Masterarbeit

WERTSCHÖPFUNG IN ZEITEN DER DIGITALEN SELBSTVERMESSUNG

Befunde zur Einstellung von Wearable-NutzerInnen in Österreich im Umgang mit persönlichen Daten im Gesundheits- und Fitnesskontext

an der Fachhochschule St. Pölten

von

Katharina Andratsch

MM1710404801

Begutachter:

FH-Prof. Priv.-Doz. Dr. Michael Litschka

Zweitbegutachter:

FH-Prof. Dr. phil. Jan Krone M.A.

St. Pölten, am 30.08.2019

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Masterarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfe bedient habe.

- ich dieses Masterarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

Diese Arbeit stimmt mit der vom Begutachter/von der Begutachterin beurteilten Arbeit überein.

....

Ort, Datum Unterschrift

Danksagung

An dieser Stelle möchte ich mich herzlich bei all jenen bedanken, die mir bei der Erstellung dieser Masterarbeit unterstützend zur Seite gestanden sind.

Großer Dank gilt Florian, der mit guten Ideen einen wichtigen Beitrag zu dieser Masterarbeit leistete und kontinuierlich zu meiner Motivation beigetragen hat. Auch bei Maresa und Martin möchte ich mich für die wertvollen Ratschläge zu dieser Masterarbeit bedanken. Danke für den stets konstruktiven Austausch mit meiner Freundin Paula. Daneben gilt mein Dank Adi für die zahlreichen Stunden des Lektorats.

Bedanken möchte ich mich an dieser Stelle auch nochmals bei den Teilnehmenden der Fokusgruppe sowie bei Nicola, die mich bei der Diskussionsrunde tatkräftig unterstützt hat. Ein herzliches Dankeschön gilt meinem Betreuer, Herrn FH-Prof. Priv.-Doz. Dr. Michael Litschka, der mich stets durch konstruktive Ratschläge unterstützt hat.

Großer Dank gilt vor allem meinen Eltern für die Unterstützung während des gesamten Studiums. Außerdem möchte ich meine KommilitonInnen und FreundInnen erwähnen, die mir während meines Studiums stets helfend zur Seite standen.

Zusammenfassung

Technologische Entwicklungen führen zu einer stetig und massiv steigenden Anzahl an Datensätzen aus unterschiedlichen Quellen wie z. B. Anwendungen des Consumer Internet of Things, Sensornetzwerke und Daten aus mobilen Anwendungen. Die Welle an Daten bietet die Chance neue Geschäftsmodelle bzw. neue oder bestehende Wertschöpfungsstrukturen zu gestalten, um generierte Informationen zu verwerten und daraus Nutzen für Organisationen zu ziehen. Produkt- und Servicelösungen im Bereich mHealth bieten gleichzeitig Potenziale für NutzerInnen: Das Beobachten, das Verorten und das eigenständige Handeln auf Basis von selbstgemessenen Daten. Die gemessenen Daten werden oftmals – bewusst und unbewusst – mit Organisationen geteilt. Es ergeben sich Problemfelder hinsichtlich der informationellen Privatheit für NutzerInnen.

Ziel dieser Masterarbeit ist es, die Wertschöpfung im Rahmen der digitalen Selbstvermessung näher zu beleuchten und Befunde zur Einstellung von Wearable-NutzerInnen in Österreich im Umgang mit persönlichen Daten im Gesundheits- und Fitnesskontext zu erheben.

Für die Beantwortung der definierten Forschungsfragen wurden eine umfangreiche Literaturrecherche sowie eine qualitative Datenerhebung mittels Fokusgruppe durchgeführt. Aufgrund der ausgewählten Methode konnten subjektive Einstellungen von Wearable-NutzerInnen in Österreich im Hinblick auf ihre Privatsphäre erhoben werden. Die Analyse dieser Daten ergibt, dass Interesse am Schutz der informationellen Privatheit besteht. Die Datenfreigabe im Alltag wird jedoch aufgrund der Abstraktion der Thematik und der Intransparenz möglicher Konsequenzen nicht bewusst wahrgenommen. Zudem können Einstellungen wie Resignation und Gleichgültigkeit der Datennutzung durch Organisationen, sowie die wahrgenommene Handlungsunfähigkeit der Individuen hinsichtlich des Datenschutzes festgestellt werden. Die Befunde zeigen, dass sich die NutzerInnen über die Relevanz persönlicher Daten für Organisationen bewusst sind. Dabei werden mögliche individuelle und gesellschaftliche Konsequenzen diskutiert.

Basierend auf diesen Ergebnissen lassen sich Handlungsempfehlungen, wie die Stärkung des Konsumentenvertrauens hinsichtlich des Datenschutzes, die Transparenz im Umgang mit persönlichen Daten und die Integration der NutzerInnen durch Kontroll- und Handlungsmöglichkeiten, für Organisationen in der Gesundheits- und Fitnessökonomie ableiten.

Abstract

Technological developments lead to a steadily and massively increasing number of data sets from different sources, e.g. Consumer Internet of Things applications, sensor networks, and mobile application data. The wave of data offers the opportunity to design new business models, as well as existing, or, new value creation structures, in order to exploit generated information and to derive benefits for organizations. At the same time, product and service solutions, in the mHealth area, offer potential for users: observing positioning and autonomous action, based on self-measured data. The measured data are often - consciously, and, unconsciously - shared with organizations. There are problems regarding informational privacy for users.

The aim of this master thesis is to take a closer look on added value in the context of digital quantified self, and to collect findings from the recruitment of wearable users, in Austria, in dealing with personal data, in regards to the context of health and fitness.

To answer the defined research questions, a comprehensive literature research, as well as, a qualitative data collection, via the focus group, was carried out. Due to the selected method, subjective attitudes of wearable users in Austria, regarding their privacy, can be raised. The analysis of the data shows that there is a specific interest in the protection of informational privacy. However, the data release in everyday life is not consciously perceived, due to the abstraction of the topic, and the lack of transparency of possible consequences. In addition, attitudes such as resignation and indifference of data use by organizations can be identified, as well as, the perceived inability to act of the individuals regarding the protection of privacy. The findings show that users are aware of the relevance of personal data usage for organizations. In this context, possible individual and social consequences are discussed.

Finally, the findings allow for deriving a set of measures for organizations in the health and fitness economy, such as the strengthening of consumer confidence, in connection with data protection, the transparency of personal data usage, and the integration of users through individual control and action options.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AEUV……Vertrag über die Arbeitsweise der Europäischen Union

CIoT……..……..Consumer Internet of Things

bzw. ……..…..…….……..beziehungsweise

d. h. ……,…….……..das heißt

EKG…….……Elektrokardiogramm

EU-DSGVO……....Europäische Datenschutz-Grundverordnung

etc. ……..……...……. et cetera

GPS……..…….……. Global Positioning System

NFC…….. Near Field Communication

o. D. …….…….……ohne Datum

OECD……...…… Organisation für wirtschaftliche Zusammenarbeit und Entwicklung

o. S. ……..……ohne Seite

PD…….…….…….Personal Data

PPM-Modell…….……. Privatsphäre-Prozess-Modell

SMS……...…….. Short Message Service

u. a. ……..……..unter anderem

WHO……..….. World Health Organization

WLAN…….……. Wireless Local Area Network

z. B. …….……...…….zum Beispiel

A. Theoretischer Teil

1 Einleitung

“If this is the age of information, then privacy is the issue of our times.” Acquisti et al. 2015, S. 1

Dieses Zitat soll die Relevanz der informationellen Privatheit für Individuen verdeutlichen. Die vorliegende Masterarbeit beschäftigt sich mit der Wertschöpfung im Rahmen der digitalen Selbstvermessung. Besonderes Augenmerk liegt dabei auf der NutzerInnenperspektive. Es wird die Einstellung von Wearable-NutzerInnen in Österreich im Umgang mit persönlichen Daten im Gesundheits- und Fitnesskontext erforscht. Die folgenden Unterkapitel bieten einen Überblick über die vorliegende wissenschaftliche Arbeit.

1.1 Ausgangslage und Problemstellung

Aktivitäten, die in der analogen Welt privat waren oder nur mit wenigen Personen geteilt wurden, hinterlassen durch die zunehmende Vernetzung digitale Datenspuren, die Aufschluss über Verhalten, Interessen und Überzeugungen von Individuen geben können. Aktivitäten in digitalen Umgebungen, wie beispielsweise das Verhalten von Individuen bei der Nutzung digitaler Geräte, Online-Transaktionen oder kommunikative Handlungen im Internet können – bewusst und unbewusst – mit Unternehmen geteilt werden. Die Explosion des Datenvolumens durch die steigende Anzahl der Datenproduzenten aufgrund neuer Technologien, sowie die Beschleunigung der Datenerfassung durch neue technologische Möglichkeiten, führen zu einer stetigen Weiterentwicklung der Aggregation von Daten und eine darauf basierte Prognose des Verhaltens der NutzerInnen (vgl. Acquisti et al. 2015, S. 184; Morlok et al. 2018, S. 180). Unternehmen entwickeln vermehrt Geschäftsmodelle, die auf der Nutzung von persönlichen Daten basieren. Organisationen mit Zugang zu diesem Rohstoff können persönliche Daten zu verbesserten Produktions- und Vertriebsabläufen, zur Produktentwicklung und –innovation (vgl. Schweitzer/Peitz 2017, S. 8), zur kundenspezifischen Personalisierung, sowie zur Verbesserung des Marketings nutzen (vgl. Novotny/Spiekermann 2015). Insbesondere Einblicke in das Verhalten von Individuen, sowie die Ableitung von Interessen, sind für Organisationen von erheblicher Relevanz (vgl. Morlok et al. 2017, S. 18f). Daher wird

persönlichen Daten, vor allem wenn diese in einer Vielzahl vorliegen, zunehmend ein ökonomischer Wert zugewiesen (vgl. Spiekermann/Korunovska 2017, S. 2-4).

Ökonomische Aspekte sind im Rahmen der Privatheitsforschung sowohl auf individueller, als auch auf gesellschaftlicher Ebene von Bedeutung (vgl. Morlok et al. 2017, S. 2). In der Literatur wird auf die ungleiche Machtverteilung zwischen NutzerInnen, die Daten generieren, und Unternehmen, die Daten verwalten, hingewiesen. Gründe dafür sind u. a. Unsicherheiten von KonsumentInnen, geprägt durch unvollständige Information und Informationsasymmetrien zugunsten von etablierten Marktakteuren, aber auch psychologische Verhaltensaspekte der NutzerInnen. Laut Acquisti/Grossklags (2005) sind Individuen bereit ihre Privatsphäre, d. h. persönliche Daten gegen Komfort oder relativ kleine Belohnungen wie Rabatte zu tauschen (S. 24-30). Dabei wurde erkannt, dass die Sensibilität der Daten, der Datenempfänger und der Kontext, in dem die Information weitergegeben wird, die Kompensationserwartungen der NutzerInnen beeinträchtigen (vgl. Spiekermann/Korunovska 2017, S. 3f). Aus wissenschaftlicher Perspektive ist es daher notwendig darauf hinzuweisen, dass Privatsphäre im Hinblick auf persönliche Daten im Internet ein kontextuelles Phänomen ist (vgl. Kokolakis 2015, S. 23). Im Allgemeinen werden informationelle Daten in unterschiedlichen Bereichen der Wirtschaft und der Forschung systematisch erhoben. Aufgrund der Kontextbezogenheit von individuellen, privatheitsbezogenen Entscheidungen beschränkt sich die vorliegende Arbeit auf persönliche Daten im Rahmen der Medienökonomie, am Beispiel von Wearables im Gesundheits- und Fitnesskontext.

Selbstvermessungstechnologien wie Wearables können unterstützende Alltagsbegleiter sein, die einer Person Autonomie und Kontrolle über Körper und Gesundheit ermöglichen (vgl. Moll et al. 2017, S. 5). Die dabei generierten Datenressourcen können verwendet werden um datengetriebene Geschäftsmodelle im Rahmen der Fitness- und Gesundheitsökonomie zu erweitern bzw. zu etablieren. Die Wertschöpfung persönlicher Information von NutzerInnen im Rahmen der digitalen Selbstvermessung ist demnach ein zentraler Kern dieser Arbeit. Damit KonsumentInnen langfristig von dieser Entwicklung profitieren und neue Geschäftsmodelle akzeptieren, gilt es deren Einstellungen hinsichtlich der informationellen Privatheit im Forschungskontext zu untersuchen.

1.2 Zielsetzung und Forschungsfragen

In dieser Masterarbeit wird das Konzept der digitalen Selbstvermessung bei der Nutzung von Wearables im Gesundheits- und Fitnesskontext beschrieben. Zudem wird die Relevanz persönlicher Daten im Rahmen der digitalen Selbstvermessung für kommerzielle Organisationen anhand der datengetriebenen Wertschöpfung skizziert. Dies bietet die Basis für die Interpretation der Thematik aus NutzerInnenperspektive, da mögliche Konsequenzen für KonsumentInnen hinsichtlich der Privatheit aufgezeigt werden können. Ziel dieser Masterarbeit ist es Befunde zur Einstellung von Wearable-NutzerInnen in Österreich im Umgang mit persönlichen Daten im Gesundheits- und Fitnesskontext zu erheben.

Die vorliegende Arbeit ist dahingehend aufgebaut folgende zentrale Forschungsfrage zu beantworten:

> » Welche Einstellungen haben NutzerInnen von Wearables im Gesundheits- und Fitnesskontext in Österreich hinsichtlich ihrer Privatsphäre? «

Diese Leitfrage wird mit folgenden Forschungsfragen präzisiert:

	Forschungsfrage	**Erkenntnisgewinnung**
FF1	Wie definieren NutzerInnen von Wearables in Österreich „Persönliche Daten“ im Gesundheits- und Fitnesskontext?	Fokusgruppe im empirischen Teil dieser Masterarbeit (Kapitel 7-9)
FF2	Wie bewerten NutzerInnen von Wearables in Österreich mögliche Konsequenzen durch die Datenfreigabe an Organisationen im Gesundheits- und Fitnesskontext?	

Tabelle 1: Forschungsfragen, eigene Darstellung.

Die Ergebnisse der explorativen Forschung, im empirischen Teil dieser Masterarbeit, sollen einen wissenschaftlichen Beitrag für die Privatheitsforschung von Individuen im Kontext von Wearables leisten. Zudem können die Erkenntnisse der Studie Relevanz für Unternehmen mit datengetriebenen Geschäftsmodellen im Bereich der Fitness- und Gesundheitsökonomie aufweisen.

Ausschlaggebend für die Auswahl des Forschungsgegenstandes ist die Relevanz der Thematik für den transformierenden Medienmarkt in Europa. Aufgrund der Zunahme der Datenvielfalt durch technologische Entwicklungen (vgl. DSGVO-Gesetz 2018a), der entsprechend vereinheitlichten regulatorischen Rahmenbedingungen, wie die europäische Datenschutz-Grundverordnung, zur Schaffung eines europäischen Binnenmarktes für personenbezogene Daten (vgl. DSGVO-Gesetz 2018b) und der Forderung nach Transparenz durch KonsumentInnen, ist diese Thematik höchst aktuell. Daher wird diese im Rahmen dieser Arbeit am Anwendungsfall Wearables in der Fitness- und Gesundheitsbranche im wissenschaftlichen Kontext erforscht.

Die Fragestellungen dieser Masterarbeit basieren auf der Konvergenz von Technologie, Internet und Medien und werden im Rahmen der Wirtschaftswissenschaften innerhalb der Medienökonomik diskutiert. Die Medienökonomik ist eine Teildisziplin der Publizistik- und Kommunikationswissenschaft, die wirtschaftliche und publizistische Phänomene des Mediensystems unter Rückgriff auf ökonomische Theorien untersucht (vgl. Kiefer/Steininger 2014, S. 41). Laut Altmeppen und Karmasin (2003) befasst sich die Medienökonomie mit jenem Teilbereich wirtschaftlichen Handelns, der mit Ressourcenallokation, Produktion, Tausch und Nutzung bzw. dem Konsum von Medien zusammenhängt (S. 7ff). Die Autorin der Masterarbeit bedient sich zur Beantwortung der Forschungsfragen außerdem an Erkenntnissen der Sozialwissenschaften und der Verhaltensökonomie.

1.3 Methodisches Vorgehen

Die vorliegende Arbeit ist in zwei Abschnitte gegliedert. Teil A umfasst den theoretischen Teil, in dem die gegenwärtige Fachliteratur dieser Thematik verarbeitet wird. Es werden Meinungen von unterschiedlichen AutorInnen zusammengeführt, ergänzt und gegenübergestellt. Auf Basis eines logischen und deduktiven Aufbaus wird eine Wissensgrundlage geschaffen, die für Teil B, der die empirische Forschung behandelt, erforderlich ist. Für die Auswahl der Literatur wurden Bücher und Journals für die Fachgebiete Business Economy, Economics of Information Security, Information Systems, Computer, Security und Recht, Marketing und Medienpsychologie herangezogen. Der Fokus der Betrachtung liegt im europäischen Raum, wobei im angelsächsischen

Kulturraum ein erheblicher Beitrag an Forschungstätigkeit zu dieser Thematik geleistet wurde.

In Teil B, der empirische Untersuchung dieser Arbeit, werden die definierte Leitfrage sowie die Sub-Forschungsfragen beantwortet. ProbandInnen der Fokusgruppe sind österreichische Wearable-NutzerInnen im Alter von 18-49 Jahren. Bei der Auswahl wird darauf geachtet, dass die Diskussionsgruppe nach Geschlecht, Alter und Beruf (in Ausbildung, selbstständig und unselbstständig erwerbstätig) ausgewogen ist, damit breit gefächerte Meinungen einer in sich homogenen Gruppe an Wearable-NutzerInnen eingeholt werden können.

Die Datenerhebung erfolgt dabei durch eine Fokusgruppe, die mithilfe der qualitativen Inhaltsanalyse nach Mayring ausgewertet wird. Anschließend werden die gewonnenen Erkenntnisse aus der Aufarbeitung der bestehenden Literatur und der Auswertung der empirischen Forschung gegenüber gestellt. In der Conclusio dieser Arbeit werden die Ergebnisse der Forschung dargelegt und die Leitfrage inklusive Sub-Forschungsfragen beantwortet und interpretiert.

1.4 Aufbau der Arbeit

Die vorliegende Masterarbeit lässt sich in neun Hauptkapitel gliedern. Das erste Kapitel, die Einleitung, bietet einen Überblick des wissenschaftlichen Vorgehens. Dabei wird näher auf die Ausgangslage und Problemstellung der Forschungsthematik, die Zielsetzung inklusive den Forschungsfragen, das methodische Vorgehen sowie auf den Aufbau der Arbeit eingegangen.

Im zweiten Kapitel werden die zentralen Begriffe dieser Arbeit definiert um grundlegende Termini zu klären. Dadurch wird für alle LeserInnen ein einheitliches Verständnis der Begriffe gewährleistet.

Die nachfolgenden Kapitel bilden die für den Forschungskontext relevanten Teile der Masterarbeit ab. Kapitel drei, vier und fünf beinhalten die Reflexion der bestehenden Literatur. Dabei werden die Themen digitale Selbstvermessung und Wearables im Gesundheits- und Fitnesskontext, datengetriebene und interaktive Wertschöpfung aus institutioneller Perspektive und Aspekte der informationellen Privatheit auf

NutzerInnenebene verarbeitet. Innerhalb dieser Kapitel werden Vorteile und Konsequenzen, die sich für Individuen aufgrund der Datennutzung durch Organisationen ergeben können, verarbeitet.

Das sechste Kapitel rundet den Literaturteil ab und setzt das Forschungsziel für die empirische Untersuchung. Die Methodologie der Forschung wird in Kapitel sieben näher erläutert. Dieses Kapitel stellt die Basis für den darauffolgenden Abschnitt, die Ergebnisse der Datenauswertung sowie deren Interpretation, dar.

Das abschließende Kapitel neun dieser Arbeit umfasst die Conclusio. Hier werden die Forschungsergebnisse nochmals zusammengefasst und interpretiert, um die Forschungsfragen zu beantworten. In diesem Zusammenhang werden auch weitere Forschungsempfehlungen und Limitierungen dieser Masterarbeit erläutert.

2 Begriffsabgrenzungen

Die nachstehenden Definitionen, der für diese wissenschaftliche Arbeit relevanten Begriffe „Persönliche Daten“ und „Informationelle Privatheit“, dienen dem grundsätzlichen Verständnis der Termini im Rahmen dieser Masterarbeit.

2.1 Der Begriff „Persönliche Daten“

Bevor der Begriff „Persönliche Daten“ definiert werden kann, muss zunächst auf die Heterogenität der Definition und auf die Klassifikation von Daten hingewiesen werden. Daten lassen sich unter anderem auf Basis ihrer Struktur (unstrukturiert, strukturiert oder semi-strukturiert), nach Datenformat (u. a. Text-, Bild-, Video-Datei), nach dem Bezug (personenbezogen oder nicht-personenbezogen), sowie aufgrund der Erzeugungsart (maschinenerzeugt oder nicht-maschinenerzeugt) unterscheiden. (vgl. Dewenter 2018, S. 5)

Zudem können Daten auf physikalischer, syntaktischer und semantischer Ebene erfasst werden (vgl. ebd.). Die physikalische Betrachtung setzt auf der Ebene des Datenträgers an. Auf syntaktischer Ebene sind Daten als Zeichen, aus denen sie bestehen, zu verstehen. Das rechtlich geschützte Gut ist dabei der binäre Code. Der Dateninhalt, wie beispielsweise der Name einer Person bei personenbezogenen Daten, ist im Rahmen des semantischen

Datenverständnisses bedeutsam. Rechtsgebiete, die für den kommerziellen Umgang mit Daten relevant sind, greifen auf syntaktischer und insbesondere auf semantischer Ebene (vgl. ebd.).

2.1.1 Begriffsdefinition und rechtliche Grundlage: „Persönliche Daten“

Der Schutz von Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht und in der Charta der Grundrechte der Europäischen Union sowie im Vertrag über die Arbeitsweise der Europäischen Union (AEUV) verankert (vgl. DSGVO-Gesetz 2018b). Aus rechtlicher Perspektive wird der Begriff personenbezogene Daten im Rahmen der EU-Datenschutz-Grundverordnung (EU-DSGVO), die 2016 beschlossen und seit 2018 in allen EU-Mitgliedsstaaten unmittelbar anwendbar ist, konkreter definiert:

> „Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person […] beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind,“ Art. 4 Nr.1 – EU-DSGVO (Datenschutz-Grundverordnung 2018d).

Die Verarbeitung von personenbezogenen Daten ist grundsätzlich verboten („Verbot mit Erlaubnisvorbehalt“). Die Erlaubnisse für eine rechtmäßige Verarbeitung sind in Artikel 6 (1) DSGVO a - f festgeschrieben, wobei mindestens einer der sechs Rechtsgrundsätze Anwendung finden muss (vgl. Jusline 2019a). In der Praxis relevant sind: Die informierte und explizite Einwilligung seitens der DateninhaberInnen (a), weiters die Vertragserfüllung (b), sowie berechtigte Interessen des Verantwortlichen oder eines Dritten, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen (f) (vgl. ebd.).

Zudem gelten besondere Datenverarbeitungsvorschriften für sensible Daten, beispielsweise für Gesundheitsdaten (vgl. Jusline 2019b). Wearable-Anbieter sind in der Regel dazu angehalten eine Einwilligung für die Erhebung und Nutzung von Gesundheitsdaten einzuholen (vgl. Moll et al. 2017, S. 27f).

Aus rechtlicher Perspektive wird der Begriff „Personenbezogene Daten“ verwendet. In der Forschungsliteratur zum Konzept der Privatheit, insbesondere aus der Perspektive der NutzerInnen, ist der Begriff „Persönliche Daten“, engl. personal data (PD), gebräuchlich. Die vorliegende Arbeit bezieht sich im Hinblick auf die Ökonomisierung persönlicher Daten auf medienökonomische Aspekte sowie auf die Betrachtung auf NutzerInnenebene. Daher wird der Begriff „Persönliche Daten“ in dieser Masterarbeit verwendet.

2.1.2 Kategorisierungsversuch „Persönliche Daten“

Im Rahmen der ökonomischen Betrachtung bei der Nutzung von Daten bietet sich eine Unterteilung in personenbezogene und nicht-personenbezogene Daten an (siehe **Tabelle 2**). Es ist zu berücksichtigen, dass pseudonyme Daten durch die Datenaggregation Informationen zu identifizierbaren Personen enthalten können (vgl. DSGVO-Gesetz 2018e). Uneinigkeit besteht darüber, ab welchem tatsächlichen Anonymisierungsgrad[1] ein Datum nicht mehr einer Person zugeordnet werden kann und wann mit aufwändigen Methoden eine Deanonymisierung möglich ist (vgl. Dewenter 2018 S. 18). Das Problem zeigt sich in der Profilbildung aus per se anonymen Daten, die durch entsprechende Maßnahmen eine Identifizierbarkeit erlauben. Ein wesentlicher Unterschied zwischen personenbezogenen und nicht-personenbezogenen Daten liegt darin, dass personenbezogene und pseudonyme Daten durch das Datenschutzrecht beeinflusst werden.

Die Erzeugungsart der Daten in der Unterscheidung zwischen maschinen- oder nutzergenerierten Daten ist kein geeignetes Kriterium zur Feststellung von Personenbezogenheit. Denn maschinell erzeugte Daten weisen insbesondere im Konsumentenbereich durch vernetzte Endgeräte im Rahmen von Consumer Internet of Things (CIoT) ein hohes Maß an Personenbezogenheit auf (vgl. Dewenter 2018, S. 6). Smartwatches und Fitnesstracker zeichnen umfangreiche und zum Teil sensible Informationen über deren NutzerInnen auf, wie beispielsweise Standort-, Aktivitäts- und Verhaltensdaten, Gesundheits- und Kommunikationsdaten.

[1] Anonymisierte Daten (d. h. nicht-personenbezogene Daten) sind Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Die Verarbeitung anonymer Daten ist nicht im Rahmen der EU-DSGVO geregelt. (vgl. DSGVO-Gesetz 2018e)

Laut OECD (2013) werden persönliche Daten von UserInnen folgendermaßen definiert*:*

> "Any information relating to an identified or identifiable individual (data subject)."

Dieses breite Konzept bezieht sich laut OECD auf folgende Arten von Daten: Nutzergenerierte Inhalte, Aktivitäts- oder Verhaltensdaten, soziale Daten, Standortdaten, demographische Daten und Daten offizieller Natur. Zusammengefasst werden unter persönliche Daten sämtliche digital verfügbaren Informationen über das Online- oder Offline-Verhalten einer Person verstanden (vgl. OECD 2013, S. 8).

In dieser Arbeit sind insbesondere Gesundheitsdaten relevant. Laut EU-Datenschutz-Grundverordnung (DSGVO) fallen Gesundheitsdaten einer natürlichen Person unter die Definition sensibler Daten, diese sind besonders schützenswert.[2] Bei Gesundheitsdaten handelt es sich um personenbezogene Daten, die sich „auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen". (vgl. DSGVO-Gesetz 2018d)

Tabelle 2 zeigt einen Kategorisierungsversuch von personenbezogenen bzw. nicht-personenbezogenen Daten sowie eine Unterteilung in maschinenerzeugte und nicht-maschinenerzeugte Daten nach Dewenter (2018) in Verbindung mit der Kategorisierung „Persönlicher Daten" laut OECD (2013) und der rechtlich im EU-Raum geltenden Definition von sensiblen Daten nach der EU-DSGVO.

[2] Weitere sensible Daten laut EU-DSGVO 2018 sind in Tabelle 2 in der Zeile „Sensible Daten" abgebildet.

EU-DSGVO Art. 9 Abs. 1	**Kategorisierung Persönliche Daten nach OECD 2013, S. 8**	**Maschinenerzeugte Daten**	**Nicht-maschinenerzeugte Daten**
	Personenbezogene Daten		
	Soziale Daten	Kontaktdaten (Telefonbucheinträge, Kontakte aus sozialen Netzwerken)	Kontaktinformationen (Name, Adresse, Telefonnummer)
	Nutzergenerierte Daten	Bilder, Videos (u. a. aus sozialen Netzwerken)	Textbeiträge, Bilder, Videos, Kommentare, E-Mails, Briefe etc.
	Standortdaten	Standortdaten (Standort- und Bewegungsprofile aus GPS-Daten des Smartphones)	
	Aktivitäts- oder Verhaltensdaten	Computer-, Netzzugang (IP-Adresse, URL, Cookies, Browserdaten, App-Nutzungsdaten)	
		Kaufverhalten (Suchanfragen, Standorte, Auswahl der Treffer, Präferenzen)	
		Suchverhalten (Suchanfragen, Standorte, Präferenzen)	
		eHealth[3] (Patientendaten, Krankheitsprofile, Medikamentierungen)	
		Wearables (Herz- und Pulsfrequenz, Bewegungs- und Aktivitätsprofile)	
		Smart Home Anwendungen (Elektrizitäts-, Gas-, und Wasserverbrauch)	
		Fahrzeugdaten (Fahrverhalten, Standortprofile)	
	Soziodemografische Daten		Persönliche Detailangaben wie Alter, Geschlecht, Geburtsdatum, Familienstand, Staatsangehörigkeit, Einkommen, sexuelle Orientierung, politische Einstellungen

[3] Daten zu eHealth, Wearables, Smart Home Anwendungen sowie Fahrzeugdaten werden nicht in OECD (2013) erwähnt. Da es sich um Aktivitäts- und Verhaltensdaten handelt, werden diese in dieser Darstellung nach Dewenter (2018) erweitert.

	Daten offizieller Natur		Kontaktinformationen wie Name, Wohnadresse, Telefonnummer
			Konto- und Finanzdaten
			Gesundheitsdaten, Sozialversicherungsnummer, Vorstrafenregister
Sensible Daten			Rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung (vgl. Jusline 2018)
	Nicht-personenbezogene Daten (Sachdaten)		
		Verkehrsdaten	Bild- und Videomaterial von Umgebungen
		Wetterdaten	Textanalysen
		Automobildaten (Verbrauch, Geschwindigkeiten etc.)	Anonyme Konsumentenbefragung
		Finanzmarktdaten	Wahlumfragen
		Maschinendaten	
		Produktionsdaten	
		Logistikdaten	

Tabelle 2: Kategorisierungsversuch „Persönliche Daten“. Eigene Darstellung in Anlehnung an Dewenter 2018, S. 8; OECD 2013, S. 8.

2.2 Der Begriff Privatheit

Das Konzept der Privatheit [4] wird seit Jahrzehnten in unterschiedlichen Wissenschaftsdisziplinen erforscht. Dabei betrachtet die wertebasierte Definition des Begriffs die allgemeine Privatsphäre als ein Menschenrecht mit wesentlichem Bestandteil des Wertesystems der Gesellschaft (vgl. Smith et al. 2011, S. 933).

Der Begriff „Privacy“ (engl.) wird in der deutschsprachigen Fachliteratur oft als Synonym für die Begriffe „Privatsphäre” oder „Privatheit” verwendet. Die Privatsphäre findet sich im rechtlichen Kontext in der Sphärentheorie (Sozialsphäre, Privatsphäre und Intimsphäre) wieder und beschreibt räumliche beziehungsweise materielle Aspekte wie das persönliche Heim, Hab und Gut (auch persönliche Daten) eines Individuums (vgl. Geminn/Roßnagel 2015 S. 705f nach Masur et al. 2018, S. 4). In akademischen Kontexten hat sich, aufgrund der ganzheitlichen Betrachtung, der Begriff Privatheit gegenüber jenem der Privatsphäre durchgesetzt (vgl. Masur et al. 2018, S. 5).

Die Privatheit eines Menschen bemisst wie stark sich dieser aus der Gesellschaft zurückzieht. Es wird daher von einer *individuellen Abgeschiedenheit* gesprochen. Die beiden Aspekte Freiwilligkeit und Kontrollmöglichkeit einer Person sind dabei essentiell. Diese finden sich in der Definition von Westin, 1967 wieder:

> „Privacy ist the voluntary and temporary withdrawal of a person from the general society through physical and psychologial means“.

Im Hinblick auf den Aspekt Freiwilligkeit sollten Individuen den Anspruch haben, für sich selbst zu bestimmen, wann, wie und in welchem Ausmaß Informationen weitergegeben werden. Neuere Definitionen gehen von der Kontrolle per se einen Schritt weiter und beschreiben die Fähigkeit des Individuums zur Kontrolle der Informationspreisgabe und Informationsverwendung (vgl. Morlok et al. 2017, S. 183f). Wenn ein Individuum persönliche Daten weitergibt, um beispielsweise eine mobile Applikation zu nutzen, könnte diese Information an Dritte weitergeleitet werden. Dies passiert oftmals bei der Verknüpfung von Online-Services bzw. Apps von Drittanbietern. Hier liegt die

[4] Das Konzept der Privatheit im digitalen Zeitalter findet in unterschiedlichen Disziplinen Anwendung: Philosophie, Sozial- und Politikwissenschaften, Recht, Psychologie, Wirtschaftswissenschaften sowie in der Informatik (vgl. Morlok et al. 2017, S. 182).

Datennutzung und -verbreitung außerhalb des Kontrollbereiches der NutzerInnen (vgl. ebd.). Es handelt sich hiermit um einen Kontrollverlust auf Seiten der NutzerInnen.

Insbesondere durch die Zunahme an vernetzten Geräten im Bereich von CIoT ergeben sich Herausforderungen für den Schutz der Privatsphäre des Individuums. Bei der Anwendung der allgemeinen Privatsphäre auf das KonsumentInnenverhalten wird der Begriff der vermehrt als Ware (vgl. Smith et al. 2011, S. 933), bzw. als wirtschaftliches Gut (vgl. OECD 2013; Spiekermann-Hoff/Korunovska 2017; Masur et al. 2018), betrachtet. Aus dieser Betrachtung ist der Terminus immer noch ein individueller und gesellschaftlicher Wert, jedoch nicht absolut, da ihm ein wirtschaftlicher Wert zugewiesen werden kann.

Demgegenüber konzeptualisieren Psychologen und Verhaltenswissenschaftler die allgemeine Privatsphäre des Individuums als subjektive Wahrnehmung und nicht als absoluten moralischen Wert, bzw. eine absolute moralische Norm (vgl. vgl. Smith et al. 2011, S. 933f). Die vielfältigen Forschungsstränge lassen unterschiedliche Konzepte der Privatheitsforschung erkennen. Diese werden in Kapitel 5 erläutert.

2.2.1 Informationelle Privatheit

Nach van Dijk (2009) weiterführend zu Westin (1967) lassen sich drei Aspekte von „Privacy“ unterscheiden:

(a) Zum einen „Physical privacy“, welche sich auf den Körper und die unmittelbare physische Umgebung einer Person bezieht. Diesen Grad der Intimität sieht van Dijk insbesondere in der Informations- und Kommunikationstechnologie sowie der Biotechnologie gefährdet. Darunter fallen Augen-, Gesichts-, Finger- oder Stimmenerkennung sowie Kontrollen in Eingangsbereichen durch Sensoren am Körper (vgl. van Dijk 2009, S. 113).

(b) Die „Relational privacy“, also das Recht Kontakte selektiv selbst zu bestimmen, umfasst jegliche Formen persönlicher Beziehungen und dem entsprechenden Verhalten. Das Aufzeichnen des Verhaltens mittels Kameras in Teilöffentlichkeiten, sowie das Aufzeichnen von Informationen zwischen Telefonnummern und elektronischen Mailboxen gefährdet diese Dimension der Privatsphäre (vgl. ebd.).

(c) Die „Informational privacy“, auch informationelle Privatheit, umfasst das Recht auf die selektive Weitergabe der persönlichen Daten (vgl. ebd., S. 14) Hierunter wird die Kontrolle, d. h. ob und wie persönliche Daten gesammelt, gespeichert, verarbeitet und verbreitet werden können, subsumiert (vgl. Kokolakis 2017, S. 2; Morlok et al. 2017, S. 183). Anstelle des Schutzes der Privatheit im Allgemeinen, rücken in dieser Dimension Datenschutz und Datensicherheit in den Fokus (vgl. van Dijk 2009, S. 114). Bei der Nutzung von Wearables und mobilen Applikationen im Bereich Gesundheit und Fitness ist diese Dimension der Privatheit betroffen, da NutzerInnen den Überblick und somit die Kontrolle über die gesammelten Daten sowie über die Verwertung der Daten verlieren können. Diese Masterarbeit bezieht sich demnach auf das Konzept der informationellen Privatheit von NutzerInnen.

2.2.2 Institutionelle Privatheit

Privatheit lässt sich zudem in soziale und institutionelle Privatheit unterteilen (vgl. Raynes-Goldie 2010). Erstere bezieht sich auf die Privatheit gegenüber gleichgestellten Mitmenschen. Unter institutioneller Privatheit ist die Privatheit des Individuums gegenüber Behörden und Unternehmen zu verstehen (vgl. ebd.). Die vorliegende Arbeit beschäftigt sich mit dem zweiten Aspekt von Privatheit, der institutionellen Privatheit. Privatheitseingriffe auf dieser Ebene entstehen einerseits durch die Kommodifizierung von Informationen und Meta-Daten, die durch die Nutzung von Anwendungen digitaler Technologien und die Online-Kommunikation geteilt werden (vgl. Sevignani 2016 nach Masur et al. 2018, S. 3) und andererseits durch die informationelle Überwachung von Personen (vgl. ebd.).

3 Digitale Selbstvermessung im Gesundheits- und Fitnesskontext

Die Konvergenz von mobilen Medien, Sensornetzwerken, GPS-gestützte Lokalisierungen, intelligenten Messverfahren und digitalen Datenauswertungen sowie die Schnittstelle zu Social-Media-Anwendungen, ermöglicht neue Praktiken der digitalen Selbstvermessung

und entwickelt damit neue Formen von Steuerungs- und Kontrollwissen für den Massenmarkt (vgl. Reichert 2016, S. 185-197).

Im folgenden Kapitel wird zunächst das Konzept der digitalen Selbstvermessung im Forschungskontext erläutert. Anschließend werden Begriffsdefinitionen und Informationen zur Wearable-Nutzung in Österreich dargestellt. Potenziale auf NutzerInnen- und Anbieterebene, sowie aufkommende Problemfelder im Rahmen der digitalen Selbstvermessung aus NutzerInnenperspektive werden in Kapitel 3.3 diskutiert.

3.1 Konzept der digitalen Selbstvermessung

Die digitale Vermessung des eigenen Körpers und seiner Aktivitäten im Alltag mit Gesundheits- und Fitness-Anwendungen ist mit dem Aufkommen entsprechender Mess-Technologien ein junges Phänomen (vgl. Wolff 2016, S. 1). Die Website http://www.quantifiedself.com, die 2007 von den amerikanischen Wired-Journalisten Gary Wolf und Kevin Kelly veröffentlicht wurde, hat eine internationale Quanitfied-Self-Bewegung ausgelöst (vgl. Wolf 2011). „Self knowledge through numbers“ ist der Leitgedanke der Vereinigung, die weltweit in mehreren Ländern Anwender, Entwickler und Anbieter digitaler Produkte für Sport, Gesundheit und anderen Bereichen der Nutzung persönlicher Daten vernetzt (vgl. Duttweiler et al. 2016, S. 22). Dabei handelte es sich in erster Linie um „Extremisten“, die einen Großteil ihres Lebens vermessen. Selbstvermessungstechnologien haben jedoch gerade im Gesundheits- und Fitnesskontext längst den Massenmarkt erreicht.

Die Verdatung von Körper- und Verhaltensfunktionen zielt im Allgemeinen auf die Herstellung eines Individuums ab, „that becomes a knowable, calculable and administrable object“ (vgl. Shove et al 2012 nach Reichert 2013, S. 187). Im Speziellen wird unter dem Begriff „Self-Tracking“ die technisch vermittelte Erforschung, Steuerung und Optimierung des Selbst durch die konstante Erhebung, Sammlung, Zusammenführung und Auswertung von Daten verstanden (vgl. Duttweiler et al. 2016, S. 10f). Dabei konnte festgestellt werden, dass Self-Tracking in der Regel eine „intime, wenig dauerhafte Praktik darstellt“ (ebd. S. 21). Pharabod et al. (2013) zeigte in einer qualitativen Studie drei Logiken der Selbstvermessung.

- Die *Logik der Überwachung* bezieht sich auf das Ziel, eine Verhaltensweise oder einen bestimmten Körperwert zu kontrollieren. Es wird ein selbstdefinierter Schwellenwert festgelegt, den es nicht zu überschreiten gilt, z. B. Gewicht. Die erhobenen Daten werden häufig nicht mit anderen geteilt, da sie als intim oder medizinisch wahrgenommen werden. (vgl. Pharabod et al. 2013 S. 108f nach Duttweiler et al. 2016, S. 21)
- Bei der *Logik der Routinisierung* geht es darum, schlechte Gewohnheiten abzuschaffen und neue Verhaltensweisen einzuüben, beispielsweise weniger zu rauchen. Diese Daten gelten in der Regel ebenfalls als intim und werden ungern geteilt (vgl. ebd. S. 21f).
- Die *Logik der Leistungsperfomance* bezieht sich in erster Linie auf sportliche Leistungen sowie das Gewicht. Es geht um das Erreichen von selbstgesteckten Zielen und nicht Schwellenwerte. Diese Messergebnisse werden gerne mit anderen geteilt. (vgl. ebd. S. 22).

3.1.1 Konzept der digitalen Selbstvermessung im Gesundheits- und Fitnesskontext

Die vorliegende Masterarbeit beschränkt sich auf Körper- und Gesundheitsdaten von Individuen. Das Zusammenspiel von Medien, Technik, Selbstreflexion und sozialer Kommunikation wird in diesem Zusammenhang konstituiert und lässt zunehmend die Grenze zwischen Selbst- und Fremdführung verschwimmen (vgl. Reichert 2016, S. 185-197). Die Fremdführung im Rahmen der digitalen Selbstvermessung verweist dabei auf das Interesse von Unternehmen, Arbeitgebern, Versicherungen und Gesundheitsbehörden (vgl. ebd. S. 193). Das Angebot an gesundheitsbezogenen mobilen Anwendungen wächst stetig und reicht von Fitness- und Ernährungs-Anwendungen bis hin zu medizinisch-orientierten Anwendungen im Bereich der Diagnostik und Therapie (vgl. Albrecht/von Jan 2016, S. 53f). Der Großteil der verfügbaren Angebote ist dabei dem kommerziellen Markt privater Organisationen zuzuordnen, der schwer zu überblicken und aufgrund des globalisierten Kontextes begrenzt regulierbar ist (vgl. Gigerenzer et al. 2016). Als Chance entsprechender Anwendungen wird jedoch die Selbstführung von KonsumentInnen im Gesundheitsgeschehen gesehen (vgl. Knöppler et al. 2016, S. 8). Auf Basis von ausgewerteten Daten können eigenverantwortlich Entscheidungen getroffen und damit

präventive Maßnahmen gesetzt werden. Der Schritt zur zunehmenden Selbstbestimmung der Individuen geht weiter in Richtung Selbstoptimierung.

Im Hinblick auf die digitale Selbstvermessung des Alltags wird seitens DatenschützerInnen auf die Verdatung, d. h. die Speicherung und Verarbeitung personenbezogener Datenbestände und die Entstehung detaillierter Datenvorräte über KonsumentInnen auf Unternehmensseite, hingewiesen (vgl. Reichert 2013, S. 186). Für etliche Marktakteure sind persönliche Daten, die aus der konstanten Verwendung von Wearables gewonnen werden, wertvoll um tiefgehende Erkenntnisse der NutzerInnen zu generieren (vgl. Wienecke et al. 2016).

3.2 Self-Tracking durch Wearables im Gesundheits- und Fitnesskontext

Digitale Technologien, wie Wearables im Bereich von Gesundheit und Fitness, bilden die Grundlage in der Beschaffung und Verarbeitung von persönlichen Nutzerdaten. Wearables (Smartwatch als Fitnesstracker, Fitnessarmband) bedeuten dabei einen Paradigmenwechsel weg vom klassischen elektronischen Endgerät in der Hand, hin zur Integration vernetzter Geräte, die nahe am Menschen sind. Durch intuitiv zu nutzende Objekte entsteht eine Mensch-Maschine-Schnittstelle, die datengetriebene Services und Produkte für NutzerInnen ermöglicht.

3.2.1 Begriffsdefinition: Wearables im Gesundheits- und Fitnesskontext

Die mobile Gesundheit, engl. „mHealth“, ist ein neues, dynamisches und expandierendes Feld der Gesundheitsversorgung (vgl. Albrecht 2016, S. 14f). Derzeit wurde kein Konsens über eine allgemein gültige Definition für den Begriff gefunden. Im Allgemeinen kann mHealth als eine durch Mobilgeräte elektronisch unterstützte Gesundheitsversorgung definiert werden (vgl. ebd.). Dazu werden Dienste wie GPS, Stimmerkennung, Short Message Service, Bluetooth genutzt (vgl. WHO 2011, S. 6). Die Gesundheitsversorgung wird demnach über jegliche Art mobiler Endgeräte geleistet, die unter Zuhilfenahme von Mobiltelefonen über Smartphones, Phablets, Tablets bis hin zu Wearables und anderen tragbaren und im Gesundheitskontext nutzbaren Geräten angeboten wird (vgl. Kay et al. 2011 nach Albrecht 2016, S. 15). Wie bereits erwähnt bezieht sich die vorliegende Masterarbeit auf die Nutzung von Wearables.

Wearable Computing Devices, Kurzform Wearables, sind am Körper tragbare, elektronische Kleingeräte wie zum Beispiel Smartwatches, Fitnessarmbänder oder Datenbrillen. Ein Gerät verfügt dabei über einen oder mehrere Sensoren zur Messung körperlicher Aktivitäten und ermöglicht die Datenübertragung über eine digitale Schnittstelle (Bluetooth, Near Field Communication (NFC) oder WLAN) an ein Smartphone oder Tablet (vgl. Delisle et al., 2016, S. 1f). Auf dem mobilen Endgerät ist eine Anwendung („App“) installiert, die Rohdaten des Wearables aggregiert und für NutzerInnen aufbereitet. Dieser Vorgang ermöglicht das Self-Tracking für NutzerInnen. Unter dem Begriff „App“ wird eine Anwendung, die auf mobilen Endgeräten genutzt werden kann, beschrieben. Apps werden häufig im mHealth-Kontext verwendet (vgl. Knöppler et al. 2016, S. 33).

Im Allgemeinen werden Fitnesstracker für das körperliche Training eingesetzt und verfügen über eine Vielzahl biometrischer Feedbackschleifen sowie Anweisungen, die NutzerInnen zu einem aktiven Handeln motivieren sollen (vgl. Reichert 2013 S. 191). Zur Aufzeichnung von Gesundheitsdaten werden Smartwatches (Armbanduhren mit Computerfunktionalität, Sensoren und Smartphone-Konnektivität) und Aktivitätstracker, insbesondere Fitnessarmbänder, verwendet. Fitnessarmbänder verfügen hauptsächlich über die Funktion der Aufzeichnung von aktivitäts- und gesundheitsbezogenen Daten (u. a. Distanzen, Zeit, Geschwindigkeit, Schrittzahl, Herzfrequenz oder Energieumsatz) (vgl. Moll et al. 2017, S. 4–6; Reichert 2013, S. 187).[5] Zu beachten ist, dass die generierten Daten nicht nur den individuellen NutzerInnen angezeigt werden. Die Wearable-Anbieter (Vertreiber der technologischen Geräte) können die generierten Inhalte erheben, speichern und nutzen (vgl. Moll et al. 2017, S. 5).

Mobile Gesundheitsanwendungen

Mobile Gesundheitsanwendungen sind Services, die im Bereich der körperlichen und geistigen Gesundheit zu Wellnesszwecken oder für medizinische Bereiche eingesetzt werden. Lucht et al. (2015) unterscheiden zwischen Medizin-Apps und Gesundheits-Apps. Gesundheits-Apps werden als mobile Anwendungen für NutzerInnen zur Erhaltung der Fitness und zur Unterstützung eines gesundheitsförderlichen Lebensstils beschrieben. Diese Applikationen können laut WHO-Definition das gesamte Spektrum von

[5] Die Funktionen von Fitnessarmbändern sind vom jeweiligen Modell abhängig und können auch Smartphone-Funktionen umfassen.

„Gesundheit“ abdecken und beziehen sich auf einen „Zustand des vollkommenen körperlichen, seelischen und sozialen Wohlbefindens und nicht die bloße Abwesenheit von Krankheit oder Gebrechen“ (WHO 1948). Laut Joiner/Lusch (2016) erfolgt die Anwendung der Service Dominant-Logic auf die Gesundheit und Gesundheitsfürsorge direkt durch mobile Technologien (S. 30) und beschreibt damit die Serviceorientiertung anstatt der reinen Güterlogik. Dies wird in Kapitel 4.1.1 im Detail erläutert.

Im Rahmen dieser Masterarbeit liegt der Fokus auf Wearables von kommerziellen Anbietern im Gesundheits- und Fitnessbereich, die sich neue Anwendungsfelder innerhalb der Gesundheitswirtschaft erschließen möchten. Medizinische Anwendungsgebiete sowie Angebote von staatlichen Institutionen werden innerhalb dieser Arbeit nicht berücksichtigt.

3.2.2 Nutzung von Wearables im Gesundheits- und Fitnesskontext

Im Rahmen der digitalen Selbstvermessung erfasst ein erheblicher Bevölkerungsanteil kontinuierlich Daten über sich selbst. 45 Prozent der chinesischen KonsumentInnen geben an, ihre Gesundheit und Fitness mit App, Fitnesstracker oder Smartwatch zu erfassen, gefolgt von den USA mit 29 Prozent und Deutschland mit 28 Prozent (vgl. GFK 2016). Für Österreich liegen derzeit keine vergleichbaren repräsentativen Daten vor. In Deutschland erheben NutzerInnen von Selbstvermessungstechnologien persönliche Daten in erster Linie in den Bereichen Fitness und Gesundheit, gefolgt von Ernährung und Finanzen (vgl. Splendid Research 2016).

Wearables spielen zur Nutzung von Fitness- und Gesundheitsapplikationen eine nennenswerte, jedoch bisher untergeordnete Rolle. In Österreich sowie im weltweiten Vergleich ist die Verbreitung der Geräte jedoch stetig steigend. Die höchste Nutzerpenetration ist in den USA (11,8%) gegeben, gefolgt von Hongkong (11,4%), dem Vereinigten Königreich (9,8%) und China (9,3%) (vgl. Statista 2019a). Studien zu Nutzerzahlen in Österreich divergieren zwischen sechs (vgl. We Are Social und Hootsuite 2018) und acht Prozent (vgl. MindTake und MMA 2016). Tendenziell werden Fitnessarmbänder (8,9%) häufiger zum Self-Tracking verwendet, als Smartwatches (8,3%) (vgl. MindTake und MMA 2016). Der Umsatz im Segment Wearables beträgt 2019 in Österreich etwa 42 Mio. Euro, laut Prognose wird im Jahr 2023 ein Marktvolumen von 54

Mio. Euro erreicht, dies entspricht einem jährlichen Umsatzwachstum von 6,0% (vgl. Statista 2019b).

Unter den Nutzenden sind Frauen und Männer in Österreich gleichermaßen vertreten (vgl. SPECTRA Marktforschungsgesellschaft 2016a). Auch die Bildung wirkt sich nicht signifikant auf die Nutzung aus (vgl. SPECTRA Marktforschungsgesellschaft 2016b). Bei der Nutzung von Wearables lassen sich jedoch Unterschiede im Alter erkennen. Bei den Jüngeren, den 15- bis 29-Jährigen, nutzen im Jahr 2018 19 Prozent Wearables. Unter den 30- bis 49-Jährigen werden diese Geräte von 13 Prozent genutzt, während vier Prozent der 50- bis 65-Jährigen und lediglich ein Prozent der ÖsterreicherInnen, die älter sind als 65 Jahre, ihre Gesundheits- und Fitnessdaten am Handgelenk messen (vgl. SPECTRA Marktforschungsgesellschaft 2018). Besonders ausgeprägt ist das Interesse an der Verwendung von Wearables bei Angestellten und bei Personen in Ausbildung (vgl. Integral 2017). Eine Korrelation mit dem Alter ist hierbei anzunehmen.

3.2.3 Gamification im Kontext von Self-Tracking

Damit Selbstvermessungstechnologien regelmäßig genutzt werden, muss eine entsprechende Motivation Seitens der NutzerInnen aufrechterhalten werden. Eine Möglichkeit liegt in der spielerischen Mediennutzung. Wearables im Rahmen der digitalen Selbstvermessung (z. B. Smartwatches, Fitnessarmbänder) entfalten ihren „informationsästhetischen Mehrwert“ erst in Verbindung mit einem Interface, bei dem Datenvisualisierungen um spieltypische Elemente und Mechaniken angereichert werden (vgl. Reichert 2016, S. 178).

Der Begriff Gamification kann definiert werden als „adopting any game elements into non-gaming system, which will accommodate user experience as well as user engagement“ (vgl. Deterding 2011, S. 2f).

Spieltypische Mechaniken und Elemente innerhalb von Selbstvermessungstechnologien zielen daher auf die Verbesserung positiver Nutzungsmuster ab, wie beispielsweise die Steigerung der Qualität und der Produktivität von Nutzeraktivitäten, sowie die Sicherstellung der Kontinuität der Systemnutzung (vgl. Gimpel et al. 2019, S. 4f). Lister et al. (2014) erforschten inwieweit Gamification in Gesundheits-Apps Anwendung findet und inwiefern Gamification von Gesundheits- und Fitness-Apps eine potenzielle Komponente

für die Beeinflussung des Gesundheitsverhaltens darstellt. Dabei wurde erkannt, dass Gamification-Elemente wie Belohnungen, Levels, Bestenlisten, Zielsetzungen und Feedbacks insbesondere im Kontext der digitalen Selbstvermessung eingesetzt werden (S. 59). Der Einsatz von spieltypischen Elementen und Mechaniken bei Wearables dient vor allem der Verhaltensänderung von Menschen (vgl. Gimpel et al. 2019, S. 4). Eine Absicht könnte darin bestehen NutzerInnen zu motivieren.

In der Regel ist das Spielen freiwillig und frei von Konsequenzen. Es ist jedoch notwendig darauf hinzuweisen, dass Kritiker der Gamification auf die autoritären Strukturen spielerischer Umgebungen und persuasiver Interaktionen aufzeigen und dabei die strategischen Zusammenhänge zwischen technischer Infrastruktur, Datenakkumulation und ökonomischer Verwertbarkeit sichtbar machen (vgl. Gerlitz 2011 nach Reichert, 2016, S. 188).

3.3 Digitale Selbstvermessung: Potenziale und Problemfelder auf NutzerInnenebene

Persönliche Informationen von NutzerInnen, die durch Wearables gesammelt werden, sind für mehrere Stakeholder äußerst relevant um detaillierte Kundenerkenntnisse zu generieren (vgl. Wienecke et al. 2016). Diese können auf unterschiedliche Art weiterverwertet werden und Wert aus Anbieter-, als auch aus AnwenderInnenperspektive generieren. Aus der Perspektive der NutzerInnen birgt die Verbreitung digitaler Selbstvermessungstechnologien sowohl Potenziale als auch Risiken für Individuen, und für die Gesellschaft. Diese werden im Folgenden skizziert.

3.3.1 Potenziale der digitalen Selbstvermessung für NutzerInnen

Digitale Medien der Selbstvermessung werden als persuasive Medien konzipiert und zielen auf Veränderungen des alltäglichen Verhaltens ab (vgl. Reichert 2013, S. 185). Dabei ergeben sich Potenziale für Individuen und für die Gesellschaft. Eine explorative

Folgenabschätzung des Projektes „Quantified Self“[6] (Hayen, 2016) identifizierte folgende Vorteile:

In erster Linie ist der **persönliche Nutzen**, vor allem bezüglich der Gesundheit, der Produktivität und der Lebensqualität zu erwähnen (vgl. Hayen 2016, S. 4) Hierzu fehlen jedoch bisher wissenschaftliche Befunde.

Die **Selbstexpertisierung** impliziert den Wunsch zu mehr Wissen (aufgrund von Datenbeständen) sowie zu stärkerem Bewusstsein über die eigene Gesundheit und den eigenen Körper. Das dadurch gewonnene Körper- und Gesundheitsbewusstsein kann zu einem gesundheitsförderlichen Verhalten beitragen.

Hinsichtlich der **Medizin** bietet eine Vielzahl an persönlichen Daten von Selbstvermessungstechnologien eine bessere Datengrundlage für die Diagnostik (vgl. Hayen, 2016, S. 5). Apple Research Kit ist ein Beispiel eines kommerziellen Anbieters, der mit Nutzerdaten medizinische Forschungseinrichtungen unterstützt (vgl. Apple). Im Rahmen der **Wissenschaft**, insbesondere der Bewegungs-, Schlaf-, und Ernährungsforschung lassen Daten auswerten, die sich auf das Alltagsverhalten der ProbandInnen beziehen (vgl. ebd.).

Zudem prognostizieren die AutorInnen eine **gesündere und sichere Gesellschaft mit geringeren Gesundheitskosten auf Makroebene** (vgl. ebd.). Hierzu gibt es bislang keine konkreten Forschungsergebnisse.

Lupton (2014) führt zudem das „communal self-tracking“ an, bei dem sich Self-Tracker als Teil einer Community ansehen und soziale Medien bzw. Plattformen nutzen, um persönlicher Daten zu vergleichen und sich auszutauschen (S. 8).

3.3.2 Digitale Selbstvermessung aus Anbieterperspektive

Das Sammeln und Analysieren persönlicher Nutzerdaten durch Self-Tracking findet bereits in einigen sozialen Kontexten Anwendung, darunter in den Bereichen Arbeitsplatz, Bildung, staatliche Gesundheitsinstitution, Versicherung, Marketing und Handel, Militär, Bürgerwissenschaft und Stadtentwicklung (vgl. Lupton 2014, S. 5). Es ist zu erwähnen,

[6] Dieses vom BMBF Deutschland geförderte Projekt wurde als Teilprojekt des Verbundprojektes „Wissenstransfer 2.0“ durchgeführt.

dass aus der Literaturrecherche nicht hervor geht, dass Organisationen im europäischen Raum Handlungen auf Basis von Daten der Selbstvermessungstechnologien durchführen. Es ist davon auszugehen, dass Unterschiede zwischen dem europäischen und dem angelsächsischen Raum vorliegen.

Die persönlichen Daten, die Individuen über sich selbst sammeln, werden häufig zu großen Datenmengen aggregiert. Menschen werden oftmals dazu ermutigt bzw. „angestupst“ (Nudge) digitale Geräte zur Überwachung von Teilbereichen ihres Lebens zu verwenden um persönliche Datensätze zu erstellen, die für unterschiedliche Zwecke verwendet werden (vgl. ebd.). In einigen Anwendungsfällen ist die Nutzung der Selbstvermessungstechnologien obligatorisch. Verwendungszwecke sind u. a. die Verwertung von Daten für Produkt- und Serviceangebote, für Preisdiskriminierungen, für den Verkauf personenbezogener Daten sowie die Verwertung von persönlichen Informationen durch den Arbeitgeber (vgl. Masur et al. 2018, S. 19). Um festzustellen welche Risiken sich im Rahmen der digitalen Selbstvermessung seitens der NutzerInnen ergeben, wird zunächst die institutionelle Perspektive der Datenverwertung im Forschungskontext erläutert. Lupton (2014) unterscheidet drei Dimensionen der institutionellen und organisationalen Nutzung von Self-Tracking-Daten:

(1) Methoden des „Pushed self-tracking“ lassen persönliche Daten von Gruppen erheben um Verhaltensänderungen wie eine bessere Gesundheit oder bestimmte Ergebnisse zu erzielen (vgl. Lupton 2014, S. 7). Die Selbstüberwachung kann dabei freiwillig erfolgen, diese wird jedoch durch Externe ermutigt (vgl. ebd.). Als Anwendungsgebiete werden die Patientenselbstversorgung, die Gesundheitsförderung und die Präventivmedizin genannt. Gerade im Rahmen der Gesundheitsförderung spielen Arbeitgeber durch den Einsatz von digitalen Selbstvermessungstechnologien eine relevante Rolle (vgl. ebd.). Finanzielle Anreize oder die Hervorhebung des „Teamgeistes“ sowie die Förderung der Produktivität sollen zur Nutzung der Anwendungen führen. Wearable-Anbieter wie Fitbit, aber auch Apple Health vermitteln Kooperationen mit Arbeitgebern und Versicherungsunternehmen zur Nutzung von Fitnesstracker und der Datenanalyse-Software (vgl. Fitbit 2019; Apple 2019). Auch Versicherungsunternehmen nutzen gesammelte Datensätze um Gesundheitsrisiken von Individuen anhand bestimmter Verhaltensmuster zu evaluieren. Dies könnte zum Ausschluss potenzieller

KundInnen oder zur Erhöhung von Beitragsprämien führen (vgl. Markus 2015 nach Wieneke et al. 2016). Die Folgen wären ungerechtfertigte Einstufungen. Diese könnten zu Diskriminierungen von Personen führen (vgl. ebd.).

(2) Das „Imposed self-tracking“ bezieht sich auf die unfreiwillige Nutzung digitaler Selbstvermessungstechnologien (vgl. Lupton 2014, S. 7). Unternehmen sind durch den Einsatz von Überwachungstechnologien, aber auch von Technologien, die für Überwachungszwecke zweckentfremdet werden können (z. B. Wearables mit GPS-Tracker), zunehmend in der Lage das Verhalten der Mitarbeiteten zu beobachten (vgl. Morlok et al. 2017, S. 19). Arbeitgeber können beispielsweise die Gewohnheiten der Mitarbeitenden messen um Daten zu sammeln, mit denen die Effizienz der Mitarbeitenden maximiert oder die Kosten gesenkt werden können (vgl. Lupton 2014, S. 9). Hierunter werden Unternehmen unterschiedlicher Branchen subsumiert, die ArbeitnehmerInnen anhalten Ausweise zu tragen, die mit RFID-Chips und anderen Sensoren ausgestattet sind. Gesundheits- und Aktivitätsdaten sowie Standortdaten der TrägerInnen werden hierbei dem Arbeitgeber übergeben (vgl. ebd., S. 9). Die Standortbestimmung wird beispielsweise in Logistikunternehmen eingesetzt um die Bewegungsmuster und das Pausenverhalten der Arbeitnehmenden zu analysieren (vgl. Morlok et al. 2017, S. 19). Daraus lässt sich ein detailliertes Abbild des Arbeitsalltags eines Individuums erschließen. In der Literatur werden Anwendungsfälle im angelsächsischen Raum beschrieben. Der Privatheitsschutz für Arbeitnehmende ist im europäischen Raum jedoch stärker verankert (vgl. Gürtler/Höffler 2015, S. 1366).

(3) Die dritte Dimension, das „Exploited self-tracking“, umfasst die Kommodifizierung von persönlichen Daten. Dabei handelt es sich um Kundenbindungsprogramme, bei denen das Tragen von Trackingarmbändern und das Ausweisen von persönlichen Fitnessdaten mit Produktermäßigungen belohnt werden. Die gesammelten Daten werden von Einzelhändlern für das Kundenmarketing verwendet und an Dritte weiterverkauft. Dabei wird das Self-Tracking oftmals mit dem Vorwand vermarktet, dass KundInnen selbst von der Weitergabe ihrer Informationen profitieren,

beispielsweise durch das Sammeln von Punkten oder Belohnungen. (vgl. Lupton 2014, S. 10f)

3.3.3 Problemfelder der digitalen Selbstvermessung auf NutzerInnenebene

Das zunehmende Wachstum von CIoT-Anwendungen, im konkreten Anwendungsfall Wearables, wirft demnach Herausforderungen hinsichtlich der Sicherheit, der Privatsphäre und dem Vertrauen von NutzerInnen auf (vgl. Sicari et al. 2015, S. 146f). Einige Autoren äußern Bedenken hinsichtlich der informationellen Privatheit der Individuen (vgl. Acquisti 2014; Wieneke et al. 2016). Die grundlegende Herausforderung der Privatsphäre bei der Nutzung von mobilen Geräten besteht in der Kombination von Person, Ort und Aktivitäten. Sämtliche Aufzeichnungen, die technologisch durchgeführt werden sind beobachtbar (vgl. Hartmann 2011, S. 192). Dabei ergeben sich - oftmals unbewusst - einige Problemfelder für NutzerInnen, da die zur Selbstvermessung generierten Daten von NutzerInnen auf eine ursprünglich nicht beabsichtigte Art und Weise genutzt werden können. KonsumentInnen sind sich oftmals nicht über die damit zusammenhängenden Folgen bewusst bzw. können diese nur subjektiv einschätzen (vgl. Moll et al. 2017, S. 37).

Aus NutzerInnenperspektive können die Datensammlungspraktiken von Organisationen zum Verlust der individuellen Kontrolle und Selbstbestimmung sowie, durch die Erstellung von Profilen und die Ableitung von Voraussagen durch „Predictive Analytics“ zur Rationalisierung und Objektivierung von Individuen führen (vgl. Duttweiler et al. 2016, S. 10).

Die Einstellungen und Verhaltensweisen von Individuen hinsichtlich der informationellen Privatheit werden in Kapitel 5 und in der empirischen Forschung erläutert. Um eine grundlegende Basis der Thematik zu schaffen und die Möglichkeiten der Datennutzung aus Anbieterperspektive aufzuzeigen, wird im nachfolgenden Kapitel 4 die Wertschöpfungsstruktur datengetriebener Geschäftsmodelle anhand der Daten-Wertschöpfungskette beschrieben. Die Geschäftsmodellpraktiken im Zusammenhang mit der Verwertung persönlicher Daten sind in der Praxis bekannt, jedoch in den Forschungsarbeiten der Wirtschaftswissenschaften weitgehend unterforscht (vgl. Morlok et al. 2017, S. 180f).

4 Datengetriebene Wertschöpfung

Technologische Entwicklungen führen zu einer stetig und massiv steigenden Anzahl an Datensätzen aus unterschiedlichen Quellen wie beispielsweise CIoT-Anwendungen, Sensornetzwerke oder Daten aus mobilen Anwendungen. Die Welle an Daten bietet die Chance neue Geschäftsmodelle und/oder neue bzw. bestehende Wertschöpfungsmodelle zu gestalten, um die gesammelten Informationen zu verwerten und daraus Nutzen für Unternehmen zu ziehen[7], sowie Wert auf KonsumentInnenseite zu schaffen. In diesem Kapitel werden zunächst Grundlagen der interaktiven Wertschöpfung erläutert. Dabei wird insbesondere auf die Relevanz der KonsumentInnen im Rahmen der Wertschöpfung eingegangen. Zudem wird die Daten-Wertschöpfungskette als Reihe von Schritten beschrieben, die zur Generierung von Wert erforderlich sind. Nachfolgend wird die Wertschöpfung persönlicher Daten anhand der Wertekette im Kontext von Wearables im Gesundheits- und Fitnessbereich skizziert. Im folgenden Kapitel werden persönliche Daten als wirtschaftliches Gut betrachtet (vgl. OECD 2013; Spiekermann-Hoff/Korunovska 2017; Masur et al. 2018) und datengetriebene Geschäftsmodelltypen aufgezeigt. Anschließend werden Problemfelder für NutzerInnen hinsichtlich des Datenschutzes in einem Zwischenfazit zusammengefasst.

4.1 Grundlagen der interaktiven Wertschöpfung durch Services

Die zunehmende digitale Transformation von Unternehmen aufgrund einer komplexen, dynamischen und kompetitiven Umwelt bedingt die Vernetzung von Akteuren wie Unternehmen und KonsumentInnen über alle Wertschöpfungsstufen hinweg, sowie den Einsatz neuer Technologien und die Nutzung von Daten (vgl. Schallmo/Rusnjak, 2017, S. 2-4). Die Fähigkeit Informationen zu verwalten und daraus Wissen zu extrahieren wird als entscheidender Wettbewerbsvorteil in digitalen Märkten angesehen (vgl. Curry 2016, S. 29). Gerade bei CIoT-Anwendungen wie Wearables ist die tatsächliche Nutzung und die

[7] Die Datenwertschöpfung beschäftigt sich „mit der Monetarisierung von Informationen auf Basis gewonnener Daten, welche mit einem Algorithmus zu werthaltigen Informationen transformiert und anschließend auf Basis der betriebswirtschaftlichen Funktionen zugänglich gemacht werden“. Die „Data Economy“ kann als eigenes Geschäftsmodell betrieben werden, oder bestehende Wertschöpfungsmodelle durch eine zunehmende Digitalisierung unterstützten, verändern oder ersetzten. (BVDW 2018, S. 4)

dabei erfolge Dateneingabe für den Erfolg des Services und damit für den Unternehmenserfolg von Relevanz.

Die „Konzentration auf den Menschen“[8] aus institutioneller Perspektive zeigt sich in diesem Zusammenhang sowohl in der Entwicklung von Technologien, die mit dem Alltag von Menschen verschmelzen, als auch in der Entwicklung datengetriebener Geschäftsmodelle (vgl. Schallmo et al. 2018, S. 4). NutzerInnen nehmen im Rahmen der interaktiven Wertschöpfung, innerhalb von datengetriebenen Geschäftsmodellen, sowohl die Produzentenrolle, also auch Konsumentenrolle ein (vgl. Bruhn/Hadwich 2015, S. 14). Ng/Wakenshaw (2018) bestätigen, dass Individuen selbst Ressourcenintegrator und Anbieter des Wertversprechens (Generierung persönlicher Daten) sein können (vgl. ebd. S. 209). Daher kommt diesen AkteurInnen in der Ausgestaltung datengetriebener Services eine entsprechende Bedeutung zu.

Die interaktive Wertschöpfung (auch Co-Creation of Value) im Dienstleistungsbereich zeichnet sich in erster Linie durch die Kundenbeteiligung aus. Aus der Unternehmensperspektive werden KundInnen nicht mehr auf die Rolle der Nachfrager einer Dienstleistung oder eines Produktes begrenzt, sondern stellen eine wertvolle Ressource innerhalb des Leistungserstellungsprozesses dar (vgl. Bruhn/Hadwich 2015, S. 5). Damit stellt die Kundeninteraktion den Kern des Dienstleistungsprozesses dar (vgl. ebd.).

Zur Verdeutlichung der wechselseitigen Integration von Marktakteuren kann der Begriff der „interaktiven Wertschöpfung“ aus einer bestimmten Partnerperspektive betrachtet werden. Werden Dritte, beispielsweise Nachfrager, in die Prozesse eines Anbieters integriert, so wird die durch die Integration erzielte anbieterseitige Wertsteigerung als *Wertschöpfung* bezeichnet. Gleichermaßen können Unternehmen oder auch andere Nachfrager in die Nutzungsprozesse von KonsumentInnen integriert werden, beispielsweise durch eine Plattform. Die durch die Integration erzielte Wertsteigerung auf NutzerInnenebene wird als *Wertschaffung* bezeichnet. (vgl. Weiber/ Ferreira 2015, S. 37).

[8] Der Mensch wird in diesem Kontext als KonsumentIn bzw. als NutzerIn betrachtet.

4.1.1 Kundenorientierung im Rahmen der Service-Dominant Logic

Kundenorientierte Geschäftsmodelle nutzen persönliche Daten um Services zu optimieren und Wert für KundInnen zu schaffen (vgl. OECD 2013, S. 39). Datengetriebene Geschäftsmodelle folgen demnach einer neuen Wertschöpfungslogik, von der Güter-Orientierung hin zur Service-Orientierung (vgl. Pellegrini 2019, S. 11). Externe Interessengruppen, wie z. B. KundInnen, werden dabei vollständig oder teilweise in die Wertschöpfungsprozesse eines Unternehmens integriert (vgl. Bruhn/Hadwich 2015, S. 5).

Im Rahmen der interaktiven Wertschöpfung nehmen KundInnen, aus Sicht der Service-Dominant Logic (im Folgenden Service-Logik), eine zentrale Rolle ein. Die Service-Logik ist ein serviceorientierter Marketingansatz, bei dem Wertschöpfung und Service die zentrale Grundlage für den Austausch zwischen MarktteilnehmerInnen bildet (vgl. Brodie et al., 2011, S. 76). Um die Service-Logik zu erläutern, eignet sich eine Gegenüberstellung mit der traditionellen Güter-Logik. Während in der Güter-Logik die Geschäftsbeziehung mit einer Transaktion endet, beispielsweise der Kauf eines Produktes, beginnt die Geschäftsbeziehung in der Service-Logik mit einer Transaktion. Güter fungieren in der Service-Logik als Distributionskanal für den Austausch, sind aber keine primären Wertträger. Die Werthaltigkeit, sowohl für NutzerInnen als auch Unternehmen, entsteht dabei im Prozess, denn alle im Tauschprozess involvierten AkteurInnen sind an der Werterstellung beteiligt. Dabei verschwimmen die Grenzen zwischen Produzenten und KonsumentInnen. (vgl. ebd. S. 76-85)

Laut Vargo/Lusch (2008) kommt dem/der KundIn die Rolle des Co-Creators zu (S. 2). Demnach entsteht erst Wert wenn ein Angebot auch angenommen und die Leistung angewendet wird. Das Unternehmen selbst kann nicht direkt Wert generieren, sondern nur Wertangebote („Value Propositions“) erbringen (vgl. Vargo/Lusch 2008, S. 3). Der/die KundIn steht dabei im Fokus des Werterstellungsprozesses und erfährt das Angebot. Obwohl die interaktive Wertschöpfung gleichermaßen von der Initiative des Anbieters als auch den KundInnen abhängt, wird der Wert letztendlich von den Nutzenden bestimmt (vgl. Bruhn/Hadwich 2015, S. 9). Der Erfolg von intelligenten Diensten hängt maßgeblich von dem Wert ab, den die Nutzenden darin erkennen (vgl. Mani/Chouk 2017, S. 1). Aus der Perspektive der Service-Dominant Logic sind Daten ein institutionelles Artefakt (vgl.

Vargo et al. 2015), d. h. ein Symbol, das nur aufgrund von Überzeugungen, der institutionalisierten Logik, Sinn ergibt (vgl. Ng/Wakenshaw 2018, S. 208).

Forschungsarbeiten der Service-Logik im Bereich Gesundheit und Fitness sind bisher kaum vorhanden. Joiner/Lusch (2016) beschreiben die Entwicklung zu einer neuen dienstleistungsdominierenden Logik für das Gesundheitswesen und verweisen dabei u. a. auf mobile Technologien (S. 30). Dabei ist zu erwähnen, dass die generierten und übertragenen Gesundheitsdaten, durch mobile Geräte, per se keinen Wert darstellen. Die Übertragung durch das Gut als Wertträger (z. B. Wearable) ähnelt dabei der Güter-Logik (vgl. ebd.). Intelligente Geräte (CIoT), die der Service-Logik entsprechen, bestehen jedoch darin, dass NutzerInnen den Wert, der vom Gerät stammenden Informationen, selbst bestimmen und diesen in die individuellen Entscheidungsfindungen und Aktivitäten des täglichen Lebens einbetten. Das Gerät, im konkreten Fall das Wearable, verbessert somit die Selbstwirksamkeit der NutzerInnen. (vgl. ebd.)

Im konkreten Anwendungsfall dieser Masterarbeit „Wearables im Gesundheits- und Fitnesskontext“ sind NutzerInnen mit der Eingabe persönlicher Daten, sowohl freiwillig und bewusst im Rahmen des Registrierungsprozesses bzw. der Eingabe von Nahrungsmitteln, sowie (oftmals) unbewusst durch die Nutzung des Services, an der Integration von Ressourcen und damit an der Wertschöpfung beteiligt. Der eigentliche Wert, im Rahmen der Service-Logik, entsteht wenn die vom Gerät stammenden Informationen in die Entscheidungsprozesse des Individuums integriert werden.

4.1.2 Wertschöpfungskette datengetriebener Services

Die Wertekette wird aufgrund der Verständlichkeit und Anwendungslogik häufig bei der Analyse von Wertschöpfung eingesetzt (vgl. Wirtz 2018, S. 97). Jedes Unternehmen führt unterschiedliche Aktivitäten entlang der Wertekette durch um das Angebot zu produzieren und zu distribuieren. In traditionellen produktzentrierten Geschäftsmodellen können die wichtigsten Unternehmensaktivitäten anhand der Wertschöpfungskette beschrieben werden (vgl. Porter 1989, S. 65). Dieses Wertschöpfungskonzept bezieht sich in erster Linie auf physische Güter und behandelt Informationen als unterstützendes Element und nicht als zentrale Ressource (vgl. Rayport/Sviokla 1995 nach Hartmann et al. 2014, S. 8).

In der Literatur wird die Wertschöpfungskette jedoch von einigen Autoren als analytisches Werkzeug auf Informationsflüsse angewandt, um die Wertschöpfung der Datentechnologie zu verstehen (vgl. Curry 2016, S. 32). In einer Daten-Wertschöpfungskette wird der Informationsfluss als eine Reihe von Schritten beschrieben, die zur Generierung von Wert und nützlichen Erkenntnissen aus Daten erforderlich sind (vgl. ebd.). Um dies zu illustrieren wurde das Rahmenmodell von Hartmann et al. (2014) adaptiert angewandt. Die vormals definierten sieben Stufen wurden in **Abbildung 1** in vier Prozessschritte zusammengefasst: Datenerhebung, Datenspeicherung, Datenanalyse und Datennutzung (vgl. Dewentner 2018, S. 17). Die Stufen der Wertschöpfungskette können unabhängig voneinander betrachtet werden, sind jedoch interdependent und beziehen sich auf den jeweiligen Kontext in dem das Unternehmen operiert (vgl. Dewenter 2018, S. 16). Darüber hinaus kann jede Stufe der Wertschöpfung Rückkopplungen zu den vorgelagerten Stufen erzeugen (vgl. ebd., S. 17).

Abbildung 1: Wertschöpfungskette für persönliche Daten, eigene Darstellung in Anlehnung an Hartmann et al. 2014, S. 11 und Dewentner 2018, S. 17.

Die Wertschöpfungskette für persönliche Daten identifiziert folgende Prozessschritte:

Datenerhebung

In der ersten Stufe der Wertekette erfolgt die Erhebung persönlicher (z. B. Profildaten, Gesundheitsdaten, Standortdaten) und nicht-persönlicher Daten (z. B. technische Daten), die relevant sind um das Geschäftsmodell des Unternehmens zu betreiben. Darüber hinaus können Daten gesammelt werden und für Dienste verwendet werden, die über das bisherige Angebot hinausgehen um zusätzlichen Wert zu generieren (vgl. Dewenter 2018, S. 16ff). Diese können in einer weiteren Stufe der Wertekette beispielsweise zur Weiterentwicklung des Dienstes, zur Erstellung neuer Dienste (primäre Datenverwertung) oder zum Handel von Daten (sekundäre Datenverwertung) genutzt werden.

Datenspeicherung

Die zweite Stufe der Wertekette betrifft die Organisation der Daten. Dies umfasst in erster Linie die Aufbereitung, die Bereinigung und die Speicherung der Daten. In weiterer Folge können einzelne Datenelemente als Datensets organisiert werden um weitere Analysen durchzuführen. Persönliche Daten können aus unterschiedlichen Quellen verarbeitet und aggregiert werden. (vgl. OECD 2013, S. 13)

Datenanalyse

Im Kontext dieser Arbeit werden Daten als wirtschaftliches Gut klassifiziert. Hierbei ist zu erwähnen, dass das Gut im Sinne des Handelswertes nicht das Datum per se darstellt, sondern Informationen, die aus der verknüpften Auswertung einzelner Datensätze abgeleitet werden (vgl. BVDW 2018, S. 5; Hartmann et al. 2014, S. 9). Diese Stufe erfordert aufgrund der großen Datenmengen enorme Rechenkapazitäten, geeignete Software sowie Expertise. Diese Leistungen können sowohl unternehmensintern aufgebaut werden, als auch extern von Analysedienstleistern bezogen werden (vgl. Dewenter 2018, S. 21).

Cheney-Lippold (2011) spricht von „algorithmischen Identitäten" und meint damit eine Identitätsbildung, die durch mathematische Algorithmen Identitätskategorien auf ansonsten anonymen Identitäten ableitet (S. 165). Durch die Verknüpfung von unterschiedlichen Datenquellen in Profilen und die Nutzung von analytischen Maßnahmen wird neue Information generiert, wodurch zusätzlicher Mehrwert für Unternehmen geschaffen wird (vgl. Dewenter 2018, S. 21). Zur Erzielung dieser Information werden statistische Methoden eingesetzt um große Mengen an Nutzerdaten zu analysieren, darin Muster und Zusammenhänge zu erkennen, und darauf aufbauend Einschätzungen über NutzerInnen oder Prognosen über deren zukünftiges Verhalten abzuleiten. Die dabei genutzten Technologien und Methoden werden unter dem Begriff Data Mining[9] zusammengefasst (vgl. Christl 2014, S. 13). Bei der Interpretation der Ergebnisse muss jedoch berücksichtigt werden, dass es sich um Wahrscheinlichkeiten handelt. Zur Analyse von Daten werden zudem mathematisch-statistische Verfahren und Technologien des Machine Learning[10]

[9] Unter Data Mining wird die Transformation von Rohdaten in „Information" verstanden (vgl. Christl 2014, S. 13).
[10] Machine Learning Anwendungen sind Computerprogramme, die automatisch lernen komplexe Muster zu erkennen und intelligente Entscheidungen zu treffen (vgl. Han et al 2011 nach Christl 2014, S. 13).

genutzt (vgl. ebd.). Diese Informationen lassen Rückschlüsse auf Verhaltensweisen und Interessen von KonsumentInnen ziehen (vgl. Morlok 2017, S. 187). Durch Analysen persönlicher Daten ergeben sich neue Möglichkeiten für die Forschung sowie für die Entwicklung und die Weiterentwicklung von Produkten und Services (vgl. ebd.; OECD 2013). Zudem dienen Datenanalysen Unternehmen der Risikominimierung bzw. der Risikovermeidung (vgl. Christl 2014, S. 13).

Distribution und Nutzung von Daten

Wie bereits erwähnt werden Daten nach der Analyse und Interpretation zu Informationen oder Wissen transformiert (vgl. BVDW 2018, S. 5; Hartmann et al. 2014, S. 9). Die Kernkompetenz datennutzender und datengetriebener Services liegt darin, die gewonnene Information entsprechend zu nutzen bzw. zu monetarisieren (vgl. Dewenter 2018, S. 22). Oftmals werden persönliche Daten in dieser Stufe der Wertekette von Unternehmen verwendet, um das KonsumentInnenverhalten vorherzusagen, sowie personalisierte Werbung und Services anzubieten (vgl. OECD 2013, S. 16). Darüber hinaus lassen sich unternehmensinterne Prozesse effizienter gestalten sowie Makrotrends, beispielsweise im Gesundheitsbereich, analysieren (vgl. ebd.).

4.2 Wertschöpfungskette persönlicher Daten im Anwendungskontext von Wearables

Um den datengetriebenen Wertschöpfungsprozess im Kontext der digitalen Selbstvermessung am Beispiel von Wearables zu skizzieren, wurde die Wertekette nach Hartmann et al. (2014), zusammengefasst nach Dewentner (2018), um Aspekte des Forschungskontextes erweitert. Die Autorin bezieht sich dabei auf Theorien skizzierter datengetriebener Werteketten (OECD 2013, S. 11; Curry 2016, S. 14) und ergänzt diese um Inhalte der Forschungsliteratur hinsichtlich der Nutzung von Wearbles im Gesundheits- und Fitnesskontext (Dewenter 2018, S. 18; Moll et al. 2017).[11]

Bevor auf die einzelnen Stufen der Wertekette eingegangen werden kann, muss die Schlüsselressource Daten im Forschungskontext erläutert werden. In Bezug auf Kapitel 2.1

[11] Es ist zu erwähnen, dass unterschiedliche Stakeholder in den einzelnen Stufen der Wertekette integriert werden können. Die Analyse dieser ist nicht Ziel der vorliegenden Arbeit.

sind im Rahmen der datengetriebenen Wertschöpfung unterschiedliche Arten der Sammlung und der Verarbeitung persönlicher Daten zu berücksichtigen: Angegebene Daten (nicht-maschinenerzeugte Daten), beobachtete Daten (maschinenerzeugte Daten) und abgeleitete Daten. Diese finden in jeder Stufe der Wertekette Anwendung (vgl. Curry 2016, S. 31).

- Zum einen geben NutzerInnen von Geräten oder Online-Services bewusst persönliche Daten preis wie z. B. bei der Registrierung eines Services (vgl. OECD 2013, S. 10). Diese werden in dieser Arbeit als *angegebene Daten* (volunteered) beschrieben. Im Kontext von Wearables werden NutzerInnen vor der Inbetriebnahme dazu aufgefordert ein persönliches Profil mit soziodemografischen Daten wie Alter, Gewicht und Größe zu erstellen (vgl. Reichert 2013, S. 187).
- Daten können *legal beobachtet* werden. Hierbei handelt es sich um Standort-, Aktivitäts- und Verhaltensdaten bei der Nutzung von internetfähigen Geräten (vgl. OECD 2013, S. 10). Im Kontext von Wearables werden die angegebenen Daten aus dem Registrierungsprozess bzw. nutzergenerierte Daten wie beispielsweise Nahrungsmittel mit den beobachteten Daten wie Standortdaten, Verhaltens- und Aktivitätsdaten verknüpft (vgl. Reichert 2013, S. 187).

- Daten können auf Basis der Analyse und Verarbeitung von angegebenen und beobachteten persönlichen Daten *abgeleitet* werden (vgl. ebd.). Diese können von Wahrscheinlichkeiten, Korrelationen oder Vorhersagen abhängen. Beispiele für diese Kategorie wäre die Einordnung in klassifizierte Risikogruppen von Versicherungen auf Basis des Nutzerverhaltens.

Da persönliche Daten noch keinen Wert per se haben, sondern dieser erst im Rahmen der wertschöpfenden Prozesse entsteht (vgl. BVDW 2018, S. 23; Dewenter 2018, S. 17) wird im Folgenden der gesamte Wertschöpfungsprozess im Detail veranschaulicht und anschließend erläutert.

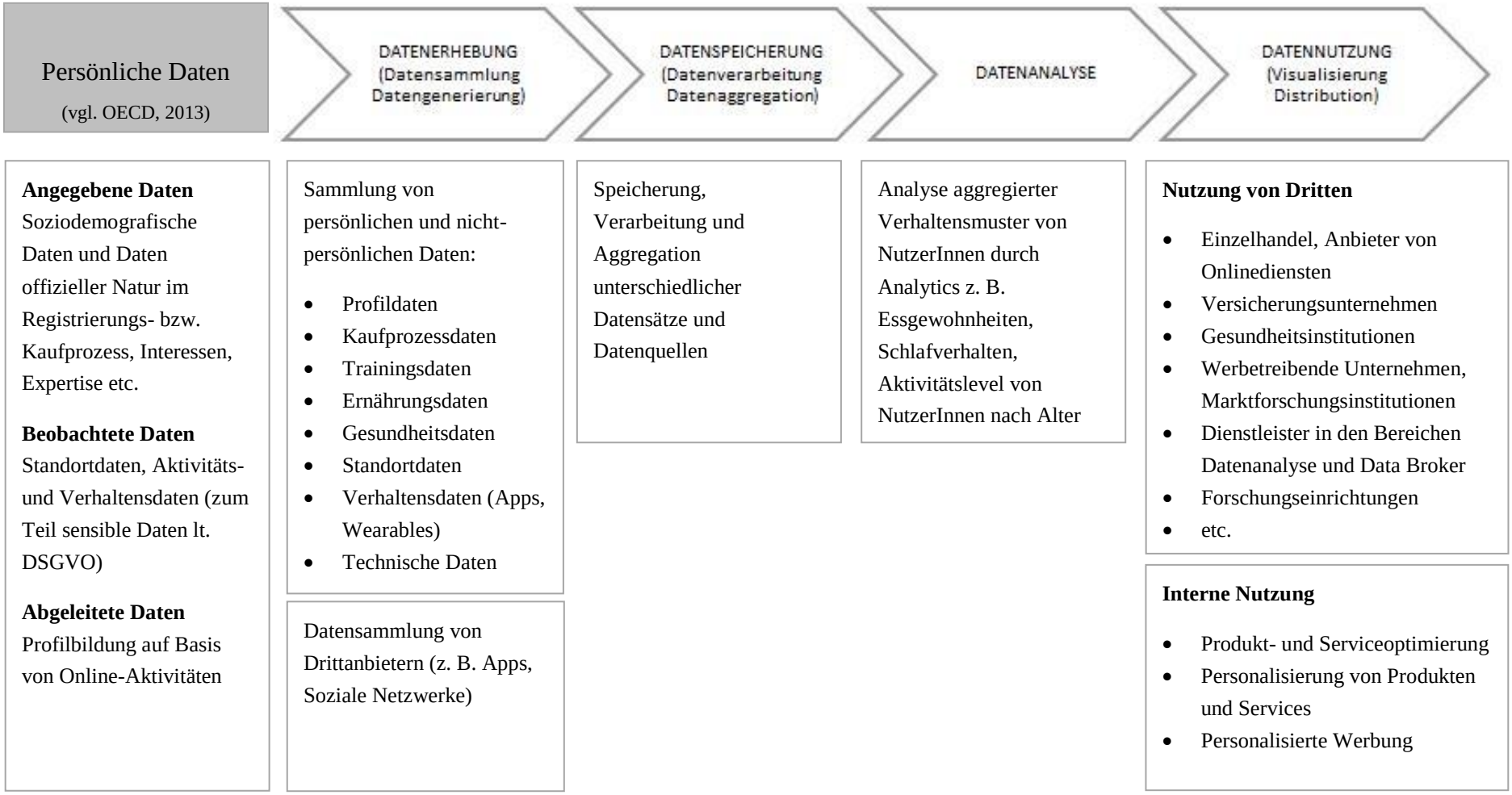

Abbildung 2: Wertschöpfungskette persönlicher Daten am Beispiel von Wearables, eigene Darstellung nach OECD 2013, S. 11; Hartmann et al. 2014, S. 11; Dewenter 2018, S. 18.

4.2.1 Datenerhebung

In der ersten Stufe der Wertekette erfolgt die Erhebung persönlicher Daten, die relevant sind um das Service für NutzerInnen zu betreiben. Diese Daten werden in erster Linie durch Sensoren gesammelt. Wearable-NutzerInnen geben im Rahmen des Registrierungsprozesses Daten wie Benutzername, Name, Passwort, E-Mail-Adresse, Geschlecht, Geburtsdatum, Größe, Gewicht oder Land an (vgl. Moll et al. 2017, S. 19). Bei kostenpflichtigen Anwendungen werden zusätzlich finanzielle Informationen im Rahmen des Kaufprozesses gespeichert. Zudem werden Trainingsdaten, d. h. Bewegungsdaten wie Schrittanzahl, zurückgelegte Strecken und manuelles Hinzufügen des Trainings aufgezeichnet. Als nutzergenerierte Information werden Ernährungsdaten (z. B. konsumierte Nahrungsmittel) verarbeitet. Eine relevante Nutzungsfunktion von Wearables für NutzerInnen sind Herzfrequenzaufzeichnungen, Pulsdaten sowie das gemessene Schlafverhalten. Diese Daten werden als Gesundheitsdaten klassifiziert.[12] Zudem lassen sich erhobene Standortdaten, Verhaltensdaten, die Aussagen über die zeitliche Nutzung von App und Wearable treffen und technische Daten, wie Produkt- und Firmenname des Wearables, sowie das Betriebssystem des verknüpften Smartphones messen (vgl. ebd.).

Zusätzlich können NutzerInnen dazu motiviert werden gemessene Daten in sozialen Netzwerken zu teilen (vgl. Christl 2014, S. 37). Die persönlichen Daten werden an den jeweiligen Netzwerkanbieter übertragen. Moll et al. (2017) überprüften die technische Datenübermittlung an Drittanbieter. Dabei wurde erkannt, dass 19 von 24 Fitness-Apps Daten an eine variierende Anzahl von Drittanbietern versenden. Darunter befinden sich vor allem Werbe- und Analytics-Anbieter (vgl. Moll et al. 2017, S. 20). Dieses Vorgehen ist von NutzerInnen kaum zu kontrollieren, da diese oftmals nicht die Datenschutzrichtlinien lesen und diese Praktiken zum Teil intransparent kommuniziert werden (vgl. ebd.).

4.2.2 Datenspeicherung

Im Allgemeinen handelt es sich in dieser Wertschöpfungsstufe um die Speicherung, Verarbeitung und Aggregation unterschiedlicher Datensätze und Datenquellen. Diese Stufe der Wertschöpfungskette kann sowohl intern, als auch durch externe Anbieter durchgeführt werden (vgl. Dewenter 2018, S. 26). Anbieter für Big Data Storage, d. h. Unternehmen, die

[12] Trainingsdaten und Ernährungsdaten können ebenfalls Aufschluss über den Gesundheitszustand einer Person geben (vgl. Moll et al. 2017, S. 12). Um die Heterogenität der aufgezeichneten Daten zu veranschaulichen wird in dieser Arbeit zwischen Trainings-, Ernährung-, und Gesundheitsdaten differenziert.

Speicherkapazitäten zur Verfügung stellen, sind am Markt vielfältig vorhanden. Es ist zu erwähnen, dass Datenspeicherung und Datenanalyse oftmals eng miteinander verbunden sind (vgl. ebd.). Die Make-or-Buy-Entscheidung kann demnach beide Stufen der Wertschöpfung betreffen.

4.2.3 Datenanalyse

Im Rahmen der Datenanalyse werden die in Kapitel 4.1.2 beschriebenen Methoden und Technologien angewandt um aggregierte Verhaltensmuster von NutzerInnen durch Analytics zu erfassen und daraus Wahrscheinlichkeiten abzuleiten. Um den Wertzuwachs in dieser Stufe der Wertekette zu veranschaulichen, wird auf eine Studie eines britischen Forschungsteams verwiesen. Dabei werden zukünftige Aufenthaltsorte von Individuen durch Smartphone-Daten auf Basis von zeitlich zurückliegender GPS- und WLAN-Protokolle, Telefonnummern, Anruf- und SMS-Listen auf wenige Meter genau vorhergesagt. Es ist zu erkennen, dass Verhaltensmuster von Bekannten dabei helfen, die Vorhersagen der Verhaltensmuster zu verbessern. (vgl. De Domenico et al 2012 nach Christl 2014, S. 20)

NutzerInnen von Wearables verfügen ebenfalls über ein mobiles Gerät mit GPS-Sensoren, zusätzlich lassen sich diese mit dem Smartphone sowie mit dem WLAN verbinden. Vorhersagen zukünftiger Aufenthaltsorte können für kommerzielle Zwecke hinsichtlich der Platzierung von Anreizen in Form von Werbung oder Rabatten zum richtigen Zeitpunkt eingesetzt werden (vgl. OECD 2013; Christl 2014, S. 20).

4.2.4 Datennutzung

In der letzten Stufe der Wertekette am Beispiel von Wearables im Gesundheits- und Fitnesskontext werden die analysierten Daten entweder intern zur Personalisierung sowie zur Entwicklung bzw. Weiterentwicklung von Produkten und Services verwendet oder an Dritte weitergegeben (vgl. Masur et al. 2017; OECD 2013; Dewentner 2018). Wie bereits in der Datenerhebung erwähnt ist der Primärmarkt, auch aufgrund der Wettbewerbsstellung, die häufigste Variante der Datennutzung von Unternehmen. Dennoch ist anzunehmen, dass eine Vielzahl an Unternehmen verfügbare Datenressourcen bisher unzureichend nutzt. Gründe dafür können z. B. unverhältnismäßig hohe Transaktions- oder Opportunitätskosten aufgrund strenger Nutzungsbedingungen, Qualitätsproblemen, Rechtsunsicherheiten oder technischer Hindernisse sein (vgl. Litschka/Pellegrini 2019, S. 6f). Sekundärmärkte, auf denen analysierte Daten vernetzter Technologien an Dritte distribuiert werden, sind vor allem im europäischen

Rechtsrahmen bisher vereinzelt verbreitet (vgl. Dewentner 2018, S. 1). In der Forschungsliteratur wird jedoch erwähnt, dass einige Marktakteure Interesse am Erwerb und an der Nutzung persönlicher Daten haben. Im Hinblick auf persönliche Daten von Wearable-NutzerInnen im Gesundheits- und Fitnesskontext lassen sich der Einzelhandel z. B. Sporthändler, Anbieter von Onlinediensten, Versicherungsunternehmen, werbetreibende Unternehmen und Marktforschungsunternehmen, Dienstleister in den Bereichen Datenanalyse und Data Broker, Forschungseinrichtungen sowie Gesundheitsinstitutionen erwähnen (vgl. Wieneke et al. 2016, S. 2).

Obwohl sowohl die Nutzung persönlicher Daten von Unternehmen, als auch der sekundäre Datenhandel bisher noch unausgeprägt stattfindet, stellen persönliche Daten potenziell einen wichtigen Input zur Erstellung von neuen oder bestehenden Produkten oder Services, auf den unterschiedlichen Stufen der Wertschöpfungskette für eine Vielzahl an Stakeholdern dar. Um die Relevanz persönlicher Daten für Service-Anbieter zu veranschaulichen werden datengetriebene und datennutzende Geschäftsmodelltypen im Überblick dargestellt.

4.3 Geschäftsmodelltypen der Datenwertschöpfung

Im Allgemeinen kann das Geschäftsmodell als modellhafte Darstellung der zentralen Geschäftsprozesse und -strukturen eines Unternehmens beschrieben werden, die der Erzeugung und der Nutzung von Werten dienen (vgl. Schallmo/Rusnjak 2017, S. 2; Dorfer 2018, S. 21). Der Untersuchungsgegenstand dieser Arbeit lässt sich im Konzept des technologieorientierten Ansatzes des E-Business-Geschäftsmodells verorten (vgl. Wirtz 2018). Es handelt sich um Geschäftsaktivitäten eines kommerziellen Unternehmens, bei dem eine „definierte Marktleistung vollständig oder weit überwiegend mit Internet-Technologien vollzogen wird“ (vgl. Schwickert 2004, S. 4 nach Dorfer 2017, S. 28).

4.3.1 Begriffsdefinition „Datengetriebenes Geschäftsmodell“

Der Begriff „Datengetriebenes Geschäftsmodell“ (engl. data-driven business model) ist in der Forschung bisher nicht eindeutig definiert und die Forschungsarbeit in diesem Bereich ist bislang unausgereift (vgl. Dorfer 2018, S. 26f). Einigkeit besteht darüber, dass das Entstehen von großen Datenmengen (Big Data) sowie die Potenziale, die mit der Verarbeitung, der Zusammenführung und der Nutzung des Datenbestands einhergehen, den Treiber für die Entwicklung neuer Geschäftsmodelle darstellen (vgl. ebd. S. 28). Im Allgemeinen werden

unter dem Begriff „Datengetriebenes Geschäftsmodell“ privatrechtliche Unternehmen, die Daten als Schlüsselressource ansehen und entsprechend nutzen, subsumiert (vgl. Hartmann et al. 2014, S. 6). Die Nutzung von persönlichen Daten in Unternehmen lässt sich im Allgemeinen in mehrere Szenarien gliedern. Zum einen dient die interne Erhebung und Verwertung von persönlichen Daten z. B. für die Produktentwicklung oder im Rahmen des Customer-Relationship-Management dem Wettbewerbsvorteil von Unternehmen, zum können persönliche Daten von NutzerInnen an Dritte vermarktet werden (vgl. Morlok et al. 2017, S. 203). Darüber hinaus kann der Geschäftszweck eines Unternehmens die Sammlung bzw. den Erwerb, die Verarbeitung und die Bereitstellung veredelter Daten beinhalten (vgl. Dorfer 2018, S. 21).

Um die „Wertschöpfung in Zeiten digitaler Selbstvermessung“ zu veranschaulichen, werden datengetriebene Geschäftsmodelltypen[13] im folgenden Kapitel im Überblick angeführt.

4.3.2 Geschäftsmodelltypen der Datenwertschöpfung im Überblick

Ähnlich wie in der Begriffsdefinition datengetriebener Geschäftsmodelle zeigt sich in der Gliederung der Geschäftsmodelltypen eine große Variationsbreite. Dies ist auf den jungen und daher bisher unausgereiften Forschungsgegenstand zurückzuführen. Die vorliegende Arbeit fokussiert sich auf Erkenntnisse von Acquisti (2014), wonach drei Märkte im Hinblick auf personenbezogene Daten unterschieden werden. Nach Tempich (2017) mit Ergänzung von Dorfer (2018) zeichnen sich vier übergeordnete auf Datenwertschöpfung basierende Geschäftsmodelltypen ab. Diese beziehen sich nicht explizit auf die Nutzung persönlicher Daten. In der Zusammenfassung lassen sich – auf Basis der angeführten Autoren – folgende datengetriebene Geschäftsmodelltypen mit dem Fokus auf persönliche Daten gliedern:

Nr	**Autor**	**Kurzbeschreibung**		**Relevanz im Forschungskontext**
		Kategorie personenbezogene Daten (nach Autor)	**Kategorie allgemeine Daten** (nach Autor)	
1	Acquisti 2014, S. 7	Traditionelle Geschäftsmodelle, die das Internet als Absatzkanal nutzen, in denen die Preisgabe persönlicher Daten als		Die Preisgabe der persönlichen Daten erfolgt unbewusst als sekundärer Aspekt einer Online-Transaktion (Acquisti 2014, S. 7).

[13] Die angeführten Geschäftsmodelltypen dienen der Veranschaulichung zur Verwertung persönlicher Daten in datengetriebenen Geschäftsmodellen. Die Auflistung stellt keinen Anspruch auf Vollständigkeit datengetriebener Geschäftsmodelle..

		sekundärer Aspekt der primären Transaktion erfolgt.		
2	Acquisti 2014, S. 8	Markt für personenbezogene Daten		
2a	Acquisti 2014, S. 8	Infomediäre, die Daten aus unterschiedlichen Quellen erwerben, aufbereiten, ggf. zu Nutzerprofilen aggregieren und an Dritte distribuieren.		Die sekundäre Verwertung von persönlichen Daten bedingt Privatheitsbedenken von NutzerInnen (vgl. Sicari et al., 2015, S. 149). Dabei kann die Bereitschaft zur Informationsfreigabe sinken (vgl. Morlok et al. 2017, S. 194).
2b	Acquisti 2014, S. 8	Intermediäre, die den Austausch zwischen zwei oder mehreren AkteurInnen ermöglichen, oftmals kostenlose Online-Plattformen.		Die kostenfreie Nutzung von Services im (oftmals) unbewussten Austausch persönlicher Daten (vgl. Dorfer 2018, S. 25).
3	Acquisti 2014, S. 8f	KonsumentInnen fragen Produkte und Dienstleistungen nach um persönliche Daten zu verwalten und zu schützen.		Potenzial neuer Geschäftsmodelle für den „Markt der Privatsphäre“; das Bewusstsein von Märkten für die Nutzung von persönlichen Daten wirkt sich auf die individuelle Bewertung der persönlichen Daten und somit auf das Schutzinteresse aus (vgl. Spiekermann/Korunovska 2017, S. 4; 16)
4	Dorfer 2018, S. 21 nach Tempich, 2017		Physische oder virtuelle Produkte, die mithilfe von Daten um datenbasierte Mehrwerte angereichert werden.	Produkte, die durch Daten angereichert werden und datenbasierte Mehrwerte, bsp. in Form der Personalisierung für NutzerInnen bieten, wodurch eine erhöhte Zahlungsbereitschaft bestehen kann (vgl. Dorfer 2018, S. 21 nach Tempich, 2017).

Tabelle 3: Überblick ausgewählter Geschäftsmodelltypen, personenbezogener und allgemeiner Daten, eigene Darstellung.

(1) Traditionelle Geschäftsmodelle, die das Internet als Absatzkanal nutzen, bilden einen Geschäftsmodelltypus. Hierbei ist zu berücksichtigen, dass die Preisgabe persönlicher Daten, und die Auswirkungen eines solchen Austausches auf den Datenschutz im Rahmen des Transaktionsprozesses als sekundärer Aspekt der primären Transaktion erfolgt (vgl. Acquisti 2014, S. 7). Dieser Geschäftsmodelltypus basiert auf der Sammlung und auf der Analyse von persönlichen Nutzungsdaten mit dem Ziel des gesteigerten Absatzes von Produkten und Services (vgl. Masur et al. 2018, S. 3; Tempich, 2017 nach Dorfer, 2018, S. 21). Im Rahmen des Kaufprozesses werden persönliche Daten gesammelt, die in weiterer Folge vom Unternehmen für Marketingzwecke, personalisierte Werbung, Produktempfehlung oder die dynamische Preisanpassung auf Basis der Kaufkraft der KonsumentInnen verwendet werden können (vgl. Masur et al. 2018, S. 16). Die Kaufkraft von KonsumentInnen kann anhand der geografischen Lage auf Basis der IP-Adresse oder aufgrund der Kaufhistorie angenommen werden (vgl. Hess/Schreiner 2012, S. 107; Masur et al. 2018, S. 16). Als Beispiel für diesen Geschäftsmodelltypus sind Unternehmen anzuführen, die Daten erheben und auswerten, um Marketingpotenziale für das eigene Produktangebot zu realisieren (vgl. Dorfer 2018, S. 21).

(2) Ein weiterer Geschäftsmodelltypus bezieht sich auf den Markt für personenbezogene Daten und lässt sich in zwei Ausprägungen unterteilen (vgl. Acquisti 2014, S. 8).

(2a) Es sind Unternehmen entstanden, die persönliche Daten aus unterschiedlichen Quellen erwerben, aufbereiten, ggf. zu Profilen aggregieren und an Werbetreibende weiterverkaufen. KonsumentInnen sind in dieser Austauschbeziehung passive Agenten und stehen mit „*Infomediären*“ indirekt in Kontakt (vgl. ebd.). Die sekundäre Verwertung von persönlichen Daten bildet eine zentrale Dimension der Privatheitsbedenken der NutzerInnen (vgl. Sicari et al., 2015, S. 149). Je eher KonsumentInnen erwarten, dass ihre persönlichen Informationen in einem zweiten Markt verkauft werden, desto weniger besteht die Bereitschaft zur Informationsfreigabe (vgl. Morlok et al. 2017, S. 194).

(2b) Als zweite Form dieses Typus lassen sich Geschäftsmodelle von „*Intermediären*“ beschreiben, die den Austausch zwischen zwei oder mehreren AkteurInnen ermöglichen (vgl. Acquisti 2014, S. 8). Der Betrachtungsfokus liegt auf Online-Plattformen, die für die Plattformteilnehmer Dienstleistungen anbieten, die Mehrwerte in Form der Sammlung, Verarbeitung und Bereitstellung veredelter Daten generieren. Als Kundengruppen des Geschäftsmodelltypus gelten NutzerInnen, denen meist kostenfrei Dienste angeboten werden um auf diese Weise Nutzerdaten zu erlangen. Die gesammelten Daten werden infolgedessen zur Monetarisierung des Dienstes, beispielsweise durch personalisierte

Werbung für Werbetreibende oder individuelle Produktangebote genutzt. (vgl. Dorfer 2018, S. 25) In diesem Typus dienen Nutzerdaten den Plattformanbietern der direkten Wertschöpfung, während aus der Sicht der NutzerInnen der Handel mit persönlichen Daten ein sekundärer, meist unsichtbarer Aspekt einer anderen sichtbaren Transaktion ist (vgl. Masur et al. 2018, S. 16). Aus NutzerInnenperspektive stellt sich die Frage, inwiefern Individuen zunehmend bereit sind ihre Privatheit zu reduzieren um kostenlose Güter bzw. Services zu erlangen (vgl. Rössler 2001, S. 218).

(3) In diesem Markt suchen KonsumentInnen nach Produkten und Dienstleistungen um ihre persönlichen Daten zu verwalten und zu schützen (vgl. Acquisti 2014, S. 8f) . Diese Geschäftsmodelle bilden die Brücke zwischen dem Markt für Datenschutz und dem Markt für persönliche Daten mit dem Ziel KonsumentInnen Selbstbestimmung im Hinblick auf ihre persönlichen Daten zu gewährleisten (vgl. ebd.). Der Erfolg dieses Geschäftsmodelltypus, sowie die Bereitschaft von KonsumentInnen mehr monetäre Leistungen für den Schutz der Online-Privatsphäre zu zahlen ist vom Bewusstsein der KonsumentInnen hinsichtlich der Datenverwendung durch Organisationen abhängig. Laut einer Studie von Spiekermann/Korunovska (2017) ist das Bewusstsein über Märkte persönlicher Daten der wichtigste Treiber für die monetäre Bewertung von persönlichen Daten (S. 21).

(4) Ein Geschäftsmodelltypus bezieht sich auf physische oder virtuelle Produkte, die mithilfe von Daten um datenbasierte Mehrwerte angereichert werden. Diese datenbasierten Mehrwerte, beispielsweise in Form der Personalisierung, führen zu einer erhöhten Zahlungsbereitschaft der Kunden und können zur Realisierung von Erlösen nutzbar gemacht werden (vgl. Dorfer 2018, S. 21 nach Tempich, 2017). Dorfer führt als Beispiel „Smart Services“ im Maschinen- und Anlagenbau an (S. 21), es können jedoch auch CIoT-Anwendungen wie Smartwatches oder Aktivitätstracker beschrieben werden. In beiden Fällen werden die physischen Produkte mit Sensoren ausgestattet, um darauf basierend Daten zu erheben, zu analysieren und in Mehrwertleistungen für KundInnen zu überführen (vgl. ebd.).

Während NutzerInnen die Offenlegung persönlicher Daten häufig nicht bewusst ist und deren Wert zumeist unbekannt ist, stellen persönliche Daten aus der Unternehmensperspektive einen Wert im Rahmen der unternehmerischen Wertschöpfung dar. Über Märkte zur Nutzung persönlicher Daten und die dort agierenden Unternehmen ist sowohl auf Markt-, als auch auf KonsumentInnenebene bisher wenig bekannt. Dies zeigt, dass die Verarbeitung von Nutzer- und Nutzungsdaten und die potenzielle Gefährdung aus der Sicht der KonsumentInnen schwer greifbar sind (vgl. Morlok et al. 2017, S. 204).

4.4 Zwischenfazit: Datenschutzrelevante Aspekte für NutzerInnen

Es kann festgestellt werden, dass KonsumentInnen als relevanter Bestandteil des Leistungserstellungsprozesses im Rahmen der interaktiven Wertschöpfung von Dienstleistungen betrachtet werden. Positive Aspekte der digitalen Selbstvermessung sowohl für NutzerInnen (Wertschaffung) als auch für Unternehmen (Wertschöpfung) werden angeführt. Gerade im Kontext der informationellen Privatheit werden Problemfelder greifbar. Im folgenden Abschnitt werden, zusätzlich zu den in Kapitel 3.3 genannten Problemfeldern der digitalen Selbstvermessung auf NutzerInnenebene, weitere mögliche Konsequenzen hinsichtlich des Datenschutzes aus Kapitel 4 zusammengefasst.

Der Besitz und die Nutzung persönlicher Daten durch andere Akteure als die Person, die diese Daten erzeugt, kann erhebliche Auswirkungen auf die soziale Diskriminierung haben (vgl. Lupton 2014, S. 13), beispielsweise im Rahmen von privaten Versicherungen. Algorithmen bringen digitale Daten auf bestimmte Weise zusammen, sodass für NutzerInnen konfigurierte „algorithmische Identitäten“ entstehen (vgl. Cheney-Lippold 2011, S. 165). Die Nutzung persönlicher Daten kann wiederum erfolgen, ohne dass Individuen Kontrolle darüber haben oder wissen, wie die Daten analysiert und verwendet werden. Eine mögliche Konsequenz in diesem Kontext ist die Verwendung großer digitaler Datensätze, um das Verhalten von Personen vorherzusagen und damit bestimmte Personen oder Personengruppen vom Zugang zu Waren und Dienstleistungen auszuschließen (vgl. ebd.). Wie bereits in Kapitel 3.3.2 erwähnt können Geräte der Selbstvermessung als Überwachungstechnologien mobilisiert werden und dadurch die soziale Benachteiligung bestimmter Gruppen weiter festigen.

Im Allgemeinen ist zu erwähnen, dass die Preisgabe persönlicher Daten oftmals unbewusst als sekundärer Aspekt einer Transaktion erfolgt (vgl. Acquisti 2014, S. 7). Dieses Verhalten ist ebenso bei der Nutzung von Wearables zu erwarten, da die Nutzung per se den primären Aspekt darstellt und die Datenfreigabe sekundär erfolgt, um das durch Daten angereicherte Produkt bzw. den Service nutzen zu können. Während Individuen Daten bewusst z. B. im Registrierungsprozess angeben, erfolgen beobachtete Daten und abgeleitete Daten unbewusst. Zudem können Dienstleister persönliche Daten an Dritte weitergegeben, ohne dass NutzerInnen darüber informiert werden (vgl. Acquisti 2014, S. 8; Morlok et al. 2017, S. 203; Dewentner 2018, S. 2). Die sekundäre Nutzung von persönlichen Daten durch Organisationen bedingt demnach Privatheitsbedenken bei NutzerInnen (vgl. Sicari et al. 2015, S. 149).

Autoren erkennen, dass dabei die Bereitschaft zur Informationsfreigabe sinkt (vgl. Morlok et al. 2017, S. 194).

Aufgrund der genannten privatheitsrelevanten Problemfelder ergeben sich neue Potenziale für den „Markt der Privatsphäre“, bei denen NutzerInnen Produkte und Services zum Schutz ihrer Online-Privatsphäre erwerben können (vgl. Acquisti 2014, 8f).

5 Informationelle Privatheit auf NutzerInnenebene

Nachdem in Kapitel 4 die datengetriebene Wertschöpfung aus der Perspektive von Organisationen und datenschutzrelevante Aspekte für NutzerInnen im Rahmen der digitalen Selbstvermessung aufgezeigt wurden, ist es im nächsten Schritt relevant theoretische Befunde der informationellen Privatheit auf NutzerInnenebene darzulegen. Im folgenden Kapitel wird die „Informationelle Privatheit“ auf NutzerInnenebene anhand des Privatsphäre-Prozess-Modells beschrieben. Anschließend werden Ergebnisse, des in der Privatheitsforschung häufig diskutierten Konzeptes, des Privacy Paradoxons, zusammengefasst und konzeptionelle Hintergründe des Privatheitsverhaltens von Individuen aus unterschiedlichen Forschungssträngen erläutert.

5.1 Privatheit auf NutzerInnenebene im Forschungskontext

Im Forschungskontext der informationellen Privatheit auf NutzerInnenebene werden unterschiedliche Positionen bedient, die zur Veranschaulichung in Modellen zusammengefasst werden. In dieser Masterarbeit wird das Privatsphäre-Prozess-Modell (Dienlin 2014) herangezogen, um drei relevante Elemente der Privatheit und deren gegenseitige Einflussnahme darzustellen. Abbildung 3 zeigt die Stufen des Modells, den *Privatheitskontext*, die *Privatheitswahrnehmung* und das *Privatheitsverhaltens,* die jeweils die nachgelagerte Prozessstufe beeinflussen. Die nacheinander folgenden Schritte werden folgendermaßen zusammengefasst: NutzerInnen haben eine Wahrnehmung hinsichtlich ihrer Privatsphäre, da sie sich in einem bestimmten Privatheitskontext aufhalten. Zudem geben NutzerInnen bestimmte Informationen preis (Verhalten), je nachdem wie privat der aktuelle Kontext wahrgenommen wird. Die Schritte folgen einem Prozessablauf. (vgl. Dienlin 2014, S. 5-11)

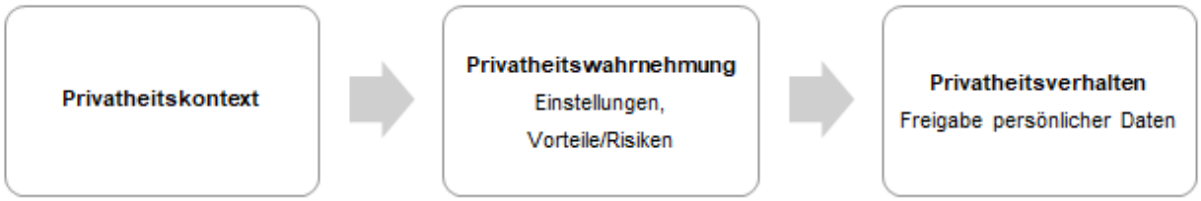

Abbildung 3: Privatsphäre-Prozess-Modell (PPM), eigene Darstellung adaptiert nach Dienlin, 2014, S. 11.

Wie bereits in Kapitel 2.2 erwähnt bedarf es im Hinblick auf die Konstitution von Privatheit eines Individuums an Freiwilligkeit und Kontrolle der Selbstoffenbarung. Laut Dienlin (2014) vergleichen Personen den tatsächlichen Zustand der Privatheit mit dem gewünschten Zustand und passen bei Abweichungen entweder den Kontext an (z. B. Verzicht auf ein Medium bzw. ein Service) oder ändern das Ausmaß der Selbstoffenbarung (Einschränkung der Freigabe persönlicher Daten). Die einzelnen Schritte des PPM werden nachfolgend beschrieben.

5.1.1 Privatheitskontext

Der Privatheitskontext entspricht der objektiven Abgeschiedenheit eines Individuums. Ein relevanter Aspekt ist die Tatsache, dass das Ausmaß der Privatheit von Individuen nicht stabil ist, sondern durchgängig fluktuiert (vgl. Masur et al. 2018, S. 5). In der Privatheitsforschung geht damit die Kontextabhängigkeit von persönlichen Daten einher. Individuen bewerten die Sensibilität ihrer persönlichen Informationen in bestimmten Kontexten unterschiedlich (vgl. Kokolakis 2017, S. 13; Masur et al. 2018). Bisherige Forschungsarbeiten im Rahmen der informationellen Privatheit beziehen sich in erster Linie auf den sozialen Kontext im Rahmen von sozialen Netzwerken bzw. Messaging-Diensten, in weiterer Folge auf den transaktionellen Kontext im Hinblick auf Online-Handel, mobile Anwendungen oder Finanz-Services (vgl. ebd. 2017, S. 22).

Die Wahrnehmung des Grades der Privatheit ist demnach kontextabhängig. In der informationellen Privatheit entspricht der Kontext der Menge an gesammelten Daten in einer bestimmten Situation (vgl. Dienlin 2014, S. 6), beispielsweise im Rahmen der Wearable-Nutzung im Gesundheits- und Fitnesskontext. Es ist festzuhalten, dass die Regeln für den Umgang mit Privatsphäre auf kulturellen, motivationalen und situationsbezogenen Kriterien basieren (vgl. Acquist 2015, S. 189). Demnach bedeutet Kontextabhängigkeit, dass Individuen hinsichtlich ihrer Online-Privatsphäre je nach Situation pragmatisch, fundamentalistisch oder gleichgültig handeln können (vgl. Westin 1967 nach Acquisti et al.

2015, S. 188). Dabei ist festzuhalten, dass Individuen persönliche Daten für geringe Vorteile wie Preisnachlässe preisgeben können, in einem anderen Kontext jedoch freiwillig erhebliche Kosten zum Datenschutz auf sich nehmen (vgl. Acquisti 2015, S. 187).

5.1.2 Privatheitswahrnehmung

Basierend auf dem objektiven Kontext der Privatheit entwickeln Individuen eine subjektive Privatheitswahrnehmung (vgl. Dienlin 2014, S. 6). Gerade im Medienkontext ist diese Unterscheidung sinnvoll, da Individuen häufig Situationen mit geringer Privatheit, wie beispielsweise das Teilen von Sportergebnissen in sozialen Netzwerken, als besonders privat einschätzen (vgl. Trepte/Reinecke, 2011, S. 70). Das bedeutet, je privater sich Menschen fühlen, desto eher sind sie bereit Informationen zu teilen. Hierbei ist zu erwähnen, dass der Wunsch nach Interaktion, Sozialisierung, Selbstoffenbarung sowie Anerkennung menschliche Motive sind, die nicht weniger relevant sind als das Bedürfnis nach Privatsphäre (vgl. Acquisti 2015, S. 188).

Die Wahrnehmung von objektiven Privatheitsverletzungen wie Identitätsdiebstahl, störende Marketingmaßnahmen oder Preisdiskriminierung schlägt sich in den Privatheitsbedenken der NutzerInnen nieder (vgl. Masur et al. 2018, S. 17). In Österreich liegen derzeit keine aussagekräftigen Daten im Hinblick auf Datenschutzbedenken von Wearable-NutzerInnen vor. Eine in Deutschland durchgeführte Studie (Moll et al. 2017, S. 37) bestätigte deutliche Datenschutzbedenken von Individuen im Kontext von Online-Anwendungen. Dabei zeigten sich Wearable-NutzerInnen (48 Prozent) tendenziell weniger besorgt als Nicht-NutzerInnen (62 Prozent), dass zu viele oder falsche Daten über sie gesammelt werden. Es ist anzumerken, dass auch Wearable-NutzerInnen mehrheitlich nicht mit einem Kontrollverlust ihrer persönlichen Daten einverstanden sind. Hinsichtlich des Forschungskontextes ist hervorzuheben, dass Wearable-NutzerInnen es zwar mehrheitlich riskant finden persönliche Daten freizugeben (62 Prozent), jedoch weniger häufig als Nicht-NutzerInnen (75 Prozent). Dabei vertrauen 50 Prozent der befragten Wearable-NutzerInnen in Online-Dienste und deren Umgang mit persönlichen Informationen, jedoch nur 39 Prozent der Nicht-NutzerInnen. Wenn es jedoch um die Weitergabe persönlicher Daten an andere Unternehmen geht zeigen sich sowohl NutzerInnen (75 Prozent) als auch Nicht-NutzerInnen (78 Prozent) besorgt.

5.1.3 Privatheitsverhalten

Im PPM-Modell definiert Dienlin (2014) das Privatheitsverhalten als jenes Verhalten, das Handlungen der Selbstoffenbarung, beispielsweise die Freigabe persönlicher Informationen, beinhaltet. Die Selbstoffenbarung ist somit eine Nachricht oder ein Teil einer Nachricht über das Selbst, die eine Person jemandem anderen mitteilt (vgl. Wheelees/Grotz, 1976 nach Dienlin 2014, S. 9). Übertragen auf den Forschungskontext ist die Mitteilung einer Person durch die Freigabe persönlicher Daten im Rahmen der Nutzung eines Gerätes bzw. eines Services gegeben. Die persönlichen Informationen werden an den Geräte-Anbieter bzw. an den App-Anbieter und gegebenenfalls an weitere Stakeholder übergeben. Zusätzlich können Informationen, wie beispielsweise Sportergebnisse, über eine Schnittstelle in sozialen Medien geteilt werden und damit eine Vielzahl an Personen erreichen.

Laut Acquisti/Grossklags (2005) treffen Individuen privatheitsrelevante Entscheidungen aufgrund mehrerer Faktoren wie: Auf Basis ihres Wissens, aufgrund der Relevanz, die der Situation der Datenfreigabe beigemessen wird, sowie hinsichtlich der Kostenintensivität und der Effektivität der Datenschutzmaßnahmen (S. 6).[14] Technologische Untersuchungen zeigen, dass NutzerInnen hinsichtlich der Preisgabe von persönlichen Informationen insbesondere auf den Informationsempfänger, die Informationsnutzung und die Informationssensitivität achten (vgl. Hartmann 2011, S. 192). Damit NutzerInnen Entscheidungen im Hinblick auf die Freigabe ihrer persönlichen Daten treffen können, ist eine entsprechende Informationsgrundlage in Bezug auf die Datenverwertung durch Organisationen relevant. Diese Erklärungen sollen VerbraucherInnen über den Umgang mit persönlichen Daten informieren. Aus rechtlicher Perspektive sind NutzerInnen erst informiert, wenn sie die Datenschutzbestimmungen eines Produktes bzw. Services gelesen und den Inhalten zugestimmt haben (siehe Kapitel 2.1).

Der Schutz persönlicher Daten ist mit erheblichen Transaktionskosten verbunden, beispielsweise beim Lesen von Datenschutzbestimmungen. Dabei stellt sich die Frage ob NutzerInnen die zeitlichen, kognitiven und motivationalen Ressourcen aufbringen, die bereitgestellte Datenschutzerklärung zu lesen bzw. in weiterer Folge die Datenschutzeinstellungen des genutzten Produktes bzw. des Services anzupassen (vgl. Moll et al. 2017, S. 32). Eine in Deutschland durchgeführte Studie zeigt, dass ein durchschnittlich

[14] Unvollständige Information, begrenzte Rationalität und systematische psychologische Verzerrungen spielen zudem eine maßgebliche Rolle in der Entscheidungsfindung (vgl. Acquisti/Grossklags 2005a, S. 6).

geübter Leser etwa acht Minuten benötigt um eine Datenschutzerklärung von Wearable- und App-Anbietern im Gesundheits- und Fitnesskontext zu lesen (vgl. ebd.).

Konzepte der privatheitsbezogenen Entscheidungsfindung sowie das entsprechende Verhalten von Individuen werden in Kapitel 5.3 aus mehreren Perspektiven beleuchtet. Zunächst wird auf das Konzept des Privacy Paradoxon eingegangen, dass in der Privatheitsforschung einen entsprechenden Stellenwert einnimmt.

5.2 Privacy Paradoxon

Ein Gefühl des Kontrollverlustes hinsichtlich der persönlichen Daten im Internet wird von 60 Prozent der befragten ÖsterreicherInnen bestätigt (vgl. Integral 2018, o. S.). Im Kontext von Wearable-NutzerInnen im Bereich Fitness und Gesundheit lässt sich erkennen, dass ÖsterreicherInnen prinzipiell Bedenken hinsichtlich des Datenschutzes äußern, jedoch aufgrund des Komforts nicht auf die Nutzung dieser Geräte verzichten möchten (vgl. Integral 2017, o. S.). Im konkreten Forschungskontext scheinen Individuen digitale Datenspuren durch die konstante Überwachung zu akzeptieren, da die Überzeugung besteht, dass Vorteile in der Nutzung die möglichen Kosten/Risiken überwiegen (vgl. Wieneke et al. 2016). In Bezug auf die Umfrageergebnisse ist zu erkennen, dass Individuen Privatheitsbedenken verspüren und besorgt sind persönliche Daten freizugeben, dennoch werden entsprechende Services genutzt.

Die Dichotomie zwischen der Einstellung zur Privatsphäre und dem tatsächlichem Verhalten der Individuen wird in der Wissenschaft mit dem Begriff „Privacy-Paradoxon“ definiert (vgl. Norberg et al. 2007, S. 101). Es gibt eine Vielzahl an Studien, die dieses Paradoxon bestätigen und einige, die durchaus einen direkten negativen Zusammenhang zwischen Privatheitsbedenken und der Selbstoffenbarung erkennen (vgl. Kokolakis 2015, S. 9-11; Masur et al. 2018, S. 14). Um diese Kontroverse zu verstehen ist zu erwähnen, dass das Verhalten im Hinblick auf die Privatsphäre ein kontextuelles Phänomen ist und zudem kulturelle Unterschiede zu erkennen sind (vgl. Kokolakis 2015, S. 11; Acquisti et al. 2015, S. 194).

Wie in Kapitel 2.2 beschrieben wird die allgemeine Privatheit des Individuums als ein Menschenrecht mit wesentlichem Bestandteil des Wertesystems der Gesellschaft definiert. Im Rahmen der informationellen Privatheit wird die Privatheit oftmals als wirtschaftliches Gut betrachtet. Aus wirtschaftswissenschaftlicher Perspektive wird zur Erklärung des Privacy Paradoxons häufig auf den wirtschaftlichen Grundsatz der Kosten-Nutzen-Analyse verwiesen

(vgl. Dinev 2014, S. 98; Wieneke et al. 2016). Das Modell der rationalen Kosten-Nutzen-Analyse (auch Privacy-Calculus) wird in Kapitel 5.3.1 im Detail erläutert.

Im Gegensatz dazu zeigt Dinev (2015), dass die Bewertung des möglichen Risikos nicht auf einer objektiven, rationalen mathematischen Berechnung der KonsumentInnen basiert, sondern auf „biased assumptions or cognitive shortcuts“ (Dinev 2015, S. 640). Weitere Autoren sehen die Dichotomie zwischen Einstellung und Verhalten als Folge des Einflusses verschiedener Faktoren, wie beispielsweise Fehleinschätzungen zwischen Kosten und Nutzen, soziale Normen, Emotionen, Heuristiken (vgl. Acquisti et al. 2015, S. 187) sowie die Unsicherheit aufgrund von unvollständiger Information und Informationsasymmetrie (vgl. Acquisti/Grossklags 2005a, S. 25).

Zur Interpretation der Entscheidungsfindung und des Verhaltens von NutzerInnen im Kontext der informationellen Privatheit werden im folgenden Kapitel unterschiedliche theoretische Stränge der Privatheitsforschung erläutert.

5.3 Konzeptioneller Hintergrund des Privatheitsverhaltens

Aktuelle Forschungsergebnisse zeigen, dass Individuen nach einem Gleichgewicht zwischen der Wahrung der Privatheit in digitalen Räumen und der Inanspruchnahme von Komfort, in Form von personalisierten Dienstleistungen und Waren, suchen (vgl. Dinev 2014, S. 97f). Um die skizzierte Komplexität der individuellen Entscheidungsfindung im Hinblick auf die Online-Privatheit zu erläutern, werden im folgenden Kapitel drei Forschungsstränge der Privatheitsforschung beschrieben: Kosten-Nutzen-Modell, Unsicherheit (Unvollständige Information, Informationsasymmetrie) und Aspekte der verhaltensökonomischen Entscheidungsfindung.

5.3.1 Kosten-Nutzen-Modell

Die Privacy-Calculus-Theorie besagt, dass Internetnutzer als rationale Agenten nach einem Kosten-Nutzen-Kalkül entscheiden, ob sie persönliche Daten preisgeben (vgl. Xu et al. 2011, S. 43). Darunter ist die Abwägung zwischen dem zu erwartetem Verlust (Risiko bzw. Kosten) der Privatsphäre und dem potenziellen Gewinn (Vorteile) durch die Offenlegung zu verstehen. Das tatsächliche Verhalten der NutzerInnen ist dabei durch das Ergebnis der Abwägung bestimmt (vgl. ebd.). Wahrgenommene Risiken hinsichtlich der Privatheit können als potenzieller Verlust der Kontrolle über persönliche Daten aufgrund von unbefugtem Zugriff,

Diebstahl oder der Weitergabe von Daten an Dritte verstanden werden (vgl. Smith et al. 2011, S. 997).

Der potenzielle Nutzen im Rahmen der Kosten-Nutzen-Entscheidung bezieht sich, laut Untersuchungen, in erster Linie auf monetäre Vorteile (z. B. Rabatte) und Komfort durch Personalisierung (vgl. ebd.). In sozialen Situationen hängt die Preisgabe an persönlichen Daten und Informationen von relationalen Beziehungen ab (vgl. Lee et al. 2013, S. 863). Wieneke et al. (2016) ergänzen im Kontext der Wearable-Nutzung Werte wie Zufriedenheit, Erfolg, Gesundheit, Selbstoptimierung und Lebensqualität. Die Interpretation der Anreize von Wearable-NutzerInnen zeigt, dass NutzerInnen vermehrt nach Genuss, Glück und Vergnügen streben. Diese Werte sind, im Vergleich zu monetären Anreizen und Komfort durch Personalisierung, hedonistischer Natur.

Das Kosten-Nutzen-Modell wird hauptsächlich in Transaktionssituationen angewandt. Individuen tätigen Transaktionen in Bezug auf ihre Privatsphäre, auch wenn die möglichen Kosten oder Risiken im Hinblick auf die Privatsphäre nicht greifbar sind, beziehungsweise wenn der Austausch personenbezogener Daten möglicherweise kein sichtbarer oder primärer Bestandteil einer Transaktion ist (vgl. Acquisti et al. 2015, S. 187).

Zusammenfassend beschreibt das Kosten-Nutzen-Modell die Bereitschaft von Individuen persönliche Daten freiwillig preiszugeben, wenn zu erwarten ist, dass die Offenlegung der Informationen die wahrgenommenen Risiken übersteigt.

5.3.2 Unsicherheit

Die auf NutzerInnenebene aufkommende Schwierigkeit eine angemessene Kontrolle über private Informationen auszuüben wird vermehrt in vernetzten und digitalisierten Informationsgesellschaften vorgefunden (vgl. Acquisti/Grossklags 2007, S. 1). Wearables sind Produkte mit Servicecharakter, bei denen die Verarbeitung persönlicher Daten zwar Bestandteil der Leistungserbringung ist, aber die Datenverwertung von Anbietern oder Dritten einen unsichtbaren, sekundären Bestandteil der primären Nutzung darstellt. Individuen sind sich oftmals unsicher, ob und inwieweit sie bei der Nutzung persönliche Daten freigeben oder schützen sollen (vgl. Acquisti/Grossklags 2007, S. 1).

Es ist anzunehmen, dass KonsumentInnen selten klare Kenntnisse darüber haben, welche Informationen von Anbietern gesammelt und von Marktakteuren verwendet werden, beziehungsweise mit welchen Konsequenzen (vgl. ebd. S. 1f). Aus diesem Grund sind sich

NutzerInnen im Zweifel nicht sicher wie viele Informationen sie mit welchen Anbietern, in welchem Kontext teilen sollen. Demnach ist davon auszugehen, dass NutzerInnen nicht in der Lage sind alle Risiken nach dem Kosten-Nutzen-Modell abzuschätzen, sondern, dass mangelndes Wissen die Einschätzung der NutzerInnen beeinflusst (vgl. Masur et al. 2018, S. 18). Privatheitsbezogene Entscheidungen sind demnach häufig durch *unvollständige Informationen* und insbesondere durch *asymmetrische Information* geprägt (vgl. Acquisti 2015, S. 18; Acquisti/Grossklags, 2007, S. 2).

Unvollständige Information drückt sich dadurch aus, dass KonsumentInnen nicht erkennen inwieweit ihr Online-Verhalten überwacht wird und wozu persönliche Daten im Detail verwendet werden (vgl. Acquisti 2014, S. 18). NutzerInnen sind daher oftmals mit zwei Unbekannten konfrontiert: Zum einen, *welche privatheitsrelevanten Resultate* in unterschiedlichen Kontexten auftreten können und zum anderen, *mit welchen Konsequenzen* (vgl. Acquisti/Grossklags 2007, S. 4). Um die Informationsasymmetrie zwischen NutzerInnen (Datensubjekt) und Unternehmen (Datenverwender) hervorzuheben ist zu erwähnen, dass Individuen wenig bzw. keine Kontrolle über die sekundäre Nutzung ihrer persönlichen Informationen haben (vgl. ebd.). Wie bereits erwähnt können Dritte legal Zugriff auf App-Daten der NutzerInnen erhalten.

Vor dem Hintergrund, dass sich KonsumentInnen in ihrer Entscheidungsfindung unsicher sind und eingeschränkte kognitive Fähigkeiten es nicht ermöglichen alle verfügbaren Informationen zu verarbeiten, um demnach rationale Entscheidungen hinsichtlich der möglichen Folgen zu treffen, suchen Individuen nach einfachen Hinweisen zur Anleitung im Entscheidungsprozess (vgl. Acquisti 2014, S. 18). Daher ersetzen NutzerInnen rationale Entscheidungsfindungsmethoden oftmals durch vereinfachte mentale Modelle und Heuristiken (vgl. Aquisti/Grossklags 2007, S. 6).

5.3.3 Aspekte der Verhaltensökonomie in der Privatheitsforschung

Aufgrund der Kritik an rationalen Kosten-Nutzen-Modellen wird zunehmend der Einfluss intuitiver Prozesse auf die privatheitsbezogene Entscheidungsfindung von Individuen untersucht (vgl. Dinev 2014, S. 100; Acquisti/Grossklags 2007, S. 6; Masur et al. 2018, S. 18f).

Einige Autoren der Privatheitsforschung, insbesondere im Bereich der informationellen Privatheit, bedienen sich an Erkenntnissen der Verhaltensökonomie. Bezugnehmend auf Camerer und Loewenstein (2004) kann die Verbindung folgendermaßen erläutert werden:

> "Behavioral economics increases the explanatory power of economics by providing it with more realistic psychology foundations."

Es ist zu erkennen, dass individuelle, soziale, kognitive und emotionale Verzerrungen wirtschaftliche Entscheidungen beeinflussen (vgl. Acquist/Grossklags 2007, S. 6). Daher geht es in der verhaltensökonomischen Forschung in erster Linie darum, kognitive Prinzipien innerhalb der Entscheidungsfindung von Individuen in die Herangehensweise von Ökonomen einzubeziehen (vgl. Goes 2013, S. 1).

Acquisti und Grossklags (2007) bedienen sich in der Erforschung individueller Entscheidungsfindung hinsichtlich der Privatheit auf Theorien der Psychologie und der Verhaltensökonomie (S. 1). Die Autoren erkennen psychologische Abweichungen von der Rationalität hinsichtlich der individuellen Entscheidungsfindung und beschreiben diese als *begrenzte Rationalität*. Zudem wird unterstrichen, dass die Annahme einer perfekten Rationalität nicht alle Nuancen des Privatheitsverhaltens umfasst (vgl. Acquisti/Grossklags 2007, S. 6). NutzerInnen von Wearables verfügen oftmals nicht über alle Informationen, die zu einer rationalen Entscheidungsfindung notwendig sind. Außerdem sind diese zum Teil nicht bereit (aufgrund zeitlicher, kognitiver oder motivationaler Ressourcen) alle relevanten Informationen zu erfassen (vgl. Moll et al. 2017, S. 32). In diesem Entscheidungsfindungsprozess ergeben sich *Verzerrungen*, denen sich Individuen nicht offensichtlich bewusst sind (vgl. Dinev 2014, S. 100).

Bisherige Forschungsergebnisse zeigen, dass sich Individuen hinsichtlich der Entscheidungsfindung im Rahmen der Online-Privatsphäre zum Teil auf *Heuristiken*, wie bisherige Erfahrungen mit einem Unternehmen beziehungsweise dessen Bekanntheit und Reputation, verlassen (vgl. Masur et al. 2018, S. 18). Eine Heuristik ist in diesem Forschungskontext eine simple und effiziente Technik, die Individuen beim Lernen oder beim Lösen von Problemen anleitet (vgl. Acquisti/Grossklags 2007, S. 7). Dies stellt einen oftmals genutzten Ansatz von Individuen dar um dem Problem der begrenzten Rationalität entgegenzuwirken.

Im Rahmen der Privatheitsforschung wurde bereits eine Vielzahl an Experimenten durchgeführt um kontextbezogene oder situationsbezogene Auswirkungen auf das

individuelle Privatheitsverhalten unter verhaltensökonomischen Aspekten zu erfassen (Acquisti/Grossklags 2005b; Acquisti/Grossklags 2007; Li et al. 2011). Dabei wurden Prinzipien der begrenzten Rationalität angewandt um Phänomene wie das Privacy Paradoxon zu erklären. Nach Acquisti/Grossklags (2007) wurden in diesem Zusammenhang u. a. folgenden Aspekte der verhaltensökonomischen Forschung identifiziert[15]:

- Framing-Effekt: Unterschiedliche Formulierungen oder Darstellungen einer Botschaft, bei gleichem Inhalt, beeinflussen das Verhalten des Empfängers unterschiedlich (vgl. ebd. S. 7). Ein Beispiel ist die Lesbarkeit oder die offensichtliche Darstellung von Datenschutzhinweisen in einem Service. Experimente bei der Auflistung möglicher Konsequenzen der Datennutzung durch Organisationen zeigen, dass die Datenfreigabe bei Services höher ist, wenn Individuen vorab informiert und überzeugt werden persönliche Daten freizugeben, als wenn Dienste erst nach der Datenfreigabe über privatheitsbezogene Konsequenzen informieren (vgl. Acquisti/Grossklags 2005b, S. 17f).
- Unter der Simulationsheuristik ist zu verstehen, dass Individuen dazu neigen, Ereignisse, die sich mental schwer vorstellen lassen, wie z. B. der Identitätsdiebstahl, als unwahrscheinlich abzuwerten (vgl. Acquisti/Grossklags 2007, S. 8).
- Ein Beispiel für die Repräsentativitätsheuristik ist, dass vertrauenswürdiges Verhalten mit einer ansprechenden Gestaltung einer Anwendung in Verbindung gebracht wird (vgl. ebd.).
- Das verhaltensökonomische Phänomen des „Hyperbolic Discounting“ bezieht sich darauf, dass Menschen eine Belohnung, die früher im Zeitverlauf stattfindet einer späteren Belohnung vorzuziehen, sofern die Verzögerung in einem absehbaren Zeitrahmen stattfindet (vgl. O’Donoghue/Rabin 2000, S. 233f). Im Rahmen des Privatheitsverhaltens ist darunter die Tendenz Kosten und Nutzen der Privatsphäre gegeneinander abzuwägen, sodass ein möglicher Verlust der Privatsphäre zugunsten einer sofortigen Befriedigung akzeptiert wird, zu verstehen (vgl. Acquisti/Grossklags 2007, S. 9).

Weitere verhaltensökonomische Aspekte, wie beispielsweise die Selbstüberschätzung oder die Theorie der rationalen Ignoranz, können sich ebenfalls auf die Entscheidungsfindung der KonsumentInnen auswirken und beeinflussen ob diese persönliche Daten schützen oder preisgeben (ebd.). Diese Aspekte unterliegen der zukünftigen Forschung.

[15] Diese Auflistung stellt einen Auszug der identifizierten Aspekte nach Acquisti/Grossklags (2007) dar.

6 Forschungsbedarf

Der empirische Teil dieser Arbeit befasst sich mit der Untersuchung der Einstellung von KonsumentInnen hinsichtlich der Nutzung von persönlichen Daten durch Organisationen. Als konkreter Anwendungsbereich werden Wearables im Gesundheits- und Fitnesskontext gewählt. Als Ausgangslage für die empirische Forschung dienen in anderen Ländern durchgeführte Studien, insbesondere jene von Wieneke et al. (2016) in der Schweiz und Moll et al. (2017) in Deutschland. Erstere bezieht sich auf die Bereitschaft des Einzelnen hinsichtlich der Freigabe persönlicher Daten durch Wearables aufgrund von wahrgenommenen Werten (z. B. Personalisierung, finanzielle Belohnungen). Moll et al. (2017) kombinieren unterschiedliche Methoden im Forschungskontext, d. h. die technische, rechtliche, lexikalische Analyse und die quantitative Befragung. Die meisten Untersuchungen im Rahmen der informationellen Privatheit wurden im sozialen Kontext (Soziale Netzwerke bzw. Messaging-Dienste) und im transaktionellen Kontext (Online-Handel, mobile Anwendungen oder Finanz-Services) durchgeführt.

Das Konzept der Privatheit aus wirtschaftswissenschaftlicher Perspektive ist im deutschsprachigen Raum weitgehend unterforscht. Morlok et al. 2017 widmen sich beispielsweise der Thematik. Forschungsarbeiten im Zusammenhang mit der informationellen Privatheit mit Wearables mit dem Fokus auf Wertschöpfungsprozesse persönlicher Daten sind darüber hinaus bislang nicht vorhanden.

Der Fokus der Arbeit liegt auf der NutzerInnenperspektive und auf möglichen Risiken hinsichtlich der informationellen Privatheit. Um diesen Zusammenhang in Österreich zu untersuchen, soll im Zuge dieser Arbeit ein an Österreich angepasstes explorativ es Forschungsdesign erarbeitet werden und als Ausgangspunkt für quantitative Forschungen in diesem Kontext dienen. Mit der Methode der Fokusgruppe wird ein qualitativer Ansatz gewählt, um die subjektiven Einstellungen der NutzerInnen zum Forschungskontext zu erfassen. Diese sind relevant, um die in Kapitel 1.2 definierten Sub-Forschungsfragen und folgende Leitfrage zu beantworten:

> » Welche Einstellungen haben NutzerInnen von Wearables im Gesundheits- und Fitnesskontext in Österreich hinsichtlich ihrer Privatsphäre? «

Die detaillierte Vorgehensweise des Methodendesigns wird in den nachfolgenden Kapiteln, im empirischen Teil dieser Arbeit, dargestellt.

B. Empirischer Teil

7 Methodologie

Um die definierten Forschungsfragen dieser Masterarbeit beantworten zu können, ist eine empirische Untersuchung der Materie unerlässlich. Vor allem aufgrund der Aktualität dieser Thematik liefert die bestehende Literatur keine ausreichenden Informationen für ein detailliertes Forschungsergebnis in Österreich.

Dieses Kapitel bietet einen Überblick der empirischen Forschungsmethode sowie zum Methodendesign dieser wissenschaftlichen Arbeit. Zu Beginn wird die methodische Vorgehensweise detailliert beschrieben. In weiterer Folge wird auf die Erhebungsmethode und auf die Datenauswertung näher eingegangen. Dies ist die Basis für die empirische Untersuchung in Kapitel 8.

7.1 Auswahl der Methodik

Da sich die vorliegende Masterarbeit mit einer explorativen Untersuchung eines Sachverhaltes unter den genannten Rahmenbedingungen beschäftigt, ist der Einsatz einer qualitativen Forschungsmethode für die Beantwortung der definierten Forschungsfragen zielführend. Aus der Sicht der Autorin eignet sich dafür besonders die Methode der Fokusgruppe. Die Auswahl der Methode wird im Folgenden näher erläutert.

Um die Forschungsfragen dieser Masterarbeit zu beantworten wird eine qualitative Studie zu den Einstellungen von Wearable-NutzerInnen (Fitnessarmbänder und Smartwatches in der Anwendung als Fitnesstracker) in Österreich hinsichtlich der Privatsphäre durchgeführt.

Der Fokus der empirischen Forschung liegt dabei auf den subjektiven Einstellungen der NutzerInnen in Bezug auf folgende Kernbereiche der Online-Privatsphäre im Forschungskontext:

- Subjektive Definition persönlicher Daten;
- Datenfreigabe und Bewusstsein der Relevanz persönlicher Daten für Organisationen;

- sowie das Vertrauen in ausgewählte Organisationen und mögliche Risiken für NutzerInnen.

Zu diesem Zweck wird eine Fokusgruppe durchgeführt. Die Methode ist besonders nützlich um das Wissen und die Erfahrungen der Menschen zu erforschen und zeigt nicht nur, was Individuen denken, sondern auch, wie sie argumentieren und warum (vgl. Kitzinger 1995, S. 299). Dieser Forschungsansatz wurde gewählt, da sich Gruppendiskussionen eignen um „[…] komplexe Einstellungs-, Wahrnehmungs-, Gefühls-, Bedürfnis-, Orientierungs- und Motivationsgeflechte von Menschen und Gruppen aus bestimmten sozialen Kontexten zu explorieren“ (Kühn/Koschel 2011, S. 33). Zudem ermöglicht der Ansatz ein tiefes Verständnis der zugrunde liegenden kognitiven Prozesse der Entscheidungsfindung von Individuen in Bezug auf ihre Online-Privatsphäre (vgl. Constantiou et al. 2014, S. 514). Die qualitative Forschung zeichnet sich dadurch aus, dass sie sich mit komplexen Sachverhalten beschäftigt, sowie Fragestellungen zur Rekonstruktion subjektiver Alltagserfahrungen ermöglicht, wofür eine relativ kleine Stichprobe herangezogen wird (vgl. Tauch/Menold, 2012, S. 5f). Aufgrund dieser Faktoren eignet sich die Fokusgruppe als Erhebungsmethode für die Ergebnisgewinnung der empirischen Forschung der vorliegenden Masterarbeit.

7.2 Erhebungsmethode

Die Fokusgruppe, in der deutschsprachigen Literatur mit dem Begriff „Gruppendiskussion“ dominierend, zählt zu den Erhebungsmethoden der empirischen Sozialforschung. Die methodologischen Grundstrukturen sowie das Untersuchungsdesign dieser Masterarbeit werden im folgenden Abschnitt erläutert.

7.2.1 Erläuterung der Methode Fokusgruppe

Gruppendiskussionen werden in Anlehnung an Morgan (1997) als Erhebungsmethode beschrieben, die Daten durch die Interaktion der Gruppenmitgliedern generiert, wobei die Thematik durch das Interesse des Forschenden bestimmt ist. Diese Definition setzt den Fokus auf die Interaktion der TeilnehmerInnen und erlaubt damit die Abgrenzung zu Gruppenmethoden, in denen dies nicht vorgesehen ist, wie dem Gruppeninterview (vgl. Mäder 2013, S. 25). Zudem unterscheidet sich diese Methode vom natürlichen

Gruppengespräch, bei dem keine Steuerung durch den Forschenden gegeben ist (vgl. ebd.). Im angelsächsischen Raum umfasst der Begriff „Focus Group“, sowohl strukturierte, als auch unstrukturierte Gruppendiskussionen, während die Bezeichnung im deutschsprachigen Raum für strukturierte Formen der Methode steht. Daher wird die Erhebungsmethode Fokusgruppe in dieser Masterarbeit als strukturiertes und moderiertes Diskursverfahren, bei dem eine Gruppe an ausgewählten TeilnehmerInnen zu vorab definierten Fragestellungen im Diskurs Ergebnisse erzeugt, beschrieben (vgl. Schulz 2012, S. 9; 29). Fokusgruppen zielen auf einen gemeinsamen Verständigungsprozess ab. Dabei werden Fragestellungen, im konkreten Fall Ableitungen der Forschungsfragen, aus unterschiedlichen Perspektiven diskutiert.

Die Fokusgruppe besticht im Vergleich zu qualitativen Einzelinterviews mit gruppendynamischen Effekten, die sowohl die Auskunftsbereitschaft als auch die Mitwirkung der Teilnehmenden innerhalb der Diskussion steigern (vgl. Schulz 2012, S. 13). Dieser Vorteil ist darauf zurückzuführen, dass die multilaterale Interaktion in der Gruppe der Alltagserfahrung näher ist, als die isolierte Formulierung in einem Einzelinterview (vgl. ebd.). Dieser Aspekt ist für diese Forschungsarbeit relevant, da die Autorin vermutet, dass sich die ProbandInnen über die Verwertung ihrer persönlichen Daten durch Organisationen, bei der Nutzung von Wearables, nicht bzw. wenig bewusst sind und der Online-Privatsphäre im Alltag wenig Aufmerksamkeit schenken. Im Hinblick auf den Forschungsgegenstand wird darauf hingewiesen, dass der kollektive Wissensbestand, auch aufgrund unterschiedlicher Erfahrungen der TeilnehmerInnen innerhalb der Fokusgruppe, leistungsfähiger ist als der einer Einzelperson (vgl. ebd.). Die Autorin geht davon aus, dass die Thematik des Forschungsgegenstandes, insbesondere Daten und Datennutzung, bisher keine Allgemeinbegriffe sind. Es ist daher anzunehmen, dass die Dynamiken der Gruppe zu breiteren Ergebnissen führen.

Ein zusätzlicher Vorteil der Fokusgrupppe ist, dass ModeratorInneneffekte aufgrund der Gruppengröße umgangen werden können (vgl. ebd.).

Die methodischen Hinweise unterschiedlicher AutorInnen zur Konzeption und Durchführung der Fokusgruppe sind vom Untersuchungsgegenstand geprägt und unterscheiden sich hinsichtlich der Auswahl der ProbandInnen (Zielgruppe, Gruppenzusammensetzung, Rekrutierung), der Kommunikation (Leitfadenentwicklung,

Moderationstechniken) und der Auswertung von Fokusgruppen (vgl. Tausch/Menold 2015, S. 5).

7.2.2 Auswahl der ProbandInnen

Die Zusammensetzung der Fokusgruppe lässt sich aufgrund der Homogenität bzw. Heterogenität der Gruppe, sowie nach der Anzahl der ProbandInnen bestimmen. Im Hinblick auf die Stichprobe ist die Zufallsauswahl einer großen Anzahl potenzieller TeilnehmerInnen oftmals nicht realisierbar und auch nicht erforderlich (vgl. Tausch/Menold 2015, S. 5; Schulz 2012, S. 13).

Die Grundlage stellt eine bewusste Auswahl an TeilnehmerInnen dar, die explizit für diese Studie rekrutiert werden und vorab keine Zusammengehörigkeit aufweisen. Diese Zusammensetzung wird Ad-hoc Gruppe genannt (vgl. Kühn/Koschel 2011, S. 76). Typischerweise erfolgt die Auswahl der TeilnehmerInnen nach zentralen Rekrutierungskriterien wie Geschlecht, Alter, Nutzungsverhalten (vgl. ebd. S. 76) oder nach dem Lebensstil (vgl. Schulz 2012, S. 13f). Die ProbandInnen werden so ausgewählt, dass hinsichtlich der Fragestellung möglichst alle inhaltlich relevanten Varianten von Problemzugängen und Erfahrungen durch wenigstens eine Person repräsentiert werden. Im Rahmen dieser Masterarbeit werden Einzelpersonen in ihrer Rolle als KonsumentIn, d. h. als NutzerIn von Wearables ausgewählt. Hintergrun der Auswahl auf Basis der Nutzung ist, dass die Thematiken der informationellen Privatheit und des Datenschutzes für alle NutzerInnen gleichermaßen relevant sind, unabhängig davon ob Interesse für die Thematiken besteht, bzw. Vorwissen vorhanden ist. Die Fragestellungen dieser Masterarbeit beziehen sich explizit auf Wearables im Gesundheits- und Fitnesskontext, da Einstellungen und Verhalten in Bezug auf die Online-Privatsphäre kontextuelle Unterschiede aufweisen (vgl. Kokolakis 2017, S. 23).

Die ausgewählten ProbandInnen sind aufgrund der Nutzungssituation homogen. Es werden im Rahmen dieser Masterarbeit NutzerInnen von Wearables in Österreich rekrutiert. Dabei werden keine Einschränkungen in Bezug auf das Geschlecht der TeilnehmerInnen getroffen, da im Hinblick auf die Forschungsthematik keine Befangenheitsaspekte zu erwarten sind. Durch Zufall sind Frauen und Männer in der Fokusgruppe jeweils zu 50 Prozent repräsentiert. Die TeilnehmerInnen werden in den Altersgruppen 18-29 Jahre und

30-49 Jahre rekrutiert, da diese am häufigsten Wearables nutzen (Siehe Kapitel 3.2.2, S. 19). Die Gruppenzusammensetzung ist bezogen auf die Soziodemografie heterogen. Der Vorteil von heterogen zusammengesetzte Gruppen ist die Möglichkeit zur Erfassung eines breiten Meinungsspektrum, da unterschiedliche Erfahrungen engagiert diskutiert werden können (vgl. Schulz 2012, S. 29). Zudem wird ein weites Spektrum von lebensgeschichtlichen Hintergründen einbezogen womit Rückschlüsse auf eine breitere Zielgruppe ermöglicht werden (vgl. Kühn/Koschel 2011, S. 81). Es ist jedoch darauf zu achten, dass die Komposition der Gruppe Auswirkungen auf die Gruppendynamik und damit auf die Ergebnisse der Forschung haben kann (vgl. Vicsek 2007, S. 27). In jedem Fall sollte Homogenität innerhalb Gruppe, in Bezug auf das Sprach- und thematisch bezogene Wissensniveau, bestehen (vgl. Kühn/Koschel 2011, S. 80). Dieser Aspekt wird bei der Rekrutierung der TeilnehmerInnen berücksichtigt.

Um eine geeignete Zusammensetzung der Gruppe zu ermöglichen wurde im Rekrutierungsprozess ein Fragebogen an potenzielle TeilnehmerInnen ausgehändigt. Zudem ermöglicht dies in der Auswertung die Zuordnung der TeilnehmerInnen zu ihrem demografischen Profil. Die ausgewählten ProbandInnen werden in einer Einzelfallanalyse anhand der Fragebogenergebnisse in **Tabelle 4** dargestellt. Die Interpretation der Gruppenzusammensetzung erfolgt in Kapitel 8.1.

ProbandIn	**Geschlecht**	**Alter**	**Tätigkeit**	**Sport pro Woche** (über 30 Minuten)	**Nutzungs-häufigkeit Wearable**	**Nutzungsmotive Wearable**
A	weiblich	22	In Ausbildung, angestellt	1-2 Mal	täglich	Sport, Ernährung
B	weiblich	23	in Ausbildung	1-2 Mal	täglich	Sport
C	männlich	25	angestellt	3-4 Mal	täglich	Sport, Gesundheit im Allgemeinen
D	männlich	29	selbstständig	3-4 Mal	täglich	Gesundheit im Allgemeinen
E	weiblich	30	angestellt	1-2 Mal	täglich	Gesundheit im Allgemeinen
F	männlich	32	angestellt	3-4 Mal	täglich	Sport, Gesundheit im Allgemeinen
G	männlich	36	angestellt	5+ Mal	täglich	Sport, Gesundheit im Allgemeinen

H	weiblich	43	angestellt	3-4 Mal	täglich	Sport, Gesundheit im Allgemeinen, Ernährung im Sinne der Leistungsfähigkeit

Tabelle 4: Einzelfallanalyse ProbandInnen, eigene Darstellung.

Die Anzahl der TeilnehmerInnen einer Fokusgruppe liegt häufig zwischen sechs und zehn (vgl. Morgan 1997, S. 5), maximal zwölf Personen (vgl. Schulz 2012, S. 13f). Für den Forschungskontext wurden acht ProbandInnen ausgewählt. Es soll eine entsprechende Sprechzeit für alle TeilnehmerInnen gewährleistet sein, damit die Autorin eine klare Einstellung und Reaktion jedes Einzelnen auf das Forschungsthema gewinnt (vgl. ebd. S. 18).

7.2.3 Vorbereitung des Diskussionsleitfadens

Fokusgruppen unterscheiden sich zudem in der Strukturiertheit, die der Moderator/die Moderatorin [16] festlegt. Die Aufgabe der Moderatorin ist es in erster Linie den Dialog zwischen den TeilnehmerInnen aufrecht zu halten und ein lebendiges Gespräch zu ermöglichen (vgl. Schulz 2012, S. 16). Der Diskussionsleitfaden dient als inhaltlicher Rahmen der Fokusgruppe.

Stärker strukturierte Ansätze für Fokusgruppen sind geeignet, wenn bereits Forschungsarbeiten zu der Thematik vorhanden sind und detaillierte Ergebnisse erzielt werden sollen (vgl. Morgan 1997, S. 12). Dabei ergibt sich jedoch das Problem, dass eine Vielzahl an vordefinierten Fragen begrenzte Daten aus der Perspektive der Teilnehmenden generiert. In der vorliegenden Arbeit gibt es bereits eine Grundlagenforschung hinsichtlich der informationellen Privatheit von Individuen. Die vorliegende Studie dient dem Verständnis der zugrunde liegenden kognitiven Prozesse der Entscheidungsfindung von Individuen in Bezug auf ihre Online-Privatsphäre bei der Nutzung von Wearables im Gesundheits- und Fitnesskontext. Daher ist es relevant die TeilnehmerInnen mit offenen Fragen zu einer möglichst natürlichen Diskussion anzuregen um unbewusste Meinungen und Einstellungen bewusst werden zu lassen. Morgan (1997) hat mit der Trichterstrategie einen Kompromiss zwischen einer strukturieren und einer unstrukturierten Diskussion gefunden. In einem trichtergestützten Interview beginnt die Gruppe mit einer offenen

[16] Die Rolle der Moderatorin wird von der Autorin selbst übernommen.

Diskussion einzelner Fragestellungen und folgt einem strukturierteren Ende, damit die Interviewerin detailliertere Ergebnisse erzielen kann. Die Trichterstrategie findet innerhalb der Fokusgruppe Anwendung und wird in der Vorbereitung des Diskussionsleitfadens berücksichtigt.

Der vorab definierte Leitfaden dient der Moderatorin als Orientierungshilfe, damit sichergestellt wird, dass alle forschungsrelevanten Aspekte während der Diskussion behandelt werden (vgl. Schulz 2012, S. 16). Der Leitfaden fungiert somit als Bindeglied zwischen der bestehenden Literatur und der empirischen Datenerhebung und bildet den inhaltlichen Rahmen des Fokusgruppendesigns.

Aufgrund der Leitfrage, sowie den Sub-Forschungsfragen und den erarbeiteten theoretischen Inhalten aus der bestehenden Literatur, wurde der Diskussionsleitfaden mit vier Kernblöcken erstellt:

1. Einleitung und Vorstellung der Teilnehmenden
2. Wearable-Nutzung im Gesundheits- und Fitnessbereich
3. Fragestellungen hinsichtlich der Privatheit
4. Mögliche Konsequenzen für NutzerInnen

Der Fokus der Diskussion liegt auf den Abschnitten drei und vier. Um den zweiten Block innerhalb der Diskussion kurz zu halten und dennoch einen transparenten Überblick über die Nutzung und die Nutzungsmotive der ProbandInnen zu erzielen, werden diese Ergebnisse im Rahmen eines Fragebogens in der Rekrutierungsphase erhoben.

7.2.4 Durchführung der Fokusgruppe

Der Ablauf der Fokusgruppe orientiert sich an drei definierten Phasen nach Schulz (2012): Planung, Durchführung und Auswertung. In der ersten Phase werden die Fragestellung, sowie der Untersuchungsgegenstand und dem folgend die inhaltliche und organisatorische Vorbereitung der Fokusgruppe durchgeführt. Die Forschungsfrage dieser Masterarbeit wird im theoretischen Teil dieser Arbeit formuliert und der Diskussionsleitfaden wird zur Beantwortung der forschungsleitenden Frage, sowie den formulierten Sub-Forschungsfragen entworfen.

In der zweiten Phase wird die Fokusgruppe durchgeführt. Die Fokusgruppe fand am 19. Juni 2019 von 18:00 Uhr bis 19:40 Uhr in Wien statt. Als geeigneter Ort wurde ein Besprechungszimmer ausgewählt, damit Stimuli mithilfe eines Flipcharts gesetzt werden können. Zudem können sich die TeilnehmerInnen ungestört auf die Thematik der Diskussion konzentrieren. Die Diskussion wird mit einem digitalen Aufnahmegerät aufgezeichnet, darüber werden die ProbandInnen zu Beginn der Gruppendiskussion informiert. Zusätzlich unterstützt eine Assistentin die Gruppendiskussion um Protokoll zu führen und die zentrale Thesen der Teilnehmenden aufzuschreiben. Damit soll sichergestellt werden, dass die Ergebnisse der Fokusgruppe aufgrund möglicher technischer Probleme verarbeitet werden können. Es wird auf eine Videoaufzeichnung verzichtet, da die Güte einer Studie mit der Nähe zur Alltagswelt der Befragten zunimmt und in natürlichen Umgebungen ehrlichere Antworten gegeben werden (vgl. Schulz 2012, S. 15f).

Die dritte Phase besteht in der Auswertung und der Analyse der generierten Daten sowie deren Interpretation (vgl. Schulz 2012, S. 16). Hierbei ist nicht nur auf die individuellen Diskussionsbeiträge des Einzelnen zu achten, sondern auf die Dynamik und das Meinungsspektrum der gesamten Gruppe (vgl. Koschel/Kühn 2011, S. 183). In dieser Phase wird Zusammensetzung der Gruppe anhand der Fragebogenergebnisse aus der Rekrutierungsphase beschrieben. Zudem werden die Ergebnisse der Tonaufzeichnungen und das Protokoll ausgewertet. Für die Auswertung der Tonaufzeichnung wird die qualitative Inhaltsanalyse nach Mayring herangezogen, die im folgenden Abschnitt erläutert wird.

7.3 Auswertung der Fokusgruppe

Nachdem die Datenerhebung durch die Fokusgruppe durchgeführt wurde, werden die Informationen anschließend systematisch ausgewertet. Die folgenden Unterkapitel beschreiben das Vorgehen der Analyse. Die Beschreibung ist relevant um den inhaltsanalytischen Vorgang der Studie nachvollziehbar und überprüfbar zu machen.

7.3.1 Transkription

Bevor die gewonnen Daten der Fokusgruppe ausgewertet werden können ist eine Transkription der Tonaufzeichnung notwendig. Die Autorin führt im Zuge der Datenauswertung eine wörtliche Transkription durch. Da die inhaltlichen Aussagen der Gruppendiskussion im Fokus der Forschung stehen, wurde auf Füllwörter wie z. B. „ähm“ oder „hm“ verzichtet. Zudem werden Dialektfärbungen in eine geschriebene Sprache gebracht um die Lesbarkeit der Texte zu vereinfachen (vgl. Hugl 2013, S. 88).

Zur Auswertung der transkripierten Gruppendiskussion wird die qualitative Inhaltsanalyse nach Mayring durchführt, die im nachfolgenden Kapitel näher erläutert wird.

7.3.2 Qualitative Inhaltsanalyse nach Mayring

Die qualitative Inhaltsanalyse stellt eine Auswertungsmethode dar, die Texte bearbeitet, welche im Rahmen sozialwissenschaftlicher Forschungsprojekte in der Datenerhebung, beispielsweise einer Fokusgruppe, anfallen (vgl. Mayring/Fenzl 2019, S. 633).

Bei der qualitativen Inhaltesanalyse werden Kategorienhäufigkeiten eruiert und im Textmaterial analysiert, womit sich dieser Ansatz gegenüber anderen Textanalysen unterscheidet (vgl. ebd.). Laut Mayring/Fenzl (2019) ist somit der Begriff „Qualitativ orientierte kategoriengeleitete Textanalyse“ konkretisierend.

Mayring (2010) fasst folgende Spezifika der Methodik zusammen:

- die Analyse von Kommunikation
- die Analyse fixierter Kommunikation
- das systematische Vorgehen
- das regelgeleitete Vorgehen
- das theoriegeleitete Vorgehen
- das Ziel verfolgen, Rückschlüsse auf bestimmte Aspekte der Kommunikation zu ziehen

Ähnlich wie in der quantitativen Inhaltsanalyse sollten vorab die inhaltsanalytischen Einheiten festgelegt werden. Dadurch kann gewährleistet werden, dass inhaltsanalytische Gütekriterien sinnvoll überprüfbar sind. Als zentrale Gütekriterien sind dabei die

Intrakoderübereinstimmung[17] und die Interkoderübereinstimmung[18] zu erwähnen (vgl. Mayring/Fenzl 2019, S. 636f).

Nach Mayring werden drei Techniken der qualitativen Inhaltsanalyse unterschieden. Neben der Explikation und der Strukturierung von Texten ist die Zusammenfassung eine mögliche Variante der Auswertungsform (vgl. Mayring/Fenzl 2019, S. 637). Aufgrund der vorliegenden Datenbasis wird die zusammenfassende Inhaltsanalyse angewandt. Dabei werden die Daten schrittweise gekürzt, sodass die für die Beantwortung der Forschungsfragen relevanten Informationen bestehen bleiben (vgl. ebd.).

Diese Analyseform ist somit für eine systematische Bearbeitung von vorliegenden Texten geeignet, mit dem Ziel die vorhandenen Informationen entsprechend zu kürzen, sodass eine adäquate Beantwortung der Forschungsfragen ermöglicht wird (vgl. Berger-Grabner 2016, S. 144).

7.3.3 Inhaltsanalytischer Vorgang

Das Grundprinzip der zusammenfassenden Inhaltsanalyse ist, dass die jeweilige Abstraktionsebene der Zusammenfassung festgelegt wird, die schrittweise auf das Material angewandt wird (vgl. Mayring 2010, S. 67). Das Ablaufmodell folgt demnach sieben Schritten, die in Abbildung 4 veranschaulicht werden. Im ersten Schritt wird das zu analysierende Material, die transkribierte Tonaufzeichnung der Fokusgruppe, festgelegt. Im zweiten Schritt werden die einzelnen Kodiereinheiten aus der Gruppendiskussion in einheitlicher Sprache formuliert und auf die relevanten Informationen beschränkt, indem Textteile ohne inhaltliche Bedeutung weggestrichen werden. Diese Maßnahme wird Paraphrasierung genannt. Anschließend werden im dritten Schritt die Paraphrasen generalisiert und verallgemeinert. Dabei gilt es im weiteren Schritt diese zu selektieren und wiederum inhaltsgleiche sowie nicht relevante Textstellen zu streichen. Im fünften Schritt des Ablaufmodells werden die vorhandenen Paraphrasen gebündelt und darauffolgend zu finalen Kategorien zusammengefasst. Dabei ist zu prüfen ob alle relevanten Paraphrasen im Kategoriensystem Anwendung finden. Im abschließenden Schritt erfolgt die

[17] Die Intrakoderübereinstimmung wird dadurch bestimmt, dass nach Abschluss der Analyse die Auswertung erneut beginnt, ohne die vorher zugeordneten Kategorisierungen anzusehen. Dadurch wird die Raliabilität sichergestellt (vgl. Mayring/Fenzl 2019, S. 636f).

[18] Bei der Interkoderübereinstimmung wird ein zweiter Kodierer herangezogen, wodurch das Kriterium für die Objektivität erfüllt wird (vgl. ebd.).

Rückprüfung der Ergebnisse am Ausgangsmaterial. Dieser Prozess wird bei Bedarf nochmals wiederholt. (vgl. Mayring 2010, S. 69)

Abbildung 4: Ablaufmodell zusammenfassender Inhaltsanalyse, eigene Darstellung in Anlehnung an Mayring 2010, S. 68.

Das Modell der zusammenfassenden qualitativen Inhaltsanalyse lässt sich in weiterer Folge für eine induktive Kategorienbildung einsetzen. Dabei werden die Kategorien direkt aus dem vorliegenden Material in einem Verallgemeinerungsprozess abgeleitet ohne dabei auf vorab formulierte Theorienkonzepte Bezug zu nehmen (vgl. Mayring 2010, S. 83). In diesem Vorgang wird eine möglichst gegenstandsnahe Abbildung des Materials erzielt, da Verzerrungen durch Vorannahmen des Forschers umgangen werden (vgl. ebd. S. 84).

8 Empirische Untersuchung

In diesem Kapitel werden die Forschungsergebnisse, die mittels Datenerhebung durch die Fokusgruppe gewonnen und anschließend mit der qualitativen Inhaltsanalyse nach Mayring ausgewertet wurden, veranschaulicht. Die Darstellung der Ergebnisse der

empirischen Forschung und die Interpretation dieser anhand des theoretischen Teils der Arbeit orientieren sich an der Struktur des Kategoriensystems (Tabelle 6), wobei einige Kategorien sinngemäß zusammengefasst werden. Um die Forschungsergebnisse zu interpretieren zu können wird zunächst die Beschreibung der Gruppenzusammensetzung durchgeführt.

8.1 Beschreibung der Diskussionsgruppe

Die Beschreibung der Gruppenzusammensetzung und der Gruppendynamik sind für die Interpretation der Forschungsergebnisse von Relevanz, denn „nicht das Wirken einzelner Teilnehmer sollte im Zentrum der Analyse stehen, sondern das Geschehen in der Gruppe als Ganzes“ (vgl. Kühn/Koschel 2013, S. 183). Im Folgenden wird der Fragebogen aus der Rekrutierungsphase ausgewertet. Zudem wird analysiert wie die TeilnehmerInnen miteinander interagieren und welche Rückschlüsse dabei auf die Interpretation der Forschungsfrage gezogen werden können.

8.1.1 Ergebnisse des Fragebogens

Die erhobenen Daten des Fragebogens wurden quantitativ analysiert und die relevanten Ergebnisse und Zusammenhänge erfasst. Die Ergebnisse geben Aufschluss über die Gruppenzusammensetzung. Diese Informationen sind in weiterer Folge relevant für die Analyse und Interpretation der generierten Forschungsergebnisse. In Bezug auf **Tabelle 4** kann eine Ausgewogenheit in der Gruppenzusammensetzung hinsichtlich des Geschlechts (50 Prozent Frauen und 50 Prozent Männer) sowie hinsichtlich des Alters (50 Prozent 18- bis 29-Jährige und 50 Prozent 30- bis 49-Jährige) festgestellt werden. Fünf ProbandInnen sind angestellt, eine Probandin befindet sich in Ausbildung und eine Probandin ist sowohl angestellt als auch in Ausbildung. Zusätzlich ist ein Teilnehmer selbstständig. Damit ist neben der Homogenität in der Nutzungssituation, eine heterogene Gruppenzusammensetzung hinsichtlich des soziodemografischen Profils der Teilnehmenden zu erkennen.

Darüber hinaus sind alle ProbandInnen prinzipiell sportlich aktiv und treiben zumindest ein bis zwei Mal pro Woche Sport (drei ProbandInnen). Die Mehrzahl (vier ProbandInnen) ist

drei bis viermal pro Woche sportlich aktiv und ein Proband ist Profisportler und treibt mehr als fünf Mal pro Woche Sport.

Besonderes Augenmerk liegt auf der Nutzungshäufigkeit von Wearables, denn jeder der Befragten nutzt seine Selbstvermessungstechnologie täglich. Hierbei ist die intensive Integration der Technologie bzw. des Services in den Alltag der NutzerInnen zu erkennen. Hinsichtlich der Nutzungsmotive waren Mehrfachantworten zulässig, die meisten ProbandInnen nutzen ihr Gerät für den Sport und/oder für ihre persönliche Gesundheit im Allgemeinen. Eine datengetriebene Kontrolle hinsichtlich der Ernährung ist für zwei ProbandInnen relevant, medizinische Hintergründe sind nicht repräsentiert.

8.1.2 Beschreibung der Gruppendynamik

Die Autorin ist der Meinung, dass innerhalb der Gruppe eine angenehme Gesprächsatmosphäre erzielt wurde, sodass die ProbandInnen in einer Gesprächssituation, ähnlich eines Alltagsgespräches, miteinander agierten. Die Rückbezüge auf Aussagen von TeilnehmerInnen und gezielte Fragestellungen zwischen den ProbandInnen, ersichtlich in der Transkription, lassen auf dieses Verhalten schließen. Während der Diskussion wird festgestellt, dass die Nutzung von Wearables ein verbindendes Element in der Gruppe darstellt. Es werden jedoch unterschiedliche Geräte hinsichtlich des Produktes und der Marke genutzt (siehe **Tabelle 5**). Zudem sind die Nutzungsmotive sowie das entsprechende Nutzungsverhalten divergierend. Dadurch konnte ein breites Spektrum an Einstellungen zur Forschungsthematik gewonnen werden. Die Ergebnisse werden im folgenden Abschnitt im Detail beschrieben.

Marke	**Anzahl der ProbandInnen**
Smartwatch (50 Prozent)	
Apple Watch	3
Galaxy Watch (Samsung)	1
Fitnessarmband (50 Prozent)	
FitBit	2
Polar	1
Xiaomi	1

Tabelle 5: Fokusgruppe: Anzahl der genutzten Wearables nach Produkt und Marke, eigene Darstellung.

8.2 Darstellung der Ergebnisse im Überblick

Im Rahmen der vorliegenden Masterarbeit bilden die innerhalb der Diskussion generierten Aussagen der ProbandInnen die Grundlage für die Kategorienerstellung. In Anlehnung an die Leitfrage und die Sub-Forschungsfragen konnten induktiv, d. h. direkt aus dem Analysematerial, sechs Hauptkategorien und insgesamt 20 Unterkategorien gebildet werden. Diese werden in der folgenden Tabelle veranschaulicht.

Hauptkategorie	**Unterkategorie**	**Kapitel**
A Nutzung Wearables	1. Nutzungsmotive	8.3.1
	2. Nutzungsanreize/Nutzerakzeptanz	8.3.1
	3. Vernetzung mit Smartphone	8.3.2
	4. Integration von Wearables im Alltag	8.3.2
	5. Funktionalitäten Wearables	8.3.3
B Persönliche Daten	1. Allgemeine Einstellungen Privatheit	8.4
	2. Begriffsverständnis	8.4.1
	3. Datenanalyse und Profilerstellung	8.4.2
	4. Datenqualität	8.4.3
C Datennutzung	1. Datennutzung durch Organisationen	8.5.1
	2. Mögliche Konsequenzen persönlich	8.5.2
	3. Mögliche Konsequenzen gesellschaftlich	8.5.3
D Privatheitsverhalten	1. Subjektives Privatheitsverhalten	8.6.1
	2. Anreize zur Datenfreigabe	8.6.1
E Datenschutz	1. Persönliche Datenschutzstrategien	8.6.2
	2. Regulatorische Rahmenbedingungen	8.6.2
F Handlungsempfehlungen	1. Vertrauen in Datenhalter	8.7.1
	2. Transparenz durch Datenhalter	8.7.2
	3. Integration der NutzerInnen	8.7.3
	4. Richtigkeit der Daten	8.7.3

Tabelle 6: Kategoriensystem Überblick, eigene Darstellung.

In der Kategorie „Nutzung Wearables“ werden die Motive der Teilnehmenden für den Gebrauch von Smartwatches und Fitnessarmbändern eruiert. Zudem werden Anreize

beschrieben, die zur laufenden Nutzung von Wearables beitragen und zu einer entsprechenden Nutzerakzeptanz führen. Besonderes Augenmerk liegt auf Gamification-Aspekten, die in Kapitel 3.2.3 beschrieben wurden. Darüber hinaus ist die Vernetzung mit dem Smartphone und die Integration von Wearables in den Alltag ein relevantes Thema. Der Aspekt „Funktionalitäten Wearables“ ergab sich im Rahmen der Diskussion, da die ProbandInnen mit Engagement über die Funktionalitäten ihrer Wearables diskutierten.

Der Fokus der Auswertung liegt auf den folgenden beiden Kategorien. In der Kategorie „Privatheit und Persönliche Daten“ werden zunächst Einstellungen zur Privatheit im Forschungskontext der ProbandInnen erfasst. Im weiteren Schritt wird das subjektive Begriffsverständnis der ProbandInnen zusammengefasst. Die Profilbildung und die Analyse auf Basis von gemessenen Wearable-Daten, sowie die Qualität von Gesundheitsdaten werden weiters angeführt.

In der Kategorie „Datennutzung“ werden Organisationen beschrieben, die im Kontext von Fitness und Gesundheit an der Nutzung von persönlichen Daten profitieren. Dabei wird auf mögliche persönliche Konsequenzen durch die Datenverwertung für NutzerInnen eingegangen. Zudem werden mögliche gesellschaftliche Auswirkungen erläutert.

Das „Privatheitsverhalten“ von NutzerInnen konnte anhand von subjektiven Erfahrungen reflektiert werden. Außerdem werden Anreize für NutzerInnen zur Datenfreigabe in dieser Kategorie zusammengefasst.

Die Kategorie „Datenschutz“ bildet persönliche Strategien der Teilnehmenden zum Schutz ihrer persönlichen Daten ab. Regulatorische Rahmenbedingungen aus der Perspektive der NutzerInnen werden zudem angeführt.

Abschließend werden Einstellungen und Vertrauensbeziehungen der ProbandInnen zu Anbietern und Unternehmen sowie deren Wünsche hinsichtlich des Umgangs mit persönlichen Daten in der Kategorie „Handlungsempfehlungen“ zusammengefasst.

8.3 Nutzung von Wearables

Der erste Part der empirischen Auswertung befasst sich mit der Nutzung von Wearables im Gesundheits- und Fitnesskontext. Dabei werden vor allem Nutzungsmotive, Anreize für

die regelmäßige Nutzung, die Vernetzung und Integration von Wearables im Alltag sowie Funktionalitäten von Wearables näher beleuchtet.

8.3.1 Nutzungsmotive und Nutzungsanreize bei der Verwendung von Wearables

Die ProbandInnen gaben im Fragebogen an Wearables täglich zu nutzen. Die Ergebnisse zeigen, dass die Aufzeichnung der Aktivität im Rahmen des Tagesablaufes einen der Hauptnutzungsgründe für die ProbandInnen darstellt, sowohl für NutzerInnen von Smartwatches als auch für NutzerInnen von Fitnessarmbändern. Die Messung der sportlichen Aktivität kann dabei einen zusätzlichen Faktor darstellen. Hervorzuheben ist, dass die Motivation durch das Wearable zur regelmäßigen Bewegung im Alltag einen Nutzungsanreiz für alle Teilnehmenden darstellt. Zwei TrägerInnen von Fitnessarmbändern nutzen die Selbstvermessungstechnologie ausschließlich zur Aufzeichnung des Tagesablaufes und der sportlichen Aktivität, weitere Funktionalitäten werden dabei bewusst nicht genutzt. Die gezielte Messung der Aktivität steht hierbei im Vordergrund.

Die Integration in den Alltag und der Anreiz zur laufenden Aktivität kann folgendermaßen begründet werden:

> „Wie gesagt, reingekommen bin ich durch den Sport, aber mittlerweile nutze ich es halt auch, eben weil ich auch – wie wir fast alle – einen Bürojob habe.“ (ProbandIn G 2019, Zeilen 275-276)

Die Motivation durch das Wearable mehr Sport zu machen und auf die Ernährung zu achten wird von den ProbandInnen als Vorteil beschrieben. Dabei schlussfolgern die Teilnehmenden der Gruppendiskussion, dass Wearables zwar motivierend wirken, aber nicht die Grundlage für einen gesunden Lebensstil bilden (ProbandIn A, D, G 2019, Zeilen 1055-1057). Ein weiterer Nutzungsgrund ist das Anzeigen der Uhrzeit.

Nutzungsakzeptanz Wearables

Die Akzeptanz zur Verwendung des Wearables liegt in erster Linie in der Bequemlichkeit und der Einfachheit der Nutzung begründet. Des Weiteren wird, vor allem bei NutzerInnen von Smartwatches, die Smartphone-Funktion als bequem beschrieben:

> „Du kannst, auch wenn du nicht erreichbar bist oder das Handy auf lautlos hast, sehen wer ruft gerade an oder welche SMS kommen rein […] Das ist sehr angenehm, finde ich.“ (ProbandIn A 2019, Zeilen 80-83)

Zudem wird darauf hingewiesen, dass es in bestimmten sozialen Situationen nicht angebracht ist einen Blick auf das Smartphone zu werfen (ProbandIn E 2019, Zeile 1152), daher werden die Funktionalitäten von Wearables präferiert. Außerdem wird die Möglichkeit der Produktpersonalisierung positiv hervorgehoben.

Nutzungsmotive Wearables

Wie in Kapitel 0 als Geschäftsmodelltypus angeführt kann ein Wearable als physisches Produkt beschrieben werden, das um datenbasierte Mehrwerte angereichert wird. Die Voraussetzung für die Funktion von Wearables ist die Sammlung und Verwertung von Daten der NutzerInnen. Die empirischen Ergebnisse zeigen, dass der Mehrwert für NutzerInnen ausschließlich auf Basis von richtigen Daten (z. B. Alter, Gewicht) entsteht (ProbandIn H 2019, Zeilen 390-395). Aufgrund dessen lässt sich der Servicecharakter des Wearables beschreiben. Die Anwendung von Datenschutzstrategien wie die Angabe falscher Daten führt dabei nicht zur Zufriedenheit der NutzerInnen. Die Funktion des Services per se, sowie die auf gesammelten Daten basierende Wertschöpfungsaktivitäten auf Anbieterseite, können nur bei regelmäßiger Nutzung der Trägerinnen gewährleistet werden. Die Forschungsergebnisse zeigen Motivationsanreize, die eine regelmäßige Wearable-Nutzung fördern. Die Funktionalitäten von Wearables stellen dabei den ersten Anreiz dar. Dieser kann folgendermaßen beschrieben werden:

> „Ich bin dann mehr und mehr reingerutscht. […] Dann hab ich mir gedacht, ich kopple es vielleicht doch, und die Funktionen haben mich mehr und mehr reingezogen und mittlerweile bin ich dauernd aktiv.“ (ProbandIn H 2019, Zeilen 124; 126-127)

Zudem werden spieltypische Mechaniken und Elemente bei der Nutzung von Wearables durchwegs positiv und als intrinsischer Motivator wahrgenommen. Die Autorität der Strukturvorgaben spielerischer Gratifikationen kann folgendermaßen beschrieben werden:

> „Einmal in der Nacht, da haben mir acht Kalorien gefehlt, damit ich meinen Ring schließe. Ich bin dann noch aufgestanden, damit ich meinen Ring schließe.“ (ProbandIn A 2019, Zeilen 1055-1056)

Damit stellt der Gamificiation-Aspekt, wie in Kapitel 3.2.3 in der Theorie beschrieben, einen Motivator für NutzerInnen dar. Zudem verweisen die Ergebnisse auf Belohnungen durch Pokale und Vibration der Uhr sowie auf positive Nutzungsanreize durch Feedback-Mechanismen.

Laut ProbandInnen führt die Kommunikation von Wearables zur Verzerrung der Realität, da stets positive Nachrichten als Feedback angezeigt werden (ProbandIn H 2019, Zeilen 1083-1085). Diese Art der Kommunikation wird als positives Nutzungserlebnis empfunden.

8.3.2 Vernetzung und Integration im Alltag

Die ProbandInnen integrieren die Selbstvermessungstechnologie in der Anwendung von Wearables in ihren Alltag. Im Gegensatz zum Smartphone besteht die Möglichkeit das digitale Gerät Tag und Nacht direkt am Körper zu tragen. Diese Möglichkeit wird zum Teil wahrgenommen, da das Schlafverhalten gemessen werden soll bzw. die Weckfunktion genutzt wird. Einige ProbandInnen lehnen die Nutzung während des Schlafes bewusst ab. Zudem lassen sich unterschiedliche Verhaltensmuster der ProbandInnen hinsichtlich der Vernetzung zwischen Wearable und Smartphone erkennen. Vor allem Smartwatch-NutzerInnen beobachten eine konstante Verbindung zwischen dem Wearable und dem Smartphone. Die Smartwatch wird dabei als „Mini-Handy auf dem Handgelenk“ beschrieben (ProbandIn A 2019, Zeile 75). Demgegenüber wird die punktuelle Verbindung mit dem Smartphone, um Aktivitätsergebnisse zu überprüfen, angeführt. Der bewusste Verzicht der Smartphone-Funktion wird folgendermaßen deutlich:

> „Ich mag nicht ständig erreichbar sein, ich will nicht noch mehr Zeit mit irgendeinem Screen verbringen, egal wie klein und praktisch er auch sein mag“. (ProbandIn E 2019, Zeilen 209-210)

Anbieter von Wearables haben in diesem Zusammenhang unterschiedliche Einstellungen und Verhaltensweisen von KonsumentInnen zu bedienen.

8.3.3 Funktionalitäten von Wearables

Die Funktionalitäten von Wearables sind ein relevantes Thema unter den NutzerInnen. Smartphone-Funktionalitäten wie die Weckfunktion, das Telefonieren, die Beantwortung von Nachrichten etc. werden sowohl von NutzerInnen von Smartwaches als auch von NutzerInnen von Fitnessarmbändern beschrieben. Darüber hinaus werden Gesundheitsfunktionen wie EKG, Pulsmesser, Messung des Schlafverhaltens, Anzahl der Schritte, Ernährungsdaten und Darstellung der Daten im Zeitverlauf angeführt. Smartwatch-NutzerInnen erwähnen außerdem einzelne App-Funktionen direkt auf der Uhr. Im Allgemeinen wird festgestellt, dass laufend neue Funktionalitäten von Wearables wie beispielsweise die Sturzerkennung von Apple, die auf Prinzipien des maschinellen Lernens basiert, für Begeisterung bei den NutzerInnen sorgen.

8.4 Privatheit und persönliche Daten im Kontext des Self-Tracking

Die empirischen Ergebnisse machen subjektive Einstellungen von Wearable-NuzterInnen in Österreich hinsichtlich der Privatheit deutlich. Dabei wird erkannt, dass sich einige ProbandInnen über die Relevanz persönlicher Daten für Organisationen bewusst sind. Man habe nichts zu verbergen und einem sei egal wer seine persönlichen Daten bekomme (ProbandIn D 2019, Zeilen 523-526), ist dabei eine Meinung. Hinsichtlich dieser Einstellung erscheinen Datenschutzstrategien irrelevant. Zum anderen sind ProbandInnen der Meinung, dass persönliche Daten einzelner NutzerInnen irrelevant für Marktakteure sind, interessant erscheint jedoch das Gesamtnutzungsverhalten von KonsumentInnen. Im Allgemeinen ist zu erkennen, dass die Aussage „Was soll schon passieren?“ (ProbandIn G 2019, Zeile 599) auf die Abstraktion der Thematik zurück zu führen ist, da die Datenfreigabe im Alltag für NutzerInnen schwer greifbar ist. Die wahrgenommene Unfähigkeit selbst Handlungen hinsichtlich des Datenschutzes zu setzen wird zudem deutlich. Dabei stellen ProbandInnen die Frage, ob man überhaupt etwas tun kann, um die Bewegung im Sinne der KonsumentInnen zu gestalten (ProbandIn E 2019, Zeilen 1020-1025).

8.4.1 Der Begriff „Persönliche Daten“ aus NutzerInnenperspektive

Im Allgemeinen ist zu erkennen, dass Teilnehmende Schwierigkeiten haben zu beschreiben welche Daten sie als persönlich empfinden. Die Moderatorin setzte nach einer kurzen Diskussion einen Stimulus mit der Auflistung von Datenarten, die durch Wearables gesammelt werden können (siehe Anhang – Stimulus Material).

Die Ergebnisse zeigen, dass die subjektive Definition des Begriffs „Persönliche Daten“ anhand der Beschreibung von möglichen Verletzungen der Privatsphäre (siehe **Tabelle 7**) oder nach der Relevanz persönlicher Daten für Organisationen erfolgt, wie beispielsweise durch folgende Aussage:

> „Größe, Gewicht, dann weiß sofort jeder wie oft du Sport machst. Das ist kein Geheimnis, dass die ganzen Daten wichtig sind für Versicherungen, Gesundheitssystem etc.“ (ProbandIn G 2019, Zeilen 350-251)

Demnach ist zu prüfen ob Daten als persönlich wahrgenommen werden wenn diese für andere Parteien Nutzen stiften.

Die nachfolgende Tabelle zeigt Einstellungen der ProbandInnen zum Begriff „Persönliche Daten“ im Forschungskontext, die unter „Verletzung der Privatsphäre“ zusammengefasst werden. Darunter werden folgende Aspekte von Wearable-NutzerInnen beschrieben: Zum einen die mögliche Erstellung von persönlichen Gesundheitsprofilen von Anbietern. Des Weiteren wird die Identifizierung des Individuums auf Basis von Profildaten mit verknüpften Verhaltens- und Standortdaten sowie die Identifizierung der Interessen des Individuums aufgrund von Verhaltensdaten und entsprechender Ausspielung personalisierter Werbung als Verletzung der Privatsphäre wahrgenommen. Einen weiteren Eingriff in die Privatsphäre könnte die Weitergabe von Profildaten durch die Verknüpfung zu sozialen Medien darstellen. Kaufprozessdaten sowie die Aufzeichnung von Standortdaten mit der möglichen Konsequenz der Nachverfolgung werden von einigen ProbandInnen als Eingriff beschreiben. Zudem werden jene Daten die nicht allgemein verfügbar oder ableitbare sind als Eingriff in die Intimsphäre des Menschen wahrgenommen. Besonders heikel werden Daten von anderen (z. B. Kontaktdaten) beschrieben.

<table>
<tr><td colspan="4">Einstellungen der ProbandInnen zum Begriff „Persönliche Daten“ im Forschungskontext
Begriffsdefinition – Verletzung der Privatsphäre[19]</td></tr>
<tr><td>Ankerbeispiel</td><td>Generalisierung</td><td>Reduktion</td><td>Kategorie</td></tr>
<tr><td>„Also ich glaube damit wird das ganze Profil von dir erstellt oder? Also es kann Blutdruck, wie gesund du bist, wie lang du schläfst. Ich weiß jetzt nicht, wenn du das GPS ausgeschalten hast, ob es dich wirklich tracken kann, ob es schauen kann, wo du bist.“ (ProbandIn C, Z. 340-343)</td><td>Erstellung eines persönlichen Gesundheitsprofils („algorithmische Identität“) mit Daten wie Blutdruck, Schlafverhalten, Standortdaten wie GPS, wäre persönlich.</td><td rowspan="3">• Erstellung von persönlichem Gesundheitsprofil
• Identifizierung des Individuums auf Basis von Profildaten mit verknüpften Verhaltens- und Standortdaten
• Identifizierung der Interessen des Individuums aufgrund von Verhaltensdaten Ausspielung personalisierter Werbung
• Profildaten mit Verknüpfung zu Social Media
• Kaufprozessdaten
• Standortdaten aufgrund der Möglichkeit der Nachverfolgung
• Sind Daten nicht allgemein verfügbar oder ableitbar werden diese als persönlich empfunden.
• Daten (z. B. Kontaktdaten) von Dritten</td><td rowspan="2">Kategorie B: Persönliche Daten

Unterkategorie 2: Begriffsdefinition

2.2 Verletzung der Privatsphäre</td></tr>
<tr><td>„Und ob man da nicht eben sogar Profile erstellen kann von denjenigen Eigennutzern, weil du hast dich ja irgendwo registriert. Also können die wissen, ok der Person C (Anmerkung: Name anonymisiert), der geht täglich dort und dort zur Arbeit, der schläft da und da und ja, man weiß es aber nicht.“ (ProbandIn C, Z. 343-34)</td><td>Identifizierbarkeit des Individuums auf Basis von Registrierungsdaten mit verknüpften Informationen zu Alltagsgewohnheiten auf Basis von Standortdaten, Ruhezeiten etc.</td></tr>
<tr><td>„Das ist wieder sehr persönlich. Genauso, die wissen jetzt ok ich war jetzt vier Tage am Nova Rock, haben gesehen, ich habe so und so viele Schritte gemacht und haben sich gedacht, eben mit GPS-Wissen, dass ich dort war und wissen okay die interessiert sich für die Musik, die mag das und da spiele ich gekonnt wieder in die Richtung Werbung etc. an.“ (ProbandIn B, Z. 366-369)</td><td>Identifizierbarkeit der Interessen des Individuums aufgrund bestimmter Verhaltensweisen und entsprechende Ausspielung personalisierter Werbung.</td><td></td></tr>
</table>

[19] Die Tabelle zeigt die Reduktion des Datenmaterials auf Kategorien. Die Basis sind sind Zitate (Ankerbeispiele) der ProbandInnen um die subjektive Beschreibung der ProbandInnen zur Thematik darzustellen.

*„Ansonsten wirkliche persönliche Daten. Mit GPS finde ich ist es halt schwierig, weil es schon nett ist, wenn ich zum Beispiel jetzt nicht mein Armband verwende, aber ich kann das ja auch aufzeichnen, zum Beispiel mit der Runtastic App. Dann finde ich es natürlich toll wenn ich sehe wie sich mein Bewegungslauf verändert, wo war ich besonders gut, wann hatte ich irgendwie einen Müdigkeitseinbruch oder sowas und gleichzeitig denk ich mir natürlich, weiß das Ding auch wo ich überall unterwegs bin, also so toll find ich es nicht." (*ProbandIn E, Z. 476-482)	Standortdaten werden aufgrund der Möglichkeit der Nachverfolgung als persönlich empfunden		
*Ich find sensibel – trotzdem die Kaufprozessdaten, weil so wie wenn er (Anmerkung: zeigt auf D) mit seiner Apple Watch dann alles zahlt, sehen die dann ja wann kaufe ich was und eventuell sogar wie viel gebe ich aus. Das finde ich, das greift mir zum Beispiel zu stark in die Privatsphäre ein. Könnt ich zum Beispiel auch mit der Uhr, mach ich nicht, weil ich zahl klassisch mit meiner Bankomatkarte. Ich finde GPS ist total interessant für einem persönlich, dass ich sehe wo war ich, wie lang war ich, wie auch immer, aber ich finde diese Daten sollten nicht weitergegeben werden. Es sollte wirklich nur für mich einsehbar sein und sonst für niemand anderen. Also bei den zwei Sachen sag ich wirklich, ok das ist persönlich. (*ProbandIn B, Z. 501-508)	Kaufprozessdaten und Standortdaten sind persönliche Daten; sollten nicht an Dritte weitergegeben werden		
„Aber man muss schon sagen, mit GPS ist es ein bisschen heikel. Es gab schon mehrere Fälle. Frauen zum Beispiel beim Laufen, dass da Muster aufgezeichnet worden sind und denen aufgelauert wurden. Also viele Apps haben das mittlerweile geändert und haben die ersten 5 Kilometer oder 10 Kilometer nicht aufgezeichnet. Ich glaube die ersten, dass du nicht genau siehst ok von wo läuft die immer weg, weil dann kann man sagen, ok wo wohnt wer, wo endet wer." (ProbandIn C, Z. 527-531)	Standortdaten sind persönliche Daten wenn Konsequenz Rückschluss auf Wohnort		

„Profildaten ist für mich schon ein bisschen ein Thema. Gerade weil ich mich sehr clever mit meinem Facebook Konto angemeldet habe, weil ich mir dann irgendwie gedacht habe, na gut, das zeichnet jetzt eh schon alle Fitness-, Gesundheitsdaten von mir auf jetzt, ist es irgendwie auch schon wurscht. Also das ist für mich schon ein bisschen ein Thema und vor allem wenn diese Schnittstelle da ist und am Anfang immer das Thema natürlich auch ist mit: Postet das dann automatisch zum Beispiel auf mein Facebook Profil? Das wäre absolutes No-Go.“ (ProbandIn E, Z. 471-475)	Profildaten werden als persönliche Daten empfunden, verstärkt durch die Schnittstelle zu Social Media; Möglicher Eingriff in die Privatsphäre durch automatisches Facebook-Posting		
„Für mich ist vielleicht noch eine Unterscheidung auch sozusagen was sind persönliche Daten und was gebe ich in dem Kontext her und was kann man sonst von mir wissen. Also wenn man jetzt sagt, ich trage das Ding über Nacht, ja jetzt gehe ich vielleicht um 21 Uhr ins Bett und stehe um 07 Uhr in der Früh auf, dann gebe ich meine Uhr weg, damit dann nicht irgendwie Herzfrequenz verstärkt über Nacht getrackt wird, weil dann weiß man, wer ist noch bei den selben GPS-Daten. Also das geht irgendwie niemanden etwas an. G: Natürlich auf Deutsch gesagt in die Intimsphäre eingreifen.“ (ProbandIn H, G; Z. 680-686)	Datenfreigabe in bestimmten Kontext (z. B. Herzfrequenz, Uhrzeit) mit Verknüpfung zu allgemein verfügbaren Daten (z. B. Standortdaten)		
„Ja und ich glaube da fängt es für mich an. Mein Name ist für mich jetzt nicht so persönlich. Selbst die E-Mail-Adresse nicht, weil man die auf Webseiten [...]. Mein Alter kann man erschließen, das ist für mich auch ok. Meine Größe und mein Gewicht kann man auch erschließen und mit der Gesundheitsvorsorge beim normalen Arzt wird man auch meine Gesundheitsdaten in dem Rahmen haben, aber dann auch so richtig privates Verhalten, was ich sonst auch nicht teilen möchte – da fängt für mich die Privatheit an.“ (ProbandIn H, Z. 687-692)	Sind Daten nicht allgemein verfügbar oder ableitbar werden diese als persönlich empfunden.		

„Da sozusagen ist es mir heikler und privater als meine persönlichen Daten sind die Daten von anderen.“ (ProbandIn H, Z. 949-950)	Heikler und privater als persönliche Daten sind Daten von anderen. (z. B. Kontakte).		

Tabelle 7: Einstellungen von Wearable-NutzerInnen in Österreich zu „Persönlichen Daten“, eigene Darstellung.

Die vorliegenden Ergebnisse zeigen, dass die Beschreibung des Begriffs „Persönliche Daten“ subjektiv erfolgt und innerhalb der Fokusgruppe variiert. Es ist zu erkennen, dass Kaufprozessdaten für eine Vielzahl der ProbandInnen besonders schützenswert sind, für andere jedoch nicht.

Im Allgemeinen wird erkannt, dass Standortdaten (GPS) von den meisten ProbandInnen als persönlich wahrgenommen werden. In diesem Kontext wiegen NutzerInnen Vorteile des GPS-Trackings gegen mögliche Nachteile, z. B. der Nachverfolgung, ab (ProbandIn B, C, E 2019). Auf Basis der Definitionen in **Tabelle 7** ist zu erwähnen, dass die Aggregation unterschiedlicher Datensätze und die Profilbildung (abgeleitete Daten), wie beispielsweise das Schließen auf Interessen auf Basis von bestimmten Verhaltensdaten, als Eingriff in die Privatsphäre wahrgenommen werden.

Unterschiedliche Einstellungen der ProbandInnen hinsichtlich der Definition von persönlichen Daten und der Einstellung zur Privatheit aufgrund des Geschlechtes oder des Alters werden nicht festgestellt. Ein wesentlicher Faktor ist jedoch, dass die ProbandInnen erkennen, dass sie sich im Rahmen ihrer sportlichen Betätigung entsprechend ihres Alters „richtig verhalten“ und demnach weniger Hemmungen bei der Freigabe der persönlichen Gesundheitsdaten haben. Die ProbandInnen sind der Meinung, dass Personen die krankheitsbedingt mit Problemen oder mit Verletzungen konfrontiert sind weniger freigiebig mit den persönlichen Gesundheitsdaten sind. Im Folgenden beschreibt eine ProbandIn den möglichen Kontrollverlust nach der Datenfreigabe an Organisationen.

> „Ich bin jetzt in einer Situation wo ich das Gefühl habe […] was wollt ihr mir vorwerfen? Ich mache eh alles richtig, nur ist es halt nichts was ich selbst auch kontrollieren und steuern kann.“ (ProbandIn H 2019, Zeilen 575-577)

8.4.2 Datenanalyse und Profilbildung

Die Profilbildung auf Basis von Daten der NutzerInnen ist ein relevantes Thema für Wearable-NutzerInnen im Rahmen der durchgeführten Fokusgruppe. Die Einstellung der ProbandInnen bei der Ableitung von Interessen aufgrund bestimmter Verhaltensweisen kann mit folgendem Zitat deutlich gemacht werden:

> „Was mich stört dabei ist, wenn ein mir bekannter oder nicht bekannter Anbieter etwas über mich weiß, was ich selber nicht weiß. Das ist glaube ich das, was mich

> daran stört, dass ich da eigentlich keine Kontrolle darüber habe.“ (Probandin H 2019, 540-542).

Die Unkenntnis von automatisierten Entscheidungsfindungen, insbesondere die Profilbildung und der damit einhergehende Kontrollverlust der NutzerInnen werden als störend wahrgenommen. Zudem haben Wearable-NutzerInnen Interesse an den erstellten Profilen auf Basis ihrer persönlichen Daten, beispielsweise Informationen zu angenommenen Interessen. Hierbei wird der Wunsch nach Transparenz von Seiten der KonsumentInnen deutlich. Als mögliches Szenario beschrieben die ProbandInnen die Nutzung von Big Data und die Profilbildung, wodurch Wahrscheinlichkeiten im Verhalten, z. B. aufgrund von Sport, Ernährung, oder der Gesundheitsdaten im Allgemeinen, nach Alter und Wohnort berechnet werden und demnach Einstufungen verschiedener Gruppen vorgenommen werden können (ProbandIn E 2019, Zeilen 711-718).

8.4.3 Datenqualität

NutzerInnen sind der Meinung, dass Gesundheitsdaten, gemessen durch Wearables, inakkurat erscheinen. Messdifferenzen unterschiedlicher Wearables, die Einstellung des Armbandes und somit die Varianz in der Messgenauigkeit sowie eine undeutliche Differenzierung im Bewegungsverhalten (stehen und sitzen wird gleich gemessen) geben den Teilnehmenden zu bedenken. Es besteht die Annahme, dass qualitativ hochwertige Gesundheits- und Fitnessdaten durch regelmäßige Dateneingabe entstehen (ProbandIn C 2019, Zeilen 632-637). Eine weitere Meinung besteht darin, dass die exakte Datenmessung des Individuums, beispielsweise die Messung des Puls irrelevant ist, die Messung des Bewegungsverhaltens im Allgemeinen von Relevanz ist (ProbandIn H 2019, Zeilen 672-678).

Es wird die Frage aufgeworfen inwieweit inakkurate Daten für Datenhalter wertvoll sein können, denn persönliche Daten, die als wirtschaftliches Gut gehandelt werden, sollen richtig und in adäquater Qualität vorliegen. Laut ProbandIn H wäre dies durch die Beteiligung der KonsumentInnen möglich:

> „Wenn wir mitreden können, dann ist die Qualität der Daten besser, dann kann es auch tatsächlich eine wirtschaftliche Ressource werden.“ (Zeile 1236)

8.5 Datennutzung u. mögliche Konsequenzen für Individuen u. die Gesellschaft

Die Nutzung von persönlichen Daten durch Organisationen erfolgt in der letzten Stufe der Wertekette (siehe Kapitel 4.1.2 und 4.2). Im Folgenden werden die Einstellungen der ProbandInnen hinsichtlich der Datenverwertung durch ausgewählte Akteure beschrieben. Anschließend werden mögliche resultierende Konsequenzen für Individuen und die Gesellschaft aus der Sicht der ProbandInnen erläutert.

8.5.1 Datennutzung durch Organisationen

Die Datennutzung durch Akteure, über die Nutzung durch Wearable-Anbieter hinausgehend, und mögliche resultierende Konsequenzen für Individuen und die Gesellschaft werden im Folgenden erläutert. In der Gruppendiskussion setzte die Moderatorin nach einer allgemeinen Diskussion einen Stimulus mit der Auflistung von Organisationen bzw. Branchen mit potenziellem Interesse an persönlichen Daten im Rahmen der digitalen Selbstvermessung (siehe **Abbildung 5**), um detaillierte Ergebnisse zu erzielen.

Abbildung 5: Stimulus Material, Auszug an Institutionen und Branchen mit potenziellem Interesse an Self-Tracking Daten, eigene Darstellung.

In der Theorie wurde beschrieben, dass NutzerInnen hinsichtlich der Preisgabe von persönlichen Daten insbesondere auf den Informationsempfänger, die Informationsnutzung und die Informationssensitivität achten (vgl. Hartmann 2011, S. 192). Empirische Daten zeigen Unterschiede in der Einstellung zum Datenschutz aufgrund des Informationsempfängers. Beispielsweise erscheint die Freigabe von Konto- und

Finanzdaten an die Bank in Ordnung, während bei der Freigabe dieser Daten an Wearable-Anbieter Bedenken geäußert werden (ProbandIn B 2019, Zeilen 510-516).

Versicherungsunternehmen

Bei privaten Versicherungen wird in Österreich die Staffelung der Beitragsprämien nach Auskunft des Versicherten vorgenommen. Die Einstufung von Versicherten und die Bezahlung von entsprechenden Beitragsprämien aufgrund von gemessenen Gesundheitsdaten erscheinen für die ProbandInnen als mögliches Zukunftsszenario realistisch.

Arbeitgeber

Die Weitergabe an persönlichen Daten (insbesondere Gesundheits-, Standort- und Verhaltensdaten) an den Arbeitgeber ist nicht erwünscht, da mögliche Ableitungen anhand von Verhaltensweisen und demografischen Merkmalen durchgeführt werden könnten (ProbandIn E 2019, Zeilen 741-743). ProbandIn B ist jedoch der Meinung, dass die Nutzung von Wearables im Rahmen der organisationalen Gesundheitsvorsorge als Anreiz zur Motivation im Team in Ordnung ist, wenn der Arbeitgeber keinen Einblick in Datensatz bekommt (Zeilen 777-782).

Online-Werbung, Marktforschung und Online-Handel

Die Verwertung persönlicher Daten durch Organisationen in den Bereichen Online-Werbung, Markforschung und Online-Handel werden von den ProbandInnen zum Großteil als Gewohnheit beschrieben. Dabei wird geschlussfolgert, dass individuelle Nutzungsdaten weniger interessant für Marktakteure erscheinen, als das Gesamtnutzungsverhalten. Bei der Datenfreigabe an Social Media Unternehmen besteht Resignation, da man das Gefühl hat "sie wissen eh schon alles" (ProbandIn E 2019, Zeile 755).

Im Allgemeinen ist zu erwähnen, dass die Weitergabe von Gesundheitsdaten für Zwecke der Forschung von den ProbandInnen positiv wahrgenommen wurde.

8.5.2 Mögliche Konsequenzen für Individuen

Die Forschungsergebnisse ergeben eine Unterscheidung zwischen „realen und virtuellen Akteuren“. Die ProbandInnen unterscheiden zwischen der Datenverwertung durch reale

Organisationen bzw. Institutionen mit möglichen direkten Folgen wie beispielsweise der Arbeitgeber, Versicherungsunternehmen oder die staatliche Gesundheitsinstitution. Hierbei wird ein Kontrollverlust hinsichtlich der möglichen Konsequenzen befürchtet, wie beispielsweise die Kündigung des Arbeitgebers oder variable Versicherungsprämien aufgrund von automatisierten Entscheidungsfindungen.

Zum anderen werden virtuelle Organisationen, wie beispielsweise Unternehmen in den Bereichen Marketing und Werbung, Social Media und Online-Handel beschrieben. In diesen Beispielen bleibt, aus der Sicht der NutzerInnen, die individuelle Entscheidungsfindung der KonsumentInnen trotz Datenverwertung durch Organisationen bestehen. Darüber hinaus sind die Auswirkungen der Datenfreigabe in diesem Kontext in der Wahrnehmung der NutzerInnen unsichtbar.

In

Tabelle 8 werden unterschiedliche Meinungen zu möglichen Konsequenzen für Individuen aufgrund der Datenverwertung durch Organisationen aus der Perspektive der Wearable-NutzerInnen beschrieben und gegenübergestellt. Die Darstellungsweise der Tabelle soll das Meinungsspektrum der Individuen zu den einzelnen Anwendungsfällen verdeutlichen.

Anwendungsfälle	**Mögliche Konsequenzen für Individuen bei der Datenverwertung durch Organisationen**[20]	**Keine erwarteten Konsequenzen für Individuen bei der Datenverwertung durch Organisationen**
Werbetreibende	Ableitung von Interessen aufgrund bestimmter Verhaltensdaten, darauf basierend Ausspielung personalisierter Werbung (ProbandIn C, Z. 360-363)	Datenfreigabe an Unternehmen zur Ausspielung personalisierter Werbung ist nicht störend (ProbandIn D, Z. 435-437)
	Manipulation von NutzerInnen aufgrund des Kaufverhaltens (ProbandIn A, Z. 735-736)	
Dritte	Datenweitergabe an Dritte im Rahmen des Registrierungsprozesses nicht gewünscht (ProbandIn F, Z. 454-456)	Künftiges „Sign in with Apple“ wird positiv wahrgenommen (ProbandIn D, Z. 440-443)

[20] Meinungen der ProbandInnen werden abgebildet. Die Tabelle enthält Reduktionen auf Basis von Zitaten der ProbandInnen entsprechend der zusammenfassenden Inhaltsanalyse nach Mayring.

Versicherungs-unternehmen	Schwierigkeiten Gesundheitsversicherung zu bekommen aufgrund von allgemeinen Annahmen basierend auf Big Data (ProbandIn G, Z. 563-567)	
	Bemessung der Versicherungsbeiträge aufgrund gemessener Gesundheitsdaten (ProbandIn E, Z. 749; ProbandIn H, Z. 987)	
Arbeitgeber	Einblick des Arbeitgebers in Daten zu sensibel (Probandin B, Z. 791; ProbandIn A, Z. 795-798)	Wearable-Nutzung im Rahmen der Gesundheitsvorsorge in Unternehmen in Ordnung, aber Einblick des Arbeitgebers in Daten zu sensibel (ProbandIn B, Z. 777-782; Z. 791)
	Kündigung als mögliche Konsequenz im Rahmen von Predictive Analytics (ProbandIn E, Z. 743-745)	

Tabelle 8: Einstellungen der ProbandInnen hinsichtlich der Datenverwertung in unterschiedlichen Anwendungsfällen, eigene Darstellung.

Bei der Verwertung von persönlichen Daten im Rahmen des Self-Tracking durch werbetreibende Unternehmen erwarten NutzerInnen die Ableitung von Interessen aufgrund bestimmter Verhaltensdaten und darauf basierend die Ausspielung personalisierter Werbung. Für einige ProbandInnen wird dies nicht als störend empfunden. Zudem wird die mögliche Manipulation durch personalisierte Werbung aufgrund des Kaufverhaltens beschrieben. Zudem sind sich NutzerInnen darüber bewusst, dass gesammelte Daten für personalisierte Werbung oder andere Zwecke verwendet werden. In der Literatur werden außerdem Produktempfehlungen oder dynamische Preisanpassungen aufgrund von Daten beschrieben.

Des Weiteren kann die Datenweitergabe an Dritte erfolgen. Dies ist laut ProbandInnen insbesondere im Rahmen des Registrierungsprozesses nicht gewünscht. Dabei wird manchen Unternehmen mehr vertraut als anderen. Beispielsweise wird ein künftiger Login in Online-Services durch Apple positiv wahrgenommen, während dem „Sign in with Facebook“ weniger vertraut wird. Das Vertrauen in die Datenschutzpraktiken eines Unternehmens ist dabei von Relevanz.

Die Ergebnisse zeigen, dass mögliche Konsequenzen bei der Datenverwertung durch Versicherungsunternehmen relevant für NutzerInnen sind. Aus der Literaturrecherche geht nicht hervor, dass Versicherungsunternehmen im europäischen Raum Handlungen auf Basis von Daten der Selbstvermessungstechnologien durchführen. Es werden zwei mögliche Problemfelder aus NutzerInnenperspektive deutlich: Zum einen die Schwierigkeiten eine Gesundheitsversicherung zu bekommen und zum anderen die Bemessung der Versicherungsbeiträge aufgrund von automatisierten Entscheidungsfindungen.

Der Einblick des Arbeitgebers in persönliche Gesundheits-, Standort- und Verhaltensdaten wird als äußerst sensibel wahrgenommen. Für einige ProbandInnen ist die Wearable-Nutzung im Rahmen der Gesundheitsvorsorge im Unternehmen in Ordnung, solang keine Datenauswertung auf individueller Ebene stattfindet. Als mögliche Konsequenz für Individuen durch die Datenverwendung des Arbeitgebers wird die Kündigung von Mitarbeitenden aufgrund von automatisierten Entscheidungsfindungen befürchtet.

8.5.3 Mögliche Konsequenzen für die Gesellschaft

In der Debatte um gesellschaftliche Auswirkungen ist in erster Linie zu erwähnen, dass gemessene Gesundheitsdaten von Wearables nicht repräsentativ für die Gesundheitsdaten der österreichischen Gesellschaft sind (ProbandIn H 2019, Zeilen 1088-1092). ProbandInnen der Fokusgruppe sind sich einig, dass die Freigabe von persönlichen Daten gesellschaftlich und langfristig zu betrachten ist. Dabei ist die Langlebigkeit der Daten und die Auswertungsmöglichkeiten durch Anwendungen des maschinellen Lernens zu berücksichtigen (ProbandIn H 2019, Zeilen 401-403).

Teilnehmende sind der Meinung, dass die Profilbildung anhand von Verhaltensmustern für die Gesellschaft langfristig bedenklich erscheint (ProbandIn A 2019, Zeilen 555-557), denn auf Basis der Datensätze könnten Wahrscheinlichkeiten abgeleitet werden, die auf NutzerInnen mit bestimmten Verhaltensweisen anzuwenden sind (ProbandIn E 2019, Zeilen 711-718).

Die Debatte um die Einstufung von Versicherungsprämien auf Basis von Gesundheitsdaten kann als gesellschaftspolitisches Thema angesehen werden. Hierbei sind laut ProbandInnen gravierende Unterschiede zwischen dem amerikanischen und dem europäischen Modell

festzustellen. Ein/e ProbandIn unterstreicht den Einfluss auf die Gesellschaft folgendermaßen:

> „Ich glaube schon, dass das […] das gesellschaftliche Leben bestimmen kann wenn diese Daten so großräumig aufgezeichnet und verwendet werden, dass das einerseits die Gesellschaft spaltet oder du gewisse Vor- oder Nachteile hast.“ (ProbandIn A 2019, Zeilen 997-1000)

Zudem werden Mangel sowie Desinteresse an Aufklärung hinsichtlich des Datenschutzes und der entsprechenden Konsequenzen der Datenfreigabe auf gesellschaftlicher Ebene deutlich.

Abschließend sind soziale Aspekte zu erwähnen. Zum einen ist die Befürchtung der sozialen Exklusion festzustellen. Da das Thema der sozialen Selbstvermessung in der Gesellschaft angekommen scheint beobachten ProbandInnen, dass man dazu gehören möchte, da "jeder trackt" und zwar unterschiedliche Aspekte des Alltags wie beispielsweise den Schlaf oder die Bewegung (ProbandIn E 2019, Zeilen 932-934). Zum anderen ist eine Diskriminierung auf Basis von Gesundheitsdaten gesellschaftspolitisch bedenklich. Die Diskriminierung durch Wearables kann bestehen, da gesunde Menschen mithalten können und „dazu gehören“ während andere Menschen ausgeschlossen werden (ProbandIn H 2019, Zeilen 1092-1097).

8.6 Privatheitsverhalten und Datenschutzstrategien von Wearable-NutzerInnen

Mit Verweis auf das in Kapitel 5.1 beschriebene Privatsphäre-Prozess-Modell legen die ProbandInnen während der Gruppendiskussion subjektive Einstellungen sowie Vorteile und Risiken hinsichtlich des Forschungsthemas dar. Reflektierte bzw. beobachtete Verhaltensmuster im Rahmen der Privatsphäre und persönliche Datenschutzstrategien werden außerdem angeführt.

8.6.1 Privatheitsverhalten der Wearable-NutzerInnen

Die empirischen Ergebnisse zeigen, dass sich Wearable-NutzerInnen oftmals der Transparenz ihres Nutzungsverhaltens und der Datenweitergabe an Dritte bewusst sind und

zum Teil nicht mit der Datenfreigabe einverstanden sind, aber „trotzdem machen es alle“ (ProbandIn G 2019, Zeilen 936-938). Das hier erläuterte Verhalten der ProbandInnen entspricht dem in Kapitel 5.2. beschriebenem Privacy-Paradoxon.

Die empirischen Ergebnisse zeigen, dass NutzerInnen Kosten und Nutzen der Datenfreigabe gegeneinander abwiegen. Dieses Verhalten wurde im Rahmen des Kosten-Nutzen-Modells in Kapitel 5.3.1 beschrieben. Eine Meinung ist, dass die Vorteile der Datenfreigabe zur Nutzung des Service die Nachteile überwiegen (ProbandIn D 2019, Zeile 1226-1227). Diese Einstellung kann im Rahmen der digitalen Selbstvermessung dadurch begründet werden, dass der Wunsch möglichst viel über das Selbst zu wissen, anders nicht möglich wäre und daher mögliche Konsequenzen in Kauf genommen werden (ProbandIn E 2019, Zeilen 930-931). Zum anderen erscheint die Bequemlichkeit (engl. convenience) der Nutzung wichtiger als der Datenschutz:

> „Ich habe das Gefühl, ich bin ein relativ aufgeklärter Mensch was Technologie mit mir macht, welche Daten von mir abgelesen werden und bin da sehr reflektiert und gleichzeitig merke ich, dass „convenience“ für mich viel wichtiger ist, was eigentlich ernüchternd ist“ (ProbandIn E 2019, Zeilen 569-572).

Wie in Kapitel 5.2 erwähnt, zeigt eine 2017 in Österreich durchgeführte Befragung von Integral ebenfalls, dass ÖsterreicherInnen im Kontext von Wearables im Bereich Fitness und Gesundheit Bedenken hinsichtlich des Datenschutzes äußern, jedoch aufgrund des Komforts nicht auf die Nutzung der Geräte verzichten möchten (vgl. Integral 2017, o. S.).

Eine weitere Einstellung ist, dass kurzfristige Interessen („etwas Interessantes sehen“) langfristige Einstellungen überwiegen (ProbandIn H 2019, Zeilen 603-604). In der Verhaltensökonomie wird dieses Phänomen unter dem Begriff „Hyperbolic Discounting“ beschrieben: Eine sofortige Belohnung wird wertvoller wahrgenommen als eine zukünftige nur weil diese früher eintrifft (Siehe Kapitel 5.3.3). Als wesentlicher Grund für dieses Verhalten wird die Abstraktion der möglichen Konsequenzen aufgrund der Datenverwertung beschrieben. Es besteht oftmals kein Bewusstsein über die Datennutzung von Akteuren während der Wearable-Nutzung im Alltag. Als eine mögliche Ursache für das geringe Bewusstsein auf NutzerInnenebene ist die Informationsasymmetrie zugunsten der Datenhalter anzuführen. Zudem zeigt die

Simulationsheuristik, ein Aspekt der Verhaltensökonomie, dass Individuen dazu neigen Ereignisse die sich mental schwer vorstellen lassen als unwahrscheinlich abzuwerten.

Ein weiteres Verhalten, das vor allem im Kontext von Social Media beschrieben wurde, ist der subjektive Zwang zur Datenfreigabe, da man ansonsten soziale Exklusion erwartet. „Ich mag es eigentlich nicht, tue es aber doch." (ProbandIn H 2019, Zeilen 394-395) Definierte Umstände (z. B. Voreinstellungen des Systems) erfordern bestimmte Handlungsweisen von Individuen auch wenn diese damit nicht einverstanden sind, da sie ansonsten auf die Nutzung des Services verzichten müssten.

Außerdem zeigen die Ergebnisse Resignation beim Lesen von unverständlichen Datenschutzerklärungen und möglichen Konsequenzen. Wearable-NutzerInnen gehen davon aus, dass eine entsprechende Transparenz durch den Anbieter nicht gleichermaßen eine Verhaltensänderung auf NutzerInnenebene bewirkt, da weder Motivation noch Zeit aufgebracht wird (ProbandIn A 2019, Zeilen 877-878). Moll et al. (2017) werfen diese These ebenfalls auf (S. 31). Die ProbandInnen sind sich einig, dass eine transparente, lesbare und vor allem eine verständliche Aufbereitung der datenschutzrelevanten Inhalte wichtig ist und eine Verhaltensänderung auf NutzerInnenebene zu einem reflektierten Datenschutz beitragen kann.

Anreize zur Datenfreigabe

Abschließend werden Anreize beschrieben, die Wearable-NutzerInnen dazu motivieren persönliche Daten zu messen und an Organisationen weiterzugeben. Alle ProbandInnen bestätigen, dass intrinsische Belohnungen durch das Wearable (wie in Kapitel 8.3.1 beschrieben) zur freiwilligen Nutzung und damit zur Datenfreigabe führen. Monetäre Anreize, wie z. B Rabatte für einen weiteren Kauf eines Wearables beim gleichen Anbieter, erscheinen lediglich für die Vertriebsstrategie relevant.

8.6.2 Datenschutzstrategien von Wearable-NutzerInnen

Um informationelle Selbstbestimmung auf NutzerInnenebene zu ermöglichen bedarf es der Möglichkeit zum Datenschutz. Regulation durch Gesetze wie die EU-DSGVO erscheinen relevant um persönliche Rechte wie Auskunftspflicht oder die Richtigstellung der Daten, durchzusetzen (ProbandIn H 2019, Zeilen 1230-1231). Darüber hinaus müssen sich NutzerInnen selbstständig über Risiken und Rechte informieren und sich

Datenschutzstrategien aneignen, die ihren persönlichen Einstellungen entsprechen. Die Verwendung unterschiedlicher E-Mail-Adressen je nach Nutzungssituation um die digitale Identität von der realen Identität zu trennen wird beschrieben (ProbandIn H 2019, Zeilen 380-382). Die Identifizierung der Identität aufgrund unterschiedlicher E-Mail-Adressen erscheint aufwendig, sei aber machbar (ebd.). Falsche Angaben zur Person sind eine weitere Datenschutzstrategie. Es ist zu erwähnen, dass lediglich ein/e ProbandIn mit der Anwendung von Datenschutzstrategien vertraut ist. Es wird demnach davon ausgegangen, dass ein hohes Maß an Kompetenz der NutzerInnen im Rahmen des Datenschutzes vorausgesetzt wird, obwohl diese oftmals nicht vorhanden ist.

8.7 Handlungsempfehlungen für Anbieter und Unternehmen

Die Ergebnisse der empirischen Forschung zeigen Einstellungen von KonsumentInnen hinsichtlich der Privatheit bei der Wearable-Nutzung. Dabei können Handlungsempfehlungen auf Basis von Wünschen und Erwartungen der NutzerInnen ermittelt werden. Da kundenorientierte Geschäftsmodelle persönliche Daten nutzen um Services zu optimieren und Wert für KundInnen zu schaffen nehmen NutzerInnen im Rahmen der interaktiven Wertschöpfung einen besonderen Stellenwert ein. Die Handlungsempfehlungen richten sich an Organisationen mit datengetriebenen Geschäftsmodellen im Bereich der Fitness- und Gesundheitsökonomie.

8.7.1 Vertrauen als Wettbewerbsvorteil

Die Studienergebnisse bestätigen, dass NutzerInnen Vertrauen in Anbieter bzw. datennutzende Organisationen hinsichtlich des Datenschutzes aufbauen. Dieses Verhalten kann auf eingeschränkte kognitive Fähigkeiten von Individuen zurückgeführt werden, die es nicht ermöglichen alle verfügbaren Informationen zu verarbeiten um rationale Entscheidungen hinsichtlich der möglichen Folgen zu treffen. Daher werden entsprechende Hinweise und Anleitungen gesucht (siehe Kapitel 5.3) um den Entscheidungsprozess zu vereinfachen, wie beispielsweise das Vertrauen in ausgewählte Organisationen.

Die Transparenz der Datenverwertung von Unternehmen trägt maßgeblich zum Vertrauen von NutzerInnen bei (ProbandIn D 2019, Zeilen 438-440). Außerdem schafft die Verschlüsselung der Daten Vertrauen bei KonsumentInnen. Es ist zu erwähnen, dass

Individuen unterschiedliche Vertrauensgrade für Unternehmen haben (ProbandIn H 2019, Zeilen 763-764). Dabei kann die aktiv kommunizierte Erfüllung von Datenschutzvorkehrungen zum Wettbewerbsvorteil werden. Vergangene Aktivitäten im Rahmen des Datenschutzes tragen maßgeblich zur Reputation des Anbieters bei (ProbandIn F 2019, Zeilen 454-462).

Darüber hinaus kann Vertrauen auf Resignation basieren, da „das Unternehmen ohnehin schon alle Daten hat“ (ProbandIn D 2019, Zeilen 450-452). Allerdings gibt es laut ProbandInnen keine Garantie für Datenschutz auf Anbieterseite: "Ich muss darauf als Konsument vertrauen, aber wir wissen es eigentlich nicht“ (Probandin A 2019, Zeile 724).

8.7.2 Transparenz im Umgang mit persönlichen Daten

NutzerInnen fordern mehr Transparenz von Seiten der Datenhalter im Umgang mit persönlichen Daten. Der Wunsch nach Information und nach Aufklärung hinsichtlich der Online-Privatsphäre und möglichen Konsequenzen für das Individuum und für die Gesellschaft werden deutlich, „weil ich mich in diesem Ganzen digitalen Chaos eigentlich nicht auskenne“ (ProbandIn 2019, Zeilen 1246-1249). Wie bereits in Kapitel 8.6.1 erwähnt ist eine entsprechend verständliche Aufbereitung der Information von Vorteil.

Zudem zeigen die ProbandInnen besonderes Interesse an den Ergebnissen der Profilbildung. Im Rahmen des Forschungskontextes werden vor allem Gesundheitsprofile beschrieben, die durch den Anbieter auf Basis der Aggregation und Analyse unterschiedlicher Datensätze entstehen (ProbandIn C 2019, Zeilen 866-868).

Die angeführten Transparenzdefizite gilt es für Organisationen mit datengetriebenen Geschäftsmodellen im Bereich der Fitness- und Gesundheitsökonomie zu schließen.

8.7.3 Integration der NutzerInnen und Richtigkeit der Daten

Eine verstärkte Integration der NutzerInnen in die Wertschöpfungsprozesse der Organisationen ist ein Anliegen der ProbandInnen (bereits in Kapitel 8.4.2 Datenqualität ersichtlich). Von Seiten der ProbandInnen besteht bei der Verwertung von persönlichen

Daten durch Organisationen in erster Linie der Wunsch nach Kontrolle und entsprechenden Handlungsmöglichkeiten[21].

Darüber hinaus erleben Wearable-NutzerInnen ein ungerechtes Machtverhältnis zu datennutzenden Organisationen wenn kostenfreie Arbeitsleistung (Generierung und Freigabe von Information) zur Wertschöpfung beiträgt und keine entsprechende Gegenleistung erfolgt. Folgendes Zitat unterstreicht diese Einstellung:

> „Aber man kriegt nichts dafür […]. Daten sind heutzutage Gold. Jede zweite App, die zum Beispiel deinen Standort verwendet, verkauft die Daten auch weiter“ (ProbandIn F 2019, Zeilen 849-851).

Zusammenfassend fordern die ProbandInnen eine Integration der KonsumentInnen durch individuelle Kontroll- und Handlungsmöglichkeiten sowie durch eine Beteiligung an den Erlösen bei der sekundären Datenverwendung.

Richtigkeit der Daten

Die Gewährleistung der Richtigkeit der abgeleiteten Daten ist eine weitere Handlungsempfehlung, die sich aus dem Datenmaterial ableiten lässt. ProbandInnen sind der Meinung, dass die Gewährleistung der Korrektheit der abgeleiteten Daten (z. B. Interessen) notwendig ist. Ist diese Voraussetzung gegeben wird auch personalisierte Onlinewerbung akzeptiert (ProbandIn H 2019, Zeilen 869-872). Darüber hinaus ist die selbstbestimmte Möglichkeit zur Anpassung oder tatsächlichen Löschung der persönlichen Daten ein Anliegen der Wearable-NutzerInnen, wodurch wiederum die Forderung nach Integration der KonsumentInnen deutlich wird.

8.8 Zusammenfassung der empirischen Untersuchung

In der durchgeführten Fokusgruppe diskutierten Wearable-NutzerInnen aus Österreich im Alter von 18 bis 49 Jahren privatheitsrelevante Fragestellungen. Neben der Homogenität in der Nutzung kann eine Heterogenität in der Gruppenzusammensetzung festgestellt werden, die sich sowohl auf das soziodemografische Profil der ProbandInnen (Kapitel 7.2.2; 8.1.1) als auch auf die genutzten Modelle und Marken der Wearables bezieht (Kapitel 8.1.2).

[21] Kontrolle und Handlungsmöglichkeiten im Rahmen des rechtlich Vorgeschriebenen.

Dadurch können unterschiedliche Nutzungssituationen und damit einhergehend ein breites Meinungsspektrum erfasst werden. Im Rahmen der explorativen Forschung wird die Abbildung einer breiten Zielgruppe möglich.

Die empirischen Ergebnisse zeigen, dass prinzipiell Interesse am Schutz der informationellen Privatheit besteht. Die Datenfreigabe im Alltag wird jedoch aufgrund der Abstraktion der Thematik und der Intransparenz möglicher Konsequenzen nicht bewusst wahrgenommen. Zudem können Einstellungen wie Resignation und Gleichgültigkeit der Datennutzung durch Organisationen (insbesondere Unternehmen), sowie die wahrgenommene Handlungsunfähigkeit der Individuen hinsichtlich des Datenschutzes festgestellt werden.

Die subjektive Definition des Begriffs „Persönliche Daten“ aus NutzerInnenperspektive erfolgt anhand von möglichen Verletzungen der Privatsphäre bzw. nach der Relevanz persönlicher Daten für Organisationen. Demenentsprechend zeigen die Befunde, dass sich die ProbandInnen über die Relevanz persönlicher Daten für Organisationen bewusst sind. Dabei wird zwischen möglichen individuellen und gesellschaftlichen Konsequenzen bei der Sammlung und Verwertung von Daten durch Organisationen unterschieden. Bei der Diskussion um mögliche Konsequenzen für Individuen wird eine Unterscheidung zwischen realen und virtuellen Akteuren deutlich, da laut ProbandInnen bei der Datenverwertung durch reale Akteure (Arbeitgeber, Versicherungen etc.) ein Kontrollverlust zu verspüren ist.

Darüber hinaus werden rationale Kosten-Nutzen-Entscheidungen, wie beispielsweise die Präferenz der Bequemlichkeit, von den ProbandInnen reflektiert. Im Rahmen der digitalen Selbstvermessung kann die Anwendung des Kosten-Nutzen-Modells dadurch begründet werden, dass der Wunsch möglichst viel über „das Selbst“ zu erfahren, durch Self-Tracking möglich ist und daher mögliche Konsequenzen der Datenwertung durch Organisationen in Kauf genommen werden. Zudem werden Aspekte der begrenzten Rationalität und die entsprechende Anwendung von Heuristiken, wie das Vertrauen in bestimmte Organisationen, erfasst. Systematische psychologische Verzerrungen, wie die Präferenz von kurzfristigen Vorteilen gegenüber langfristigen Einstellungen, werden auf Basis der Alltagserfahrungen der ProbandInnen beschrieben.

Die empirische Untersuchung zeigt abschließend folgende Handlungsempfehlungen für Organisationen in der Fitness- und Gesundheitsökonomie:

- Stärkung des Konsumentenvertrauens hinsichtlich des Datenschutzes,
- Transparenz im Umgang mit persönlichen Daten (sowohl die tatsächliche Einhaltung der gesetzlichen Auflagen der EU-DSGVO als auch darüber hinausgehende Informations- und Aufklärungsarbeit),
- Verstärkte Integration der NutzerInnen durch Kontroll- und Handlungsmöglichkeiten und deren Beteiligung an Erlösen der sekundären Datenverwendung,
- sowie die Gewährleistung der Richtigkeit der Daten im Rahmen der Profilbildung.

9 Schlussbetrachtung

Diese Masterarbeit hat das Ziel, die Wertschöpfung im Rahmen der digitalen Selbstvermessung näher zu beleuchten und Befunde zur Einstellung von Wearable-NutzerInnen in Österreich im Umgang mit persönlichen Daten im Gesundheits- und Fitnesskontext zu erheben. Um dieses Ziel zu erreichen wurde im ersten Schritt der aktuelle Wissensstand der bestehenden Literatur dargelegt. In weiterer Folge wurden, aufgrund der Methode der Fokusgruppe subjektive Einstellungen von Wearable-NutzerInnen in Österreich im Hinblick auf ihre Privatsphäre erhoben und mit der Hilfe der Inhaltsanalyse nach Mayring ausgewertet. Im folgenden Kapitel werden nun sämtliche Erkenntnisse zusammengefasst und interpretiert.

9.1 Zusammenfassung und Interpretation der Ergebnisse

Die Zusammenfassung und die Interpretation der theoretischen und empirischen Befunde werden zur Übersichtlichkeit in Teilabschnitte gegliedert.

Digitale Selbstvermessung

Die starke Bedeutung „des Selbst“ lässt sich im Rahmen der digitalen Selbstvermessung feststellen. Zu erkennen sind das Beobachten, das Verorten und das eigenständige Handeln auf Basis von selbstgemessenen Daten (vgl. Wolff 2016, S. 32). Wie in Kapitel 3 erläutert,

erfolgt im digitalen Zeitalter die Selbstvermessung, vor allem im Gesundheits- und Fitnessbereich, vermehrt durch Wearables, d. h. Smartwatches mit Fitnesstrackern oder Fitnessarmbänder mit der dazugehörigen App.

Empirische Ergebnisse zeigen, dass Wearables direkt auf dem Körper getragen und durch die tägliche Nutzung in den Lebensalltag der NutzerInnen integriert werden. Zudem werden unterschiedliche Verhaltensmuster in der Wearable-Nutzung im Gesundheits- und Fitnesskontext erfasst, wobei die Aufzeichnung der Aktivität innerhalb des Tagesablaufes einen der Hauptnutzungsgründe darstellt. Die gezielte Messung der sportlichen Aktivität stellt für einige NutzerInnen einen Zusatznutzen dar. Eine maßgebliche Unterscheidung im Nutzungsverhalten ist in der Vernetzung sowie bei der Verwendung von Smartphone-Funktionalitäten zu erkennen. Die Ergebnisse der Auswertung zeigen zudem, dass spieltypische Mechaniken und Elemente als intrinsischer Motivator zur Nutzung von Wearables wahrgenommen werden und in weiterer Folge zu mehr Bewegung bzw. zu einer bewussteren Ernährung führen. ProbandInnen merken jedoch an, dass Wearables zwar motivierend wirken aber nicht die Grundlage für einen gesunden Lebensstil darstellen. Hierbei ist zu erwähnen, dass die Nutzung des Services per se und die intrinsische Motivation durch Gamification-Aspekte als Anreiz dient, um persönliche Daten, u. a. Gesundheitsdaten, preiszugeben. Monetäre Anreize wie Rabatte erscheinen lediglich für die Vertriebsstrategie des physischen Produktes relevant.

Datengetriebene Wertschöpfung im Rahmen der digitalen Selbstvermessung

Kapitel 4 zeigt, dass die Zunahme an produzierten Daten, deren Generierung, Speicherung und Auswertung Chancen bietet neuartige Geschäftsmodelle und Wertschöpfungsstrukturen zu gestalten, um die gesammelten Daten zu verwerten und daraus Nutzen für Organisationen zu ziehen sowie Wert auf NutzerInnenebene zu schaffen. Es bleibt zu erwähnen, dass persönliche Daten per se noch keinen Wert haben, sondern erst durch den wertschöpfenden Prozess neue Informationen entstehen, die für Stakeholder von Interesse sein können (vgl. BVDW 2018, S. 23; Dewenter 2018, S. 17). Um diese Potentiale auszuschöpfen benötigen Unternehmen Zugriff auf die Datensätze. Rechtliche Bestimmungen hinsichtlich der Einwilligung der NutzerInnen können hierbei Hindernisse darstellen.

Güter fungieren im Rahmen der Service-Logik als Distributionskanal und stellen damit die Grundlage für die Werterstellung zwischen NutzerIn und Anbieter dar (vgl. Brodie et al. 2011, S. 78). ProbandInnen der Fokusgruppe bestätigen die tägliche Nutzung von Wearables, wodurch laut eigenen Angaben die Datenbasis und somit die Funktion des Services verbessert wird. Die Angabe von falschen Daten führt zu einem negativen Nutzungserlebnis. Datenschutzstrategien, wie die Angabe falscher Daten, sind in diesem Kontext daher nicht anwendbar. Das Wearable als Gut kann als physisches Produkt beschrieben werden, das in Interkation mit dem/der NutzerIn um datenbasierte Mehrwerte angereichert wird. Wert im Rahmen der Service-Logik entsteht jedoch erst bei der Integration der vom Gerät stammenden Information in den Entscheidungsprozess des Individuums (vgl. Joiner/Lusch 2016, S. 30). Vor diesem Hintergrund können KonsumentInnen als relevanter Bestandteile des Leistungserstellungsprozesses im Rahmen der interaktiven Wertschöpfung von Dienstleistungen betrachtet werden. Daher erscheint es notwendig, die Herausforderungen für den Schutz der informationellen Privatheit auf NutzerInnenebene zu erforschen.

Informationelle Privatheit auf NutzerInnenebene

Um informationelle Selbstbestimmung auf NutzerInnenebene zu ermöglichen, bedarf es der Möglichkeit zum Datenschutz. Dies ist durch europäische Rechtsgrundsätze, wie der Charta der Grundrechte der Europäischen Union bzw. durch den umfassenden Rechtsrahmen der EU-DGSVO, geregelt. Darüber hinaus ist es notwendig, dass KonsumentInnen selbst Entscheidungen treffen, ohne durch die Vorgaben von Anbietern, beispielsweise durch Voreinstellungen, beeinflusst zu werden (vgl. Acquisti 2015, S. 192). Dies erfordert ein hohes Maß an Kompetenz auf NutzerInnenebene. Es liegt daher an den KonsumentInnen, sich eigenständig über Risiken und Rechte zu informieren und sich Datenschutzstrategien anzueignen (vgl. Masur et al. 2018, S. 18). Unter den ProbandInnen beschreibt lediglich eine Person die Anwendung von Datenschutzstrategien.

Wie ausführlich in Kapitel 9.2 dargestellt, zeigen empirische Befunde dieser Arbeit, dass der Schutz der informationellen Privatheit für die ProbandInnen relevant ist, aber dass die Datenpreisgabe im Alltag abstrakt erscheint. Zudem beeinflussen Resignation, Gleichgültigkeit und die wahrgenommene Handlungsunfähigkeit der Individuen hinsichtlich des Datenschutzes das Privatheitsverhalten. Ein scheinbar paradoxes Verhalten wird in diesem Kontext deutlich. Außerdem wird erkannt, dass die subjektive Definition

des Begriffs „Persönliche Daten“ durch NutzerInnen zwischen den Individuen, trotz der Homogenität in der Nutzung von Wearables, variiert. Smith et al. (2011) betrachten die Privatsphäre des Individuums ebenfalls als subjektive Wahrnehmung und nicht als absoluten moralischen Wert, bzw. eine absolute moralische Norm (S. 933f). Zudem lässt sich eine situationsabhängige Beurteilung der ProbandInnen im Hinblick auf Gesundheitsdaten erkennen, da die Schutzwürdigkeit der Daten nach dem Gesundheitszustand des Individuums variiert.

Bei der Beschreibung des Begriffs „Persönliche Daten“ werden vor allem mögliche Verletzungen der Privatsphäre angeführt, zusätzlich wird auf die Relevanz der persönlicher Daten für Organisationen verwiesen. Studienergebnisse belegen demnach, dass sich die NutzerInnen über die Relevanz persönlicher Daten für Organisationen und der Verwertung dieser bewusst sind. Mögliche Konsequenzen aus der Perspektive der NutzerInnen werden auf individueller und gesellschaftlicher Ebene anhand der Forschungsfrage 2 beantwortet.

Handlungsempfehlungen für Organisationen der Gesundheits- und Fitnessökonomie

Es lassen sich folgende Handlungsempfehlungen für Anbieter und Organisationen im Rahmen der Gesundheits- und Fitnessökonomie aus den Forschungsergebnissen ableiten.

Zunächst wird das Vertrauen in Organisationen hinsichtlich des Datenschutzes als Wettbewerbsvorteil wahrgenommen. Theoretische und empirische Befunde belegen, dass sich Wearable-NutzerInnen bei der privatheitsrelevanten Entscheidungsfindung oftmals auf Heuristiken, wie bisherige Erfahrungen mit einem Unternehmen bzw. dessen Reputation hinsichtlich des Datenschutzes, verlassen. Unterschiedliche Vertrauensgrade für Unternehmen werden deutlich.

Empirische Ergebnisse zeigen, dass sich die Transparenz im Umgang mit persönlichen Daten positiv auf das Kundenvertrauen auswirkt. Das Bedürfnis der ProbandInnen nach verständlich aufbereiteter Information hinsichtlich des Zwecks der Datenverarbeitung, der Empfänger (z. B. Dritte), die Information über das Bestehen einer automatisierten Entscheidungsfindung, insbesondere der Profilbildung sowie die Korrektheit der angegebenen Daten werden hierbei deutlich. Diese Aspekte entsprechen den gesetzlichen Regelungen der EU-DSGVO in Art. 5, Art. 12 und Art. 13. (vgl. Datenschutz-Grundverordnung 2018a; 2018b; 2018c). Darüber hinaus sind abgeleitete Daten, sowie die Korrektheit dieser im Rahmen der Profilbildung auf Basis der angegebenen und

beobachteten Nutzerdaten von Interesse. Auf individueller und gesellschaftlicher Ebene besteht der Wunsch nach Aufklärung hinsichtlich der möglichen Konsequenzen der Datenverwendung durch Organisationen.

„Persönliche Daten“ werden in diesem Forschungskontext als wirtschaftliches Gut betrachtet (OECD 2013; Spiekermann-Hoff/Korunovska 2017; Masur et al. 2018). Die ProbandInnen gehen davon aus, dass von Wearables gesammelte Gesundheitsdaten inakkurat erscheinen (ungenaue Messung, Messdifferenzen zwischen Anbietern etc.). Diese werfen die Frage auf, inwieweit inakkurate Daten für Datenhalter wertvoll sein können, da persönliche Daten, die als wirtschaftliches Gut gehandelt werden, richtig und in adäquater Qualität vorliegen sollten. Aus diesem Grund verweisen die ProbandInnen auf die Notwendigkeit der Beteiligung der KonsumentInnen bei der Verbesserung der Datenqualität, damit tatsächlich von einer wirtschaftlichen Ressource gesprochen werden kann. Das Bedürfnis zur selbstständigen Kontrolle der Daten wird hierbei deutlich. Voraussetzung dafür ist das Bewusstsein der KonsumentInnen über die Relevanz persönlicher Daten für Organisationen und die Verwertung dieser. Die empirischen Ergebnisse zeigen, dass sich die ProbandInnen dessen bewusst sind.

Nach der Zusammenfassung der erhobenen Ergebnisse und deren Interpretation wird im nächsten Kapitel auf die zu Beginn gestellten Forschungsfragen eingegangen.

9.2 Beantwortung der Forschungsfragen

In diesem Kapitel werden die in Kapitel 1.2 aufgestellte Leitfrage sowie die beiden Sub-Forschungsfragen zusammenfassend beantwortet. Zur Übersicht werden diese nochmals dargestellt und es wird der Reihe nach darauf Bezug genommen.

Leitfrage: Welche Einstellungen haben NutzerInnen von Wearables im Gesundheits- und Fitnesskontext in Österreich hinsichtlich ihrer Privatsphäre?

Aufgrund der Zunahme der Datenvielfalt durch technologische Entwicklungen, beispielsweise vernetzte Geräte im Bereich des CIoT, ergeben sich neue Möglichkeiten und gleichzeitig Herausforderungen für den Schutz der informationellen Privatheit des Individuums.

Die ProbandInnen (NutzerInnen von Wearables in Österreich) sind prinzipiell am Datenschutz interessiert. Die Datenfreigabe wird jedoch aufgrund der Abstraktion der Thematik und der Intransparenz möglicher Konsequenzen im Alltag nicht bewusst wahrgenommen. Empirische Befunde zeigen, dass Resignation und Gleichgültigkeit hinsichtlich der Datenverwertung durch Organisationen, insbesondere in den Bereichen Online-Werbung, Social Media und Online-Handel, die Entscheidungsfindung der NutzerInnen beeinflussen. Hierbei ist zu erwähnen, dass privatheitsrelevante Einstellungen der Wearable-NutzerInnen subjektiv erfolgen und zwischen den Individuen variieren. Während bestimmte Datenarten, wie beispielsweise Kaufprozessdaten, für einige NutzerInnen schützenswert sind, empfinden andere Gleichgültigkeit in der Datenfreigabe.

Wearable-NutzerInnen äußern gerade im Gesundheits- und Fitnesskontext den Wunsch nach Transparenz der Datenverwendung, insbesondere bei der Profilbildung und der automatisierten Entscheidungsfindung. Hierbei erscheint die Richtigkeit der angegebenen und abgeleiteten Daten von Relevanz. Neben der Transparenz der gespeicherten Daten und der Datenverwendung durch Organisationen ist das Bedürfnis der NutzerInnen nach verständlich aufbereiteter Information, im Gegensatz zu umfassenden Datenschutzinformationen in juristischer Sprache, zu erkennen. Dieser Aspekt ist im Rahmen der EU-DSGVO gesetzlich geregelt. Darüber hinaus wünschen sich die ProbandInnen Aufklärung zu möglichen Konsequenzen auf individueller und gesellschaftlicher Ebene. Diese gehen jedoch davon aus, dass Transparenz und Aufklärung nicht gleichermaßen eine Verhaltensänderung auf NutzerInnenebene bewirkt, da weder Motivation noch Zeit aufgebracht werden. Die NutzerInnen sind sich jedoch einig, dass eine transparente, lesbare und vor allem eine verständliche Aufbereitung der datenschutzrelevanten Inhalte wichtig ist, um reflektierter mit der Thematik Datenschutz umzugehen und die Verhaltensanpassung auf NutzerInnenebene zu fördern.

Auch wenn sich NutzerInnen informiert und aufgeklärt fühlen werden systematische psychologische Verzerrungen (z. B. Hyperbolic Discouting), angewandte Heuristiken (das Vertrauen in Unternehmen) oder die Anwendung des Kosten-Nutzen-Modells deutlich.

Darüber hinaus wird eine wahrgenommene Handlungsunfähigkeit der Individuen hinsichtlich des Datenschutzes festgestellt, auch wenn sich diese prinzipiell für den Schutz der persönlichen Daten interessieren. Vor dem Hintergrund des ungleichen Machtverhältnisses zwischen Organisationen und KonsumentInnen stellt sich die Frage, ob

Letztere überhaupt etwas tun können, um die Bewegung im Sinne der KonsumentInnen zu gestalten. Aufgrund der zunehmenden Verschiebung der Wertschöpfungsprozesse von der Produktion hin zum Service, und der Ausstattung physischer Produkte mit nachgelagerten, digitalen Dienstleistungen, erscheint die Integration der KonsumentInnen in den interaktiven Wertschöpfungsprozess von Relevanz. Empirische Befunde zeigen, dass NutzerInnen von Wearables im Gesundheits- und Fitnesskontext in Österreich besonders auf Unternehmen vertrauen, die sensibel auf den Datenschutz reagieren. Zudem wünschen sich NutzerInnen eine stärkere Integration durch individuelle Kontroll- und Handlungsmöglichkeiten im Hinblick auf den Schutz und die Richtigkeit ihrer persönlichen Daten sowie eine Beteiligung an den Erlösen bei der sekundären Datenverwendung. Es ist anzunehmen, dass Organisationen von der verstärkten Integration der NutzerInnen und der entsprechenden Verbesserung der Datenqualität profitieren.

Forschungsfrage 1: Wie definieren NutzerInnen von Wearables in Österreich „Persönliche Daten“ im Gesundheits- und Fitnesskontext?

In der Privatheitsforschung zeigen Studien, dass Individuen die Sensibilität ihrer persönlichen Daten in bestimmten Kontexten unterschiedlich bewerten (vgl. Kokolakis 2017, S. 13; Masur et al. 2018). Empirische Befunde dieser Arbeit befassen sich mit einem Kontext, der Wearable-Nutzung im Gesundheits- und Fitnesskontext, und zeigen, dass die Definition des Begriffs „Persönlichen Daten“ subjektiv erfolgt und innerhalb der Diskussionsgruppe (Wearable-NutzerInnen in Österreich) variiert. Kaufprozessdaten sind für eine Vielzahl der ProbandInnen besonders schützenswert, für andere jedoch nicht. Im Allgemeinen wird erkannt, dass Standortdaten (GPS) von den meisten ProbandInnen als persönlich wahrgenommen werden. Hierbei wiegen NutzerInnen Vorteile des GPS-Trackings gegen mögliche Nachteile, wie der Nachverfolgung, ab. Es wird das Kosten-Nutzen-Modell zur menschlichen Entscheidungsfindungen angewandt.

Neben unterschiedlichen Meinungen zu bestimmten Datenarten zeigen die empirischen Ergebnisse, dass die Definition des Begriffs „Persönliche Daten“ im Forschungskontext anhand der **Beschreibung von möglichen Verletzungen der Privatheit** oder nach der **Relevanz persönlicher Daten für Organisationen** erfolgt. Folgende Aspekte werden von den ProbandInnen als „mögliche Verletzung der Privatheit“ wahrgenommen: Die Erstellung von persönlichen Gesundheitsprofilen von Anbietern, die Identifizierung des Individuums auf Basis von Profildaten mit verknüpften Verhaltens- und Standortdaten, die

Identifizierung der Interessen des Individuums aufgrund von Verhaltensdaten und entsprechender Ausspielung personalisierter Werbung, die Weitergabe von Profildaten durch die Verknüpfung zu sozialen Medien, die Weitergabe von Kaufprozessdaten an Anbieter bzw. an Dritte, die Aufzeichnung von Standortdaten mit der möglichen Konsequenz der Nachverfolgung. Außerdem werden Daten die nicht allgemein verfügbar oder ableitbar sind, sowie Daten von anderen (z. B. Kontaktdaten) als besonders heikel beschrieben. Laut Spiekermann/Korunovska (2017) ist das Bewusstsein über Märkte persönlicher Daten der wichtigste Treiber für die monetäre Bewertung von persönlichen Daten (S. 21). Ähnliche Ergebnisse zeigt die Empirie dieser Arbeit. Um den Begriff „Persönliche Daten“ zu beschreiben, wird auf die Relevanz persönlicher Daten für Organisationen verwiesen. Demnach ist durch weitergehende Forschung zu prüfen ob Daten als persönlich wahrgenommen werden, wenn diese für andere Parteien Nutzen stiften.

Theoretische und empirische Ergebnisse dieser Arbeit bestätigen außerdem die Wahrnehmung eines Kontrollverlustes aufgrund der Datenpreisgabe. Im Forschungskontext lässt sich eine situationsbezogene Bewertung der Individuen feststellen: Einerseits erscheint die Datenfreigabe in Ordnung, wenn positive Gesundheitsdaten gemessen werden. Sobald in der Wahrnehmung der NutzerInnen eine Verschlechterung der Daten aufgrund von Krankheiten auftritt, wird die Datenweitergabe negativ bewertet und die Daten werden als schützenswert empfunden. Die situationsabhängige Beurteilung der ProbandInnen kann im Vergleich zur Einordnung von Gesundheitsdaten im Rahmen der EU-DSGVO als sensible Daten, die als besonders schützenswert gelten, betrachtet werden.

Forschungsfrage 2: Wie bewerten NutzerInnen von Wearables in Österreich mögliche Konsequenzen durch die Datenfreigabe an Organisationen im Gesundheits- und Fitnesskontext?

Empirische Befunde dieser Arbeit zeigen, dass sich die ProbandInnen über die Relevanz persönlicher Daten für Organisationen bewusst sind. Dabei wird zwischen möglichen individuellen und gesellschaftlichen Konsequenzen bei der Sammlung und Verwertung von Daten durch Organisationen unterschieden.

Theoretische und empirische Befunde zeigen, dass NutzerInnen hinsichtlich der Preisgabe von persönlichen Daten auf den Informationsempfänger achten.

Im Allgemeinen wird bei der Diskussion um mögliche Konsequenzen für Individuen eine Unterscheidung zwischen „realen und virtuellen Akteuren“ deutlich, da laut ProbandInnen bei der Datenverwertung durch sogenannte „reale Akteure“ (Arbeitgeber, Versicherungsunternehmen etc.) ein Kontrollverlust befürchtet wird. Als mögliche Konsequenz auf individueller und gesellschaftlicher Ebene erscheinen die Profilbildung anhand von angegebenen und beobachteten Daten und die entsprechende Ableitung von Wahrscheinlichkeiten auf Basis dieser Datensätze bedenklich. Hierbei ist anzumerken, dass im europäischen Raum, im Gegensatz zum amerikanischen Raum, keine theoretischen Erkenntnisse darüber vorliegen, dass entsprechende Akteure Gesundheitsdaten sammeln und Entscheidungen auf Basis dieser Daten treffen. Ein mögliches Szenario erscheint laut ProbandInnen gerade bei Versicherungsunternehmen realistisch, wobei auf gesellschaftlicher Ebene gravierende Unterschiede zwischen dem europäischen und dem amerikanischen Modell erkannt werden. Bei „virtuellen Organisationen“, z. B. Unternehmen im Online-Handel, im Marketing und der Werbung, im speziellen Social Media, bleibt laut NutzerInnen die individuelle Entscheidungsfindung trotz Datenverwertung durch Organisationen bei den KonsumentInnen. Außerdem sind die Auswirkungen der Datenfreigabe für NutzerInnen in diesem Kontext unsichtbar. Die Weitergabe von Gesundheitsdaten für Zwecke der Forschung wird von den ProbandInnen positiv wahrgenommen.

Die Datenverwertung durch Dritte ist laut ProbandInnen insbesondere im Rahmen des Registrierungsprozesses nicht gewünscht. Dabei sind unterschiedliche Vertrauensgrade für Unternehmen erkennbar. Die Stärkung des Konsumentenvertrauens hinsichtlich des Datenschutzes erscheint daher von Relevanz für Unternehmen und Anbieter.

9.3 Limitationen und Forschungsempfehlungen

Es ist anzumerken, dass die Ergebnisse des Forschungsansatzes Einschränkungen unterliegen, die bei der weiteren Forschung berücksichtigt werden sollten. Im ersten Schritt werden Limitationen in Bezug auf die Gütekriterien qualitativer Forschung angeführt. In der empirischen Sozialwissenschaft erscheinen insbesondere zwei Gütekriterien von

Relevanz: Zum einen die Reliabilität d. h. die Zuverlässigkeit, Stabilität und Genauigkeit der Messung (vgl. Schulz 2012, S. 18). Dabei lassen sich Zuverlässigkeitsprüfungen der quantitativen Forschungen nicht für die qualitative Sozialforschung übernehmen. Gründe dafür sind die mangelnde Standardisierung der interpretativen Datenauswertung und die schwer kontrollierbare Messung (vgl. ebd.). Eine Reproduzierbarkeit des Datenmaterials erscheint daher nicht möglich, wird aber auch nicht angestrebt (vgl. Lamnek 1995a 158ff nach Schulz 2012, S. 18).

Zum anderen ist die Validität, d. h. die Gültigkeit und Belastbarkeit der formulierten Annahmen, anwendbar für die qualitative Sozialforschung, da diese im Allgemeinen gültigere Ergebnisse als die quantitative Forschung produziert (vgl. ebd.). Die Möglichkeit des Nachfragens reduziert dabei Missverständnisse. Die vorliegende Studie bezieht sich auf die regelmäßige Nutzung von Wearables, d. h. Fitnessarmbänder und Smartwatches mit der Nutzung von Fitnesstrackern. Es kann davon ausgegangen werden, dass Datenschutzrisiken von Nicht-NutzerInnen oder jenen Personen, die Wearables nicht mehr verwenden als relevanter erachtet werden als von d ausgewählten ProbandInnen.

Da grundlegende Einstellungen von Wearable-NutzerInnen im Gesundheits- und Fitnesskontext in Österreich hinsichtlich ihrer Privatsphäre erforscht wurden, obliegt es der weiteren Forschung einzelne Aspekte quantitativ zu untersuchen, um generalisierende Ergebnisse zur Thematik zu generieren. Diese Masterarbeit befasst sich mit der NutzerInnenperspektive. Setzt man den Fokus auf Ergebnisteilbereiche, die Implikationen auf Organisationen haben, dienen folgende Hypothesen als Ausgangspunkt für weitere Forschungen.

Die empirischen Ergebnisse dieser Arbeit zeigen, dass die subjektive Definition des Begriffs „Persönliche Daten“ vor allem anhand der Beschreibung von möglichen Verletzungen der Privatsphäre (siehe **Tabelle 7**) oder nach der Relevanz persönlicher Daten für Organisationen erfolgt. Ausgehend von dieser Erkenntnis lässt sich nachfolgende Hypothese aufstellen, die zur Prüfung in zwei Teilhypothesen aufgegliedert wird.

Hypothese 1: Daten sind für NutzerInnen persönlich, wenn Kenntnis über den Einfluss datennutzender Organisationen besteht.

Hypothese 1a: Daten sind für NutzerInnen persönlich, wenn die Datennutzung durch Organisationen die eigene Privatsphäre verletzt.

Hypothese 1b: Daten sind für NutzerInnen persönlich, wenn Kenntnis darüber besteht, dass persönliche Daten für Organisationen Nutzen stiften.

Ein weiteres Ergebnis der empirischen Forschung ist das Vertrauen in Organisationen bei der privatheitsrelevanten Entscheidungsfindung von NutzerInnen. Diese verlassen sich oftmals auf Heuristiken, wie bisherige Erfahrungen mit einem Unternehmen bzw. dessen Reputation hinsichtlich des Datenschutzes, um dem Problem der begrenzten Rationalität entgegenzuwirken. Diese Erkenntnis führt zu folgender Hypothese:

Hypothese 2: Das Kundenvertrauen in Organisationen hinsichtlich des Datenschutzes beeinflusst die Preisgabe persönlicher Daten von NutzerInnen.

Abschließend ist anzumerken, dass die Perspektive von Wearable-Anbietern und datennutzenden Organisationen im Gesundheits- und Fitnesskontext bislang unterforscht ist. Dabei ist empirisch zu untersuchen, welchen Stellenwert KonsumentInnen für Organisationen im Rahmen der interaktiven Wertschöpfung einnehmen und inwieweit die Generierung und Verwertung von persönlichen Daten in den Wertschöpfungsprozessen der Organisationen stattfindet.

Literaturverzeichnis

Acquisti, A. (2014). The Economics and Behavioral Economics of Privacy. In Lane, J., Stodden, V., Bender, S., Nissenbaum, H. (Hrsg.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement.* Cambridge: Cambridge University Press. 76-95. DOI: 10.1017/CBO9781107590205.005.

Acquisti, A., Brandimarte, L., Loewenstein, G. (2015). Privacy and human behavior in the age of information. *American Association for the Advancement of Science*. Science Vol. 347, Nr. 6221, S. 509-514. DOI: 10.1126/science.aaa1465.

Acquisti, A., Grossklags, J. (2005a). Privacy and Rationality in Decision Making. *IEEE Security and Privacy*, 3(1), 24-30. DOI: 10.1109/MSP.2005.22.

Acquisti, A. and Grossklags, J. (2005b). *Uncertainty, Ambiguity, and Privacy, Proceedings of Workshop on the Economics of Information Security* (WEIS ‘05).

Acquisti, A., Grossklags, J. (2007*).* What can behavioral economics teach us about privacy? In: *Digital Privacy: Theory, Technologies and Practices,* Auerbach Publications (Taylor and Francis Group), Abington.

Albrecht, U.-V. (2016). Kapitel Kurzfassung. In: Albrecht, U.-V. (Hrsg.), *Chancen und Risiken von Gesundheits-Apps (CHARISMHA).* Medizinische Hochschule Hannover. 14–47.

Altmeppen K-D., Karmasin M. (2003). Medien und Ökonomie - Intentionen und Überblick. In: Altmeppen K-D., Karmasin M. (Hrsg.) *Medien und Ökonomie*. VS Verlag für Sozialwissenschaften. 7-17. DOI: 10.1007/978-3-322-80394-8_1.

Apple (2019). *Corporate Wellness.* https://www.apple.com/watch/corporate-wellness/. Zugegriffen: 14.06.2019.

Apple (k. D). *ResearchKit*. https://www.apple.com/de/researchkit/. Zugegriffen: 03.06.2019.

Berger-Grabner, D. (2016). *Wissenschaftliches Arbeiten in den Wirtschafts- und Sozialwissenschaften: Hilfreiche Tipps und praktische Beispiele*. 3., aktualisierte und erw. Aufl. Wiesbaden: Springer Gabler.

Brodie, R. J., Saren, M., Pels, J. (2011). Theorizing about the service dominant logic: The bridging role of middle range theory. *Marketing Theory*, 11(1), 75–91. DOI: 10.1177/1470593110393714.

Bruhn, M., Hadwich, K. (2015). *Interaktive Wertschöpfung durch Dienstleistungen. Strategische Ausrichtung von Kundeninteraktionen, Geschäftsmodellen und sozialen Netzwerken.* In: Springer Fachmedien Wiesbaden 2015.

BVDW (2018). *Datenwertschöpfung und Qualität von Daten.* https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/data_economy/BVDW_Datenwertschoepfung_2018.pdf. Zugegriffen: 16.06.2019.

Camerer, C., Loewenstein, G. (2004). Behavioral Economics: Past, Present, Future. In Camerer, C., Loewenstein, G., Rabin M. (Hrsg.). *Advances in Behavioral Economics.* Princeton, NJ: Princeton University Press. 3-51.

Cheney-Lippold, J. (2011). A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control. *Theory, Culture & Society*, *28*(6), 164–181. DOI: 10.1177/0263276411424420.

Christl, W. (2014*). Kommerzielle digitale Überwachung im Alltag. Cracked Labs im Auftrag der Bundesarbeitskammer.* https://www.arbeiterkammer.at/infopool/wien/Digitale_Ueberwachung_im_Alltag.pdf Zugegriffen: 16.05.2019.

Constantiou, I. D., Lehrer, C., Hess, T. (2014). Changing Information Retrieval Behaviours: An Empirical Investigation of Users' Cognitive Processes in the Choice of Location-based Services. *European Journal of Information Systems*, 23(5), 513-528. DOI: 10.1057/ejis.2014.12.

Curry, E. (2016). The Big Data Value Chain: Definitions, Concepts, and Theoretical Approaches. In Cavanillas, J. M., Curry, E., Wahlster, W. (Hrsg.). *New Horizons for a Data-Driven Economy: A Roadmap for Usage and Exploitation of Big Data in Europe.* Springer Berlin / Heidelberg, 29-37. DOI: 10.1007/978-3-319-21569-3_3.

Datenschutz-Grundverordnung (2018a). *Art. 5 – EU-DSGVO – Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten*. https://www.datenschutz-grundverordnung.eu/grundverordnung/art-5-ds-gvo/. Zugegriffen: 04.06.2019.

Datenschutz-Grundverordnung (2018b). *Art.12 – EU-DSGVO – Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person.* https://www.datenschutz-grundverordnung.eu/grundverordnung/art-12-ds-gvo/. Zugegriffen: 28.07.2019.

Datenschutz-Grundverordnung (2018c). *Art.13 – EU-DSGVO – Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person* https://www.datenschutz-grundverordnung.eu/grundverordnung/art-13-ds-gvo/. Zugegriffen: 28.07.2019.

Datenschutz-Grundverordnung (2018d). *Art. 4 – EU-DSGVO – Begriffsbestimmungen*. https://www.datenschutz-grundverordnung.eu/grundverordnung/art-4-ds-gvo/. Zugegriffen: 10.08.2019.

Delisle, M., Jülicher, T. (2016). *Step Into » The Circle « – Wearables und Selbstvermessung im Fokus.* ABIDA-Dossier. http://www.abida.de/sites/default/files/09%20Wearables.pdf. Zugegriffen: 05.05.2019.

Deterding, S., Khaled, R., Nacke, L.E., Dixon, D. 2011. Gamification: Toward a Definition. In: *CHI 2011 Gamification Workshop Proceedings*, Vancouver, BC, Canada.

Dewenter, R. (2018). *Gutachten: Datenhandel und Plattformen*. ABIDA. http://www.abida.de/sites/default/files/ABIDA_Gutachten_Datenplatformen_und_Datenhandel.pdf Zugegriffen: 05.06.2019.

Dienlin, T. (2014). The privacy process model. In: Garnett S., Halft S., Herz M., Mönig J.-M. (Hrsg.), *Medien und Privatheit*. Passau, Germany: Stutz. 105-122.

Dinev, T. (2014). Why would we care about privacy? *European Journal of Information Systems,* 23(2), 97–102. DOI: 10.1057/ejis.2014.1.

Dorfer L. (2018). Empirische Exploration der Erfolgsstrategien datenzentrischer Geschäftsmodelle. In: Dorfer L. (Hrsg.), *Erfolgsstrategien datenzentrischer Geschäftsmodelle*. *Medienmanagement und E-Business.* Springer Gabler, Wiesbaden.

DSGVO-Gesetz (2018a). *Erwägungsgrund 6. Gewährleistung eines hohen Datenschutzniveaus trotz Zunahme des Datenaustausches.* https://dsgvo-gesetz.de/erwaegungsgruende/nr-6/. Zugegriffen: 04.06.2016.

DSGVO-Gesetz (2018b). *Erwägungsgrund 5. Zusammenarbeit der Mitgliedsstaaten zum Datenaustausch.* https://dsgvo-gesetz.de/erwaegungsgruende/nr-5/. Zugegriffen: 04.06.2019.

DSGVO-Gesetz (2018c). *Erwägungsgrund 1. Datenschutz als Grundrecht.* https://dsgvo-gesetz.de/erwaegungsgruende/nr-1/. Zugegriffen: 04.06.2019.

DSGVO-Gesetz (2018d). *Erwägungsgrund 35. Gesundheitsdaten.* https://dsgvo-gesetz.de/erwaegungsgruende/nr-35/. Zugegriffen: 04.06.2019.

DSGVO-Gesetz (2018e). *Erwägungsgrund 26. Keine Anwendung auf anonymisierte Daten.* https://dsgvo-gesetz.de/erwaegungsgruende/nr-26/. Zugegriffen: 04.06.2019.

Fitbit (2019). *Fitbit Health Solutions*. https://healthsolutions.fitbit.com/employers/. Zugegriffen: 14.06.2019.

GFK (2016). *Jeder vierte deutsche Internetnutzer setzt auf Gesundheits-Apps oder Fitness Tracker.* https://www.gfk.com/de/insights/press-release/jeder-vierte-deutsche-internetnutzer-setzt-auf-gesundheits-apps-oder-fitness-tracker/. Zugegriffen: 08.06.2019.

Gigerenzer, G., Schlegel-Matthies, K., Wagner, G. G. (2016). *Digitale Welt und Gesundheit: eHealth und mHealth - Chancen und Risiken der Digitalisierung im Gesundheitsbereich*. Berlin: Bundesministerium der Justiz und für Verbraucherschutz.

Gimpel, H., Nüske, N., Rückel, T., Urbach, N., von Entress-Fürsteneck, M. (2019). *Self-Tracking and Gamification : Analyzing the Interplay of Motivations, Usage and Motivation Fulfillment*. 14th International Conference on Wirtschaftsinformatik (WI), Siegen, Deutschland, 1130-1144.

Goes, P. (2013). Information systems research and behavioral economics. Editor's comments. *MIS Quarterly*, 37(3), 3-8.

Gürtler, O., Höffler, F. (2015). Monitoring of workers and product market competition: The role of works councils. *Economic Inquiry,* 53(2), 1366–1379. DOI: 10.1111/ecin.12182.

Hartmann, M. (2011). Mobile Privacy: Contexts. In: Trepte S., Reinecke L. (Hrsg.), *Privacy Online*. Springer, Berlin, Heidelberg, DOI 10.1007/978-3-642-21521-6_14.

Hartmann, P., Zaki, M., Feldmann, N., Neely, A. (2014). *Big Data for Big Business? A Taxonomy of Data-Driven Business Models Used by Start-Up Firms*. Cambridge Service Alliance.

Heyen, Nils B. (2016): *Digitale Selbstvermessung und Quantified Self. Potenziale, Risiken und Handlungsoptionen*. Karlsruhe: Fraunhofer ISI.

Hugl, U. (2013). *Qualitative Inhaltsanalyse und Mind-Mapping.* Wiesbaden: Springer Gabler.

Integral, AIM – Austrian Internet Monitor (2017). *Nutzerpotenzial Wearables 2017 Q3.* https://www.integral.co.at/downloads/Pressetext/2017/11/Pressetext_AIM-C_Q3_2017.pdf. Zugegriffen: 20.05.2019.

Integral (2018). *Einstellung zum Datenschutz in Österreich 2018.* http://www.marktmeinungmensch.at/studien/einstellung-zum-datenschutz-in-oesterreich-2018/. Zugegriffen: 20.05.2019.

Joiner, K. A., Lusch, R. F. (2016*).* Evolving to a new service-dominant logic for health care. *Innovation and Entrepreneurship in Health*, 3, 25–33. DOI: 10.2147/IEH.S93473.

Jusline (2019). *EU-DSGVO. Artikel 6 Rechtmäßigkeit der Verarbeitung.* https://www.jusline.at/gesetz/dsgvo/paragraf/6. Zugegriffen am 22.06.2019.

Jusline (2019a). *EU-DSGVO. Artikel 6 Rechtmäßigkeit der Verarbeitung.* https://www.jusline.at/gesetz/dsgvo/paragraf/6. Zugegriffen: 08.06.2019.

Jusline (2019b). *EU-DSGVO. Artikel 9 Verarbeitung besonderer Kategorien personenbezogener Daten.* https://www.jusline.at/gesetz/dsgvo/paragraf/9. Zugegriffen: 22.06.2019.

Kiefer, M. L.; Steininger, C. (2014). *Medienökonomik: Einführung in eine ökonomische Theorie der Medien.* 3. Auflage, Oldenbourg Verlag: München.

Kitzinger, J. (1995). *Qualitative research: Introducing focus groups.* British Medical Journal, 311, 299-302. DOI:10.1136/bmj.311.7000.299.

Knöppler, K., Neisecke, T., Nölke, L. (2016). Digital-Health-Anwendungen für Bürger. Kontext, Typologie und Relevanz aus Public-Health-Perspektive. Entwicklung und Erprobung eines Klassifikationsverfahrens. *Bertelsmann Stiftung*, 1–92

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

Kraus-Füreder, H. (2018): *Gesundheits-Apps. Grundlagenpapier unter besonderer Berücksichtigung des Aspekts Gesundheitskompetenz.* Graz: Institut für Gesundheitsförderung und Prävention.

Kühn, T., Koschel, K. (2011). *Gruppendiskussionen. Ein Praxis-Handbuch*. VS Verlag für Sozialwissenschaften, Springer Fachmedien Wiesbaden.

Lister C., West J. H., Cannon B., Sax T., Brodegard D. (2014). Just a Fad? Gamification in Health and Fitness Apps. *JMIR Serious Games 2014*; 2(2):e9. DOI: 10.2196/games.3413.

Litschka, M., Pellegrini, T. (2019**).** Considerations on the Governance of Open Data – an Institutional Economic Perspective. *International Journal of Intellectual Property Management.*

Lucht, M., Boeker. M, Donath J, Güttler J, Leinfelder D, Kramer U. *Gesundheits- und Versorgungs-Apps. Hintergründe zu deren Entwicklung und Einsatz. Universitätsklinikum Freiburg und sanawork Gesundheitskommunikation*, Freiburg. https://www.uniklinik-freiburg.de/fileadmin/mediapool/09_zentren/studienzentrum/pdf/Studien/150331_TK-Gesamtbericht_Gesundheits-und_Versorgungs-Apps.pdf. Zugriff am 20.05.2019.

Lupton, D. (2014). Self-Tracking Modes: Reflexive Self-Monitoring and Data Practices. *SSRN Electronic Journal*. DOI: 10.2139/ssrn.2483549

Mäder, S. (2013). Die Gruppendiskussion als Evaluationsmethode – Entwicklungsgeschichte, Potenziale und Formen. *Zeitschrift für Evaluation,* 12(1), 23–51.

Mani, Z., Chouk, I. (2017). Drivers of consumers' resistance to smart products. *Journal of Marketing Management*, 33(1–2), 76–97. DOI: 10.1080/0267257X.2016.1245212.

Masur, P. K., Teutsch, D., Dienlin, T. (2018). Privatheit in der Online-Kommunikation. In: Schweiger, W., Beck, K. (Hrsg.), *Handbuch Online-Kommunikation*. Wiesbaden, Germany: Springer.

Mayring P., Fenzl T. (2019). Qualitative Inhaltsanalyse. In: Baur N., Blasius J. (Hrsg.), *Handbuch Methoden der empirischen Sozialforschung.* Springer VS, Wiesbaden.

MindTake, & MMA. (2016). *Nutzung von Wearables in Österreich im Jahr 2016*. In Statista - Das Statistik-Portal. https://ezproxy.fhstp.ac.at:2081/statistik/daten/studie/454523/umfrage/nutzung-von-wearables-in-oesterreich/. Zugegriffen am: 05.06.2019.

Moll, R., Schulze, A., Rusch-Rodosthenous, M., Kunke, C., Scheibel, L. (2017). Wearables, Fitness-Apps und der Datenschutz: Alles unter Kontrolle?. *Verbraucherzentrale NRW* e.V. (Hrsg.). http://www.marktwaechter.de/digitale-welt/marktbeobachtung/wearables-und-fitness-apps. Zugegriffen am: 01.05.2019.

Morlok, T., Matt, C., Hess, T. (2017). Privatheitsforschung in den Wirtschaftswissenschaften: Entwicklung, Stand und Perspektiven. In: Hess, T. (Hrsg.), *Arbeitsbericht des Instituts für Wirtschaftsinformatik und Neue Medien (Nr. 1/17),* München, LMU.

Ng, I., Wakenshaw, S. (2018). Service Ecosystems: A timely worldview for a connected, digital and data-driven economy. In: Lusch, R., Vargo, S., (Hrsg.), *Handbook of Service Dominant Logic*, Sage, 195–213.

Novotny, A., Spiekermann, S., (2015). Personenbezogene Daten privatwirtschaftlich nachhaltig nutzen. Regulatorische und technische Zukunftskonzepte. *Datenschutz und Datensicherheit*, 39 (7). 460-465.

O'Donoghue, T., Rabin, M. *(*2000*). The economics of immediate Gratification. Journal of Behavioral Decision Making,* Nr. 13: *233–250.*

OECD (2013). Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value. *OECD Digital Economy Papers*, Nr. 220, OECD Publishing, Paris. DOI: 10.1787/5k486qtxldmq-en.

Pellegrini, T. (2019). *Data Driven Business*. Vortrag an der Fachhochschule St. Pölten im Rahmen des FoP-NET - Future of Production Network, Zukunftsakademie Mostviertel am 13.03.2019.

Porter, M. E. (1989). *Wettbewerbsvorteile: Spitzenleistungen erreichen und behaupten*, Frankfurt am Main/New York: Campus.

Quanitfiedself Deutschland, 2019. *Über Quantified Self Deutschland.* http://qsdeutschland.de/info/. Zugegriffen: 08.06.2019.

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*, 15(1). DOI: 10.5210/fm.v15i1.2775.

Rössler, B. (2001). *Der Wert des Privaten.* Frankfurt a. M.: Suhrkamp.

Reichert, R. (2016). Social Surveillance: Praktiken der digitalen Selbstvermessung in mobilen Anwendungskulturen. In: Duttweiler, S., Gugutzer, R., Passoth, J-H., Strübing, J. (Hrsg.), *Leben nach Zahlen: Self-Tracking als Optimierungsprojekt?* Bielefeld: Transcript Verlag, 185–200.

Schallmo, D. (2018). Technologische Trends. In: Schallmo, D., Reinhart, J., Kuntz, E. (Hrsg*.), Digitale Transformation von Geschäftsmodellen erfolgreich gestalten. Springer Fachmedien Wiesbaden*, Gabler Verlag, 1-24.

Schallmo, D., Rusnjak, A. (2017). Roadmap zur Digitalen Transformation von Geschäftsmodellen. In: Schallmo, D., Rusnjak, A. (Hrsg.), *Digitale Transformation von Geschäftsmodellen. Schwerpunkt: Business Model Innovation*, Springer Fachmedien Wiesbaden, Gabler Verlag, 2-28.

Schweitzer, H., Peitz, M. (2017). Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf*?. ZEW Discussion Paper* Nr. 17-043, Mannheim.

Sicari, S., Rizzardi, A., Grieco, L. A., Coen-Porisini, A. (2015). Security, privacy and trust in Internet of things: The road ahead. *Computer Networks*, 76, 146–164. DOI: 10.1016/j.comnet.2014.11.008.

Smith H. J., Dinev, T., Xu, H. (2011). Information Privacy Research: An Interdisciplinary *Review. MIS Quarterly*, 35(4), 989-1015. DOI: 10.2307/41409970.

SPECTRA Marktforschungsgesellschaft. (2016a). Verwenden bzw. tragen Sie selbst einen Aktivitäts-Tracker bzw. Fitness-Armband?. In *Statista - Das Statistik-Portal.* https://ezproxy.fhstp.ac.at:2081/statistik/daten/studie/625221/umfrage/umfrage-in-oesterreich-zur-verwendung-von-fitness-trackern-nach-geschlecht/. Zugegriffen am: 05.06.2019

SPECTRA Marktforschungsgesellschaft. (2016b). *Verwenden bzw. tragen Sie selbst einen Aktivitäts-Tracker bzw. Fitness-Armband?.* In Statista - Das Statistik-Portal. https://ezproxy.fhstp.ac.at:2081/statistik/daten/studie/625272/umfrage/umfrage-in-oesterreich-zur-verwendung-von-fitness-trackern-nach-schulbildung/. Zugegriffen am: 05.06.2019.

SPECTRA Marktforschungsgesellschaft. (2018). Welche der folgenden Geräte nutzen Sie persönlich, und zwar privat oder beruflich?. In: *Statista. – Das Statistik Portal* https://ezproxy.fhstp.ac.at:2081/statistik/daten/studie/585466/umfrage/umfrage-zur-nutzung-von-internetfaehigen-endgeraeten-in-oesterreich-nach-alter/. Zugegriffen am: 05.06.2019.

Spiekermann, S., Korunovska, J. (2017). Towards a Value Theory for Personal Data. *Journal of Information Technology*, Vol. 32, Issue 1, 62-84.

Splendid Research (2016). *Studie: Quantified Wealth Monitor 2016.* https://www.splendid-research.com/de/quantified-wealth.html. Zugegriffen: 08.06.2019.

Statista (2019a). *Marktverzeichnis Wearables Weltweit, Nutzerpenetration,* 2019. https://de.statista.com/outlook/319/100/wearables/weltweit#market-arpu. Zugegriffen am: 16.05.2019.

Statista (2019b). *Marktverzeichnis Wearables Österreich*, 2019. Abrufbar unter: https://de.statista.com/outlook/319/128/wearables/oesterreich#market-revenue. Zugegriffen am: 16.05.2019.

Studies, I. J. H., Lee, H., Park, H., Kim, J. (2013). Why do people share their context information on Social Network Services ? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *Journal of Human Computer Studies,* 71(9), 862–877. DOI: 10.1016/j.ijhcs.2013.01.005.

Trepte, S., Reinecke, L. (2011). *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web.* Springer-Verlag Berlin Heidelberg, DOI 10.1007/978-3-642-21521-6.

Vargo, S. L., Lusch, R. F. (2008). Service-dominant logic: Continuing the evolution. *Journal of the Academy of Marketing Science,* 36(1), 1–10. DOI: 10.1007/s11747-007-0069-6.

Vargo, S. L., Wieland, H., Akaka, M. A. (2015). Institutions in innovation: A service ecosystems perspective. *Industrial Marketing Management*, 44(1), 63–7.

We Are Social, Hootsuite. (2016). Welche (Telekommunikations-)Endgeräte nutzen Sie derzeit? *In Statista - Das Statistik-Portal.* https://ezproxy.fhstp.ac.at:2081/statistik/daten/studie/430641/umfrage/umfrage-in-oesterreich-zu-genutzten-endgeraeten/. Zugegriffen am: 05.06.2019.

Weiber R., Ferreira K., (2015). Von der Value Co-Creation zur Co-Creation of Value. In: Bruhn M., Hadwich K. (Hrsg.). *Interaktive Wertschöpfung durch Dienstleistungen.* Springer Fachmedien Wiesbaden. DOI 10.1007/978-3-658-08518-6_2.

WHO –World Health Organization (2011*). mHealth. New horizons for health through mobile technologies.* Abrufbar unter: http://www.who.int/goe/publications/goe_mhealth_web.pdf . Zugegriffen: 04.07.2019.

Wieneke, A., Lehrer, C., Zeder, R., Jung, R. (2016). Privacy-related Decision-making in the Context of Wearable Use. In *Proceedings of the 20th Pacific Asia Conference on Information Systems (PACIS 2016)*. Chiayi, Taiwan.

Wirtz, B. W. (2018). *Business Model Management*, 4. Auflage, Springer Fachmedien Wiesbaden.

Wolf G. (2011). *What is The Quantified Self?* https://quantifiedself.com/blog/what-is-the-quantified-self/. Zugegriffen: 08.06.2019.

Wolff, E. (2018). Das "Quantified Self" als historischer Prozess. Die Blutdruck-Selbstmessung seit dem frühen 20. Jahrhundert zwischen Fremdführung und Selbstverortung. *Medizin, Gesellschaft und Geschichte 36.*

Xu, H., Luo, X., Carroll, J. M., Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, 51(1), 42–52. DOI: 10.1016/j.dss.2010.11.017.

C. Anhang

Gesprächsleitfaden Fokusgruppe

Im Rahmen dieser Masterarbeit sollen „Einstellungen von Wearable-NutzerInnen in Österreich im Umgang mit persönlichen Daten im Gesundheits- und Fitnesskontext“ untersucht werden. Gewonnene Daten aus der Diskussion dienen ausschließlich dem Forschungsinteresse und werden vertraulich behandelt.

1. **Begrüßung der Teilnehmenden**
   1.1 Unterzeichnung der Einverständniserklärung von allen Teilnehmenden

2. **Einleitung**
   2.1 Für die Teilnahme bedanken
   2.2 Information über den Ablauf und das Thema der Diskussion
   2.3 Anonymität der Teilnehmenden garantieren
   2.4 Vorstellungsrunde: Die Moderatorin und jeder der DiskussionsteilnehmerInnen stellt sich kurz vor, sodass ein Überblick über die teilnehmenden Personen gewonnen und erste Vertrautheit hergestellt werden kann (Name, Alter, Beruf, …)

3. **Wearable-Nutzung im Gesundheits- und Fitnessbereich allgemein**
   3.1 Warum nutzt ihr eure Smartwatch oder euer Fitnessarmband und welche Erfahrungen habt ihr bisher damit gemacht?

4. **Privatheitsbezogene Fragestellungen**
   4.1 Welche Daten nehmt ihr an werden mit eurer Smartwatch bzw. eurem Fitnessarmband gesammelt und welche davon sind für euch persönliche Daten?
   4.2 Welche Daten empfindet ihr als besonders sensibel und schützenswert? *Stimulus durch Flipchart*

   4.3 Für wen können diese Daten noch relevant sein, außer für euch selbst? (Bewusstsein)
   4.3.1 Wie steht ihr dazu? (Einstellung)

5. Mögliche Konsequenzen

5.1 Wir haben vorher darüber gesprochen für wen persönliche Daten im Gesundheits- und Fitnessbereich interessant sind. Wem würdet ihr eure persönlichen Gesundheits- und Fitnessdaten übermitteln und warum bzw. warum nicht?

Stimulus durch Flipchart

5.2 Welche Auswirkung kann das haben für euch persönlich, aber auch für andere Personen, die keine Wearables nutzen möchten?

5.3 Wie steht ihr zu folgendem Statement: „Es macht mir nichts aus Daten, die ich als persönlich erachte, für kostenlose Services preiszugeben, wenn ich dafür bestimmte Vorteile bekomme."

5.4 Welche Vorteile können das sein?

6. **Abschluss**

6.1 Für die Teilnahme bedanken

6.2 Gibt es noch Fragen oder etwas dass ihr mir und meiner Arbeit mitgeben möchtet?

Fragebogen der Rekrutierungsphase

Thema der Fokusgruppe: Einstellung von Wearable-NutzerInnen in Österreich im Umgang mit persönlichen Daten im Gesundheits- und Fitnesskontext

1. Zu welcher Altersgruppe gehörst du?
   - 18 - 28
   - 29 - 49
   - 49+

2. Was machst du beruflich?
   - Ich bin in Ausbildung
   - Ich bin angestellt
   - Ich bin selbstständig
   - Ich bin in Pension
   - Keine der genannten Möglichkeiten

3. Wie oft pro Woche treibst du Sport? (über 30 Minuten)
   - Keinmal
   - 1-2 Mal
   - 3-4 Mal
   - 5+

4. Wie häufig benutzt du ein Wearable*?
   - Ich habe eine/eines, nutze es aber aber nicht (mehr)
   - Ich nutze es eher selten
   - Ich nutze es eher wöchentlich
   - Ich nutze es täglich

5. Zu welchem Zweck nutzt du eine ein Wearable*? (mehrfach Auswahl möglich)
   - Sport
   - Gesundheit im Allgemeinen
   - Ernährung (z. B. Gewichtreduktion)
   - Aufgrund einer Vorerkrankung

*Wearable: Fitnessarmband bzw. Smartwatch in der Anwendung als Fitnesstracker

Stimulus Material der Fokusgruppe

1. Beschreibung des Begriffs „Persönliche Daten“

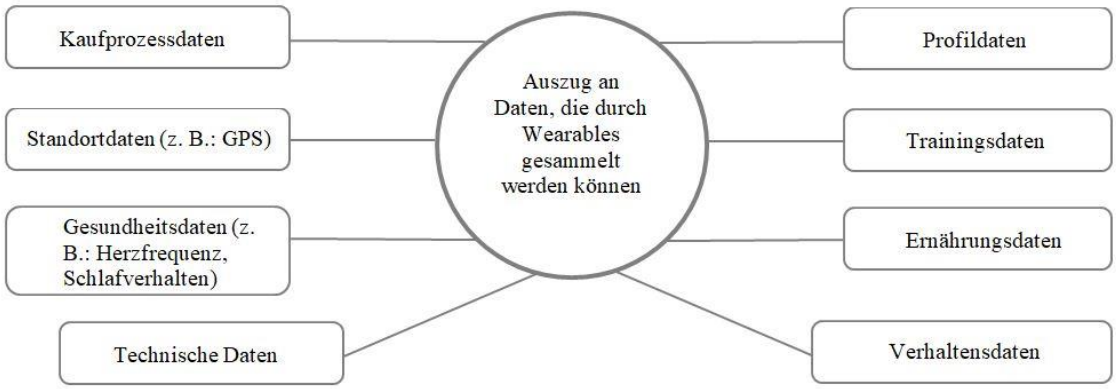

Abbildung 6: Stimulus Material, Datenarten im Rahmen von Wearables, eigene Darstellung.

2. Mögliche Konsequenzen der Datennutzung durch Organisationen

Abbildung 5: Stimulus Material, Auszug an Institutionen und Branchen mit potenziellem Interesse an Self-Tracking Daten, eigene Darstellung.

Exposé Master These 1. Abgabe

Familienname	**Andratsch**	
Vorname	Katharina	
Matrikelnummer	mm171801	
Mailadresse	mm171801@fhstp.ac.at	
Telefonnummer		
Datum	11.01.2019	
Name Betreuer	FH-Prof. Priv.-Doz. Dr. Michael Litschka	**Bestätigung der Betreuung durch Unterschrift des Betreuers**
Thema	Wirtschaft, Medien- und Internetethik, Recht Angrenzendes Fach zur Master-Thesis (laut Prüfungsliteratur): Mediensysteme, International Media Markets & Trends, Kommunikationswissenschaft	
Arbeitstitel	Information Privacy: Wie UserInnen mit persönlichen Daten umgehen	
Problemstellung Forschungsfrage	Innerhalb der digitalen Wirtschaft sind Geschäftsmodelle entstanden, deren Angebot auf den ersten Blick „kostenlos“ erscheint. Das Geschäftsmodell basiert darauf, dass NutzerInnen persönliche Daten preisgeben und dafür ein nachgefragtes Gut ohne oder für geringere monetäre Zahlungen erhalten (vgl. Kretschmer et al, 2018). Die ehemalige europäische Verbraucherschutzkommissarin Meglena Kuneva beschrieb die Situation der Datenmärkte 2009 folgendermaßen: „Persönliche Daten sind das neue Öl des Internets und die neue Währung der digitalen Welt.“ Persönlichen UserInnendaten, vor allem wenn sie in einer Vielzahl vorliegen (Netzwerkeffekte), wird zunehmend ein wirtschaftlicher Wert zugewiesen (vgl. Spiekermann/Korunovska, 2016). Die Bosting Consulting Group schätzt den ökonomischen Wert persönlicher Daten auf bis zu 330 Milliarden Euro p.a. für europäische Unternehmen im Jahr 2020 (vgl. Rose et al, 2012). Laut Acquisti/Grossklags (2005) sind Individuen bereit ihre Privatsphäre, d. h. persönliche Daten gegen Bequemlichkeit (convenience) oder relativ kleine Belohnungen wie Rabatte zu tauschen. Dabei wurde erkannt, dass die Sensibilität der Daten, der Datenempfänger und der Kontext, in dem die Information weitergegeben wird, die Kompensationserwartungen beeinträchtigen (vgl. Spiekermann-Hoff/Korunovska, 2017). Im Rahmen dieser Arbeit werden die Einstellung und das Verhalten im Hinblick auf den Umgang mit persönlichen Daten auf UserInnenebene in	

	Österreich erforscht. Dabei spielt die persönliche Wahrnehmung der UserInnen bezüglich Datenschutzbedenken im Internet eine erhebliche Rolle. Die Ergebnisse der in Österreich durchgeführten Umfrage des Gallup-Instituts im Juni 2018 zeigen, dass 67% der Befragten gewisse oder sehr große Bedenken hinsichtlich der Sicherheit ihrer persönlichen Daten beim Onlineeinkauf haben. Ebenso gaben im Dezember 2017 60% der befragten ÖsterreicherInnen an, das Gefühl zu haben keine Kontrolle über ihre Daten im Internet zu haben (vgl. Integral, 2017). Diese Ergebnisse zeigen, dass Individuen Datenschutzbedenken im Internet haben und besorgt sind persönliche Daten freizugeben, dennoch veröffentlichen sie eine Vielzahl an persönlichen Informationen im Internet. Die Dichotomie zwischen der Einstellung zur Privatsphäre und dem tatsächlichem Verhalten der UserInnen ist in der Wissenschaft als „Privacy-Paradoxon“ definiert (vgl. Brown, 2001; Norberg et al, 2007). Es gibt Studien die dieses Paradoxon bestätigen und jene die es wiederlegen (vgl. Kokolakis, 2015). Um diese Kontroverse zu verstehen ist zu erwähnen, dass das Verhalten im Hinblick auf die Privatsphäre ein kontextuelles Phänomen ist und kulturelle Unterschiede zu erkennen sind (vgl. ebd., 2015). Zur Interpretation des Privacy Paradoxons werden im Rahmen dieser Arbeit folgende Theorien ausgewählt: Die Privacy-Calculus-Theorie und verhaltensökonomische Ansätze wie Verhaltensheuristiken und die kognitive Verzerrung. Die Privacy-Calculus-Theorie besagt, dass Internetnutzer als rationale Agenten nach einem Kosten-Nutzen-Kalkül entscheiden, ob sie persönliche Daten preisgeben. Darunter ist die Abwägung zwischen zu erwartetem Verlust der Privatsphäre und dem potenziellen Gewinn durch die Offenlegung zu verstehen (vgl. Jiang et al., 2013). Demgegenüber ist die menschliche Entscheidungsfindung durch kognitive Verzerrung und Verhaltensheuristiken geprägt (vgl. Acquisi/Grossklags, 2007). Damit UserInnen Entscheidungen im Hinblick auf die Freigabe ihrer persönlichen Daten treffen können ist Information relevant. Tatsächlich verfügen jedoch die wenigsten UserInnen über notwendige kognitive Fähigkeiten Datenschutzrisiken und potenzielle Vorteile gegeneinander abzuwiegen, um in weiterer Folge informierte Entscheidungen zu treffen. Der Zugang zu allen diesbezüglich relevanten Informationen ist eingeschränkt (vgl. Kokolakis, 2015). Unvollständige Information und Informationsasymmetrie werden in dieser Masterarbeit ebenfalls erläutert. Diese Wissensgrundlage ist für den empirischen Teil der Arbeit bedeutsam. Aufgrund der Zunahme der Datenvielfalt durch neue Technologien, der dadurch wachsenden Datenmärkte, der Forderung nach Transparenz im Rahmen von neuen regulatorischen Rahmenbedingungen (EU-DSGVO, E-Privacy Verordnung) und die

	daraus folgende Einschränkung datengetriebener Geschäftsmodelle ist diese Thematik höchst aktuell und wird im Rahmen dieser Arbeit im wissenschaftlichen Kontext auf UserInnenebene erforscht. Die Einstellung und das Verhalten der UserInnen, hat neben den regulatorischen Rahmenbedingungen, eine maßgebliche Bedeutung für künftige Geschäftsmodelle datengetriebener Märkte. In dieser Masterarbeit wird das Forschungsthema Information Privacy unter Berücksichtigung aktueller Forschung des Information Privacy Paradoxons anhand ausgewählter Theorien im Literaturteil interpretiert. Mittels eines Laborexperiments (survey experiment) wird die Einstellung und das Verhalten auf UserInnenebene (Studierende der FH St. Pölten) im Umgang mit persönlichen Daten empirisch erforscht. Dabei wird untersucht ob der Anreiz Transparenz der Datenverwendung Auswirkungen auf die freiwillige Datenfreigabe der UserInnen hat. **Leitfrage** Inwiefern ist eine Diskrepanz zwischen der Einstellung und dem Verhalten österreichischer UserInnen im Umgang mit persönlichen Daten bei der Nutzung digitaler Dienste festzustellen? Diese Leitfrage wird mit folgenden zwei Forschungsfragen präzisiert: FF1: Inwiefern beeinflusst die Transparenz der Datenverwendung die freiwillige Datenfreigabe ausgewählter Studierender der FH St. Pölten? *Erkenntnisgewinnung mittels Experiment* FF2: Welche Einstellung haben diese ProbandInnen zum Thema Privatsphäre im Internet? *Erkenntnisgewinnung mittels quantitativem Fragebogen (ex-post)*
Aufbau und Gliederung	Inhaltsverzeichnis I Abbildungsverzeichnis II Tabellenverzeichnis III Abkürzungsverzeichnis IV 1. Einleitung 1.1 Ausgangslage und Problemstellung 1.2. Zielsetzung und Forschungsfragen 1.3. Methodik und Aufbau der Arbeit 2. Definition und Begriffsabgrenzung 2.1. Daten 2.2. Information Privacy 2.3. Rechtliche Rahmenbedingungen 3. Interpretation des Privacy Paradoxon 3.1. Vertrauens- und Risikowahrnehmung von Datenschutz im Internet

	3.2. Unvollständige Information und Informationsasymmetrie 3.3. Privacy-Calculus-Theorie 3.4. Verhaltensheuristiken und kognitive Verzerrung 4. Methodenteil 4.1. Auswahl der Probanden 4.2. Erläuterung der Erhebungsmethode Survey Experiment 4.3. Operationalisierung und Vorgehensweise 5. Empirische Untersuchung 5.1. Detailbetrachtung der Ergebnisse 5.2. Interpretation der Ergebnisse 5.3. Beantwortung der Forschungsfragen 6. Schlussbetrachtung 6.1. Conclusio 6.3. Handlungsempfehlungen 6.2. Limitationen Quellenverzeichnis Anhang
	Die vorliegende Arbeit ist in zwei Bereiche gegliedert. Der erste Teil ist der Literaturteil, in dem die gegenwärtige Fachliteratur für diese Thematik wiedergegeben wird. Dabei werden Meinungen von unterschiedlichen Autoren und Studienergebnissen zusammengeführt, ergänzt und gegenübergestellt. Mittels eines logischen und deduktiven Aufbaus wird eine Wissensgrundlage aufgebaut, die für die nachfolgende empirische Forschung erforderlich ist. Für die Auswahl der Literatur werden Bücher und Journals für die Fachgebiete Business Economy, fachgeleitete Sozialpsychologie, Information Technology, Computer, Security und Recht herangezogen. Der zweite Teil beinhaltet die empirische Untersuchung der definierten Forschungsfragen. Da diese Arbeit die Einstellung und das Verhalten von UserInnen erforscht, eignet sich die Kombination aus einem Experiment und einer Befragung (survey experiment). Eine Umfrage eignet sich um Einstellungen von Personengruppen abzufragen, jedoch nicht um das tatsächliche Verhalten in einem Kontext zu erforschen (vgl. Kokolakis, 2015, S. 13). Die Zielsetzung von Experimenten ist es, kausale Wirkungszusammenhänge zu überprüfen. Dabei werden formulierte Aussagen durch einen systematischen Ablauf auf ihren Wahrheitsgehalt überprüft, indem bestimmte Bedingungen des Experiments aktiv verändert werden. Das Experiment wird als Laborexperiment durchgeführt. Der Vorteil ist, dass die Versuchsbedingungen kontrolliert werden können, wodurch eine hohe interne Validität sicherstellt wird. Dadurch sind Veränderungen im Verhalten der Versuchsperson (abhängige Variable) eindeutig auf die bewusste Veränderung der unabhängigen Variablen zurückzuführen. Der Nachteil ist jedoch, dass hierbei nicht auf die natürliche Umgebung der ProbandInnen Rücksicht genommen wird (vgl. Nieding/Ohler, 2004). Als ProbandInnen werden Studierende der Fachhochschule St. Pölten herangezogen. Diese werden in zwei Gruppen, eine Experimental- und eine Kontrollgruppe,

<table>
<tr>
<td></td>
<td>aufgeteilt. Die Einordnung in die jeweilige Gruppe erfolgt nach dem Zufallsprinzip bzw. nach der „Randomisierung“ (vgl. Baur/Blasius, 2014, S. 139). Um einen Wirkungszusammenhang zu erkennen wird bei der Experimentalgruppe ein Stimulus gesetzt, die Kontrollgruppe erhält diesen jedoch nicht. In einem Experiment wird der Einfluss der unabhängigen Variablen auf die abhängigen Variablen gemessen. Die unabhängigen Variablen sind jene Elemente, die während des Versuches aktiv durch einen Stimulus beeinflusst werden, während die abhängigen Variablen innerhalb der Kontrollgruppe vorherrschend sind. Durch diesen Vorgang können kausale Rückschlüsse über die Beeinflussung durch den gesetzten Stimulus auf die Einstellung, das Verhalten oder andere psychische Konstrukte gezogen werden (vgl. ebd., S. 139f).
<table>
<tr><th></th><th>Unabhängige Variable</th><th>Abhängige Variable</th></tr>
<tr><td>Soziodemografische Daten</td><td rowspan="3">Experimentalgruppe

Transparenz der Datenverwendung</td><td rowspan="3">Kontrollgruppe

Keine Transparenz der Datenverwendung</td></tr>
<tr><td>Interessendaten</td></tr>
<tr><td>Sensible Daten (Definition gem. DSGVO)</td></tr>
</table>
Ein Experiment wird häufig in Verbindung mit einer weiteren Methode, der Befragung, durchgeführt (vgl. Hermann/Homburg/Klarmann, 2008, S. 31). Die quantitative Befragung eignet sich um Einstellungen zur Privatsphäre abzufragen, diese wird mittels quantitativem Fragebogen (post-study) durchgeführt.
Anschließend werden die gewonnenen Erkenntnisse aus der Aufarbeitung der bestehenden Literatur und der Auswertung der empirischen Forschung gegenübergestellt und näher erläutert. In der abschließenden Conclusio werden die Ergebnisse der Forschung, die definierten Forschungsfragen beantworten, zusammengefasst und interpretiert. Zudem werden Empfehlungen für weiterführende Forschungen abgeleitet.</td>
</tr>
<tr>
<td>Literaturhinweise</td>
<td>
Acquisti, A., Grossklags, J. (2005). Privacy and Rationality in Individual Decision Making, *IEEE Security and Privacy*, IEEE Computer Society, Vol. 3, No. 1, January/February 2005, pp. 26-33.

Acquisti, A., Grossklags, J. (2007). What can behavioral economics teach us about privacy?, in: A. Acquisti, S. Gritzalis, S. Di Vimercati, C. Lambrinoudakis (Eds.), "Digital Privacy: Theory, Technologies, and Practices," Auerbach Publications, pp. 363-379.

Brown, B. (2001). Studying the internet experience. HP Laboratories Technical Report (HPL-2001-49). Zugriff am 3. Jänner 2019. Verfügbar unter http://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf.

Baur/Blasius (2014): Handbuch Methoden der empirischen Sozialforschung. Springer Fachmedien Wiesbaden.

Das Österreichische Gallup-Institut. n.d. Haben oder hätten Sie bei einem Onlinekauf Bedenken, ob Ihre persönlichen Daten sicher sind bzw. missbraucht werden könnten?. Statista. Zugriff am 3. Januar 2019. Verfügbar unter https://ezproxy.fhstp.ac.at:2081/statistik/daten/studie/909659/umfrage/umfrage-zu-bedenken-hinsichtlich-der-datensicherheit-in-oesterreich/.
</td>
</tr>
</table>

	Hermann/Homburg/Klarmann (2008): Handbuch Marktforschung. Methoden – Anwendung – Praxisbeispiele, 3. Auflage, Wiesbaden: Gabler. INTEGRAL. n.d. Wie sehr stimmen Sie den folgenden Aussagen zu?. Statista. Zugriff am 3. Januar 2019. Verfügbar unter https://ezproxy.fhstp.ac.at:2081/statistik/daten/studie/716891/umfrage/aussagen-zur-internetsicherheit-in-oesterreich/. Kokolakis (2015): Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. In: Computers & Security. Koschate, N. (2008): Grundlagen experimenteller Marktforschung, in: Hermann/Homburg/Klarmann (Hrsg.): Handbuch Marktforschung. Methoden – Anwendung – Praxisbeispiele, 3. Auflage, Wiesbaden: Gabler. Kretschmer et al. (2018): Datenkapitalismus — eine ökonomische Betrachtung. In Wirtschaftsdienst, Ausgabe 7/2018. Nieding, G., Ohler, P. (2004). Laborexperimentelle Methoden. In R. Mangold, P. Vorderer & G. Bente, (Hrsg.). Lehrbuch der Medienpsychologie (Kap. 15). Norberg, P.A., Horne D.R., Horne D.A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviour. Journal of Consumer Affairs, 41(1), pp. 100-126. Rose/Röber/Rehse (2012). The value of our digital identitiy. In: Liberty Global Policy Series, L. Global (Ed.). Liberty Global Policy Series. Spiekermann-Hoff, Sarah and Korunovska, Jana (2017) Towards a value theory for personal data. Journal of Information Technology, 32 (1). pp. 62-84. ISSN 1466-4437.