die Personen im Raum und ihre Bedürfnisse anpasst. Als zweites werden intelligente Haushaltsgeräte genannt. Exemplarisch sind hier smarte Kühlschränke anzuführen, die ein Signal senden, sobald sich beispielsweise die Milch dem Ende ihres Haltbarkeitsdatums nähert und anschließend selbstständig neue Milch bestellen, oder ein Wäschetrockner, der sich online über die Tageszeit mit den kostengünstigsten Strompreisen informiert und sich dann danach selbst steuert. Auch die Unterhaltung der Bewohnenden des Smart Homes ist als wichtiger Punkt zu nennen. Nach Lee et. al. verfügt das intelligente Haus über ein verknüpftes Entertainmentsystem, auf das von überall im Haus zugegriffen werden kann. Den vierten Punkt bildet die Sicherheit der Wohnenden. Die Bandbreite der Möglichkeiten erstreckt sich hier über Rauchmelder, biometrische Schlüssel und Überwachungskameras bis hin zu Bewegungsmeldern, die an das Kommunikationssystem des Hauses gekoppelt sind und den Bewohnenden oder der Polizei automatisch Bericht erstatten. Des Weiteren bildet die Regulierung des Klimas einen wichtigen Bereich im Smart Home. Hierbei handeln Heizung und Klimaanlage selbstständig intelligent und passen die Temperatur an die äußeren Gegebenheiten und die Bedürfnisse der Bewohnenden an. Abschließend wird von Lee die Unterstützung im Haushalt genannt. Durch ein intelligentes Zuhause können Personen, die aufgrund von Alter oder körperlichen Beeinträchtigungen Hilfe benötigen, im Alltag unterstützt werden. So ist es beispielsweise möglich, dass ein intelligenter Fußboden selbst Hilfe verständigt, wenn er registriert, dass eine Person niedergefallen ist und nicht mehr selbstständig aufstehen kann.[227]

All diese unterschiedlichen Bereiche funktionieren durch verschiedene Sensoren, die teilweise nicht miteinander verbunden sind und auch unabhängig voneinander funktionieren können. Dennoch ist es wichtig, das Smart Home nicht als eine Ansammlung von einzelnen, alleinstehenden Bereichen zu verstehen. Es ist vielmehr ein heterogenes Netz aus vielen unterschiedlichen Sensoren, Detektoren und Informationen, die miteinander kommunizieren können, es aber nicht müssen.

---

[227] Vgl. Lee, Changmin/Luca Zappaterra/Kwanghee Choi/Heyeong-Ah Choi, „Securing Smart Home: Technologies, Security Challenges, and Security Requirements“, in: *Proceedings of the IEEE Conference on Communications and Network Security*, Oktober 2014, S. 68.

4.2 Soziologischer Ansatz

Im Folgenden wird das Smart Home hinsichtlich der bereits herausgestellten soziologischen Fragestellungen untersucht. Zygmunt Baumans Vorstellung der flüchtigen Moderne und der in ihr stattfindenden flüchtigen Überwachung steht in diesem Teil der Analyse neben dem Sujet der Freiwilligkeit, dem Begriff der Gefühlswelt und der lateralen Überwachung im Mittelpunkt.

4.2.1 Flüchtige Moderne / Flüchtige Überwachung

Zygmunt Bauman spricht im Dialog mit David Lyon davon, dass postmoderne Menschen in der „schönen neuen flüchtig-modernen Welt ihr jeweils persönliches Panoptikum selbst hervorbringen und auf dem eigenen Buckel mitschleppen“[228]. Diese Aussage tätigte Bauman in Hinsicht auf die flächendeckende Verbreitung des Smartphones, vor allem unter Geschäftsleuten, die durch ständige Erreichbarkeit ihren eigenen kleinen Apparat der Überwachung in der Hemdtasche bei sich tragen.
Nun stellt sich die Frage, ob sich dieses Konzept des flüchtigen Überwachungsapparates, mit dem die Menschen sich freiwillig überwachen lassen und sich gleichzeitig auch selbst überwachen, auch auf das Smart Home übertragen lässt. Hierbei sind einige Eigenschaften zu beachten, die Bauman als grundlegend für die Überwachung der flüchtigen Moderne definierend festlegt.
Im Gegensatz zum klassischen Panoptikum nach Bentham, bei dem der Wärter von einem festen Punkt in der Mitte des runden Gebäudes aus überwacht, gibt es in Baumans flüchtig-moderner Version keinen verorteten Fixpunkt mehr, von dem aus der Vorgang der Überwachung stattfindet.[229] Stattdessen findet der Akt der Überwachung von mehreren, möglicherweise unzähligen, einzelnen Punkten im Smart Home statt. Des Weiteren sind auch diese vielen Überwachungsstationen nicht unbedingt fixiert. Wie bereits in 4.1 festgestellt, zeichnet sich das Internet der Dinge durch Miniaturisierung und Mobilität aus. Die einzelnen Gegenstände der Überwachung können sich also im Smart Home frei bewegen oder von den Bewohnenden bewegt werden. Ein weiterer Schwerpunkt, der laut Bauman die flüchtige Moderne ausmacht und diese von der soliden Moderne unterscheidet, ist die Verflüchtigung von sozialen und zwischenmenschlichen Beziehungen.[230] Hier stellt sich die Frage, wie sich dieser Zerfall

[228] Bauman/Lyon, *Daten, Drohnen, Disziplin*, S. 78.
[229] Vgl. Ebd., S. 22ff.
[230] Vgl. Ebd., S. 21.

der menschlichen Kontakte in den technischen Strukturen des Smart Home wiederfinden lässt. Zum einen lassen sich durch die technologischen Gadgets, die den Nutzenden im Smart Home das Leben erleichtern sollen, einige zwischenmenschliche Begegnungen feststellen, die eliminiert werden können. Beispielhaft sind hier jene zufällige Zusammentreffen beim Einkaufen von Lebensmitteln oder anderen alltäglichen Gegenständen anführen. Wo in der soliden Moderne der physische Weg in den Einzelhandel stattfand, bestellt möglicherweise schon morgen der intelligente Kühlschrank neue Milch und der smarte Toilettenrollenhalter neues Papier. Zwischenmenschlicher Zusammenstoß beim Einkauf kann also möglicherweise vollständig eliminiert werden. Als weiteres Exempel lässt sich in diesem Zusammenhang der menschlichen Beziehungen *Amazon Echo*[231], das Audio-Wiedergabegerät des Onlinegroßhändlers *Amazon*, anführen. Neben Lautsprecher- und simplen Wiedergabeeigenschaften enthält Amazon Echo den sprachgesteuerten Assistenten *Alexa*[232]. Neben Software wie Apples *Siri* oder Microsofts *Contana* erscheint Alexa nach Aussagen von Eike Kühl, Journalist beim *Zeit Magazin*, „am menschlichsten“[233]. Dies liegt laut Kühl unter anderem daran, dass Alexa nicht nur die Regeln des Smalltalks beherrscht, Witze erzählt und Anspielungen aus der Popkultur versteht, sondern auch weil der Sprachassistent lernfähig ist.[234] Kleine Unterhaltungen werden möglich und ersetzen denkbarerweise den Dialog mit dem Nachbarn über banale Themen wie das Wetter. Des Weiteren lässt sich Amazon Echo mit Smart-Home-Anwendungen verbinden, die dann durch Sprachsteuerung bedient werden können.[235] Auch durch diese Anwendungsmöglichkeit lassen sich kleine Konversationen mit anderen Mitgliedern des Haushaltes umgehen.

Offen bleibt die Frage, wie sehr sich das Smart Home mit dem oft besprochenen Panoptikum vergleichen lässt. Baumans Ansatz, in dem das Smartphone als moderne, „cyborgisierte“[236] Form des Panoptikums vorgestellt wird, lässt sich auf das Beispiel des Smart Home nur teilweise übertragen. Die Ähnlichkeiten in Form der mobilen Überwachung, ohne verortbare Fixpunkte, der Allgegenwärtigkeit und der Abschaf-

---

231 O.N., „Amazon Echo“, *Amazon*, https://www.amazon.de/Amazon-SK705DI-Echo-Schwarz/dp/B01GAGVCUY, Zugriff: 09.11.2016.

232 Vgl. Ebd..

233 Kühl, Eike, „Alexa. Ich bin dein Vater“, *zeit.de*, http://www.zeit.de/digital/mobil/2016-10/amazon-echo-alexa-test-deutschland, Zugriff: 09.11.2016.

234 Vgl. Ebd..

235 Vgl. O.N., „Amazon Echo“.

236 Bauman/Lyon, *Daten, Drohnen, Disziplin*, S. 74.

fung der personifizierten Überwachungsinstanz wurden bereits festgestellt. Unterschiede lassen sich beispielsweise in der räumlichen Ordnung finden. Während beim Mobiltelefon keinerlei räumliche Begrenzung besteht, so erinnert das Smart Home mit seinen abgrenzenden Mauern, die sich vor der Außenwelt verschließen, anfänglich an einen gefängnisartigen Raum, dessen Überwachung man sich durch Verlassen desselbigen entziehen kann. Diese Idee lässt sich allerdings durch genauere Betrachtung als unwahr feststellen. Zwar gibt es Mauern, die den scheinbaren Überwachungsraum begrenzen, aber die Überwachung des Raumes findet über diese Mauern hinweg statt. Beispielsweise geben Smart-Home-Apps, die mithilfe von GPS-Technologie den Standort der Nutzenden orten, diese Informationen an das intelligente Haus weiter. Den Geräten, die sich im Haus befinden, ist es dann möglich festzustellen, wann eine Bewegung in Richtung des Hauses stattfindet. Dort kann dann zum passenden Zeitpunkt beispielsweise die Heizung eingeschalten oder das Abendessen automatisch erwärmt werden.[237] Dies ist nur eines von vielen Beispielen, wie die Überwachung über die Mauern des Hauses hinweg funktioniert und sich daher nicht räumlich beschränken lässt. Daher ist ein Vergleich des Smart Homes mit Baumans Idee des mobilen Panoptikums ohne Zweifel festzustellen.

4.2.2 Freiwilligkeit und Selbsttermination

> „Wir verzichten auf unser Recht auf Privatsphäre und lassen uns freiwillig zur Schlachtbank führen. Möglicherweise stimmen wir dem Verlust der Privatsphäre aber auch zu, weil er ein akzeptabler Preis für das tolle Zeug ist, das wir im Tausch dafür erhalten. Oder aber der Druck, unsere persönliche Autonomie dem Schlachthaus zu überantworten, ist, wie bei einer Herde Schafe, derart übermächtig, daß nur außergewöhnlich rebellische, stolze, kämpferische und willensstarke Menschen in der Lage sind, einen ernsthaften Versuch des Wiederstandes zu unternehmen.“[238]

Eine der wohl wichtigsten Eigenschaften, die der Überwachung im Smart Home innewohnt und die sie von den meisten anderen Formen der Kontrolle unterscheidet, ist die, dass die Nutzenden sie freiwillig zulassen. Daher kann die These aufgestellt werden, dass sie freiwillig auf ihr Recht auf Privatsphäre verzichten. Bauman stellt nach dieser Feststellung auch die Frage in den Raum, ob der Druck, der von außen auf die

---

[237] Vgl. Tunze, Wolfgang, „Smart-Home-Ideen mit Charme“, *faz.net*, 20.09.2013, http://www.faz.net/aktuell/technik-motor/umwelt-technik/intelligenter-haushalt-smart-home-ideen-mit-charme-12575578.html, Zugriff: 11.11.2016.

[238] Bauman/Lyon, *Daten, Drohnen, Disziplin*, S. 35.

Menschen einwirkt, so stark ist, dass sich Nutzende nicht freiwillig dazu entscheiden, sondern stattdessen vielmehr freiwillig vor dem System kapitulieren. Neben selbstterminierter Entscheidung und Kapitulation bleibt allerdings auch noch die Möglichkeit der Unwissenheit. Viele Nutzende gehen „routinemäßig, achtlos und freiwillig“[239] mit ihren Daten und dadurch dem Schutz ihrer Privatsphäre um, weil ihnen die Folgen ihres Handelns schlicht nicht bewusst sind.

Diese Feststellung von Bauman zielt vor allem auf technische Gadgets ab, die sich die Nutzenden freiwillig in ihr Smart Home integrieren, um das alltägliche Leben zu erleichtern oder den Lebensstandard zu heben. Hier ist die Möglichkeit der Unfreiwilligkeit nicht in Frage zu stellen. Was aber geschieht, wenn Betroffene zu Anwendern werden, die möglicherweise nicht mehr selbstterminiert die Entscheidung für die Nutzung eines und die Überwachung durch ein Smart Home treffen können? In Bezug auf den Aspekt der Freiwilligkeit lässt sich daher die Anwendung von *Ambient Assisted Living*[240] untersuchen.

> „AAL beschreibt die Möglichkeit, dass durch eine technische Infrastruktur in Kombination mit „intelligenten Objekten“ eine Umgebung entsteht, die Patienten oder alte gebrechliche Menschen aktiv in ihrem gewohnten Umfeld (Haushalt) unterstützt - das technische System soll sie dabei nicht durch eine Vollautomatisierung entmündigen, sondern ihnen situationsabhängig gleichsam »unter die Arme greifen«.“[241]

Die Begrifflichkeit AAL steht also stellvertretend für die „zunehmende Technisierung der Patientenversorgung“[242] in den Bereichen Gesundheit und Pflege im häuslichen Umfeld. Diese Entwicklung des IoT spielt vor allem im Hinblick auf den demografischen Wandel der westlichen Gesellschaft eine nicht zu ignorierende Rolle.[243] Die Entscheidung für technisierte Unterstützung und Pflege wird in den meisten Fällen nicht von den später Nutzenden selbst getroffen, sondern von Vormunden, die ihnen Entscheidungen dieser Art abnehmen.

Die Möglichkeiten des AAL erstrecken sich bereits heute von Fußböden und Teppichen, die Bewegungen und Stürze wahrnehmen, über elektrische Schließanlagen, die

---

239 Ebd., S. 25.

240 Der Begriff *Ambient Assisted Living* wird im Folgenden auch durch AAL abgekürzt.

241 Botthof/Bovenschulte, „Das »Internet der Dinge«“, S. 51.

242 Ebd..

243 Vgl. Rieger, Stefan, „Smart Homes. Zu einer Medienkultur des Wohnens“, in: *Internet der Dinge: Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt*, Hg. Christoph Engemann, Florian Sprenger, Bielefeld: transcript (Digitale Gesellschaft) 2015, S. 369.

aus der Ferne gesteuert werden können, bis hin zu intelligenten Systemen, die so programmiert sind, dass sie gefährliche Situationen erkennen.[244] „Registriert das System beispielsweise gleichzeitig offene Fenster oder einen angeschalteten Herd während der Bewohner die Haustür von außen verschließt, kann eine Erinnerungsfunktion ausgelöst werden.“[245] Bisher ist es in Systemen dieser Art nicht möglich, eine einheitliche Form der Übermittlung von Notfällen zu gestalten. In Deutschland sind automatisierte Notrufe durch Maschinen, bei den staatlichen Notrufnummern 110 und 112, sogar rechtlich untersagt.[246]

All dies geschieht allein durch die Kontrolle des Smart Home. Durch den Einzug in einen durch AAL unterstützten Wohnraum erklären sich Nutzende dazu bereit, überwacht zu werden und die aufgenommenen Daten mit den InstallateurInnen der Überwachungsgeräte zu teilen. Dies geschieht im speziellen Fall von AAL größtenteils nicht freiwillig durch die Handelnden, da sie sich über den Verlust ihrer Privatsphäre meist nicht im Klaren sind und sein können. Wo heute nahestehende Angehörige und vertraute Ärzte zu WärterInnnen des telemedizinischen Panoptikums werden und der Aspekt der Fürsorge im Vordergrund steht, könnten in naher Zukunft Verwaltungsangestellte von Krankenkassen ein Auge auf die Bewohnenden werfen, die eher wirtschaftliche Ziele verfolgen. Der Aspekt der Freiwilligkeit ist demnach beim Einzug in das Smart Home in Frage zu stellen.

4.2.3 Laterale Überwachung

Die eben beschriebene Überwachung durch technische AAL-Einrichtungen, eingerichtet von Menschen aus dem persönlichen Umfeld der Überwachten, lässt sich als Unterform der lateralen Überwachung zählen. Der von Marc Andrejevic geprägte Begriff beschreibt nicht die Überwachung durch Obrigkeiten, sondern innerhalb einer gesellschaftlichen, meist privaten Gruppe, in der Überwachende und Überwachte größtenteils gleichgestellt sind.

---

244 Vgl. O.N., „GreenGuide – Smart Home 2015“, *Deutsches CleanTech Institut*, Juli 2015, http://www.dcti.de/fileadmin/user_upload/GreenGuide_SmartHome_2015_Webversion.pdf, Zugriff: 14.11.2016, S. 64f.

245 Ebd., S. 64.

246 Vgl. Klebsch, Wolfgang/Julia Masurkewitz/Thorsten Witusch/Axel Heßler/Til Landwehrmann/Siegfried Pongratz/Cornelia Riß/Mathias Wilhelm, „Smart Home. IT-Sicherheit und Interoperabilität als Schrittmacher für den Markt“, *VDE (Verband der Elektrotechnik Elektronik Informationstechnik)*, 2014, http://partner.vde.com/smarthome/news/statusbericht/documents/broschuere%20statusbericht%20smart%20home_a4_60%20seiten.pdf, Zugriff: 14.11.2016, S. 48.

Diese Art der Kontrolle findet jedoch nicht nur zu AAL-Zwecken der Gesundheitsüberwachung, Kranken- oder Altenpflege statt, bei der die Überwachten nicht vor eine Wahl gestellt, sondern meist mit den getroffenen Entscheidungen konfrontiert werden. Außerdem begegnen sich Objekt und Subjekt der Überwachung auf Augenhöhe und tauschen möglicherweise auch die Rollen. Andrejevic beschreibt in seiner Abhandlung, dass die Menschen zur Überwachung ähnliche, oder die gleichen Methoden anwenden, wie sie auch von der Regierung zu Überwachungszwecken herangezogen werden.[247] Des Weiteren teilt Andrejevic die Überwachten in drei Hauptzielgruppen ein - „three main categories: romantic interests, family, and friends or acquaintances.“[248] Es bleibt also festzuhalten, dass laterale Überwachung nur auf eine bestimmte Weise und an einer bestimmten Gruppe des persönlichen Umfeldes der Überwachenden angewendet werden kann. Möglichkeiten dieser Art lassen sich im Smart Home wiederfinden. Beispielhaft ist hier das GPS-Tracking anzuführen. Während eine Lokalisierung in früheren Zeiten nur stattfand, um sicherzustellen, dass Mobiltelefone erreichbar sind, so dient die Ortung heute auch anderen Zwecken. Beispielsweise können Tracking-Apps, die ursprünglich herangezogen wurden um das eigene Smartphone wiederzufinden, falls dieses verlegt worden ist, auch eingesetzt werden, um immer genau zu wissen wo sich Freunde und Familienangehörige befinden. Als aktuelles Exempel lässt sich hier die App „Finde mein Handy“[249] anführen. Nach der Installation ist es möglich, das eigene Mobiltelefon zu orten. Daneben ist es des Weiteren möglich, die Standorte der mobilen Geräte von Freunden oder Familienmitgliedern einzusehen. Um diese Funktion nutzen zu können, müssen die jeweils Georteten dem Dienst mit einer Bestätigung-SMS zustimmen und somit Zugriff auf die persönlichen Daten des eigenen Mobiltelefons gewähren. Nach Zulassung dieser Ortungsfunktion ist es für die Georteten nicht nur möglich, überwacht zu werden, sondern auch den ursprünglich Überwachenden zu kontrollieren.[250] Dieser Vorgang erfüllt die zwei von Andrejevic definierten Eigenschaften der lateralen Überwachung. Der Akt der Überwachung findet durch Technologie statt, die ursprünglich nicht für den privaten Gebrauch bestimmt war. Außerdem findet die Kontrolle einvernehmlich statt und zwar nur im persönlichen Umfeld von Familie und Freunden. Diese Form der

---

247 Andrejevic, „The work of watching one another: Lateral surveillance, risk, and governace.“, S. 479.
248 Ebd., S. 488.
249 O.N., „Finde mein Handy“, *Google Play Store*, https://play.google.com/store/apps/details?id=com.fsp.android.phonetracker&hl=de, Zugriff: 16.11.2016.
250 Vgl. Ebd..

lateralen Überwachung lässt sich noch über die Grenzen des Mobiltelefons hinaus weiterdenken. Sensoren zur Ortung müssen nicht in Handys eingebaut werden, sondern könnten ebenso gut in bestimmten Trackingarmbändern, Smart Watches oder Schmuckstücken platziert werden.
Dies ist nur eines von mehreren Beispielen, wie die laterale Überwachung im Smart Home ihren Platz findet. Dieses gegenseitige aufeinander Achten erzeugt ein Miteinander und ein Gefühl von Geborgenheit und Sicherheit, auf das im folgenden Punkt noch weiter eingegangen wird.

4.2.4 Gefühlswelt der Überwachten

An diesem Punkt ist der Frage nicht mehr auszuweichen, welche Gefühle diese Arten der Überwachung in Überwachten und Überwachenden auslösen. Hierbei sind die eben beschriebene, freiwillige, laterale Art der Überwachung, die meist unfreiwillige Form im Zuge von Ambient Assisted Living und die allgemein selbstterminierte Überwachung durch technische Geräte unabhängig voneinander zu betrachten, da sie durch unterschiedlichen Intentionen ausgelöst werden und daher unterschiedliche Gefühle herbeiführen.
Lyon und Bauman stellten gemeinsam fest, dass in der heutigen Gesellschaft die Angst vor der Ausgrenzung eine viel schlimmere darstellt, als die vor Arrest und Isolation.[251]
Um das genauer zu erläutern, ziehen sie erneut den Vergleich zum Panoptikum heran. Sie merken an, dass „der Alptraum des Panoptikums – du bist nie allein – heute als hoffnungsvolle Botschaft wiederkehrt - »Du mußt nie wieder allein (verlassen, übersehen, vernachlässigt, überstimmt und ausgeschlossen) sein«“[252], lautet stattdessen der Leitspruch des 21. Jahrhunderts. Auch Bigos bereits erwähnte Begrifflichkeit des Bannoptikums, das dazu dient, „bestimmte Minderheiten als »unerwünscht« zu identifizieren“[253], lässt sich an dieser Stelle passend anführen. Die von Lyon und Bauman beschriebene Art der dauerhaften Überwachung beschreibt eine Gruppe scheinbar glücklicher Menschen, die sich zusammengehörig und verstanden fühlen. Bigos Begriff beschreibt dieses Zusammengehörigkeitsgefühl. Menschen, die nicht dazugehören, sind gebannt und erfahren ein Gefühl der Ausgeschlossenheit.
Bauman stellt außerdem in einem früheren Werk fest, dass die Gesellschaft der flüchtigen Moderne darauf eingerichtet ist, ihren Bewohnenden das Leben mit der Angst so

[251] Vgl. Bauman/Lyon, *Daten, Drohnen, Disziplin,* S. 37.
[252] Ebd., S. 37.
[253] Ebd., S. 81.

angenehm wie möglich zu machen.[254] Es gilt also festzustellen, dass für Bewohnende durchaus ein Gefühl der Angst im Zusammenhang mit der Verwendung des Smart Home entstehen kann – allerdings ein »möglichst angenehmes«.

An diesem Punkt der Analyse wird die These aufgestellt, dass in einer Gesellschaft, in der sich Einzelne freiwillig der omnipräsenten Überwachung unterziehen, selbige zwangsläufig positiv, oder zumindest nicht negativ, konnotiert sein muss. Dies trifft vor allem auf die selbstterminierte und die laterale Überwachung zu. Personen, die in der Vergangenheit zuhause und im privaten Leben auf sich allein gestellt waren, sind mithilfe der technischen Unterstützung nicht mehr zwangsläufig allein. Das Smart Home vermittelt den Nutzenden ein Gefühl von Sicherheit und Entlastung im Alltag.[255] Durch die laterale Überwachung werden diese Gefühle noch dazu personifiziert und um menschliche Fürsorge erweitert.

Diese Gefühle der Entlastung, Fürsorge und Sicherheit treffen ebenso auf die Überwachung im Bereich des AAL zu – allerdings darf die unterschiedliche Termination nicht außer Acht gelassen werden. Während sich die Nutzenden des Smart Home selbst für die technische Unterstützung entscheiden, die Kosten selbst tragen und die Folgen der Überwachung ebenfalls selbst erleben, sind die Machtverhältnisse im Bereich AAL anders gesetzt. So wie der Umzug aus dem eigenen Haus in ein Altersheim, ist auch die Umrüstung zum AAL meist nicht von den Bewohnenden selbstterminiert, sondern von bevollmächtigten Angehörigen, da Schritte wie diese meist mit geistiger Einschränkung oder Demenz einhergehen.[256] Gefühle, die mit dieser Bevormundung einhergehen, lassen sich daher schlecht in Kategorien einordnen.

In diesem Zusammenhang ist es allerdings auch wichtig, auf Sicherheitslücken hinzuweisen, die in vielen potentiellen Nutzenden Angst auslösen können.[257] Die hier bearbeitete soziologische Fragestellung beschäftigt sich daher aus Gründen des Umfangs mit der Idee einer funktionierenden Version des Smart Home und nicht ausschließlich mit dem intelligenten Zuhause des Jahres 2017, dessen „zentrale[s] Problem [...] seine Sicherheit“[258] ist.

---

254 Vgl. Bauman, Zygmunt, *Liquid Fear*, Cambridge: Polity Press 2006, S. 6.
255 Vgl. Illek, „Smart Home in Deutschland“, S. 4.
256 Vgl. Botthof/Bovenschulte, „Das »Internet der Dinge«“, S. 52.
257 Vgl. Illek, „Smart Home in Deutschland“, S. 6.
258 Pichler, Georg, „Die Leiden des jungen Smart Home“, *derStandard.at*, 18.11.2016, http://derstandard.at/2000047736462/Die-Leiden-des-jungen-Smart-Home, Zugriff: 18.11.2016.

4.3 Medialer Ansatz

Verdatung[259], Gamifizierung[260], Self-Tracking[261] - diese und eine unzählige Fülle an weiteren Anglizismen und Wortneuschöpfungen, betiteln mediale Verfahren, mit deren Hilfe personenbezogene Daten gesammelt, gespeichert und anschließend ausgewertet werden können. Ansätze, Theorien und Erklärungsversuche für Überwachungsverfahren dieser Art wurden bereits zu Beginn dieser Arbeit ausgeführt.
Im Folgenden soll untersucht werden, in welcher Form die mediale Überwachung durch die Technologie des Smart Home im eigenen Zuhause stattfinden kann. Hierzu werden Beispiele der unterschiedlichen Möglichkeiten der Verdatung angeführt, erklärt und anhand der von Deborah Lupton eingeführten Kategorien der Selbstkontrolle in den Kontext der medialen Überwachung gesetzt.

4.3.1 *Private Selftracking* - Biometrische Daten

Haggerty und Ericson definieren mit der von ihnen beschriebenen *Surveillant Assemblage* ein System, in dem eine höher gestellte Instanz das Objekt der Überwachung von seinem räumlichen Umfeld trennt, es einzig und allein als eine Ansammlung von größeren Datensträngen ansieht und so auch weiter verwertet.[262] Durch technische Anwendungen der Selbstkontrolle im Smart Home werden die Nutzenden auf ähnliche Weise zu einer Ansammlung von Daten. Indem die Bewohnenden ihre biometrischen Daten sammeln, kann das Smart Home einen Nutzen aus eben diesen ziehen.
Im vorangegangenen Abschnitt 3.3.3 wurden „Fingerabdrucke, DNA-Spuren, Iris-Muster, sonstige Gesichtsmerkmale [und die] Zusammensetzung der Stimme“[263] bereits als einige biometrische Merkmale des Menschen angeführt. Nun stellt sich die Frage, für welche technischen Funktionen die Nutzenden die ausgewerteten Daten verwenden können. Biometrische Daten spielen im Smart Home vor allem zur Bedienung von Zutrittskontrollsystemen eine große Rolle. Irisscanner und AFIS[264]-Systeme wurden bereits in den 1990er Jahren entwickelt und existieren heute beinahe weltweit.[265]

---

259 Reichert, „Digitale Selbstvernetzung“, S. 66.
260 Ebd., S. 68.
261 Lupton, *Self-Tracking Modes.*
262 Vgl. Haggerty/Ericson, „The Surveillant Assemblage“, S. 62.
263 O.N., „Schaffung geeigneter Regelungen zur Videoverwendung (Aufzeichnung/Überwachung) und zur Biometrie“.
264 Automated Fingerprint Identification System
265 Vgl. Simon/Simon, *Ausgespäht und abgespeichert,* S. 202.

> „Einen Schlüssel oder eine Ausweiskarte kann man verlieren oder man kann sich aussperren; eine PIN kann man vergessen oder sie wird ausgespäht; seinen Finger hat man hingegen ständig bei sich […].“[266]

Mit dieser einfachen Erklärung stellt Dr. Leopold Gallner, Geschäftsführer von *Ekey*, einer führenden österreichischen Firma für biometrische Sicherheitssysteme, die wichtigste Eigenschaft des biometrischen Schlüssels heraus. Sicherheitslücken, die möglicherweise durch gefälschte Fingerabdrücke, oder sogar abgetrennte Finger zustande kommen können, wurden 2008 von Simon und Simon (vgl. 3.3.3) als sehr wahrscheinlich nachgewiesen. Während bei Simon und Simon noch die Rede davon war, dass sich drei Viertel der handelsüblichen elektronischen Geräte mit dem kopierten Fingerabdruck täuschen lassen[267], spricht Gallner, von einer „Fehlerquote von eins zu einer Million“[268] bei Fälschungen und auch das Argument des abgetrennten Fingers erklärt er bereits 2009 als „praktisch Bedeutungslos“[269]. Laut *Ekey* lässt sich das biometrische Schloss außerdem grundsätzlich als ein einfacher Schalter verstehen, „der einen Stromkreis schließt, wodurch ein Gerät eingeschaltet wird“[270]. Die Idee des Fingers als Schlüssel, lässt sich daher nicht nur auf Verschlusssysteme, sondern beispielsweise auch als Kindersicherung anwenden. Verbrannte Kinderhände durch aus Versehen angestellte Herdplatten würden sich vermeiden lassen, wenn der Herd nur durch die Fingerabdrücke befugter Erwachsener eingeschaltet werden könnte.

Diese Sammlung von biometrischen Daten der eigenen Person und möglicherweise der Familie lässt sich nach Lupton in den Bereich des „private Self-Tracking“[271] einordnen. Auch wenn keine Optimierung der nutzenden Person selbst stattfindet, sondern nur eine Verbesserung der Sicherheit des Zuhauses und dadurch der Lebensqualität, so ist die Einordnung in Luptons Kategorien dennoch zutreffend. Bei der Verwendung von biometrischen Schließsystemen werden persönliche Daten in einem technischen System aus freien Stücken gesammelt und nur in diesem System von den Nutzenden selbst verwendet. Eine Überwachung vom Verlassen und Betreten des Smart Homes findet durch die Anwendung statt und fällt unter Luptons Gruppe des private Self-Tracking. Auch wenn die Überwachung der biometrischen Daten durch

---

266 Hickisch, Kurt, „Der Finger als Schlüssel. Die Firma *Ekey* ersetzt den Schlüssel durch einen Fingerprint“, *Öffentliche Sicherheit* 3-4, 2009, S. 134.
267 Vgl. Simon/Simon, *Ausgespäht und abgespeichert*, S. 203.
268 Hickisch, „Der Finger als Schlüssel“, S. 134.
269 Ebd..
270 Ebd..
271 Lupton, *Self-Tracking Modes*, S. 5.

das technische Gerät stattfindet, bleibt die Instanz der Überwachung die/der Nutzenden selbst, sofern kein Fremdeingriff in das Steuerungssystem der zentral verwalteten Schließanlage stattfindet.[272]

4.3.2 *Pushed* & *Imposed Self-Tracking* - Gesundheitsüberwachung

Bereits im soziologischen Ansatz wurde auf den Aspekt der Freiwilligkeit bei der Überwachung im Smart Home eingegangen. Auch vom medialen Standpunkt aus spielt dieser Punkt eine wichtige Rolle. Deborah Lupton unterscheidet das pushed Self-Tracking vom bereits beschriebenen personal Self-Tracking (siehe 4.3.1) durch die veränderte Intention, die hinter den Handlungen der Überwachung steht. Während die Handelnden der persönlich dominierten Variante selbst entscheiden, wie sie überwacht werden und was mit den gesammelten Daten geschieht, so ist beim pushed Self-Tracking zwar der Vorgang gleich, doch die Intention, die hinter der Handlung steht, ist unterschiedlich.[273] Noch einen Schritt weiter geht hier das von Lupton beschriebene imposed Self-Tracking. Hier ist nicht nur die Intention, die hinter der Überwachung steht, fremdterminiert, sondern auch der Akt der Überwachung selbst geht von einer fremden, übergeordneten Instanz aus.[274] Die bereits thematisierte Freiwilligkeit spielt in diesem Zusammenhang eine wichtige Rolle.

Vor allem im Bereich der Gesundheitsüberwachung zuhause lassen sich für diese zwei Arten der Selbstkontrolle interessante Beispiele herausstellen. Zum einen besteht bereits die Möglichkeit, dass Bewohnende selbst, mithilfe von technischen Gadgets ihren Gesundheitszustand überwachen. Dazu dienen unter anderem Gesundheits-Apps, die beispielsweise Schritte zählen und auf Bewegungen achten, intelligente Kühlschränke, die sich die Ernährungsgewohnheiten der Nutzenden einprägen und zu „Food Management Systemen“[275] werden, die gesundes Essen nachbestellen. Aber auch Wecker oder Weck-Apps, die Schlafens- und Weckzeiten vermerken und somit feststellen, ob die Bewohnenden genügend Ruhezeiten einhalten[276] sowie möglicherweise intelligente Toiletten, die Nutzende wiegen und ein Warnsignal abgeben, falls sich beispielsweise

---

272 Vgl. Hickisch, „Der Finger als Schlüssel“, S. 135.
273 Vgl. Reichert, „Digitale Selbstvernetzung“, S. 75.
274 Vgl. Lupton, *Self-Tracking Modes*, S. 9.
275 Sterbenz, Benjamin, „Weise Ware. Kühlschrank wird zum Food Management System“, *futurezone.at*, 08.01.2013, https://futurezone.at/produkte/kuehlschrank-wird-zum-food-management-system/24.590.904, Zugriff: 26.11.2016.
276 Vgl. O.N., „Sleep Cycle alarm clock“, *iTunes Store*, https://itunes.apple.com/at/app/sleep-cycle-alarm-clock/id320606217?mt=8, Zugriff: 26.11.2016.

Blut oder besorgniserregende Bakterien in Urin oder Stuhl befinden sollten[277], gehören dazu. Gesammelte Daten und Informationen über den eigenen Gesundheitsstand werden dann von den Nutzenden an Institutionen wie Krankenkassen, telemedizinische Zentren oder schlicht den betreffenden Hausarzt weitergeleitet. Diese sind nur als einige von unzähligen Beispielen anzuführen, wie Nutzende ihre Gesundheitsdaten selbst an Dritte weitergeben. Diese weitgehend freiwillige Überwachung geschieht vor allem aus dem Grund, dass Nutzende eine positive Konsequenz für die eigene Person aus den weitergegebenen Daten ziehen wollen. Eine Benachrichtigung auf dem Smartphone mit dem Inhalt „Bitte suchen Sie unverzüglich einen Arzt auf. Ihre Blutwerte haben sich besorgniserregend verschlechtert!“[278], könnte demnach eine mögliche positive Folgerung der medizinischen Überwachung sein, da diese Veränderung der Blutwerte möglicherweise sonst nicht aufgefallen wäre. Andere Meldungen, etwa „Verringern Sie ihren Alkoholkonsum. Andernfalls müssen Sie mit einer deutlichen Erhöhung Ihrer Versicherungsprämie rechnen.“[279] könnten von Nutzenden zwar als gesundheitsfördernd, aber dennoch als eher negativ bewertet werden. Sowohl die Seite der möglichen Vorteile, als auch die der möglicherweise auftretenden Nachteile ließe sich an dieser Stelle beliebig erweitern – welcher Art die Konsequenzen des pushed Self-Tracking auch sein mögen, die Nutzenden können sich selbst dafür in die Verantwortung ziehen. Anders hingegen ist die Suche nach Verantwortlichen im Bereich des imposed Self-Tracking anzugehen. Das gemeinhin eher negativ konnotierte Verb *impose* bedeutet, dass die Kontrolle den Objekten der Überwachung ohne ihre Zustimmung und ihren freien Willen auferlegt wird. Der Willen der Überwachung wird über Sie erlassen und sie müssen sich fügen. Beispielhaft ist hier die bereits erwähnte Gesundheitsüberwachung im Bereich des Ambient Assisted Living anzuführen. Auch wenn sie in den größten Teilen ähnlich vonstattengeht, wie die bereits beschriebene Gesundheitskontrolle im Bereich des pushed Self-Tracking, so ist die Intention eine andere. Die Termination ist nicht durch die Überwachten selbst geleitet, sondern geschieht von einer fremden Stelle aus. Auch wenn die Überwachten selbst in diesen ausschlaggebenden Prozessen der Intention und Termination nicht berücksichtigt werden, so muss diese fremdterminierte Kontrolle keineswegs Nachteile mit sich bringen. Wie von Lupton beschrieben, haben die Objekte der Überwachung keinen Einfluss auf den Prozess und

---

277 Vgl. Campion, Gilles, „Hightech-Lokus analysiert Urin und misst Blutdruck“, *Welt.de,* 01.09.2010, https://www.welt.de/gesundheit/article9325629/Hightech-Lokus-analysiert-Urin-und-misst-Blutdruck.html, Zugriff: 26.11.2016.

278 Schaar, *Das Ende der Privatsphäre,* S. 71.

279 Ebd..

stehen diesem hilflos gegenüber. Hierbei stellt sich allerdings die Frage, ob das nur zu Ihrem Nachteil sein muss. Auch wenn Lupton sich zu Beginn nur dafür ausspricht, dass diese Art der Selbstkontrolle hauptsächlich zum Vorteil der Überwachenden ausfällt, so ziehen dennoch auch die Überwachten einen Gewinn aus der beschriebenen Situation.[280] Im gewählten Beispiel des AAL gehören nicht nur Ärzte oder Institutionen (z.B. Krankenkassen) zu den Gewinnern der Überwachungssituation und Datensammlung, sondern in größtem Maße auch die Angehörigen, von welchen die Intention zur Installation des AAL-Systems ausging. Mit der Überwachung geht für sie ein Gefühl der Sicherheit mit einer ungemeinen Entlastung des Alltags einher. Auch die Überwachten, deren Gesundheitszustand unter der unfreiwilligen Beobachtung steht, sind Gewinner dieser Situation.
Auch wenn ein Teil der Privatsphäre verloren geht, überwiegen die Vorteile, die sich für die Gesundheit und das Leben der Betroffenen ergeben.

4.3.3 *Exploited Self-Tracking* - Der Mensch als Kunde

> „In Zukunft wird ein intelligenter Kühlschrank selbstständig Lebensmittel bestellen, meinen Bedürfnissen entsprechend. Nach kurzer Zeit hat er aufgrund meines Einkaufsverhaltens gelernt, welche Lebensmittel ich wann und wie oft konsumiere. Also braucht es mich als Konsumenten zunächst nur noch, wenn ich etwas Außergewöhnliches kaufen möchte und zum Beispiel nach einem Jahr des Konsums von Haselnussjoghurt plötzlich auf Früchtejoghurt umschwenke. Aber auch das lernt der intelligente Kühlschrank.“[281]

Die Vorstellung eines intelligenten Kühlschranks, der die Besitzenden und ihre Bedürfnisse und Verlangen möglicherweise besser kennt als diese es selbst tun, liegt für Normalverbraucher, die den Begriff Smart Home nur aus Zeitungen und dem Internet kennen weit außerhalb der Vorstellungskraft für das eigene Zuhause. Es stellt sich die Frage, wie weit intelligente Einkaufshilfen und andere der beschriebenen Technologien wirklich noch aus den Küchen und Vorratsräumen der Nutzenden entfernt sind.
Aus einer bereits erwähnten Studie, die 2014 in Deutschland von der Organisation Bitkom durchgeführt wurde, ging hervor, dass 37 % der Befragten den Einbau von

---

280 Vgl. Lupton, *Self-Tracking Modes*, S. 9f.

281 Binswanger, Mathias, „Das Ende des souveränen Konsumenten“, *Die Zeit* 12/2016, März 2016; http://www.zeit.de/2016/12/kuenstliche-intelligenz-internet-der-dinge-konsumenten-kaufentscheidung, Zugriff: 28.03.2016.

Smart Home Geräten als zu aufwändig empfanden und 33 % von ihnen als zu kostspielig bewerteten. Rund ein Viertel der befragten Gruppe gab als Grund die komplizierte Bedienung an. Erst auf dem vierten Platz der meistgenannten Antworten ließ sich in dieser Studie die Angst um die eigene Privatsphäre einordnen.[282]

Die Reaktion auf Smart Home Technologie, die sowohl einfach zu installieren und bedienen, als auch günstig, beziehungseise kostenlos zur Verfügung gestellt wird, lässt sich aktuell am Beispiel des *Amazon Dash Buttons* erkennen. Der besagte »rasende Knopf« wurde im September 2016 in Deutschland und Österreich eingeführt und ist seitdem für Premiumkunden des Online-Versandhändlers *Amazon* erhältlich. Für ein geringes Entgelt, das noch dazu beim ersten Einkauf als Gutschein verrechnet wird, wird der *Dash Button* direkt zu den Konsumierenden nach Hause geschickt. Dort wird er mit dem WLAN verbunden und über die zugehörige App eingerichtet. Nach der Einrichtung wird der Knopf an der entsprechenden Stelle im Haus platziert, um dann bei Bedarf gedrückt werden zu können. Binnen eines Tages trifft das gewünschte Produkt anschließend im Smart Home ein.[283] Zwar bestellt dieser intelligente Knopf (noch) nicht eigenständig den Bedarf an alltäglichen Verbrauchsgegenständen nach, aber der simple Knopfdruck stellt durchaus einen erheblich kleineren Arbeitsaufwand dar, als der tatsächliche Gang in den Drogerie- oder Supermarkt.

Wie aber findet nun an dieser Stelle eine Form der Selbstkontrolle statt? Deborah Lupton definiert das exploited Self-Tracking so, dass die Nutzenden freiwillig oder unfreiwillig Daten über sich und ihr Kaufverhalten sammeln und diese dann an Dritte weitergeben, die sich im Anschluss kommerziell daran bereichern. Im gewählten Beispiel findet eine freiwillige Selbstkontrolle statt. Die Nutzenden bestellen den intelligenten Knopf aus freien Stücken. Dadurch geben sie dem Unternehmen *Amazon* freiwillig preis, in welcher Regelmäßigkeit sie Interesse an welchen genauen Produkten haben. Sie speisen also Informationen über ihr Kaufverhalten in den großen Datenpool von Big Data ein.

Auch an dieser Stelle lässt sich wieder auf den soziologischen Ansatz von Bauman verweisen, der feststellt, dass Menschen den Verlust der Privatsphäre gern in Kauf nehmen, sofern sie im Gegenzug mit entsprechenden Leistungen entschädigt werden.[284] Durch die persönlichen Einstellungen wird dem Versandhändler der Bedarf an

---

[282] Vgl. Illek, „Smart Home in Deutschland“, S. 6.

[283] Vgl. O.N., „Amazon Dash Button“, *Amazon*, https://www.amazon.de/dashbutton, Zugriff: 28.11.2016.

[284] Vgl. Bauman/Lyon, *Daten, Drohnen, Disziplin*, S. 35.

gewissen Produkten vermittelt. Wie bereits von Reichert beschrieben, findet somit eine „Ökonomisierung von Biodaten“[285] statt.

Durch die Nutzung des *Amazon Dash Buttons* legen die Nutzenden sich auf ein Produkt fest. Der Onlinehändler benötigt dadurch keine Produktvielfalt mehr und das *Long Tail* Prinzip[286], könnte möglicherweise bald der Vergangenheit angehören. „Die Nachfrage wird auf diese Weise mehr und mehr vom Menschen unabhängig. Aus der Konsumentensouveränität wird eine neue Computersouveränität.“[287] Mathias Binswanger beschreibt mit dieser Aussage das Phänomen und seine möglichen Folgen. Da sich die Nutzenden nicht mehr dem System der freien Marktwirtschaft aussetzen, müssen sie nicht mehr umworben werden. Eine Auswahl an unterschiedlichen Produkten wird überflüssig. Neben dem Verlust der Kundensouveränität verlieren die Kaufenden des Weiteren das Recht auf Information über die Preisbildung. Während des Knopfdrucks erfahren die Konsumierenden weder, wie viel das gewünschte Produkt im Moment beim Händler kostet noch, ob es bei anderen Anbietern günstiger zum Kauf angeboten wird.[288] Neben der Speicherung von Kundendaten und Kaufverhalten wird vor allem durch diese intransparente Preisbildung der kommerzielle Nutzen durch das exploited Self-Tracking nach Lupton bestätigt.[289] Die Aufwands- und Zeitersparnis, die für die Kaufenden entsteht, ist zwar durchaus nicht von der Hand zu weisen; allerdings ist fraglich, ob diese mit dem Profit, den die überwachenden Unternehmen aus dem aufgezeichneten Kaufverhalten ziehen, aufzuwiegen ist.

---

285 Reichert, „Digitale Selbstvernetzung“, S. 76.

286 Das „Long Tail Prinzip“ besagt, dass Onlinehändler den Großteil ihres Umsatzes nicht mit den immer gleichen Bestsellern verdienen, sondern mit Nischenprodukten, die (vor allem aufgrund teurer Lagerflächen) im physischen Geschäften oft nicht erhältlich sind.

287 Binswanger, „Das Ende des souveränen Konsumenten“.

288 Vgl. Hayon, Dominik, „Verbraucherschützer warnen: Warum Sie die Finger vom Amazon Dash Button lassen sollten“, *chip.de*, 06.09.2016, http://www.chip.de/news/Kritik-am-Dash-Button-Verbraucherschuetzer-warnen-vorm-Amazon-Knopf_99480939.html, Zugriff: 27.11.2016.

289 Vgl. Lupton, *Self-Tracking Modes*, S. 10.

4.4 Post-Privacy Debatte

> „Durch Wikileaks erlebten wir 2010, dass ein einzelner Whistleblower einer Supermacht wie der USA vor aller Welt die Hosen ausziehen kann. 2013 bestätigte Edward Snowden nicht nur, dass das möglich ist – wir erfuhren, dass auch wir selbst schon lange ohne Hosen dastehen. Die weltweiten Möglichkeiten zur Datensammlung, -verbreitung und –auswertung haben Dimensionen angenommen, mit denen wir nicht gerechnet haben. Wir haben die Kontrolle verloren. Egal, ob Regierung, Unternehmen, Institution oder Privatperson – alle sind betroffen.“[290]

Michael Seemann zeigt nochmals auf, dass das Zeitalter der Post-Privacy längst nicht mehr in der Zukunft liegt, sondern bereits zu einem Bestandteil unserer Wirklichkeit geworden ist. Wie konnte es so weit kommen?

Im Jahr 2010 sorgte Google für Aufregung in Deutschland, als mit Kameras ausgestattete Autos Aufnahmen von Straßen und Häusern für das damals neu eingeführte *Google Street View*-Feature durchführten. Nach allgemeiner Entrüstung der BürgerInnen und einem medialen Aufstand gab das Unternehmen seine Idee einer allumfassenden Dokumentation auf. Bewohnenden war es fortan möglich, ihr eigenes Haus in der Online-Anwendung unkenntlich zu machen.[291]

Diese Forderung auf ein Recht nach Privatsphäre erscheint in Hinblick auf die Überwachung durch das Smart Home in gewisser Weise ironisch. Während vor einigen Jahren ein kleiner gesellschaftlicher Aufstand losbrach, um die äußere Hülle der Privatsphäre zu schützen, hat sich die Haltung zum Schutz der Privatheit bis zum heutigen Tag scheinbar merklich gewandelt. Waren die Nutzenden früher nicht bereit, ein Bild der Außenfassade ihres Zuhauses preiszugeben, so zeigen sich heute immer mehr Verbrauchende bereit, der Überwachung in Form von intelligenten Anwendungen und Technologien freiwillig den Zutritt in ihr Heim zu gewähren. Im Folgenden wird versucht, anhand des Beispiels Smart Home zu erklären, inwiefern der Kontrollverlust über die Daten der Bewohnenden stattfindet und welche Folgen dieser Verlust nach sich zieht.

---

290 Seemann, *Das Neue Spiel*, S. 16.
291 Vgl. Ebd., S. 39.

4.4.1 Privatheit

Beim Versuch darüber zu sprechen, wie der Mensch die Kontrolle über seine Privatheit verliert, ist es wichtig, diese zuerst genau zu definieren und einzugrenzen. Beate Rössler beschreibt die Privatheit vor mehr als 15 Jahren folgendermaßen:

> „[A]ls privat gilt etwas dann, wenn man selbst den Zugang zu diesem »etwas« kontrollieren kann. Umgekehrt bedeutet der Schutz von Privatheit dann einen Schutz vor unerwünschtem Zutritt anderer. »Zugang« oder »Zutritt« kann hier sowohl die direkte, konkret-physische Bedeutung haben, so etwa wenn ich beanspruche, den Zugang zu meiner Wohnung selbst kontrollieren zu können; es kann jedoch auch metaphorisch gemeint sein: in dem Sinn, dass ich Kontrolle darüber habe, wer welchen »Wissenszugang« zu mir hat, also wer welche (relevanten) Daten über mich weiß; und in dem Sinn, dass ich Kontrolle darüber habe, welche Personen »Zugang« oder »Zutritt« in Form von Mitsprache- oder Eingriffsmöglichkeiten haben bei Entscheidungen, die für mich relevant sind.“[292]

Rössler spricht davon, dass bestimmte Personen, die eigenmächtig in Gruppen geordnet werden, keinen Zugriff auf bestimmte Bereiche des Lebens, die ebenfalls von den Handelnden selbst definiert werden, erhalten dürfen. Diese Verweigerung des Zugriffs ist, wie Rössler beschreibt, nicht nur physischer Natur, sondern auch geistiger. Somit lässt sich zum Schutz der Privatheit nicht nur die räumliche Gegebenheit des Zuhauses betrachten, sondern auch das geistige Eigentum der Bewohnenden.

Woher aber kommt diese Unterscheidung zwischen den Teilen des Lebens, die öffentlich gelebt und denen, die privat gehalten werden? Seit mehreren Jahrhunderten ist diese Unterscheidung zweier Lebensteile omnipräsent - die Unterscheidung der beiden Sphären lässt sich bis in die griechische Antike zurückverfolgen: Die „private Ordnung des Hauses“[293] stand hier der „öffentlich-politischen Sphäre des Marktplatzes“[294] gegenüber. Auch die Römer hielten an dieser Lebensweise fest und prägten damit eine Weltanschauung, die bis in die heutige Zeit vorhält. Auch etymologisch fand die Privatheit hier ihren Ursprung. Der lateinische Begriff *privatus*, abgeleitet vom Verb *privare*, das übersetzt *berauben* bedeutet, bezeichnete einen Menschen, der sich an nicht öffentlichen Orten der öffentlichen Beobachtung entzog und ihr dadurch *beraubt*

---

292 Rössler, Beate, *Der Wert des Privaten*, Frankfurt am Main: Suhrkamp Verlag 2001, S. 23f.
293 Schaar, *Das Ende der Privatsphäre*, S. 15.
294 Ebd..

wurde.[295] Das deutsche Wort *privat* ist etwa seit dem 16. Jahrhundert im Sprachgebrauch angekommen und bezeichnet seitdem unabhängige Personen und Sachverhalte, die für sich selbst stehen.[296]

Einen bedeutenden Einschnitt in der Geschichte von Öffentlichkeit und Privatheit brachten die modernen Medien mit sich. Durch die flächendeckende Popularisierung der Zeitung nahm die Möglichkeit der Informationsverbreitung an Geschwindigkeit zu. Auch die Empfangenden der Informationen wurden zahlenmäßig mehr, als es bis dahin durch der Möglichkeit der mündlichen Überlieferung von Informationen der Fall gewesen war. Dadurch ließen sich (möglicherweise persönliche) Informationen über Einzelne schlechter zurück- und privat halten.[297] „Je »öffentlicher« die Öffentlichkeit wurde, je größer also der Radius der veröffentlichten Informationen wurde, desto dringender wurde der Schutz der Privatheit.“[298]

Bekanntermaßen stellt die Entwicklung der Zeitung nicht das Ende in der Herausbildung der Massenmedien dar. Die Entwicklung des Fernsehens rückte auf der Suche nach möglichen Sendeformaten das Private mehr und mehr in die Öffentlichkeit. Diese unterliegt bekanntlich der Prägung durch Medien. Die flächendeckende Verbreitung des Internets reiht sich ein in diese Liste der Revolutionen, ausgelöst durch Medien. Web 2.0 und Social Media Plattformen bilden einen nächsten Schritt. Durch diesen können Privatpersonen mit ihrem privaten Leben Teil der Öffentlichkeit werden. Diese neue Medienrevolution unterscheidet sich jedoch grundlegend von der, die durch die Verbreitung der Zeitung angestoßen wurde. Der Mensch des 21. Jahrhunderts versucht nicht mehr, private Informationen zusammenzuhalten, sondern gibt sie in sozialen Plattformen aus freien Stücken Preis. Die Intention hinter der Revolution hat sich verändert und auch das Ziel ist ein anderes geworden. In diese Reihe der Entwicklungen lässt sich auch der Mittelpunkt dieser Arbeit – das Internet der Dinge und im speziellen das Smart Home - einordnen. Durch Eigenschaften wie Ubiquität, Personalisierung, Konvergenz und Konnektivität ist das IoT prädestiniert dafür – gefüttert mit persönlichen, privaten Daten der Nutzenden – als Verbindungsstück zwischen Privatsphäre und Öffentlichkeit zu fungieren. Der Verfall der einstigen Privatsphäre schreitet voran. Das Zeitalter nach der Privatsphäre, der Post-Privacy, ist bereits eingeläutet.

---

295 Vgl. Ebd., S. 15f.

296 Vgl. Ruetz, Bernhard, „Kleine Geschichte der Privatheit“, in: *Das Recht auf sich selbst: Bedrohte Privatsphäre im Spannungsfeld zwischen Sicherheit und Freiheit,* Hg. Konrad Hummler, Gerhard Schwarz, Zürich: NZZ Libro 2003, S. 27.

297 Vgl. Schaar, *Das Ende der Privatsphäre*, S. 17.

298 Ebd..

4.4.2 Postdigitalität

> „The transition from an industrial age to a post-industrial or information age has been discussed so much and for so long that we may not have noticed that we are passing into a post-information age.“[299]

Der postdigitale Vordenker Nicholas Negroponte beschreibt hier in seiner Abhandlung „Being Digital“, wie das „Postinformationszeitalter“[300] beinahe unbemerkt einsetzen konnte. In einer immer schneller werdenden Gesellschaft, deren charakteristisches Merkmal der ständige Wandel zu sein scheint, wird ein solcher fließender Übergang offensichtlich erst nach seiner Vollendung realisiert. Zeitlich parallel zu diesen Anfängen der Postdigitalitat[301] lässt sich auch das langsame Einsetzen der Post-Privacy verorten, das die Eigenschaft des unbemerkten Auftauchens mit dem Postinformationszeitalter gemein hat. Vor allem deshalb stellt der Begriff der Postdigitalität ein weiteres, wichtiges Schlagwort in Zusammenhang mit der biopolitischen Post-Privacy Debatte dar.

Der technologische Fortschritt des Internet der Dinge lässt sich, wie bereits erwähnt, in die von Bauman definierte flüchtige Moderne einordnen. Aber auch abseits der soziologischen Perspektive lässt sich das Zeitalter genauer beschreiben. Wie aber definiert sich diese Postdigitalität? Florian Cramer stellt im Jahr 2014 bei seiner Auseinandersetzung mit dieser Frage fest, dass der Übergang vom digitalen zum postdigitalen Zeitalter ein fließender Vorgang ist, der keineswegs das Ende des Informationszeithalters bedeutet. Stattdessen stehen die immer noch andauernde Digitalität und ihre Folgen im Vordergrund.[302]

> „In this sense, the post-digital condition is a post-apocalyptic one: the state of affairs after the initial upheaval caused by the computerisation and global digital networking of communication, technical infrastructures, markets and geopolitics.“[303]

---

299 Negroponte, Nicholas, *Being Digital*, London: Cornet Books - Hodder and Stoughton 1996, S. 163.

300 Negroponte Nicholas, *Total Digital. Die Welt zwischen O und 1 oder die Zukunft der Kommunikation*, München: C. Bertelsmann Verlag GmbH [4]1995, S. 201; (Orig. *Being Digital*, New York: Alfred A. Knopf 1995).

301 Die Begriffe Postdigitalität und Postinformationszeitalter werden im Folgenden Synonym füreinander verwendet. Negroponte selbst verwende den Begriff der Postdigitalität aber erst 2012

302 Vgl. Herwig, Jana, „Postdigitaler Vordenker oder digitaler Antagonist? Zu Nicholas Negropontes Entwurf des Digitalen (1995)“, in: *Post-digital Cluture*, Hg. Daniel Kulle, Cornelia Lund, Oliver Schmidt, David Ziegenhagen, http://www.post-digital-culture.org/herwig, Zugriff: 23.12.2016, S. 1.

303 Cramer, Florian, „What is ‚Post-Digital‘?“, in: *APRJA (A peer-reviewed journal about / Post Digital Research*), 23.01.2014, Hg. Christian Ulrik Andersen, Geoff Cox, Georgios Papadopoulos, http://www.aprja.net/?p=1318, Zugriff: 23.12.2016.

Dieser Zustand, den Cramer beschreibt, beinhaltet beispielsweise Eigenschaften wie die „Entzauberung digitaler Informationssysteme“[304]. Nach den Aufdeckungen von Edward Snowden ist der Glaube an ein allwissendes Internet, das ohne Gegenleistungen zu fordern auf der Seite der Nutzenden steht, erloschen, oder wie Cramer es beschreibt, „entzaubert“ worden. Des Weiteren führt er an, dass im Postinformationszeitalter Technologie, die einer zu sterilen Ästhetik entspricht, von den Nutzenden abgelehnt wird. Aufgrund dieser Ablehnung rückt die Idee des *glitch*, eines zufälligen Fehlers, in den Vordergrund.[305] Optisch führt der Trend seiner Meinung nach also zum „revial of ‚old‘ media“[306], technologisch zur Zurückweisung der „digital low quality“[307].

Während Cramers Analyse sich auf erwiesene Tatsachen beruft, versucht Nicholas Negroponte schon 1995 dem Postinformationszeitalters theoretische Eigenschaften zuzuschreiben, die rückblickend bereits vor mehr als 20 Jahren den digitalen Lebensraum der Gesellschaft des 21. Jahrhunderts definierten. Zu Beginn des digitalen Zeitalters vergrößerte und verkleinert sich das Publikum der Massenmedien gleichermaßen. Während große Nachrichtendienste ein breites Publikum bedienten, sprachen private Kabelanbieter und Bezahlsender ein kleineres Nischenpublikum an. Diese Beziehung zwischen Sender und Empfänger veränderte sich mit dem Fortschreiten der Digitalität immer weiter und hat in der heutigen Postdigitalität bereits persönliche Züge angenommen.[308] „Im Postinformationszeitalter hat man es häufig mit einem Einpersonenpublikum zu tun. Alles kann speziell angefordert werden, wodurch Informationen einen sehr persönlichen Charakter erhalten.“[309] Hierbei geht die Technologie, wie bereits beschrieben, noch einen Schritt weiter und wartet nicht nur bis spezielle Informationen angefordert werden, sondern bietet den Nutzenden bereits ungefragt personalisierte Information an.[310] Negroponte beschreibt also bereits 1995, dass Menschen zukünftig fast ausschließlich als Datensätze wahrgenommen werden. Außerdem spricht er von der Möglichkeit der asynchronen Mediennutzung[311], die sich heute beispielsweise bei Video-on-Demand Plattformen wie *Netflix*[312], Mediatheken wie der *ORF*

304 Herwig, „Postdigitaler Vordenker oder digitaler Antagonist?“, S. 1.
305 Vgl. Ebd..
306 Cramer, „What is ‚Post-Digital‘?“.
307 Ebd..
308 Vgl. Negroponte, *Total Digital*, S. 201f.
309 Ebd. S. 202.
310 Vgl. Ebd. S. 203.
311 Vgl. Ebd. S. 206.
312 O.N., „Netflix“, http://www.netflix.com, Zugriff: 27.12.2016.

TVThek[313] oder bei der allgemeinen Beschaffung von Information im World Wide Web wiedererkennen lässt. Die wohl wichtigste Eigenschaft der Postdigitalität stellt für ihn jedoch die Unterscheidung zwischen den Übertragungsmöglichkeiten von Bits und Atomen dar.

> „The industrial age, very much an age of atoms, gave us the concept of mass production, with the economies that come from manufacturing with the uniform and repetitious methods in any one given space and time. The information age, the age of computers, showed us the same economies of scale, but with less regard for space and time. The manufacturing of bits could happen anywhere, at any time […].“[314]

Während Gegenstände die aus Atomen bestehen, aufwendig zu befördern sind, Transportkosten verursachen und lange Reisezeiten auf sich nehmen müssen, um verschickt zu werden, haben Bits den Vorteil, dass sie problemlos innerhalb weniger Momente online gesendet und empfangen werden können. Durch diese Unterscheidung lassen sich geographische Grenzen überwinden und auch Beschränkungen durch Raum und Zeit treten in den Hintergrund.[315] Hierbei ist es wichtig, darauf hinzuweisen, dass Negropontes Überlegungen nur hypothetisch stattfinden. Seine Aussagen berücksichtigen nur die theoretische Möglichkeit einer Idee. Beispielsweise spricht er von den universellen, unbegrenzten, kostenlosen Zugriffsmöglichkeiten[316] auf Information, Literatur oder Musik, die sich durch die Übertragung von Bits ermöglichen ließe.[317] „Digital books never go out of print. They are always there.“[318]
All die Eigenschaften, die Negroponte hypothetisch beschreibt und die für Cramer und Herwig bereits Teil des alltäglichen Lebens sind, machen nicht durch ihre Anwesenheit auf sich aufmerksam, sondern diese tritt viel mehr in den Hintergrund.

> „Like air and drinking water, being digital will be noticed only by its absence, not its presence. The decades ahead will be a period of comprehending biotech, mastering nature, and realizing extraterrestrial travel, with DNA computers, microrobots, and nanotechnologies the main characters on the technological stage. Computers as we know them today will a) be boring, and b) disappear into things that are first and fore-

313 O.N., „ORF TvThek“, http://tvthek.orf.at, Zugriff: 30.12.2016.
314 Negroponte, *Being Digital*, S. 163.
315 Vgl. Negroponte, *Total Digital*, S. 204f.
316 Auch wenn diese Zugriffsmöglichkeiten theoretisch nach Negropontes Vorstellungen möglich wären, werden bei seiner Überlegung praktische Grenzen von Urheberrecht oder ähnlichem außer Acht gelassen. Die grundsätzliche technische Realisierbarkeit steht für ihn im Vordergrund.
317 Vgl. Negroponte, *Total Digital*, S. 4.
318 Negroponte, *Being Digital*, S. 13.

> most something else: smart nails, self-cleaning shirts, driverless cars, therapeutic Barbie dolls, […]. Computers will be a sweeping yet invisible part of our everyday lives: We'll live in them, wear them, even eat them. A computer a day will keep the doctor away.“[319]

„The most profound technologies are those that disappear“[320], stellte Mark Weiser bereits sieben Jahre zuvor fest und wurde damit zum Vordenker des Internet der Dinge. Auch Nicholas Negroponte gibt seine Zustimmung zu dieser Aussage. Während Personal Computer für ihn zunehmend zu ‚langweiligen' Spielzeugen werden, verschwinden ihre Eigenschaften in intelligente Gegenstände, die die postdigitale Ära prägen und gestalten.

Einen weiteren wichtigen Bestandteil des Postinformationszeitalters stellt der Verlust der Kontrolle über persönliche Informationen durch die beschriebene Technologie dar, mit dem sich das Folgende auseinandersetzen wird.

4.4.3 Kontrollverlust

> „Wer schweigt, kann immer noch reden. Wer dagegen geredet hat, kann darüber nicht mehr schweigen.“[321]

Niklas Luhmann macht mit dieser Aussage eine äußerst wichtige Feststellung über die Wirkung von Informationen. Kontrollverlust ist kein Novum, das sich in Zusammenhang mit dem Digitalen entwickelt hat, sondern ein Nebeneffekt der maßgeblichen Struktur der Information, um die es sich handelt. Es gibt in keiner denkbaren Welt, weder in der analogen, noch in der digitalen, Möglichkeiten, um Informationen, die einmal übertragen worden sind, wieder zurück zu holen.[322]

Michael Seemann beschreibt den Kontrollverlust, den der Zustand der Post-Privacy für ihn bedeutet, als ein simples enttäuschen und nicht gerecht werden von Erwartungshaltungen. Nutzende erwarten sich, dass jede Information, die sie freiwillig preisgeben oder die von ihrem Smart Home über sie gesammelt wird, einen positiven Rücklauf erzeugt. Sie haben eine positive Erwartungshaltung gegenüber der abgegangenen

---

319 Negroponte, Nicholas, „Beyond Digital“, *Wired*, 01.12.1998, https://www.wired.com/1998/12/negroponte-55/, Zugriff: 23.12.2016.

320 Weiser, „The Computer for the 21st Century“, S. 3.

321 Luhmann, Niklas, „Geheimnis, Zeit und Ewigkeit“, in: *Reden und Schweigen*, Hg. Niklas Luhmann, Peter Fuchs, Frankfurt am Main: Suhrkamp Verlag ²1992, S. 105.

322 Vgl. Seemann, *Das Neue Spiel*, S. 17.

Information über ihr Privatleben. Die Information wird von ihnen nur deshalb freiwillig abgegeben, um dafür einen positiven Effekt für das eigene Leben zu erlangen. Der Kontrollverlust wird hierbei nicht bei der Preisgabe dieser Informationen empfunden, sondern erst ab dem Zeitpunkt, „wenn eine Erwartungshaltung enttäuscht wird“[323]. In diesem Fall stellt die öffentliche Freigabe von Daten keine Bereicherung mehr für den Mensch dar, sondern nur einen simplen Datenverlust.

Nun stellt sich die Frage, welche Sachverhalte notwendig sind, um den Kontrollverlust auszulösen. Seemann weist auf drei unterschiedliche Punkte hin, die allesamt zum Verlust der Kontrolle beitragen. Zum einen ermöglicht eine Fülle von immer intelligenter werdender Sensorik und Anwendungsbreite eine Verschmelzung der analogen und digitalen Welt. Zum anderen verändern sich die technischen Grundgegebenheiten, die einen Kontrollverlust über eine riesige Menge an Daten überhaupt erst möglich machen. Speichermedien und Datenträger werden immer leistungsfähiger und verfügen über eine immer größer werdende Kapazität, während die Kosten für die erwähnten Datenträger immer geringer werden. Als dritten Punkt führt Seemann an, dass die Möglichkeiten zur Analyse der bereits gespeicherten Daten kontinuierlich bessere Leistungen bringen und somit auch aus den bereits bestehenden Datensätzen immer mehr Informationen erlangt werden können.[324]

Seemann definiert weiter, dass Nutzende die Kontrolle über ihre persönlichen Daten bereits auf dreifache Weise verloren haben. Zum einen ist es den Handelnden nicht mehr möglich, Klarheit darüber zu erlangen, wann wo welche Informationen über sie aufgezeichnet werden. Durch die Digitalisierung der Welt und die dazugehörige ubiquitäre Verbreitung von Sensoren an allen erdenklichen Plätzen und Orten wird die Bestandsaufnahme für Laien unüberschaubar. Zum anderen gehören die gesammelten Daten nicht mehr zum privaten Eigentum der Handelnden selbst, wodurch die Überwachten die Kontrolle darüber verlieren, wie und von wem die gesammelten Daten weiter verwahrt und verwendet werden. Des Weiteren liegt es außerhalb der Reichweite der Überwachten, welche Kraft die persönlichen Daten in der Hand der Institutionen möglicherweise entfalten könnten.[325] Seemann fasst diese Aufzählung kurz und prägnant zusammen:

---

[323] Ebd., S. 17.
[324] Vgl. Ebd., S. 20.
[325] Vgl. Ebd., S. 38.

> „Daten, von denen wir nicht wussten, dass es sie gibt, finden Wege, die nicht vorgesehen waren, und offenbaren Dinge, auf die wir nie gekommen wären.“[326]

Um den Verlust der Privatheit im Smart Home zu verdeutlichen, lässt sich beispielhaft die sogenannte *Kinect-Technologie* anführen, über die eine technische Erweiterung der Microsoft Spielekonsole *Xbox One* verfügt. Der Name *Kinect* ist ein Neologismus aus den englischen Worten *kinetic* für *kinetisch* und *connect* für das deutsche Verb *verbinden.*[327] Die Konsole ermöglicht es den Spielenden, sie mithilfe von Sprachbefehlen und Gesten, also kinetischen Verbindungen, zu bedienen.[328] Wie der Name *Kinect Sensor*[329] bereits deutlich macht, geschieht dies durch Sensoren im Gerät. Die technologische Neuheit wird durch eine eingebaute Kamera mit Weitwinkelobjektiv, eine Nachtsichtkamera, Infrarotsensoren und vier Mikrofone möglich gemacht. Alljene sind in der Konsole verbaut. Laut Angaben von *Xbox* sind die Sensoren auch im Standby-Modus aktiv, protokollieren allerdings keine Signale, sondern scannen die Umgebung nur nach dem Befehl »Xbox On« ab, wodurch die Konsole eingeschaltet wird.[330] *Microsoft* selbst wirbt damit, dass das Gerät Nutzende an der Sprache und am Abbild erkennt.[331]

> „Kinect »sieht« eine 3D-Repräsentation des Raumes und registriert in Echtzeit die Bewegungen aller Menschen darin. Kinect kann verschiedene Individuen auseinanderhalten, sieht, ob sie lachen oder angestrengt gucken, misst die Körpertemperatur und kann sogar den Puls anhand der Veränderung der Hautpigmente ablesen. Was für eine großartige Technologie – was für ein Überwachungsalptraum.“[332]

Seemann macht mit diesen Worten deutlich, dass die Technologie von *Kinect* eine gewisse Janus-Artigkeit innehat. So verblüffend und innovativ die technischen Aspekte des Gerätes zu sein scheinen, so spiegeln sie ebenso einen Alptraum der Überwachung im eigenen Zuhause wieder. Diese Angst vor Überwachung bildet außerdem

---

326 Ebd..
327 Vgl. Ebd., S. 22.
328 Vgl. O.N., „Kinect für Xbox One“, *xbox.com*, http://www.xbox.com/de-AT/xbox-one/accessories/kinect-for-xbox-one#fbid=eiCi-vyj4D-, Zugriff: 30.11.2016.
329 Während die Technologie von Microsoft im deutschsprachigen Raum unter dem Namen *Kinect* geführt wird, steht die Konsolenerweiterung auf dem internationalen Markt unter der Bezeichnung *Kinect Sensor* zum Verkauf. Vgl. O.N., „Kinect Sensor für Xbox One“, *MicrosoftStore.com*, https://www.microsoftstore.com/store/msusa/en_US/pdp/Kinect-Sensor-for-Xbox-One/productID.2267482500, Zugriff: 02.12.2016.
330 Vgl. Sterbenz, Benjamin, „Xbox Kinect: Totale Kontrolle ohne Ausweg“, *futurezone.at*, 23.05.2013, https://futurezone.at/produkte/xbox-kinect-totale-kontrolle-ohne-ausweg/24.597.542, Zugriff: 30.11.2016.
331 Vgl. O.N., „Kinect für Xbox One“.
332 Seemann, *Das Neue Spiel*, S. 22.

eine Inhaltskorrespondenz mit den Nutzungsbedingungen von *Microsoft*, denen Nutzende unweigerlich zustimmen müssen, um die Konsole verwenden zu können.

> „Soweit dies notwendig ist, um Ihnen und anderen die Dienste bereitzustellen […], um Sie und die Dienste zu schützen und um die Produkte und Dienste von Microsoft zu verbessern, gewähren Sie Microsoft eine weltweite und gebührenfreie Lizenz für geistiges Eigentum zur Verwendung Ihrer Inhalte, z. B. um Kopien Ihrer Inhalte zu erstellen oder Ihre Inhalte aufzubewahren, zu übertragen, neu zu formatieren, mithilfe von Kommunikationswerkzeugen zu verteilen und über die Dienste anzuzeigen.“[333]

Verwendende treten an dieser Stelle beispielsweise die Lizenz für ihr eigenes geistiges Eigentum an *Microsoft* ab, sofern dieses möglicherweise notwendig ist, um „Dienste von *Microsoft* zu verbessern“ [334]. Diese ist nur eine von mehreren Passagen des *Microsoft*-Servicevertrags, denen Nutzende der Konsole *Xbox One* zustimmen müssen. Eine Deaktivierung der dauerhaften Überwachung durch das installierte Gerät ist nicht möglich. Es bleibt nur, die Spielekonsole nicht zu kaufen. Ansonsten ist es scheinbar nicht möglich, der totalen Überwachung im eigenen Wohnzimmer zu entgehen.[335]
Die eben beschriebenen Daten, die Microsoft über die Nutzenden sammelt, unterscheiden sich in keiner Weise von den anderen persönlichen Daten, die durch intelligente Geräte im Smart Home über die Bewohnenden generiert werden – die Intention hinter ihrer Generierung und der späteren Nutzung kann hingegen unterschiedlich sein. Seemann weist in seiner Abhandlung über das Ende der Privatsphäre wiederholt auf den zunächst simpel erscheinenden Grund der Speicherung von Daten hin. „Schon immer war jede Speicherung auf den Moment ihrer Abfrage hin ausgerichtet.“[336] An dieser Stelle stellt sich die Frage, welchen Nutzen und welche Folgen diese Abfrage mit sich bringt und was dies für die Überwachten bedeutet.

---

333 O.N., „Microsoft-Servicevertrag“, *microsoft.com*, 15.07.2016, https://www.microsoft.com/de-at/servicesagreement/, Zugriff: 01.12.2016.
334 Ebd..
335 Vgl. Sterbenz, „Xbox Kinect: Totale Kontrolle ohne Ausweg“.
336 Seemann, *Das Neue Spiel,* S. 64.

4.4.4 Folgen des Kontrollverlustes

Seit einigen Jahren kursiert in Abhandlungen, Ansprachen und Artikeln die Metapher eines Frosches im heißen Wasser.

> „Ein Frosch, den man in einen Kessel sprudelnd heißen Wassers wirft, springt reflexartig sofort wieder heraus. Setzt man den Frosch hingegen in einen Topf mit kaltem Wasser und erwärmt ihn allmählich, so bleibt er drin. Zunächst mag das sich erwärmende Wasser sogar recht angenehm sein. Wenn das Wasser weiter erhitzt wird, sind seine Kräfte erlahmt. Wenn es den Siedepunkt erreicht hat, ist er tot."[337]

Die Allegorie des Frosches soll verdeutlichen, dass ganze Gesellschaften in gewissen Situationen ein ähnliches Reaktionsvermögen wie die Amphibie an den Tag legen. Werden Handelnde schnell und abrupt mit einer gravierenden Änderung konfrontiert, gibt es Aufschreie in der Gesellschaft und die Menschen wehren sich. Ebenso tut es der Frosch aus dem genannten Beispiel, der schnell wieder aus dem Kessel springt. Werden sie jedoch langsam an die sich verändernden Umstände gewöhnt, dann geschieht die fortschreitende Veränderung unbemerkt und vielleicht sogar angenehm. Das immer heißer werdende Wasser und die Tatsache seiner Existenz stehen metaphorisch für die Überwachung, die seit längerer Zeit mehr und mehr zunimmt. Whistleblower Edward Snowden enthüllte, wie bereits erwähnt, schon vor einigen Jahren, wie das private und das gesellschaftliche Leben der Einzelnen von staatlichen Instanzen kontrolliert und überwacht wird. Durch Zeitungsartikel, Berichterstattungen im Fernsehen, Interviews, Dokumentationen, Bücher und letztendlich einen Kinofilm über das Geschehene sollte die Tatsche der Überwachung durch den Staat in das Gedächtnis der westlichen Welt eingebrannt sein. Metaphorisch betrachtet müsste dem Frosch also mittlerweile klar sein, dass er sich in einem Topf mit heißem Wasser befindet.
Rechtfertigung für diese Überwachung wird durch das Argument der Sicherheit des Staates versucht. Neben dieser Überwachung durch staatliche Überordnungen sollte auch die Datenkontrolle durch wirtschaftliche Instanzen keine Überraschung mehr darstellen. In der vorangegangenen Abhandlung zu Überwachungspraktiken im Bereich des Internet der Dinge wurde deutlich gemacht, wie Unternehmen als Auftraggeber von Datensammlungen auftreten und wirtschaftlich davon profitieren können. Wie genau dieser Nutzen für staatliche und wirtschaftliche Instanzen aussieht, wird an

[337] Schaar, *Das Ende der Privatsphäre,* S. 11.

dieser Stelle allerdings aus Gründen des Umfanges nicht weiter thematisiert. Stattdessen stehen die Folgen und Nutzen für die Objekte der Überwachung im Vordergrund. Der Medien- und Kulturwissenschaftler Michel Seemann, dessen Gedankengut in dieser Arbeit bereits mehrfach zitiert wurde, bezeichnet die Zeit der Post-Privacy, die Zeit nach dem digitalen Kontrollverlust, als „Das Neue Spiel“[338]. Das spielen dieses neuen Spieles stellt eine Metapher für das Leben in einer Zeit dar, in der die Menschen die Kontrolle über persönliche Daten und private Informationen im eigenen Zuhause verloren haben. Um ein Spiel zu spielen, ist es notwendig, sich über genaue Regeln bewusst zu sein und diesen zu folgen.

> „Langsam beginnen wir zu begreifen, dass die Verdatung der Welt […] nicht vor unserer Haustür haltmachen wird, sondern vielmehr längst dabei ist, mit Sensoren unsere Haut zu durchschreiten und die Funktion unserer Organe transparent zu machen.“[339]

Seemann stellt fest, dass die Verdatung der Welt unaufhaltsam fortschreitet und in Form von Smart Home Technologien bereits auch Teil des privaten, häuslichen Lebens geworden ist. Eine Studie von Bitkom weist darauf hin, dass die Umrüstung vom analogen Heim zum Smart Home beim Großteil der Befragten bisher vor allem daran scheitert, dass Technologie und Fortschritt noch zu aufwendig und zu kostspielig sind.[340] Seemann weist diesbezüglich darauf hin, dass die Verbreitung von technologischem Forstschritt hauptsächlich in der Hand der Produzenten liegt. Er macht diesbezüglich deutlich, dass die Verbreitung von Technologie nur dann immer weiter fortschreitet, wenn die Produzenten das wollen. Wird technischer Fortschritt einfacher zu bedienen und günstig erhältlich sein, steigt auch die Wahrscheinlichkeit, dass eine Verbreitung dieser besagten Technologie stattfindet.[341] Um auf die Metapher des Spiels zurückzukommen bleibt festzustellen, dass die Spielregeln in der Hand der Obrigkeiten liegen. Medienumbrüche wie dieser sind kein Novum in der Geschichte der Menschheit. So ist es nur wahrscheinlich, dass die bereits erwähnte Revolution des Digitalen[342] im Bereich der IoT-Technologie eintreten wird. Durch die immer einfacher zu bedienende Hardware rückt der Akt der Verdatung und Übertragung von Information zusehends in den Hintergrund. Während die Informationsübertragung früher

---

338 Vgl. Seemann, *Das Neue Spiel,* S. 64.
339 Ebd., S. 153f.
340 Vgl. Illek, „Smart Home in Deutschland“, S. 6.
341 Vgl. Seemann, *Das Neue Spiel,* S. 155.
342 Vgl. Adamowsky, „Vom Internet zum Internet der Dinge“, S. 121.

mit Arbeitsaufwand gleichzusetzen war, geschieht sie heute durch die verbesserten technischen Grundvoraussetzungen beinahe unbemerkt.[343]

Des Weiteren stellt sich die Frage, wieso der Schutz der Privatsphäre gemeinhin als extrem wichtig deklariert wird, aber sich der Großteil der Nutzenden selbst nicht dafür einsetzt und einfache Grundregeln zur Prävention nicht befolgt. Seemann beschreibt in seiner Abhandlung das sogenannte *Privacy Paradox* anhand einer wissenschaftlichen Studie[344]:

> „In einer Studie wurden zwei fiktive Online-Shops erstellt. Einer verlangte weniger persönliche Daten von den Kundinnen, dafür waren die DVDs dort einen Euro teurer als bei dem zweiten Shop, der sehr viel mehr über seine Kunden wissen wollte. Fast alle wählten den billigeren Shop. Sogar wenn die Preise bei beiden gleich hoch waren, entschied sich nur die Hälfte er Versuchspersonen für die Datenschutzfreundliche Variante. Wir sin anscheinend nicht bereit, für unserer Privatsphäre einen Preis zu zahlen, egal wie niedrig dieser Preis ist.“[345]

Während Zygmunt Bauman darauf plädiert, dass die Nutzenden den Verlust der Privatsphäre als angemessenen Preis für „das tolle Zeug“[346] ansehen, das sie im Austausch dafür bekommen, stimmt die erwähnte Studie dieser Aussage nicht zu. Baumanns Theorie fußt auf dem Sachverhalt, dass den Nutzenden beim Kauf von intelligenten Gegenständen oder beim Einzug in ein Smart Home bewusst ist, dass sie durch diesen Akt ihre Privatsphäre verlieren. Durch die Studie zum Privacay Paradox wird allerdings die Tatsache herausgestellt, dass Handelnde sich oft nicht darüber im Klaren sind, welche Folgen ihr Handeln mit sich bringt. Sie agieren unbewusst, unbedarft und in manchen Fällen sogar gleichgültig.

Aufgrund dieser genannten Argumente stellt Seemann den Verlust der Kontrolle über die Daten der Nutzenden als gegeben voran. Diese Analyse befindet sich an einem Punkt, an dem ihm nicht widersprochen werden kann – die vorangegangenen Ausführungen haben bestätigt, dass eine ubiquitäre Überwachung und Sammlung von personenbezogenen Daten in beinahe allen Lebensbereichen bereits stattfindet, oder bald stattfinden könnte. Big Data ist kein simples medienwirksames Schlagwort mehr, sondern steht an der Tagesordnung des persönlichen Lebens. Diese Tatsache scheint nicht

---

343 Vgl. Seemann, *Das Neue Spiel,* S. 162.

344 Vgl. Beresford, Alistair/Dorothea Kübler/Sören Preibusch, „Unwillingness to pay for privacy: A field experiment“, in: *Economic Letters 117,* 2012, S. 25-27.

345 Seemann, *Das Neue Spiel,* S. 168.

346 Bauman/Lyon, *Daten, Drohnen, Disziplin,* S. 35.

mehr zu ändern zu sein. Daher ist es wichtig, sich an die Gegebenheiten anzupassen, mit ihnen umzugehen und sie bestmöglich zu nutzen.

In Anbetracht des Analysebeispiels Smart Home stellt sich die Frage, welche Daten die Nutzenden in ihrem intelligenten Zuhause produzieren. Beantworten lässt sich dieser Gegenstand bereits durch die vorangegangenen Punkte dieser Abhandlung. Ein voll ausgerüstetes Smart Home speichert GPS-Daten, Daten zu Gesundheit und körperlicher Fitness, Informationen über Angehörige, Beziehungen und Bekannte, biometrische Daten und Daten über Konsum- und Kundenverhalten der Bewohnenden. Außerdem ist es denkbar, dass Kommunikation überwacht wird und bereits genannte Geräte möglicherweise Bilder und Videos aufzeichnen und dem Datenpool zuführen. Die Möglichkeit der Kontrolle über die Daten wird in den jeweiligen Nutzungsbedingungen der einzelnen Geräte festgelegt. Am Beispiel des bereits erwähnten *Kinect Sensor* der *Xbox One* lässt sich exemplarisch herausstellen, dass Nutzungsbedingungen und Datenschutzerklärungen dieser Art meist zu Gunsten der Hersteller ausfallen. Mit der Akzeptanz dieser Bedingungen, die im Normalfall mit dem Erwerb der jeweiligen Produkte einhergeht, beginnt der angesprochene Kontrollverlust. Zu diesem Zeitpunkt ist er für Nutzende jedoch noch nicht spürbar.

Seemann weist, wie im Vorfeld thematisiert, darauf hin, dass für Überwachte der Kontrollverlust erst merklich beginnt, „wenn eine Erwartungshaltung enttäuscht wird“[347]. Solange für die Nutzenden also nur Vorteile aus den gesammelten Daten entstehen und keine spürbaren Enttäuschungen oder bemerkbaren Nachteile stattfinden, sind sie mit der totalen Überwachung einverstanden oder ihr gegenüber zumindest nicht negativ eingestellt. Jede Art der Überwachung beinhaltet Vor- und Nachteile für Überwachte und Überwachende. Vorteile für Überwachende entstehen allerdings meist auf Kosten der Überwachten. Einige dieser Vor- und Nachteile, die durch technische Anwendungen im Smart Home für Nutzende entstehen, wurden in dieser Abhandlung bereits erläutert. Beispielhaft sind hier nochmals der Sicherheitsaspekt, der durch GPS-Tracking oder biometrische Daten entsteht, die überdurchschnittlich gute Möglichkeit der Gesundheitskontrolle und die Möglichkeit durch intelligente Systeme Kosten einzusparen, anzuführen. Als Nachteile lassen sich an dieser Stelle nochmals Marketingfallen und der Verlust der Privatsphäre auf Kosten von Big Data anführen. Neben dieser Analyse der Verdatung lässt sich auch der Aspekt der Freiheit im Zeitalter der Post-Privacy in Frage stellen.

---

[347] Seemann, *Das Neue Spiel,* S. 17.

Christian Heller weist darauf hin, dass Privatsphäre grundsätzlich mit persönlicher Freiheit gleichgesetzt werden kann. Anhand historischer Beispiele zeigt er auf, dass eine Beraubung der Privatsphäre durch den Staat auch immer zu einer Beraubung der persönlichen Freiheit geführt hat. Beispielhaft führt er in diesem Zusammenhang die Zeit des Nationalsozialismus an, als Familienplanung zur Sache des Staates wurde, oder den Stalinismus, der Privatbesitzt mit Diebstahl am Kollektiv gleichsetzte.[348] Während die Privatsphäre und ein Recht auf persönliche Freiheit zum Ende des 20. Jahrhunderts hin zum Bürgerrecht wurden, scheint es, als würden die Nutzenden von Smart Home Technologien und anderen postmodernen Techniken zur Verdatung es eilig haben, dieses Recht mit der Akzeptanz der jeweiligen Nutzungsbedingungen wieder abzugeben. Die Post-Privacy erscheint aus diesem Blickwinkel wie eine Zeit, in der Nutzende freiwillig, oder auf Grund von Unwissenheit ihre Rechte abtreten.

Am Beispiel des Smart Home lässt sich dieses surreale Bild besonders gut anschaulich machen. In Orwells dystopischem Roman *1984* zwang die staatliche Instanz die Bewohnenden von *Ozeanien* dazu, in Häusern zu leben, in welchen jeder Raum unter Videoüberwachung stand.[349] Obwohl diese furchteinflößende Erzählung über den »großen Bruder« seit Jahrzehnten als Inbegriff des totalitären Überwachungsstaates gilt, scheint seine Bedeutung mehr und mehr zu verblassen. Wie sonst würde es sich erklären lassen, dass der Mensch des 21. Jahrhunderts keine Angst vor der totalen Überwachung und Datenaufzeichnung über sein Zuhause und sein privates Lebens hat? Diese Überlegung legt nahe, dass das frühe Zeitalter der Post-Privacy, in dem wir uns heute befinden, ein Zeitalter der Unwissenheit ist.

[348] Vgl. Heller, „Post-Privacy – Vom Ende der Privatheit“, S. 42f.
[349] Vgl. Ebd., S. 43f.

5 Resümee

> „Electronic mail arrives from the company that made her garage door opener. She lost the instruction manual, and asked them for help. They have sent her a new manual, and also something unexpected - a way to find the old one. According to the note, she can press a code into the opener and the missing manual will find itself. In the garage, she tracks a beeping noise to where the oil-stained manual had fallen behind some boxes. Sure enough, there is the tiny tab the manufacturer had affixed in the cover […]“[350]

Mark Weisers erstaunlich treffende Zukunftsvorstellung einer allgegenwärtigen Informationstechnologie ist gleichermaßen beeindruckend und erschreckend. Tatsächlich zieht die Wirklichkeit gewordene Idee der ubiquitären Digitalität in Form des Internet der Dinge in unser Zuhause des 21. Jahrhunderts ein. Das genannte Beispiel des Garagentores zeigt, dass selbst unscheinbare Firmen von denen es nicht erwartet wird, zu überwachenden Instanzen werden können. Diese Firmen haben dann möglicherweise mehr Wissen über das Privatleben der Nutzenden, als diese selbst.

Zusammenfassend bleibt zu sagen, dass sich durch die Analyse in dieser Abhandlung die vorangestellte These teilweise bestätigt hat. Die Abhandlung hat deutlich gezeigt, dass ein Verlust der Privatsphäre im Internet der Dinge im Allgemeinen und im Smart Home im Speziellen stattfindet. Durch die Integration des Internet der Dinge in das private Zuhause verwischen die Grenzen zwischen Öffentlichkeit und Privatheit mehr und mehr. Mithilfe von technischen Gadgets, Smart Home Elektronik, sozialen Onlinenetzwerken und neuesten Kommunikationstechnologien sind sämtliche unserer Lebensprozesse von Digitalität durchzogen. Eine Trennung von realem und digitalem Leben scheint an dem Punkt, an dem wir uns heute befinden, nicht mehr möglich.

Viele Autoren, die in der Übersicht des aktuellen Forschungsstandes zitiert werden, betonen, dass Bewohnende der westlichen Welt in der digitalen und der postdigitalen Gesellschaft mittlerweile (nur noch) als ein Datendouble ihrer selbst existieren. Dieser Aussage stimme ich eingeschränkt zu. Aus privatwirtschaftlicher und staatlicher Sicht mag diese Aussage zutreffen. Auch im privaten Bereich legen wir durch unterschiedliche Methoden des Selftracking die Grundsteine für unsere Daten-Doppelgänger.

---

[350] Weiser, „The Computer for the 21st Century“, S. 9.

Auch wenn es nach der Fülle an Information, die diese Arbeit zu vermitteln versucht, erscheinen mag, als wäre die technische Entwicklung unserer Umgebung abgeschlossen, so ist dem keinesfalls so. Wir stehen immer noch am Anfang des Entwicklungsprozesses unserer smarten Umgebung.

Eine Umkehrung der allumfassenden Digitalisierung des alltäglichen Lebens und der ubiquitären Überwachung, die diese mit sich bringt, erscheint zum jetzigen Zeitpunkt nicht realistisch. Daher gilt es meiner Meinung nach, die positiven Aspekte, die durch die neue Technologie entstehen, bestmöglich für uns zu nutzen und die Entwicklung in die richtige Richtung zu lenken. Wie bereits beschrieben, vermitteln Überwachung und Kontrolle bis zu einem gewissen Grad ein Gefühl von Sicherheit und Geborgenheit. In besonderen Fällen, wie beispielsweise der lateralen Überwachungsform, die bei der Ambient Assisted Living Technologie zum Einsatz kommt, greifen diese positiv konnotierten Gefühle sowohl bei der Instanz als auch beim Objekt der Überwachung. Es ist also falsch, neuartige Technologie und die daraus folgende Überwachung, die die Postdigitalität mit sich bringt, als grundlegend negativ zu beurteilen.

Beim Blick auf den aktuellen Forschungsstand der Surveillance Studies wird deutlich, dass die unterschiedlichen Theorien zur Überwachung zwar passend zurechtgelegt und auf die personenbezogene Datenüberwachung im Internet der Dinge projiziert werden können, aber dennoch nicht immer passgenau zum Sachverhalt sind. Diese Abhandlung soll einen Schritt hin zu einer ausstehenden Überwachungstheorie für das Postinformationszeitalter bedeuten.

Des Weiteren unterstütze ich die Meinung, dass Überwachung und Kontrolle in der Postinformationsgesellschaft, in der wir heute leben, trivialisiert wird. Deshalb plädiere ich für mehr Aufklärung im Bereich der Verdatung – jetzt und auch in Zukunft. Das Motiv der Freiwilligkeit aus den vorangegangenen soziologischen Theorien von Bauman und Lyon muss genauer hinterfragt werden. Auch wenn die Entscheidung hin zur Überwachung von den Handelnden freiwillig getroffen wird, geschieht sie dennoch meist in Unwissenheit. Nutzende müssen aber wissen, auf welche Form der Kontrolle sie sich einlassen und welche Folgen möglicherweise auf sie zukommen. Das Attribut »unwissend« sollte in diesem Zusammenhang – zumindest zum aktuellen

Zeitpunkt - mit »unmündig« gleichgesetzt werden müssen. Dieses Wissen darf nicht vorausgesetzt werden, sondern muss vermittelt und erlernt werden. Es muss dazu aufgerufen werden, Dinge zu hinterfragen, statt sie als gegeben hinzunehmen. Andernfalls liegt eine dystopische Zukunft, wie wir sie aus fiktiven Romanen wie *1984* oder *The Circle* kennen, vielleicht nicht mehr in allzu ferner Zukunft.

Nutzende müssen sich im Klaren über das volle Ausmaß und die Folgen ihres Handelns sein. Erst dann wissen sie, dass sie wie der Frosch im heißen Wasser sitzen und dass ein Blick auf das Thermometer von Zeit zu Zeit angebracht wäre.

6 Quellenangaben

Adamowsky, Natascha, „Vom Internet zum Internet der Dinge. Die neue Episteme und wir“, in: *Internet der Dinge: Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt*, Hg. Christoph Engemann, Florian Sprenger, Bielefeld: transcript (Digitale Gesellschaft) 2015, S. 119–135.

Albrechtslund, Anders, „Online social networking as participatory surveillance“, *first monday – pre-reviewed journal on the internet* 13, 03.03.2008, http://firstmonday.org/ojs/index.php/fm/article/view/2142/1949, Zugriff: 28.09.2016.

Anderson, Chris, „The End of Theory: The Data Deluge Makes the Scientific Mehtod Obsoltete“, *Wired,* 23.06.2008, https://www.wired.com/2008/06/pb-theory/, Zugriff: 24.10.2016.

Andre, Thomas, „Die Tyrannei des Internets. Diskussion um US-Bestseller »The Circle«“, *spiegel.de,* 04.08.2014, http://www.spiegel.de/kultur/literatur/dave-eggers-roman-dystopie-the-circle-a-982663.html, Zugriff: 18.10.2016.

Andrejevic, Marc, „The work of watching one another: Lateral surveillance, risk, and governace.“, *Surveillance & Society* 2/4, 2005, S. 479-497; http://www.surveillance-and-society.org/articles2(4)/lateral.pdf, Zugriff: 30.09.2016.

Bart, Simon, „The Return of Panopticism: Supervision, Subjection and the New Surveillance“, *Surveillance & Society* 3/1, 2005, http://surveillance-and-society.org/Articles3(1)/return.pdf, Zugriff: 10.06.2016.

Bauman, Zygmunt, *Flüchtige Moderne,* Frankfurt am Main: Suhrkamp 2003; (Orig. *Liquid Modernity,* Cambridge: Polity Press 2000).

Bauman, Zygmunt, *Liquid Fear,* Cambridge: Polity Press 2006.

Bauman, Zygmunt/David Lyon, *Daten, Drohnen, Disziplin: Ein Gespräch über flüchtige Überwachung*, Berlin: Suhrkamp 2013; (Orig. *Liquid Surveillance. A Conversation*, Cambridge: Polity Press 2013).

Beresford, Alistair/Dorothea Kübler/Sören Preibusch, „Unwillingness to pay for privacy: A field experiment", in: *Economic Letters 117*, 2012, S. 25-27.

Bigo, Didier, „Globalized (in)security. The field and the Ban-opticon", in: *traces 4. Translation, Biopolitics, Colonial Difference*, Hg. Naoki Sakai, Jon Solomon, Hong Kong: Hong Kong University Press 2006, S. 109-156.

Binswanger, Mathias, „Das Ende des souveränen Konsumenten", *Die Zeit* 12/2016, März 2016; http://www.zeit.de/2016/12/kuenstliche-intelligenz-internet-der-dinge-konsumenten-kaufentscheidung, Zugriff: 28.03.2016.

Bogard, William, „Surveillance assemblage and lines of flight", in: *Theorizing surveillance. The panopticon and beyond*, Hg. David Lyon, Portland: Willan Publishing 2006, S. 97–122.

Bogost, Ian, „Das Internet der Dinge, die wir nicht brauchen", in: *Internet der Dinge: Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt*, Hg. Christoph Engemann, Florian Sprenger, Bielefeld: transcript (Digitale Gesellschaft) 2015, S. 89–100.

Botthof, Alfons/Marc Bovenschulte (Hg.), „Das »Internet der Dinge«. Die Informatisierung der Arbeitswelt und des Alltags", *Hans Böckler Stiftung*, Juli 2009, http://ernaehrungsdenkwerkstatt.de/fileadmin/user_upload/EDW-Text/TextElemente/Medien/RFID_Internet_der_Dinge_Arbeit_Alltag_Boeckler_2009.pdf, Zugriff: 08.11.2016.

Boyd, Danah, "We googled you: Should Fred hire Mimi despite her online history?", *Harvard Business Review*, Juni 2007, http://www.danah.org/papers/HBRJune2007.html, Zugriff: 29.09.2016.

Brignall, Tom III, „The New Panopticon: The Internet Viewed as a Structure of Social Control“, *Theory & Science* 3/1, 2002, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.5894&rep=rep1&type=pdf, Zugriff: 08.06.2016.

Burrus, Daniel, „The Internet of Things Is Far Bigger Than Anyone Realizes“, *Wired*, 19.11.2014, http://www.wired.com/insights/2014/11/the-internet-of-things-bigger/, Zugriff: 06.07.2016.

Campion, Gilles, „Hightech-Lokus analysiert Urin und misst Blutdruck“, *Welt.de*, 01.09.2010, https://www.welt.de/gesundheit/article9325629/Hightech-Lokus-analysiert-Urin-und-misst-Blutdruck.html, Zugriff: 26.11.2016.

Čas, Johann/Walter Peissl, *Beeinträchtigung der Privatsphäre in Österreich. Teil 1 Bestandsaufnahme: Datensammlungen über ÖstereicherInnen*, Wien: Institut für Technisfolgen-Abschätzung der Österreichischen Akademie für Wissenschaften 2000, http://epub.oeaw.ac.at/ita/ita-projektberichte/d2-2a24.pdf, Zugriff: 29.10.2016.

Cramer, Florian, „What is ‚Post-Digital‘?“, in: *APRJA (A peer-reviewed journal about / Post Digital Research)*, 23.01.2014, Hg. Christian Ulrik Andersen, Geoff Cox, Georgios Papadopoulos, http://www.aprja.net/?p=1318, Zugriff: 23.12.2016.

Daugman, John, „How the Afghan Girl was Identified by Her Iris Pattern“, *University of Cambridge Computer Laboratory*, http://www.cl.cam.ac.uk/~jgd1000/afghan.html, Zugriff: 30.10.2016.

Delleuze, Gilles, „Postscript on the Societies of Control“, *October* 59, Winter, 1992, S. 3-7.

Dworschak, Bernd/Helmut Zaiser/Leif Brand/Lars Windelband, „Qualifikationsentwicklung durch das Internet der Dinge und dessen Umsetzung in der Praxis“, in: *Qualifikationsentwicklungen durch das Internet der Dinge. Trends in Logistik, Industrie und „Smart House“*, Hg. Lothar Abicht, Georg Spöttl, Bielefeld: W. Bertelsmann Verlag 2012, S. 7.

Eick, Volker, „Überwachung“, in: *Handbuch kritische Stadtgeographie*, Hg. Bernd Belina, Matthias Naumann, Anke Strüver, Münster: Westfälisches Dampfboot ^{2}2016, S. 163–168.

Evans, Dave, „Das Internet der Dinge. So verändert die nächste Dimension des Internet die Welt“, *Cisco*, April 2011, http://www.cisco.com/c/dam/global/de_de/assets/executives/pdf/Internet_of_Things_IoT_IBSG_0411FINAL.pdf, Zugriff: 04.11.2016.

Foucault, Michel, *Discipline and punish: The birth of the prison*, New York: Vintage Books 1979; (Orig. *Surveiller et punir – la naissance de la prison*, Paris: Gallimard 1975).

Foucault, Michel, *The Archeology of Knoweledge & The Discourse on Language.* New York: Pantheon Books 1972; (Orig. *L’Archéologie du Savoir,* Paris: Gallimard 1969).

Foucault, Michel, *Überwachen und Strafen. Die Geburt des Gefängnisses*, Frankfurt a. Main: Suhrkamp 1994; (Orig. *Surveiller et punir. la naissance de la prison*, Paris: Gallimard 1975).

Fuchs, Christian/Kees Boersma/Anders Albrechtslund/Marisol Sandoval, „Introduction: Internet and Surveillance“, in: *Internet and Surveillance. The Challenges of Web 2.0 and Social Media*, Hg. Christian Fuchs, Kees Boersma, Anders Albrechtslund, Marisol Sandoval, New York: Routledge 2011, S. 1-28.

Gant, Diana/Kiesler Sara, „Blurring the boundaries: cell phones, mobility and the line between work and personal life.“, in: *Wireless world: social and interactional aspects of the mobile age,* London: Springer-Verlag 2001, S. 121-131.

Glasberg, Ronald, „Studienreihe zur Heimvernetzung. Konstumennutzen und persönlicher Komfort“, *BITKOM - Bundesverband für Informationswirtschaft, Telekommunikation und neue Medien e.V.*, Oktober 2008, https://www.bitkom.org/Publikationen/2008/Leitfaden/BITKOM-Studie-Konsumentennutzen-und-persoenlicher-Komfort/Studie-Konsumentennutzen.pdf, Zugriff: 02.11.2016.

Gordon, Diana R., „The Electronic Panopticon: A Case Study of the Development of the National Criminal Record System“, in: *Surveillance, Crime & Social Control,* Hg. Clive Norris, Dean Wilson, Aldershot: Ashgate 2006, S. 383-411; (Orig. *Politics & Society* 15, 4, 1986-87, S. 483-511).

Greenfield, Adam, *Everyware. The dawning age of ubiquitous computing,* Berkley: New Riders 2006.

Gröger, Anne-Christin, „Generali erfindet den elektronischen Patienten“, *sueddeutsche.de,* 21.11.2014, http://www.sueddeutsche.de/geld/neues-krankenversicherungsmodell-generali-erfindet-den-elektronischen-patienten-1.2229667, Zugriff: 16.10.2016.

Haggerty, Kevin D./Richard V. Ericson, „The Surveillant Assemblage“, in: *Surveillance, Crime & Social Control*, Hg. Clive Norris, Dean Wilson, Aldershot: Ashgate 2006, S. 61-78; (Orig. *The British Journal of Sociology,* 51/4, Dezember 2000, S. 605-622).

Hardens, Immo, *Die elektronische Überwachung von Straffälligen. Entwicklungen, Anwendungsbereiche und Erfahrungen in Deutschland und im europäischen Verlgeich.*, Mönchengladbach: Forum Verlag Godesberg 2014.

Heesen, Jessica, „Keine Freiheit ohne Privatsphäre. Wandel und Wahrung des Privaten in informationstechnisch bestimmten Lebenswelten“, in: *1984.exe – Gesellschaftliche und juristische Aspekte moderner Überwachungstechnologien*, Hg. Sandro Gaycken, Constanze Kurz, Bielefeld: transcript Verlag 2008, S. 231-248.

Heller, Christian, „Post-Privacy – Vom Ende der Privatheit“, in: *»Wir nennen es Wirklichkeit« Denkanstöße zur Netzkultur*, Hg. Peter Kemper, Alf Mentzer, Julika Tillmanns, Stuttgart: Philipp Reclam jun. 2014, S. 26-36.

Heller, Christian, *Prima leben ohne Privatsphäre*, München: Verlag C.H.Beck oHG 2011.

Herwig, Jana, „Postdigitaler Vordenker oder digitaler Antagonist? Zu Nicholas Negropontes Entwurf des Digitalen (1995)“, in: *Post-digital Cluture*, Hg. Daniel Kulle, Cornelia Lund, Oliver Schmidt, David Ziegenhagen, http://www.post-digital-culture.org/herwig, Zugriff: 23.12.2016.

Hier, Sean P., „Probing the Surveillant Assemblage: on the dialectics of surveillance practices as processes of social control.“, *Surveillance & Society* 1/3, 2003, http://www.surveillance-and-society.org/articles1(3)/probing.pdf, Zugriff: 24.05.2016.

Illek, Christian P., „Smart Home in Deutschland“, *BITKOM – Bundesverband für Informationswirtschaft, Telekommunikation und neue Medien e.V.*, 18.12.2014, https://www.bitkom.org/Publikationen/2014/Studien/Smart-Home-in-Deutschland-Praesentation/Praesentation-Smart-Home.pdf, Zugriff: 13.07.2016.

Jeschke, Sabina/Tammo Andersch/Karsten Schulze/Dorothée Fritsch/Katherina Marquardt/Tobias Meisen/Anja Richert/Max Hoffmann/Christian Tummel, „Industrie 4.0 *ante Portas.* Praradigmenwechsel im deutschen Maschienen- und Anlagebau“, in: *Internet der Dinge: Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt*, Hg. Christoph Engemann, Florian Sprenger, Bielefeld: transcript (Digitale Gesellschaft) 2015, S. 241-279.

Jespersen, Julie Leth/Anders Albrechtslund/Peter Øhrstrøm/Per Hasle/Jørgen Albretsen, *Surveillance, Persuasion, and Panopticon*, 2007, https://www.researchgate.net/publication/229031001_Surveillance_Persuasion_and_Panopticon, Zugriff: 07.06.2015.

Kammerer, Dietmar/Thomas Waitz, „Überwachung und Kontrolle. Einleitung in den Schwerpunkt“, *Zeitschrift Für Medienwissenschaft* 13, 2016, S. 10-20.

Klebsch, Wolfgang/Julia Masurkewitz/Thorsten Witusch/Axel Heßler/Til Landwehrmann/Siegfrid Pongratz/Cornelia Riß/Mathias Wilhelm, „Smart Home. IT-Sicherheit und Interoperabilität als Schrittmacher für den Markt“, *VDE (Verband der Elektrotechnik Elektronik Informationstechnik),* 2014, http://partner.vde.com/smarthome/news/statusbericht/documents/broschuere%20statusbericht%20smart%20home_a4_60%20seiten.pdf, Zugriff: 14.11.2016.

Krichmayr, Karin, „Wir sind noch nicht am Ende des Zufalls“, *derStandard.at,* 28.10.2014, http://derstandard.at/2000007420701/Wir-sind-noch-nicht-am-Ende-des-Zufalls, Zugriff: 24.10.2016.

Kühl, Eike, „Alexa. Ich bin dein Vater“, *zeit.de*, http://www.zeit.de/digital/mobil/2016-10/amazon-echo-alexa-test-deutschland, Zugriff: 09.11.2016.

Kulick, Christian, „Vor dem Boom – Marktaussichten für Smart Home“, *BITKOM - Bundesverband für Informationswirtschaft, Telekommunikation und neue Medien e.V.*, 23.10.2014, https://www.bitkom.org/Publikationen/2014/Studien/Marktaussichten-fuer-Smart-Home/141023-Marktaussichten-SmartHome.pdf, Zugriff: 02.11.2016.

Kulick, Christian, „Wohnform des 21. Jahrhunderts – neue Smart-Home-Studie“, *BITKOM - Bundesverband für Informationswirtschaft, Telekommunikation und neue Medien e.V.*, 2015, https://www.bitkom.org/Themen/Internet-Telekommunikation-Netze/Smart-Home/SmartHomeStudie15.html, Zugriff: 02.11.2016.

Lee, Changmin/Luca Zappaterra/Kwanghee Choi/Heyeong-Ah Choi, „Securing Smart Home: Technologies, Security Challenges, and Security Requirments“, in: *Proceedings of the IEEE Conference on Communications and Network Security*, Oktober 2014, S. 67–72.

Lohr, Steve, „Unblinking Eyes Track Employees. Workplace Surveillance Sees Good and Bad“, *nytimes.com*, 21.06.2014, http://www.nytimes.com/2014/06/22/technology/workplace-surveillance-sees-good-and-bad.html?_r=0, Zugriff: 16.10.2016.

Luhmann, Niklas, „Geheimnis, Zeit und Ewigkeit“, in: *Reden und Schweigen*, Hg. Niklas Luhmann, Peter Fuchs, Frankfurt am Main: Suhrkamp Verlag ^{2}1992, S. 101–138.

Lupton, Deborah, „The digitally engaged patient: Self-monitoring and self-care in the digital health era“, *Social Theory & Health* 11/3, 2013, S. 256-270, http://link.springer.com/article/10.1057/sth.2013.10, Zugriff: 15.10.2016.

Lupton, Deborah, „Understanding the Human Machine“, *IEEE Technology & Society Magazine* 32/4, Dezember 2013, S. 25-30, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6679313, Zugriff: 16.10.2016.

Lupton, Deborah, *Self-Tracking Modes: Reflexive Self-Monitoring and Data Practices*, 27.08.2014, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2483549, Zugriff: 15.10.2016.

Lutolf, R., „Smart Home Concept and the Integration of Energy Meters into a Home Based System“, in: *Proceedings of the Seventh International Conference on Metering Apparatus and Tariffs for Electricity Supply* 367, November 1992, S. 277–278.

Lyon, David (Hg.), *The electronic eye: The rise of surveillance society*, Cambridge: Polity Press 1994.

Lyon, David, *Theorizing surveillance. The panopticon and beyond*, Portland: Willan Publishing 2006.

Mably, Gabriel Bonnot de, *De la legislation*, *Œvres completes*, Bd. IX, Paris: 1789, zit. Nach Michel Foucault, Überwachen und Strafen. Die Geburt des Gefängnisses, Frankfurt a. Main: Suhrkamp 1994; (Orig. *Surveiller et punir – la naissance de la prison*, Paris: Gallimard 1975).

Mathiesen, Thomas, *Silently Silenced. Essays on the Creation of Acquiescence in Modern Society*, Winchester: Waterside Press 2004, S. 98-102.

Mitchell, William J., *Me++: The Cyborg Self and the Networked City*, Cambridge: MIT Press 2003.

Negroponte Nicholas, *Total Digital. Die Welt zwischen O und 1 oder die Zukunft der Kommunikation*, München: C. Bertelsmann Verlag GmbH [4]1995; (Orig. *Being Digital*, New York: Alfred A. Knopf 1995).

Negroponte, Nicholas, *Being Digital*, London: Cornet Books - Hodder and Stoughton 1996.

Negroponte, Nicholas, „Beyond Digital“, *Wired*, 01.12.1998, https://www.wired.com/1998/12/negroponte-55/, Zugriff: 23.12.2016.

Niedermeier, Cornelia, „Der Bauch des Wals“, *derStandard.at*, 07.04.2003, http://derstandard.at/1264666/Der-Bauch-des-Wals, Zugriff: 07.08.2016.

Nogala, Detlef, „Der Frosch im heißen Wasser. Wie in der informatisierten Gesellschaft des 21. Jahrhunderts Überwachung trivialisiert wird.“, in: *Vom Ende der Anonymität. Die Globalisierung der Überwachung*, Hg. Christiane Schulzki Haddouti, Hannover: Verlag Heinz Heise GmbH & Co KG 2000, S. 139-155.

O.N. (Anonym: gshwach), „Walgreens Incentivizes Self-Tracking“, *Medicine in the Age of Networked Intelligence*, http://networkedmedicine.tumblr.com/post/47422186125/walgreens-incentivizes-self-tracking, Zugriff: 17.10.2016.

O.N., „Schaffung geeigneter Regelungen zur Videoverwendung (Aufzeichnung/Überwachung) und zur Biometrie“, *ARGE DATEN Privacy Service*, 02.11.2002, http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=11563vpp, Zugriff: 17.10.2016.

O.N., (Anonym: pte), „Webseite macht US-Strafregister kostenlos zugänglich“, *derStandard.at*, 04.08.2008, http://derstandard.at/1216918474464/Webseite-macht-US-Strafregister-kostenlos-zugaenglich, Zugriff: 27.08.2016.

O.N., „GreenGuide – Smart Home 2015“, *Deutsches CleanTech Institut*, Juli 2015, http://www.dcti.de/fileadmin/user_upload/GreenGuide_SmartHome_2015_Webversion.pdf, Zugriff: 14.11.2016.

O.N., „Geschäfte mit dem gläsernen Kunden“, *FoeBuD e.V.*, 07.06.2005, https://archiv.foebud.org/pc/docs/pc_sz050607_geschaefteMitDemGlaesernenKunden.html, Zugriff: 29.10.2016.

O.N., „Things That Think Consortium: MIT Media Lab“, *MIT Media Lab*, http://ttt.media.mit.edu/, Zugriff: 08.06.2016.

Pichler, Georg, „Die Leiden des jungen Smart Home“, *derStandard.at*, 18.11.2016, http://derstandard.at/2000047736462/Die-Leiden-des-jungen-Smart-Home, Zugriff: 18.11.2016.

Poster, Mark, „Database as Discourse; or, Electronic Interpellations“, in: *Computers, Surveillance and Privacy*, Hg. David Lyon, Elia Zureik, Minneapolis: University of Minnesota 1996, S. 175-192; (Orig. Marc Poster, *The Second Media Age*, Cambridge: Polity Press 1995).

Rämö, Hans/Mats Edenius, „Time Constraints in New Mobile Communication: Practices among Senior Managers“, *KronoScope* 8/2, 2008, S. 147-157.

Reichert, Ramón, *Big Data: Analysen zum digitalen Wandel von Wissen, Macht und Ökonomie*, Bielefeld: transcript Verlag 2014.

Reichert, Ramón, „Digitale Selbstvermessung. Verdatung und soziale Kontrolle“, *Zeitschrift Für Medienwissenschaft* 13, 2016, S. 66-77.

Rieger, Stefan, „Smart Homes. Zu einer Medienkultur des Wohnens“, in: *Internet der Dinge: Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt*, Hg. Christoph Engemann, Florian Sprenger, Bielefeld: transcript (Digitale Gesellschaft) 2015, S. 363–381.

Rössler, Beate, *Der Wert des Privaten*, Frankfurt am Main: Suhrkamp Verlag 2001.

Ruetz, Bernhard, „Kleine Geschichte der Privatheit“, in: *Das Recht auf sich selbst: Bedrohte Privatsphäre im Spannungsfeld zwischen Sicherheit und Freiheit*, Hg. Konrad Hummler, Gerhard Schwarz, Zürich: NZZ Libro 2003.

Ruoff, Michael, *Foucault-Lexikon: Entwicklung, Kernbegriffe, Zusammenhänge*, Stuttgart: UTB 2009.

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

Schipper, Lena, „Was eigentlich ist das Internet der Dinge? Ein Schlagwort macht Karriere: Im „Internet der Dinge" kommuniziert alles mit allem. Bloß ohne Menschen.", *faz.net*, 17.03.2015, http://www.faz.net/aktuell/wirtschaft/cebit/cebit-was-eigentlich-ist-das-internet-der-dinge-13483592.html, Zugriff: 07.08.2016.

Seemann, Michael, „Was ist Postprivacy (für mich)?", *ctrl+verlust*, 23. März 2011, http://www.ctrl-verlust.net/was-ist-postprivacy-fur-mich/, Zugriff am 19.10.2016.

Seemann, Michael, *Das Neue Spiel. Strategien für die Welt nach dem digitalen Kontrollverlust*, Freiburg: orange-press 2014.

Shove, Elizabeth/Mike Pantzar/Matt Watson, *The Dynamics of Social Practice. Everydady Life and How it Changes*, London: SAGE Publications 2012.

Simon, Anne Catherine/Thomas Simon, *Ausgespäht und abgespeichert. Warum uns die totale Kontrolle droht und was wir dagegen tun können*, München: Herbig Verlag 2008.

Sprenger, Florian/Christoph Engemann, „Im Netz der Dinge: Zur Einleitung", in: *Internet der Dinge: Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt*, Hg. Christoph Engemann, Florian Sprenger, Bielefeld: transcript (Digitale Gesellschaft) 2015, S. 7–58.

Sprenger, Polly, „Sun on Privacy: »Get over it«", *Wired*, 26.01.1999, http://archive.wired.com/politics/law/news/1999/01/17538, Zugriff: 19.10.2016.

Stephan, Felix, „Der Schwarm als Meute", *zeit.de*, 26.09.2016, http://www.zeit.de/kultur/literatur/2016-09/in-shitgewittern-jon-ronson-soziale-netzwerke, Zugriff: 19.10.2016.

Sterbenz, Benjamin, „Weise Ware. Kühlschrank wird zum Food Management System“, *futurezone.at*, 08.01.2013, https://futurezone.at/produkte/kuehlschrank-wird-zum-food-management-system/24.590.904, Zugriff: 26.11.2016.

Sterbenz, Benjamin, „Xbox Kinect: Totale Kontrolle ohne Ausweg“, *futurezone.at*, 23.05.2013, https://futurezone.at/produkte/xbox-kinect-totale-kontrolle-ohne-ausweg/24.597.542, Zugriff: 30.11.2016.

Stone, Brad, „If You Run a Red Light, Will Everyone Know? “, *nytimes.com*, 03.08.2008, http://www.nytimes.com/2008/08/03/technology/03essay.html?ref=technology, Zugriff: 27.08.2016.

Tate, Ryan, „Google CEO: Secrets Are for Filthy People“, *Gawker*, 04.12.2009, http://gawker.com/5419271/google-ceo-secrets-are-for-filthy-people, Zugriff: 19.10.2016.

Tunze, Wolfgang, „Smart-Home-Ideen mit Charme“, *faz.net*, 20.09.2013, http://www.faz.net/aktuell/technik-motor/umwelt-technik/intelligenter-haushalt-smart-home-ideen-mit-charme-12575578.html, Zugriff: 11.11.2016.

Wallner, Anna-Maria, „Wir stecken in der digitalen Pubertät“, *DiePresse.com*, 21.06.2012, http://diepresse.com/home/leben/gesundheit/767929/print.do, Zugriff: 24.10.2016.

Wang, Jun/Yaling Yang/William Yurcik, *Secure Smart Environments: Security Requirements, Challenges and Experiences in Pervasive Computing*, 2005, http://citeseer.ist.psu.edu/viewdoc/download?doi=10.1.1.60.4730&rep=rep1&type=pdf, Zugriff: 13.07.2016.

Weiser, Mark, „The Computer for the 21st Century“, *ACM SIGMOBILE. Mobile Comuputing and Communications Review* 3/3, 1999 S. 3-11; (Orig. *Scientific American* 265/3, September 1991, S. 94-104).

Wende, Jörg, „Die fünf Dimensionen des Internets der Dinge (Internet of Things – IoT)“, *IBM advertorial – Online Themenspecial IT-Trends 2014: BigData/Hadoop und Internet der Dinge*, 2014, https://www-935.ibm.com/services/multimedia/Die_5_dimensionen_von_IoT_WUO12360DEDE.pdf, Zugriff: 08.11.2016, S. 1-4.

Wenzel, Bernhard, „RFID in der Hauptbücherei Wien“, *Vortrag im Rahmen von O-DOK 2007 (12. Österreichisches Online-Informationstreffen, 13. Österreichischer Dokumentartag)*, Graz: 20. September 2007, https://www.uibk.ac.at/o-dok/ppt/wenzl.pdf, Zugriff: 07.08.2016.

Werner, Hendrik, „Das Web 2.0 hat seine besten Tage hinter sich“, *Welt.de*, 02.12.2009, http://www.welt.de/wirtschaft/webwelt/article5400784/Das-Web-2-0-hat-seine-besten-Tage-hinter-sich.html, Zugriff: 06.07.2016.

Ziegler, Peter-Michael, „München stellt Bibliotheken auf RFID-Technik um“, *heise online*, 24.01.2006, http://www.heise.de/newsticker/meldung/Muenchen-stellt-Bibliotheken-auf-RFID-Technik-um-168454.html, Zugriff: 07.08.2016.

6.1 Internetquellen

Britz, Paul-Christian, „Ich will jetzt sofort einen Flirt“, *zeit.de*, 22.08.2014, http://www.zeit.de/digital/mobil/2014-08/app-test-happn-dating-tinder, Zugriff: 29.10.2016.

Hayon, Dominik, „Verbraucherschützer warnen: Warum Sie die Finger vom Amazon Dash Button lassen sollten“, *chip.de*, 06.09.2016, http://www.chip.de/news/Kritik-am-Dash-Button-Verbraucherschuetzer-warnen-vorm-Amazon-Knopf_99480939.html, Zugriff: 27.11.2016.

Hickisch, Kurt, „Der Finger als Schlüssel. Die Firma *Ekey* ersetzt den Schlüssel durch einen Fingerprint“, *Öffentliche Sicherheit* 3-4, 2009, S. 134-135.

Holl, John, „High-tech thieves use laptops to steal cars“, *ForbesAUTOS.com*, 26.06.2006, http://www.nbcnews.com/id/13507939/ns/business-autos/t/high-tech-thieves-use-laptops-steal-cars/#.V6WOhvmLQdU, Zugriff: 07.08.2016.

O.N., „Amazon“, https://www.amazon.de/, Zugriff: 18.12.2016.

O.N., „Amazon Dash Button“, *Amazon*, https://www.amazon.de/dashbutton, Zugriff: 28.11.2016.

O.N., „Amazon Echo“, *Amazon*, https://www.amazon.de/Amazon-SK705DI-Echo-Schwarz/dp/B01GAGVCUY, Zugriff: 09.11.2016.

O.N., „Balance Rewards for healthy choices“, *Walgreens*, https://www.walgreens.com/steps/brhc-loggedout.jsp, Zugriff: 17.10.2016.

O.N., „Finde mein Handy“, *Google Play Store*, https://play.google.com/store/apps/details?id=com.fsp.android.phonetracker&hl=de, Zugriff: 16.11.2016.

O.N., „facebook“, https://www.facebook.com/, Zugriff: 07.09.2016.

O.N., „Gillette – Über Gillette“, http://gillette.de/de-de/ueber-gillette, Zugriff: 10.08.2016.

O.N., „happn“, https://www.happn.com/de/, Zugriff: 12.01.2017.

O.N., „Health Apps & Devices“, *Walgreens*, https://www.walgreens.com/steps/appmarket.jsp?ban=BRHC_DMI_earnban, Zugriff: 17.10.2016.

O.N., „Kinect für Xbox One“, *xbox.com*, http://www.xbox.com/de-AT/xbox-one/accessories/kinect-for-xbox-one#fbid=eiCi-vyj4D-, Zugriff: 30.11.2016.

O.N., „Microsoft-Servicevertrag“, *microsoft.com*, 15.07.2016, https://www.microsoft.com/de-at/servicesagreement/, Zugriff: 01.12.2016.

O.N., „Netflix“, http://www.netflix.com, Zugriff: 27.12.2016.

O.N., „ORF TvThek“, http://tvthek.orf.at, Zugriff: 30.12.2016.

O.N., „runtastic“, https://www.runtastic.com/de/apps/runtastic, Zugriff: 18.01.2017.

O.N., „15 Runtastic-Features, die Du ausprobieren solltest“, https://www.runtastic.com/blog/de/technologie/runtastic-features-2015/, Zugriff: 16.10.2016.

O.N., „SkyLINK: The Next Generation in Theft Recovery.“, http://www.mysky-link.com/, Zugriff: 29.10.2016.

O.N., „Sleep Cycle alarm clock“, *iTunes Store*, https://itunes.apple.com/at/app/sleep-cycle-alarm-clock/id320606217?mt=8, Zugriff: 26.11.2016.

O.N., „Surveillance & Society“, http://surveillance-and-society.org/, Zugriff: 07.09.2016.

O.N., „Surveillance Study Center“, http://www.sscqueens.org/about, Zugriff: 07.09.2016.

O.N., „The Perfect Shave – Lieferbedingungen“, *The Perfect Shave*, https://www.perfect-shave.de/zahlungsarten-lieferbeschraenkungen, Zugriff: 10.08.2016.

O.N., „The Perfect Shave – The Gillette Box“, *The Perfect Shave*, https://www.perfect-shave.de/gillette-box, Zugriff: 10.08.2016.

O.N., „Tinder“, https://www.gotinder.com/, Zugriff: 12.01.2017.

O.N., „Twitter“, https://twitter.com/, Zugriff: 19.10.2016.

O.N., „Wenn sich das Navi verfährt“, *AugsburgerAllgemeine.de*, 26.07.2007, http://www.augsburger-allgemeine.de/panorama/Wenn-sich-das-Navi-verfaehrt-id2814791.html, Zugriff: 29.10.2016.

Ronson, Jon, „How One Stupid Tweet Blew Up Justine Sacco’s Life“, *nytimes.com*, http://www.nytimes.com/2015/02/15/magazine/how-one-stupid-tweet-ruined-justine-saccos-life.html, Zugriff: 19.10.2016.

6.2 Weiterführende Literatur

Albrechtslund, Anders/Thomas Tyberg, „Participatory Surveillance in the Intelligent Building“, *Massachusetts Institute of Technology DesignIssues* 27/3, Sommer 2011, S. 35-46.

Albrechtslund, Anders/Peter Lauritsen, „Spaces of everyday surveillance: Unfolding an analytical concept of panopticon“, *Geoforum* 49, 2013, S. 310-316.

Angerer, Marie-Luise/Bernd Bösel, „Capture All, oder: who’s afraid of a pleasing little sister?“, *Zeitschrift Für Medienwissenschaft* 13, 2016, S. 48-56.

Bialobrzeski, Arndt/Jens Ried, „Privatheit in der Online-Welt. Facebook als politische Herausforderung“, *Die Politische Meinung* 497, April 2011, S. 74-78.

Bunz, Mercedes, „Die Dinge tragen keine Schuld. Technische Handlungsmacht und das Internet der Dinge“, in: *Internet der Dinge: Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt*, Hg. Christoph Engemann, Florian Sprenger, Bielefeld: transcript (Digitale Gesellschaft) 2015, S. 163–180.

Coupland, Douglas, *Generation X. Geschichten für eine immer schneller werdende Kultur*, München: Goldmann Verlag ^{8}1995; (Orig. *Generation X. Tales for an Accelerated Culture,* New York: St. Martin’s Press 1995).

Eggers, Dave, *Der Circle*, Köln: Verlag Kiepenheuer & Witsch ^{5}2014; (Orig. *The Circle*, New York: Alfred A. Knopf 2013).

Heidegger, Martin, „Die Frage nach der Technik“, in: *Gesamtausgabe. I . Abteilung: Veröffentlichte Schriften 1910-1976, Band 7: Vorträge und Aufsätze,* Hg. Friedrich-Wilhelm von Herrmann, Frankfurt am Main: Vittoria Klostermann 2000, S. 5-40; (Orig. Vortrag, gehalten am 18. November 1953 im Auditorium Maximum der Technischen Hochschule München, in der Reihe *Die Künste im technischen Zeitalter*, veranstaltet von der Bayerischen Akademie der Schönen Künste unter Leitung des Präsidenten Emil Preetorius).

Heider, Fritz, *Ding und Medium*, Berlin: Kulturverlag Kadmos 2005. (Orig. *Symposion* 1 (Heft 2 von 1926), 1927, S. 109-157.).

Helbing, Dirk/Bruno S. Frey/Gerd Gigerenzer/Ernst Hafen/Michael Hagner/Yvonne Hofstetter/Jeroen van den Hoven/Roberto Zicari/Andrej Zwitter, „Digitale Demokratie statt Datendiktatur: Big Data, Nudging, Verhaltenssteuerung: Droht uns die Automatisierung der Gesellschaft durch Algorithmen und künstliche Intelligenz? Ein gemeinsamer Appell zur Sicherung von Freiheit und Demokratie“, *Spektrum der Wissenschaft* 1/16, 2016, S. 51–60.

Hoof, Florian, „Ist jetzt alles »Netzwerk«? Mediale »Schwellen« und Grenzobjekte“, in: *Jenseits des Labors. Lavor, Wissen, Transformation*, Hg. ders. Eva-Maria Jung, Ulrich Salaschek, Bielefeld: transcript 2011, S. 45-62.

Howard, Philip N., *Finale Vernetzung. Wie das Internet der Dinge unser Leben verändern wird*, Köln: Quadriga 2016; (Orig. *Pax Technica. How the Internet of Things May Set Us Free or Look Us Up*, New Haven: Yale University Press 2015).

Kurz, Constanze/Frank Rieger, *Die Datenfresser. Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen*, Frankfurt am Main: S. Fischer 2011.

Licklider, Joseph Carl Robnett/Robert William Taylor, „The Computer as a Communication Device“, *Signal Lake*, http://signallake.com/innovation/LickliderApr68.pdf, Zugriff: 10.12.2016, (Orig. *Science and Technology*, April 1968).

Lupton Deborah, „M-health and health promotion: The digital cyborg and surveillance society“, *Social Theory & Health* 10/3, 2012, S. 229-244, http://link.springer.com/article/10.1057/sth.2012.6, Zugriff: 15.10.2016.

Lupton, Deborah, *Self-tracking cultures: towards a sociology of personal informatics*, 2014, http://dl.acm.org/citation.cfm?doid=2686612.2686623, Zugriff: 15.10.2016.

Mathiesen, Thomas, „The Viewer Society. Michel Foucault's »Panopticon« Revisited", *Theoretical Criminology 1/2, 1997, S. 215-234.*

Spigel, Lynn, „Designing the Smart House", *European Journal of Cultural Studies* 8 (4), 2005, S. 403-426.

Thacker, Eugene, „Netzwerke – Schwärme - Multitudes", in: *Schwärme – Kollektive ohne Zentrum. Eine Wissensgeschichte zwischen Leben und Information*, Hg. Eva Horn, Lucas Marco Gisi, Bielefeld: transcript Verlag 2009, S. 27-68.

7 Anhang

7.1 Zusammenfassung (Deutsch)

Das Thema der Überwachung von Individuen oder einer ganzen Gesellschaft gewann bereits mit der flächendeckenden Verbreitung von E-Mails und dem World Wide Web ungemein an Bedeutung. Nun steigert sich diese neue Möglichkeit der Kontrolle und Informationssammlung durch einen technologischen Fortschritt möglicherweise ins Unermessliche. Wie bereits Mark Weiser mit seinen Theorien über Ubiquitous Computing in den 90er Jahren voraussah, lässt sich der technologische Fortschritt aus unserem alltäglichen Leben nicht mehr wegdenken. Das Schlagwort Internet der Dinge spielt bei dieser fortschreitenden Form der privaten Überwachung eine besonders wichtige Rolle.

Beim Gedanken an diese möglicherweise flächendeckende Überwachung der Gesellschaft, durch simpel wirkende, technische Gadgets, die den Nutzenden das tägliche Leben auf den ersten Blick erleichtern und nicht beschwerlicher machen sollten, eröffnet sich eine Frage: Wie sehr wirkt sich Überwachung durch das Internet der Dinge auf unser Leben aus und in wie fern sind wir selbst dafür verantwortlich, indem wir diese Kontrolle unseres privaten Lebens zulassen?

Zur Beantwortung dieser Frage soll zunächst der Aktuelle Forschungsstand im Bereich der Surveillance Studies erläutert werden. Hierzu werden, unter anderem, Abhandlungen von Diana R. Gordon, Mark Poster, David Lyon und Anders Albrechtslund als Beispiele herangezogen und bearbeitet. Anschließend findet eine einführende Definition des Internet der Dinge statt und es wird mithilfe der Abhandlung von Mark Weiser historisch an das Thema herangeführt. Danach soll die Relevanz des Themas erläutert werden. Abschließend findet die theoretische Analyse des Beispiels *Smart Home* statt. Diese Analyse findet transdisziplinär statt und beinhaltet eine medienwissenschaftliche, eine soziologische und eine biopolitische Perspektive.

7.2 Abstract (Englisch)

Surveillance of the society and its individuals has become an increasingly important issue, since time internet, electronic mail and world wide web have conquered the world. The ongoing technical progress will raise the level of surveillance to an unprecedented scale, one can hardly imagine at this point.

“The Computer for the 21st Century” - Mark Weiser’s theory about the triumph of ubiquitous computing - no longer is a fictional story, as it was in the 90s. Ubiquitous computing has become part of our reality. Nowadays the buzzword “Internet of Things” takes a meaningful part in the ongoing process of monitoring individual-related data.

Considering the possibility of exhaustive surveillance of the society, by the help of simple technical gadgets, such as an intelligent fridge or a biometric door lock, there are a lot of questions that come up: In what ways does Smart Home surveillance and other technical surveillance in private space, made possible by the Internet of Things, affect the personal lives of single individuals? Are the users themselves to blame for this kind of surveillance, because of the permission they give to institutions and government, to control their individual-related data?

In order to answer these questions, this paper starts with a comprehensive theoretical analysis of different scientific theories from the genre of surveillance studies. The theoretical part deals with works by authors such as Diana R. Gordon, Mark Poster, David Lyon and Anders Albrechtslund among others. Afterwards the topic’s relevance will be explained and a historical introduction, which investigates the work of Mark Weiser, will lead to the main part of the paper. The paper will conclude with the transdisciplinary, theoretical analysis of the chosen example “Smart Home”. The analysis will include three focal points – media studies, sociology and biopolitics.

7.3 Lebenslauf

Persönliche Daten:

Name	Patricia Eva Groll
Geburtsdatum	23.01.1991
Nationalität	Deutschland

Ausbildung

2014 – Heute	Universität Wien Universitätsring 1, 1010 Wien, Österreich Masterstudium: Theater-, Film- und Mediengeschichte Voraussichtlicher Abschluss: Master of Arts
2010 – 2013	Universität Regensburg Universitätsstraße 31, 93053 Regensburg, Deutschland Bachelorstudium: Hauptfach: Medienwissenschaften, Nebenfach: Kunstgesichte Abschluss: Bachelor of Arts (2,3) am 29.08.2013
2001 – 2010	Gymnasium Starnberg Rheinlandstraße 2, 82319 Starnberg, Deutschland Abschluss: Allgemeine Hochschulreife (2,4) am 25.06.2010
1997 – 2001	Grund- und Teilhauptschule Söcking Bismarckstraße 13, 82319 Starnberg, Deutschland