Die Privatsphäre ist am Ende. Oder?

Die Debatte um das Ende der Privatsphäre aus der Nutzerperspektive.

Dominique Facciorusso[*]

Abstract

Privatsphäre – ein viel diskutierter Begriff, der zunehmend Gegenstand öffentlicher Debatten geworden ist. Doch was meint das Wort, dessen Ende bereits eingetroffen zu sein scheint, von manchen befürchtet und von anderen sogar gefordert wird? Welche Bedeutung hat das Private für uns und unsere Gesellschaft und welche Funktionen sind ihm inhärent? Handelt es sich bei der Privatsphäre tatsächlich um ein Auslaufmodell, das im Hinblick auf die Nutzung und Ausbreitung datenerfassender Technologien obsolet geworden ist? Fakt ist: Neben wirtschaftlichen und politischen Akteuren stellen die Nutzer selbst ein zunehmendes Risiko für die Privatsphäre dar, indem sie zunehmend Daten von sich preisgeben. Gleichzeitig geben Nutzer aber an, dass Ihnen ihre Privatsphäre wichtig ist. Wie aber lässt sich solch ein (scheinbar) widersprüchliches Privatsphäreverhalten erklären? Und in welchem Verhältnis steht dieses Verhalten zur Debatte um das Ende der Privatsphäre? Diese Fragen versucht der hier vorliegende Beitrag zu beantworten.

1. Privatsphäre 2.0 – ein Auslaufmodell?

Das Internet hat sich zur selbstverständlichen und unverzichtbaren Infrastruktur unseres öffentlichen und privaten Lebens entwickelt. Auch wer keine sozialen Netzwerke nutzt oder online einkauft, ist fast rund um die Uhr vernetzt, denn immer mehr Prozesse und Systeme

* Die Verf. ist wissenschaftliche Mitarbeiterin am Mainzer Medieninstitut. Frau Facciorusso hat Publizistik (B.A.) und Kommunikationswissenschaft (M.A.) am Institut für Publizistik (IfP) der Johannes Gutenberg-Universität in Mainz studiert. 2014 wurde sie für ihre Bachelorarbeit zum Thema „Google – the World Brain. Was passiert, wenn die ganze Welt zum Index wird? Zur Entwicklung, Auswirkung und Bedeutung von Google für unsere Informationsgesellschaft“ mit dem Wissenschaftspreis 2014 des Datenschutzbeauftragten Rheinland-Pfalz ausgezeichnet.

UFITA 2/2018, DOI: 10.5771/2568-9185-2018-2-459

werden in Online-Versionen überführt bzw. von ihnen ersetzt. Im Zuge dieser technikgetriebenen, scheinbar exponentiellen Entwicklung werden auch private und zum Teil hochsensible Lebensbereiche zunehmend erschlossen.

Die Privatsphäre ist am Ende, meinen daher Vertreter der sogenannten „Post-Privacy"-Bewegung. Demnach kann es in Zeiten umfassender Datenerfassung keine Privatsphäre mehr geben, weshalb ihr Schutz hier als illusionär gilt. Das extreme Lager der Bewegung verfolgt den Ansatz, dass eine flächendeckende Vernetzung ohne Zugangsbeschränkungen und Geheimnisse sogar positive Effekte für Individuum und Gesellschaft habe. Die totale Datenverfügbarkeit führe demnach zu einer „Waffengleichheit" zwischen Bürger und Staat, die ein System von Kontrolle und Gegenkontrolle ermöglicht (Bosesky und Brüning, 2014, S. 86).Denn dort, wo alles transparent und öffentlich ist, ließe sich auch nichts mehr verbergen, so die Idee. Doch ganz so einfach ist es nicht, denn die online erfassten personenbezogenen Daten und das daraus generierbare Wissen befinden sich nicht in den Händen der Öffentlichkeit, sondern auf den Servern privater Konzerne sowie im Besitz unbekannter Dritter.

Ähnlich argumentiert auch Mark Zuckerberg, Gründer und CEO von Facebook: „If people share more, the world will become more open and connected. And a world that's more open and connected is a better world" (Zuckerberg, 2010). Daraufhin nimmt der Konzern eine Generalüberholung der Privatsphäre-Einstellung vor, die ihm ab da an mehr Zugriffsrechte auf private Nutzerdaten erlaubt. Damit dies nicht als Eingriff in die Privatsphäre der Nutzer gewertet wird, erklärt Zuckerberg das Konzept kurzerhand als Auslaufmodell: „People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time." (Zuckerberg zitiert nach Kirkpatrick, 2010).

Die Erklärung, dass weniger Datenschutz dem aktuellen Zeitgeist entspricht und Nutzer ihre Daten aufgrund der damit verbundenen Vorteile bewusst und gerne preisgeben bzw. "teilen", steht stellvertretend für das Marketing einer gesamten datengetriebenen Branche, deren Motive rein wirtschaftlicher Natur sind. Denn Nutzerdaten sind unter werberelevanten Aspekten viel wert und dienen Google, Facebook und Co. als äußerst erfolgreiches und tragendes Geschäftsmodell. Doch Nutzerdaten sind auch unter politischen Aspekten von Interesse, wie die Enthüllung Edward Snowdens oder der Datenmissbrauch um Cambridge Analytica jüngst erst wieder deutlich gemacht hat.[1]

Die Privatsphäre wird aber nicht nur durch Konzerne und Regierungen bedroht. Eine zunehmende Gefahr geht auch von den Nutzern selbst aus, verbringen diese immer mehr Zeit im Internet (Frees und Koch, 2018) und geben dort zunehmend Daten von sich preis (Bosesky und Brüning, 2014; Wewer, 2013; Schiedermair, 2012). Vor diesem Hintergrund wird Nutzern oft ein mangelndes Problembewusstsein im Umgang mit ihren Daten im Netz

1 Für mehr Informationen zum Datenmissbrauch um Cambridge Analytica vgl. Facciorusso, Dominique (2018): Facebook: Datenmissbrauch um Cambridge Analytica. Verfügbar unter: https://www.mainzer-medieninstitut.de/facebook-datenmissbrauch-um-cambridge-analytica/ [10.01.2019].

nachgesagt (Horn, 2013; Wewer, 2013; Bolz, 2012). Untersuchungen zeigen aber, dass diese (vor allem die jungen Nutzer) sehr wohl Risiken wahrnehmen und sich um den Schutz ihrer Privatsphäre sorgen, auch wenn sie bei der Nutzung onlinebasierter Anwendungen eine Menge privater Daten von sich preisgeben (Barnes, 2006; Trepte/ Masur und Pape, 2015; Turow et al., 2015; Facciorusso,[2] 2017; Marwick und Hargittai, 2018). Wie aber lässt sich solch ein scheinbar widersprüchliches Verhalten erklären? Und in welchem Verhältnis steht dies zur Debatte um das Ende der Privatsphäre?

Der Beantwortung dieser Fragen versucht sich der hier vorliegende Beitrag in den nächsten Kapiteln zu nähern. Hierfür wird zunächst definiert, was wir heute unter dem Begriff Privatsphäre überhaupt verstehen. Anschließend werden die Funktionen und die Bedeutung des Konzepts theoretisch erläutert, um deutlich zu machen, warum ein Ende der Privatsphäre schwere Folgen für Individuum und Gesellschaft hätten. Im Anschluss soll sich der Frage genähert werden, warum Menschen ihre Privatsphäre online gefährden, obwohl sie diese als schützenswert erachten. Hierfür werden insgesamt drei Bereiche aus der Privatsphärenforschung vorgestellt, die sich mit dem (scheinbar) paradoxen Selbstoffenbarungsverhalten der Internetnutzer befassen. Abschließend werden die Kernergebnisse zusammengefasst und Stellung zur Debatte um das Ende der Privatsphäre bezogen.

2. Privatsphäre 2.0 – Wovon sprechen wir hier eigentlich?

2.1 Was verstehen wir heute unter Privatsphäre?

Bevor man sich der Frage nähert, was heute unter dem Konzept verstanden wird, muss zunächst deutlich gemacht werden, dass es sich bei „Privat", „Privatheit" oder „Privatsphäre" um historisch relativ junge Begriffe handelt,[3] deren Bedeutung schon immer eng mit der geschichtlichen Entwicklung und den jeweiligen kulturellen Gegebenheiten verwoben war. Schon in der griechischen Antike unterscheidet Aristoteles zwischen einer häuslichen (*Oikos*) und politischen Sphäre (*Polis*) (Schiedermair, 2012). Zu jener Zeit ist das Private mit dem Hausherrn als Herrschenden über Familie und Sklaven hierarchisch strukturiert und durch *Unfreiheit* geprägt. Die Öffentlichkeit hingegen wird als Ort der freien Entfaltung und Anerkennung gesehen und gilt als positiver Gegenpol zum Privaten (ebd.). Dieses Bild von Privatsphäre hat sich dann im 18. und 19. Jahrhundert im Zuge der Aufwertung des Individuums und der damit einher-gehenden Freiheitsrechte in sein Gegenteil verkehrt.

Medienhistorisch gewinnt die Privatsphäre erstmals im 20. Jahrhundert an Bedeutung, indem sich mit der Etablierung der Massenmedien zunehmend private Informationen über Personen der Öffentlichkeit verbreiten (Grimm und Krah, 2014). Diese mediale Veröffentli-

2 Die Studie "*Privacy is no longer a social norm." – Eine qualitative Befragung junger Erwachsener über das Verständnis von und die Einstellung zur Privatsphäre im Internet* von Dominique Facciorusso wurde im Rahmen einer Masterarbeit durchgeführt. Die Ergebnisse werden in dem hier vorliegenden Beitrag als wichtige Grundlage herangezogen.

3 In dem hier vorliegenden Beitrag werden die Begriffe synonym verwendet.

chung des Privaten kritisieren und thematisieren Warren und Brandeis in ihrem Aufsatz „The Right to Privacy" und definieren dort die Privatsphäre erstmals als „right to be let alone" (Warren und Brandeis, 1890/1984).

Die weiteren technikgetriebenen Entwicklungen im späten 20. und frühen 21. Jahrhundert wie die Computerisierung, Vernetzung sowie voranschreitende Digitalisierung sorgen dafür, dass die Veröffentlichung und Erfassung des Privaten beispiellos zugenommen hat – ein Ende ist nicht in Sicht. Die Entwicklung entzündet damit erneut die Debatte um die Form und Daseinsberechtigung der Privatsphäre sowie die Frage, wie wir jetzt und in Zukunft als Gesellschaft leben wollen.

Was also verstehen wir heute unter dem Begriff?

Der Blick in die Literatur zeigt, dass sich aktuell keine konstante und allgemein gültige Definition finden lässt (Solove, 2007; Paine et al., 2007; Buchmann, 2013). Vielmehr wird die Komplexität und Vielschichtigkeit des Begriffs deutlich, da das Private je nach Perspektive ganz unterschiedlich verstanden wird. Dennoch stößt man in der Forschungsliteratur vor allem auf zwei Perspektiven, aus denen heraus Privatsphäre aktuell diskutiert wird: Zum einen wird das Konzept aus einer individualistischen und zum anderen aus einer sozialen Perspektive heraus betrachtet (Seubert und Helm, 2017).

Zunächst zur *individualistischen Perspektive*: Hier wird vor allem auf *drei zentrale Ansätze* zurückgegriffen, die das Konzept beschreiben (Trepte und Dienlin, 2013). Der Rechtswissenschaftler Alan Westin (1967) definiert Privatsphäre als einen freiwilligen und temporären physischen oder psychischen Rückzug eines Individuums von der Gesellschaft (S. 7), der in vier Zuständen münden kann (Einsamkeit bzw. Für-sich-sein, Intimität, Anonymität, Zurückgezogenheit). Der Sozialpsychologe Irwin Altmann (1975) erweitert Westins Ansatz und betont Privatheit als einen Prozess zwischenmenschlicher Grenzkontrolle, indem das Individuum sein Bedürfnis nach Interaktion mit Individuen oder Gruppen mit dem nach Rückzug je nach Situation immer wieder neu ausbalancieren kann, um ein optimales Level an Privatsphäre zu erreichen (S. 18). Dies liegt vor, wenn das vorhandene Level an Privatsphäre dem angestrebten entspricht (Dienlin, 2019).

Nach Trepte und Dienlin (2013) hat die Kommunikationswissenschaftlerin Judee Burgoon (1982) anschließend das Verständnis von Privatsphäre entscheidend bereichert, indem sie den Zugang zum Selbst in vier Bereiche systematisiert hat. Demnach gibt es die (1.) *physische Privatheit*, die den territorialen Zugang zu einer Person wie etwa zu deren Haus oder Körper beschreibt. Die (2.) *soziale Privatheit* betrifft die Kontrolle über die sozialen Kontakte und Interaktionen. Mit der (3.) *psychologischen Privatheit* ist die Kontrolle gemeint, die eigenen Gedanken und Gefühle äußern bzw. von anderen aufnehmen zu können. Mit der (4.) *informationellen Privatheit* beschreibt Burgoon zuletzt die Kontrolle über die Erfassung der eigenen personenbezogenen Daten, sprich darüber, wer was über einen weiß (ebd.).

In der individualistischen Perspektive wird das Private also meist als räumlicher Rückzug und Kontrollmechanismus von Individuen verstanden. Die Privatsphäre ist demnach

das „Nicht-Öffentliche“ (Seubert und Niesen, 2010; Gräf/ Halft und Schmöller, 2011) bzw. das Recht „to shut out the community“ (Thomas, 1970, S. 545). Hier zeigt sich auch nach hundert Jahren noch die Grundidee des von Warren und Brandeis formulierten „right to be let alone“ (1890/1984). Wichtig ist, den Zugang zu bzw. die Informationen über sich selbst kontrollieren zu können. Die Rechtsprechung versteht die Privatsphäre daher als Abwehr des Zugriffs Dritter. Denn im Gegensatz zur Öffentlichkeit ist es dem Individuum im Privaten möglich, sich der sozialen Interaktion und der Beobachtung anderer entziehen zu können und nur denen ausgesetzt zu sein, deren Anwesenheit es selbst kontrollieren kann (Worms und Gusy, 2012; Seubert, 2012).

Zum anderen wird Privatsphäre aktuell aus einer *sozialen Perspektive* heraus betrachtet, die kritisiert, dass die individualistische Konzeptualisierung die Privatsphäre nicht ausreichend als gesellschaftlichen Wert betrachtet (Seubert, 2017). Demnach ist Privatsphäre in erster Linie nicht für die Autonomie des Einzelnen von Bedeutung, sondern sie ermöglicht vielmehr „ein integrales Moment der Dynamik sozialer Beziehungen“ (ebd., S. 126). Denn Individuen entwickeln sich nicht völlig autonom, sondern innerhalb eines sozialen Geflechts und gesellschaftlicher Werte und Normen. Zudem ist die Realisierung privater Schutzansprüche auf eine soziale Gemeinschaft angewiesen, die diese Bedürfnisse anerkennt und schützt (Seubert, 2017). In der sozialen Perspektive wird Privatheit daher als „Instrument für ein selbstbestimmtes Leben in der Gemeinschaft“ verstanden (Braun und Trepte, 2017, S. 5).

Um diese soziale und politische Bedeutung der Privatsphäre hervorzuheben, haben die Medienpsychologen Sabine Trepte und Kollegen im Zuge des interdisziplinären Langzeitprojekts „Strukturwandel des Privaten“ eine konzeptionelle Neubestimmung der Privatheit vorgenommen. Diese wird anhand von drei Dimensionen beschrieben: Demnach hat sich Privatheit im digitalen Zeitalter (1.) „*von einem individualistischen hin zu einem sozialen Freiheitsverständnis“* verändert (Strukturwandel des Privaten, 2018). Das bisherige Konzept beruht auf einem negativen Freiheitsverständnis, indem die abwehrrechtliche Funktion der Privatsphäre im Fokus steht. Der Perspektivwechsel hin zu einem sozialen Verständnis ermöglicht hingegen, Privatheit, Freiheit und Demokratie in ein Bedingungsverhältnis zu setzen und so die Möglichkeiten für den Schutz der Privatheit durch rechtliche und technische Maßnahmen zu erweitern und Machtasymmetrien abzubauen (Eichenhofer, 2017).

Weiterhin habe sich (2.) das „*Recht allein gelassen zu werden“* aufgrund der Etablierung einer globalen Kommunikationsinfrastruktur zu einem „*Recht auf geschützte Kommunikationsräume“* gewandelt (Strukturwandel des Privaten, 2018). Die Autoren verstehen Privatheit also weniger als Anspruch, sich von anderen abgrenzen zu wollen, sondern vielmehr als „soziale und kommunikative Handlungsfreiheit“, die das Mitwirken anderer voraussetzt und es gleichzeitig bedingt (ebd.). Vor diesem Hintergrund bedeute Privatheit „selbst über den Grad der eigenen Vergesellschaftung entscheiden zu können.“ (ebd.). Da dieser Prozess auch in digitalen Kommunikationsräumen stattfindet, die Pluralismus sowie politische Handlungsfähigkeit ermöglichen, sind diese von gesellschaftlicher Bedeutung und daher zu schützen (ebd.).

Zuletzt hat sich Privatheit nach Trepte und Kollegen (3.) *von der Zugangskontrolle zum „social boundary-process"* gewandelt (ebd.). Im Zuge der digitalen Kommunikation werden personenbezogene Daten erfasst, verwertet und an Dritte übermittelt, was dazu führe, dass die Anforderung an den Selbstdatenschutz der Onliner zunimmt. Demnach weiche die Kontrolle über den „Zugang zu Räumen, Informationen oder Entscheidungen" einem „soziale[n] und gesellschaftliche[n] Grenzziehungsprozess", so die Autoren (ebd.). Um diesen Kontrollverlust auszugleichen, müssen daher neben den Maßnahmen zur Regulierung und Förderung von Selbstschutzfähigkeit zusätzlich solche für „Systemdatenschutz" greifen (ebd.).

Es kann festgehalten werden: Bei dem Versuch einer Begriffsdefinition zeigt sich sogleich der multidimensionale Charakter der Privatsphäre, denn es handelt sich hier um kein allgemeingültiges, sondern um ein vielschichtiges, komplexes Konzept (siehe auch Burgoon et al., 1989; Paine et al., 2007; Solove, 2007; Bergmann, 2011; Buchmann, 2013). Privatsphäre ist zudem nicht starr, sondern dynamisch, hat es sich im Verlauf der Geschichte stets an den Kontext gesellschaftlicher Entwicklungen angepasst. Vor dem Hintergrund, dass wir heute in einer vernetzten Welt leben, steht die Rejustierung des Privatsphäre-Verständnisses wie es Trepte und Kollegen unternehmen daher in der Tradition, das Konzept entlang aktueller Gegebenheiten anzupassen bzw. neu zu denken. Die Anpassung ist zudem als unausweichliche Maßnahme zu sehen, will man auf gesellschaftlicher Ebene handlungsfähig bleiben und das Private für die Zukunft nicht leichtfertig aufgeben. Denn dem Privaten sind wichtige Funktionen für unser Zusammenleben inhärent, die im nächsten Kapitel erörtert werden.

2.2 Die Funktionen und Bedeutung der Privatsphäre

Nach Westin (1967) unterstützt die Privatsphäre Individuen in vier zentralen Funktionen, die auch Jahrzehnte später nicht an Gültigkeit verloren haben und für das Funktionieren einer demokratischen Gesellschaft essentiell sind. Diese Funktionen der Privatsphäre werden jedoch durch die Datenerfassung (zum Teil massiv) gefährdet.

(1.) So ermöglicht Privatsphäre etwa die *persönliche Autonomie*, sprich die Entscheidungs- und Handlungsfreiheit sowie selbstbestimmte Lebensgestaltung, die verhindern soll, von anderen manipuliert, beherrscht oder entblößt zu werden. Denn wirklich autonome Entscheidungen können nur solche sein, die ohne den direkten bzw. indirekten Einfluss Dritter entschieden werden (Westin, 1967; vgl. hierzu auch dezisionale Privatheit von Rössler, 2001).

Mit Blick auf das Internet und die Möglichkeiten der automatischen Datenverarbeitung gewinnt Autonomie in Form der *informationellen Selbstbestimmung* zunehmend an Bedeutung. So haben Personen das Recht, selbst über die Preisgabe und Verwendung ihrer Daten bestimmen zu können (BVerfG 65, 1, Volkszählungsurteil). Doch Algorithmen können selbst unscheinbare Daten auswerten, mit anderen verknüpfen und daraus Prognosen ableiten. Auch Datensparsamkeit verhindert nicht, dass sich im Netz Anhaltspunkte finden las-

sen, die Rückschlüsse auf Privates zulassen. Was wir nicht (bewusst) mitteilen, können sich Data Mining Instrumente zum Teil selbst aus unserem Onlineverhalten ableiten. IT-Konzerne und unbekannte Dritte können so mehr über uns und unser Umfeld erfahren, als wir selbst dazu imstande wären (Hotter, 2011).

(2.) Menschen spielen täglich diverse Rollen, um unterschiedliche Beziehungen zu pflegen und gesellschaftlich Anerkennung zu erlangen. Im Schutze des Privaten können wir diese Masken ablegen, frei von sozialem Druck und gesellschaftlichen Erwartungen Ruhe finden und die innere Balance wiederherstellen. Die Privatsphäre als Rückzugsraum von sozialen Restriktionen dient dem Individuum daher auch zur *emotionalen Entlastung*. Sind diese Möglichkeiten des Rückzugs nicht vorhanden, kann dies nach Westin zu physischen und psychischen Problemen führen (Westin, 1967; Hotter, 2011).

Mit Blick auf das Internet können soziale Restriktionen jedoch bis ins Private hineinwirken, indem sich Nutzer über eine, im Sinne Noelle-Neummans,[4] anonyme (und damit nicht zu kontrollierende) Urteilsinstanz bewusst sind, die sie als Bedrohung wahrnehmen. So haben Gregory White und Kollegen in ihrer Studie „The Chilling Effects of Surveillance: Deindividuation and Reactance" (1975) erstmals gezeigt, dass Menschen zu Verhaltenskonformität und Selbst-zensur neigen, je mehr sie sich überwacht fühlen. Auf das Internet übertragen zeigen Studien, dass sich Nutzer seit den Snowden-Enthüllungen im Sinne des „Chillig Effect" ebenfalls anpassen, indem intime und politisch riskante Begriffe und Artikel weitaus seltener gesucht werden als zuvor (Marthews und Tucker, 2015; Penney, 2016).

(3.) Weiterhin ermöglicht die Privatsphäre die *Selbstevaluation*, indem dort persönliche Erfahrungen reflektiert, bewertet und daraus Folgen gezogen werden können. Diese Integration der persönlichen Erfahrung ist nach Westin für die eigene Identitätsfindung von großer Bedeutung (ebd.). Auch andere Autoren betonen die Bedeutung der Privatsphäre für die Subjektivität eines Individuums. Denn nur dort sei es imstande zu reflektieren, sich selbst in Frage zu stellen und sich zu seiner Umgebung ins Verhältnis zu setzen. Der Prozess der Selbstvergewisserung sei notwendig, damit es in der Auseinandersetzung mit der Öffentlichkeit bestehen und zu ihrer inhaltlichen Gestaltung überhaupt erst beitragen kann (ebd.).

Im Online-Kontext erklärt Sauter, dass das Social Web hier neue Möglichkeiten bietet. Ehemals private Subjektivierungsprozesse werden zunehmend öffentlich sichtbar, indem Nutzer von sozialen Netzwerken private Details aus ihrem Leben preisgeben. Dieses Kundtun versteht Sauter weniger als reine Selbstdarstellung, sondern auch als Mechanismus der Selbstregulierung, der das Bewusstsein über den Einblick der anderen in den Prozess der eigenen Subjektivität miteinbezieht (Sauter, 2014).

(4.) Zuletzt ermöglicht die Privatsphäre die *geschützte Kommunikation*, indem jeder selbst darüber bestimmen kann, mit wem er welche Informationen austauschen möchte.

4 Nach Noelle-Neumann ist der Mensch aufgrund seiner Sozialnatur nicht frei vom Einfluss der öffentlichen Meinung, da er sich sozial nicht isolieren, sondern in der Gemeinschaft integrieren will. Diese Öffentlichkeit empfindet er als Bedrohung und analysiert daher permanent seine Umgebung und passt sein dort gezeigtes Verhalten an (Noelle-Neumann, 1979; siehe auch Lamp, 2009).

Durch den differenzierten Grad an Privatheit kommen Beziehungen verschiedener Intensität und Qualität zustande (Westin, 1967; Hotter, 2011).

Auch online kann etwa auf Facebook der Grad an gewünschter Privatheit auf horizontaler Ebene mithilfe vielfältiger Privatsphäre-Einstellungen reguliert werden. Jedoch ändern sich die Einstellungen auf den Plattformen immer wieder, sind für die Nutzer oft schwer zu finden und zu verstehen. Zudem gilt die Differenzierung des Zugangs zu den privaten Daten nicht gegenüber den Plattformanbietern sowie unbekannten Dritten. Wer alles einen Zugriff auf die Kommunikationsdaten hat bzw. haben kann und inwiefern diese Daten heute oder in Zukunft verwertet bzw. missbraucht werden können, ist den Nutzern in der Regel also meist nicht bewusst. Der Rechtswissenschaftler Johannes Eichenhofer (2017) erklärt daher, dass umso weniger der Einzelne den Zugang zu seinen privaten Informationen, Räumen oder Entscheidungen selbst bestimmen oder gar kontrollieren kann, desto mehr ist er auf das Vertrauen angewiesen, dass die Kommunikationsräume adäquat geschützt werden. Demnach finde aktuell ein Wechsel vom Selbstbestimmungs- zum Vertrauensparadigma statt, so Eichenhofer.

(5.) Über Westins Funktionen hinaus wird immer wieder die Bedeutung des Privaten für die *Entstehung von Öffentlichkeit* betont, da man seine zunächst privat gewonnenen Erfahrungen nach außen trägt und so Impulse für die öffentliche Agenda setzt (Hotter, 2011). Auf diese Art kommen Themen zur Geltung, die nicht nur für das Individuum, sondern auch für die Gemeinschaft von Bedeutung sind. Nach Solove ist die Privatsphäre „not the trumpeting of the individual against society's interests but the protection of the individual based on society's own norms and practices". Schon hier wird der gesellschaftliche Wert des Konzepts betont. Demnach sei Privatsphäre eine „internal dimension of society. Therefore, privacy has a social value. Even when it protects the individual, it does so for the sake of society" (Solove, 2007, S. 15; siehe auch Klinger, 2018). Wichtig ist also nicht nur, dass die Gemeinschaft dem Einzelnen Rechte und Freiräume zugesteht, die ihr am Ende selbst zugutekommen. Es geht vor allem darum, dass es keine Öffentlichkeit ohne den Schutz des Privaten geben kann.

(6.) Damit bedingen sich auch *Privatsphäre und Demokratie* gegenseitig. Indem Privatsphäre eine politische Öffentlichkeit ermöglicht, in der Wissen geteilt, Themen gesetzt, Interessen vertreten sowie Konsens ausgehandelt wird, werden die Grundvoraussetzungen für eine demokratische Gesellschaft geschaffen. Demokratie lebt vom Pluralismus, der friedlich nebeneinander existiert und allenfalls in den argumentativen Wettstreit tritt und das Private generiert vor diesem Hintergrund Vielfalt, schützt Minderheiten und bildet so ein freiheitliches Korrektiv zum demokratischen Mehrheitsprinzip (Eichenhofer, 2017).

Es kann festgehalten werden, dass die Privatsphäre viele Funktionen für das Individuum und damit einhergehend für das Funktionieren einer demokratischen Gesellschaft hat. Im Kontext des Internets und der voranschreitenden technologischen Möglichkeiten werden besonders die Autonomie im Sinne der *informationellen Selbstbestimmung* sowie die *geschützten Kommunikationsräume* zunehmend bedroht, die essenziell für die Sicherung von Vielfalt und der politischen Handlungsfähigkeit von Individuen sind. Nun geht aber eine

zunehmende Gefährdung der Privatsphäre von den Nutzern selbst aus, indem diese scheinbar bereitwillig jede Menge Daten von sich im Netz preisgeben, gleichwohl sie sich um ihre Privatsphäre sorgen und diese als schützenswert erachten (Facciorusso, 2017). Wie aber lässt sich solch ein scheinbar widersprüchliches Verhalten erklären?

3. Das (scheinbar) paradoxe Privatsphäreverhalten im Netz

Um sich einer Antwort auf die Frage zu nähern, warum Menschen mit ihrem Verhalten im Netz ihre Privatsphäre gefährden, obwohl sie diese als wichtig und schützenswert erachten, soll im folgenden Kapitel untersucht werden. Hierfür werden *drei* Stränge aus der Privatsphärenforschung vorgestellt, die sich mit dem scheinbar paradoxen Privatsphäreverhalten der Internetnutzer befassen.

3.1 Das Privacy Paradox

Das sogenannte *Privacy Paradox* beschreibt etwa die Diskrepanz, dass Nutzer Sorgen um ihre Privatsphäre haben und gleichzeitig jede Menge private Daten von sich online preisgeben (Trepte und Teutscht, 2016). Sprich die Sorgen der Nutzer bezüglich der Verletzung der Privatsphäre scheinen keinerlei Effekt auf deren Selbstoffenbarungsverhalten im Netz zu haben (Dienlin, 2019).

So untersuchen Barry Brown und Abigail Sellen mithilfe einer qualitativen Befragung (2001) das Onlineverhalten von 19- bis 58-Jährigen im Kontext des *E-Commerce*. Im Fokus steht unter anderem, die mit der Privatsphäre verbundenen Einstellungen und Nutzungsmotive der Onliner zu erfassen. Obwohl alle Befragten mit der Datenerfassung im Netz diverse Sorgen verbinden, zeigen diese eine hohe Bereitschaft, Daten von sich preiszugeben (siehe im kommerziellen Kontext auch Norberg/ Horne und Horne, 2007).

Ein viel größerer Forschungsbereich untersucht das Privacy Paradox im Kontext des *Social Web*. Hier stellt etwa Susan Barnes in einer qualitativen Studie (2006) mit Teenagern zu ihrem Verhalten auf Netzwerkseiten fest, dass sich diese widersprüchlich verhalten, indem sie Bedenken äußern und gleichzeitig online wesentlich mehr Daten von sich preisgeben als offline. Zudem zeigt sich, dass sich fast keiner über den öffentlichen Charakter der Online-Kommunikation und die Verwendung seiner Daten bewusst ist. Die zentrale Erkenntnis lautet daher: Auch wenn sich junge Nutzer um ihre Privatsphäre sorgen, so wird dies online nicht adäquat durch deren Selbstoffenbarungsverhalten reflektiert (Barnes, 2006). Auch andere Studien bestätigen das Phänomen im Kontext sozialer Netzwerke (Acquisti und Gross, 2006; Tufekci, 2008; Taddicken, 2013).

Es gibt in der Forschung zum Privacy Paradox jedoch auch Studien, die zeigen, dass das Paradoxon so nicht existiert (für einen Überblick über alle wichtigen Studien zum Paradox siehe Kokolakis, 2017). So zeigen zum Beispiel Lemi Baruh und Kollegen (2017) in einer ersten Meta-Studie empirischer Arbeiten, dass Menschen, die sich vermehrt um ihre Privatsphäre sorgen, im Durchschnitt auch etwas weniger bereit sind, private Daten von

sich in sozialen Netzwerken preiszugeben. Auch wenn der Effekt der Sorgen auf das Verhalten nicht besonders groß ist, so kann das Paradoxon in seiner Extremform wiederlegt werden (Dienlin, 2019).

Auch die Ergebnisse von Dominique Facciorusso (2017), die mithilfe qualitativer Interviews untersucht, was 19- bis 29-Jährige unter Privatsphäre verstehen und wie sie das Konstrukt in ihrer alltäglichen Internetnutzung bewerten, zeigen, dass Sorgen der Befragten einen Effekt auf deren Verhalten im Netz haben können. In diesen Fällen berichten die Teilnehmer von Handlungsstrategien, um ihre Privatsphäre in spezifischen Situationen im Netz zu schützen. So wird etwa der spezifischen Sorge, dass andere Facebook-Nutzer negative Rückschlüsse auf die eigene Person ziehen könnten die Strategie entgegengesetzt, nur solche Daten preiszugeben, die ein möglichst positives Image der Person erzeugen (mehr dazu siehe Kapitel 3.2). Nutzer berichten aber auch von diffusen Sorgen und Ängsten bezüglich der Privatsphäre, die sie nicht richtig greifen und beschreiben können, weil ihnen die Zusammenhänge des Internets zu abstrakt und obskur erscheinen und die Folgen der Datenerfassung ihnen daher nicht verständlich sind (siehe hierzu auch Kapitel 3.3). Diese Sorgen können dem eigenen Verhalten im Netz demnach auch nicht zugeordnet werden (vgl. hierzu auch Schenk et al., 2012).

Identifizieren Studien dennoch ein widersprüchliches Nutzerverhalten, so kann das unterschiedliche Gründe haben (z.B. methodische Ursachen). Im Folgenden werden ohne Anspruch auf Vollständigkeit drei Faktoren erläutert, die diesen Widerspruch erklären können (für weitere Faktoren siehe Kokolakis, 2017).

(1.) Informationsasymmetrien

In der Regel herrscht bei den Nutzern eine sogenannte *Informationsasymmetrie*, die unter anderem erklären kann, warum diese Angebote nutzen bzw. Daten von sich preisgeben, die ihre Privatsphäre gefährden. So ist den meisten Nutzern in der Regel nicht bewusst, wer wann welche personenbezogenen Daten in welchem Umfang von ihnen erfasst und für welche konkreten Zwecke die Daten verwendet werden (Henne, 2014; Grimm und Krah, 2014; Facciorusso, 2017). Zudem haben Nutzer in der Regel keine Kenntnis über den Marktwert ihrer Daten (Facciorusso, 2017). Ohne das Wissen über die Erfassung und Verwertung von Daten, den Grad an Öffentlichkeit oder Privatheit einer Situation sowie die einem zustehenden Datenschutzrechte, fehlt die notwendige Basis, um autonom entscheiden und handeln zu können.

So stellen zum Beispiel Schenk und Kollegen (2012) in einer Studie zum Privatsphäreverständnis junger Onliner und den Einflussfaktoren auf deren Selbstoffenbarungsverhalten in sozialen Netzwerken fest, dass diese nicht verstehen, in welchem Verhältnis ihre Onlinenutzung zur eigenen Privatsphäre steht. Auch in der DIVSI-Studie (2014) ist für junge

Onliner nicht ersichtlich, was an formalen Daten wie zum Beispiel Name, Alter oder Wohnort schützenswert sein soll.[5]

Facciorusso (2017) zeigt ebenfalls, dass Onliner wenig über die Hintergründe und Möglichkeiten der Datenerfassung und -verarbeitung sowie über die damit verbundenen Risiken für die Privatsphäre wissen. So sehen zum Beispiel die meisten Befragten nur auf horizontaler (Peer-Group wie Freunde und Familie), nicht aber auf vertikaler Ebene (Institutionen wie Konzerne und Regierungen) eine Gefährdung ihrer Privatsphäre im Netz (siehe auch Livingstone, 2008). Vielen ist auch nicht bewusst, dass die Privatsphäre im Netz weitaus mehr umfasst als die Selbstdarstellung auf sozialen Netzwerken. Insgesamt zeigt sich, dass die Befragten die *Datenschutzproblematik im Netz als zu abstrakt und komplex* empfinden. So werden Daten meist losgelöst voneinander und nicht kumuliert als Nutzerprofil verstanden. Viele können sich auch nicht vorstellen, warum andere ein Interesse an ihren Daten haben sollten. Zudem werden meist nur die Daten als gefährdend für die Privatsphäre wahrgenommen, deren negative Auswirkungen unmittelbar und damit konkret erfahrbar bzw. greifbar sind. So sind sich die meisten bei der Nutzung bestimmter Angebote bzw. der Preisgabe bestimmter Daten nicht darüber bewusst, dass dies überhaupt ein Risiko für ihre Privatsphäre darstellt (Facciorusso, 2017).

Der Wissensmangel kann zum einen damit erklärt werden, dass die hierfür benötigten Informationen dem Nutzer zwar vorliegen, er deren Auslegung aber nicht wirklich versteht. Zum anderen wird der Aufwand sich mit den vorhandenen Informationen auseinanderzusetzen bzw. relevante zu beschaffen, im Sinne einer Kosten-Nutzen-Rechnung meist als zu hoch empfunden. In den Fällen scheint der unmittelbare Nutzen der Angebote im Vordergrund zu stehen, während die Suche nach relevanten Informationen zur Datenverarbeitung und die Auseinandersetzung mit diesen einen monetär, zeitlich sowie kognitiv zu hohen Aufwand darstellen. Die Kosten-Nutzen-Logik des in Kapitel 3.2 vorgestellten Privacy Calculus-Ansatz greift hier weniger in der Abwägung der Vorteile gegenüber der wahrgenommenen Risiken, sondern eher in der Abwägung des unmittelbaren Nutzens gegenüber dem Aufwand, sich über die mit der Nutzung verbundenen Risiken fundiert zu informieren.

(2.) Kognitive Wahrnehmungsverzerrung

Betrachtet man Untersuchungen zum tatsächlichen Entscheidungsverhalten, so zeigt sich weiterhin, dass Menschen ihre Urteile nicht immer anhand logisch-rationaler Regeln treffen. Vielmehr zeigen sich in der Entscheidungsfindung oft Verzerrungen, die auf bestimmte Heuristiken deuten. Heuristiken sind geistige Verknüpfungen, die unser Verhalten steuern. Sie erlauben, komplexe Sachverhalte zu reduzieren, um zu schnellen und effizienten bzw. persönlich akzeptierten Urteilen und Lösungen zu kommen, ohne großen kognitiven Aufwand betreiben zu müssen. Die Ressourcen Zeit und mentale Verarbeitungskapazität sind

5 Hier wurde die allgemeine Internetnutzung sowie die Haltung von 9- bis 24-Jährigen zum Thema Privatsphäre im Netz und den damit verbundenen Themen Vertrauen und Sicherheit in einem zweistufigen Verfahren untersucht.

begrenzt. Heuristiken sind daher notwendig, um das Gehirn kognitiv zu entlasten, da es nicht alle für die Entscheidung relevanten Informationen berücksichtigen kann (Kuzmanovic, 2016).

Vor dem Hintergrund verzerrter Entscheidungsfindungen stellt hier der *Optimism Bias* (dt.: optimistische Verzerrung) einen interessanten Erklärungsansatz für das Privacy Paradox dar. Der Fehlschluss zeigt sich darin, dass Menschen dazu neigen, das eigene Risiko für unerwünschte Ereignisse in der Zukunft stark zu unterschätzen, während die Wahrscheinlichkeit für erwünschte Ereignisse eher überschätzt wird (ebd.). Bezogen auf die Onlinenutzung: Während etwa bei der Informationssuche die unmittelbaren Vorteile durch Google überbewertet werden, werden die mit der Nutzung verbundenen Langzeit-risiken eher unterschätzt.[6]

Verwandte Ansätze im Sinne einer kognitiven Wahrnehmungsverzerrung im Kontext der Mediennutzung finden sich im *Third Person Effect*, der 1983 erstmals von Philipps Davison beschrieben wird. So heißt es: „people will tend to overestimate the influence that mass communications have on the attitudes and behavior of others." (Davison, 1983, S. 3). Individuen haben demnach die Auffassung, dass andere Menschen (*third person*) stärker von medialen Inhalten beeinflusst werden als sie selbst (*first person*). Dies trifft vor allem auf Inhalte negativer bzw. unerwünschter Art zu wie etwa Gewalt in den Medien, Pornografie oder Werbung. Debatin et al. (2009) sehen im Third Person Effect einen möglichen Erklärungsansatz für das Privacy Paradox. In einer Studie zur Facebook-Nutzung stellen sie fest, dass die Befragten potentielle Risiken hinsichtlich der Verletzung der Privatsphäre vor allem anderen zuschreiben und nicht sich selbst. Teilnehmer, deren Privatsphäre online schon einmal verletzt wurde, berichten dabei eher von Anpassungen ihrer Privatsphäre-Einstellung als jene, die nur davon gehört haben, dass andere bereits schlechte Erfahrungen gesammelt haben (Debatin et al., 2009). Erfahrung scheint demnach ein wichtiger Einflussfaktor auf die Wahrnehmungsverzerrung zu sein, die eine Korrektur des Verhaltens im Netz zur Folge haben kann.

Auch Facciorusso (2017) identifiziert solche Wahrnehmungsverzerrungen, die erklären könnten, warum Nutzer bestimmte Sorgen äußern und gleichzeitig Daten von sich preisgeben, die ihre Privatsphäre dort gefährden. Auch hier bewerten alle Befragten die mit der Datenpreisgabe unmittelbar verbundenen Vorteile im Sinne des Optimism Bias höher als die damit auf lange Sicht verbundenen Risiken für die Privatsphäre. Viele berichten auch im Sinne des Third Person Effects, dass vor allem andere aufgrund ihres Verhaltens im Netz von Privatsphärerisiken betroffen sind. So bemerkt etwa eine 29-Jährige, die einige datenschutzkritische Dienste nutzt:

> „Ja weil ich ja schon darauf achte, was ich preisgebe und weil das so wenig ist, was man da finden kann, deswegen mache ich mir darum jetzt nicht so die Sorgen. Also wenn ich mein komplettes Leben auf Facebook preisgeben würde, so wie andere, dann schon. [...] Für die wäre

6 Für mehr Informationen zu den mit Google verbundenen Risiken siehe auch Facciorusso (2013).

> es vielleicht wichtig, dass das alles besser geschützt ist. Aber ich mache so was eh nicht.“ (Facciorusso, 2017, S. 67f.)

Die Erfahrung spielt auch hier eine entscheidende Rolle (ebd.). So berichten Onliner, vor allem dort potentielle Risiken in Betracht zu ziehen und sehr vorsichtig im Umgang mit ihren Daten zu sein, wo ihre eigene Privatsphäre oder die von Menschen aus ihrem sozialen Umfeld bereits verletzt worden ist.

Die Studie identifiziert eine weitere Facette der Wahrnehmungsverzerrung, die in gewissem Sinne dem Third Person Effect zugeordnet werden kann. So ist die Aussage, dass man vor anderen *nichts zu verbergen* und daher auch nichts zu befürchten habe (siehe auch Solove, 2007; Paine et al., 2007; Marwick und Hargittai, 2018), ein beliebtes Argument mit dem die Befragten ebenfalls ihre Sorgen abschwächen. Dabei geht es den Onlinern in erster Linie darum, dass sie anhand ihrer Daten für nichts Unrechtes oder Strafbares belangt werden können: „Da ist nirgendwo ein Bankraub auf Video, weswegen es jetzt Stress geben könnte. Von daher.“ (Facciorusso, 2017, S. 68). Denn mit der Preisgabe bestimmter Daten wird vor allem befürchtet, dass andere etwas Schlechtes oder aufgrund fehlender Informationen oder eines unpassenden Kontextes gar etwas Falsches von ihnen denken könnten, was letztlich zu einem negativen *Image* führt. Obwohl die Befragten an anderer Stelle bekräftigen, wie wichtig ihnen der Privatsphärenschutz ist, wird innerhalb dieser Argumentation Kritikern der Datenerfassung latent unterstellt, dass diese etwas zu verbergen hätten.

Auch Michael Adorjan und Rosemary Ricciardelli zeigen in einer qualitativen Studie (2018) zur Wahrnehmung und Erfahrung mit Cyber-Risiken, dass jungen Menschen ihre Privatsphäre im Netz nicht egal ist, diese aber dennoch eine Gleichgültigkeit in Form des Nothing-to-Hide-Arguments ausdrücken. Diese Haltung, die laut den Autoren mit dem Teenagealter sogar zu wachsen scheint, wird als pragmatische Anpassung an eine öffentlichen Debatte interpretiert, in der die Verletzung der Privatsphäre als unvermeidlich und deren Schutz als unmöglich betrachtet sowie dem Individuum eine zu hohe Selbstverantwortung zugeschrieben wird (ebd.).

(3.) Habitualisierung der Onlinenutzung

Eine habitualisierte Nutzung bestimmter Online-Angebote und ein damit einhergehendes Vertrauen könnten zusätzlich erklären, warum Bedenken relativiert werden bzw. Sorgen und Ängste nur einen geringen Effekt auf das Verhalten der Nutzer haben. Denn Routinen und Gewohnheiten zeichnen sich allgemein durch eine kognitive Passivität und Non-Selektivität aus. Übertragen auf die Mediennutzung heißt das, dass Nutzer ihre Selektionsentscheidungen mit nur wenig kognitivem Aufwand fällen. Hat sich in der Vergangenheit eine bestimmte Entscheidung oder Handlung bewährt, so speichert das Gehirn den Vorgang ab und ruft ihn automatisch auf, sobald die Bedingungen dafür vorliegen (Schweiger, 2007). So sind etwa die tägliche Nutzung von Instant-Messengern wie WhatsApp oder die Suche über Google nicht als bewusste, sondern als habitualisierte Vorgänge zu sehen. Solche Rou-

tinen entlasten uns kognitiv und ermöglichen unter nur minimalem Aufwand, schnelle und für uns effiziente Entscheidungen treffen zu können (ebd.).

Da sich das Internet für viele Nutzer heute zum integralen Bestandteil ihres Alltags entwickelt hat, wird angenommen, dass die regelmäßige Nutzung bestimmter Angebote ebenfalls anhand gewisser Alltagsroutinen erfolgt (Debatin et al., 2009). So identifizieren Sabine Trepte und Leonard Reinecke im Kontext von Web 2.0-Angeboten sogenannte „Desensibilisierungs- bzw. Habitualisierungstendenzen", die bei häufiger Nutzung eintreten und die Hemmschwelle zur Datenpreisgabe senken (Trepte und Reinecke, 2009, S. 36f.). Auch Monika Taddicken identifiziert einen „Desensibilisierungseffekt", demnach Personen bei regelmäßiger Nutzung einzelner Angebote besonders viele und vor allem sensible Daten von sich preisgeben (Taddicken, 2011, S. 286). Dies wird darauf zurückgeführt, dass der Fokus auf nur wenige Anwendungen mit einer Bindung und *Vertrautheit* zu diesen einhergeht, was letztendlich zu einer erhöhten Bereitschaft zur Selbstoffenbarung führt (ebd.). Auch Catherine Dwyer und Kollegen (2007) zeigen in einer qualitativen Studie, dass Nutzer, die angeben in Facebook ein größeres Vertrauen zu haben als in andere genutzte Netzwerke, dort auch im Vergleich mehr Daten von sich preisgeben.

Dem schließen sich die Ergebnisse von Facciorusso (2017) an. So sind vor allem die Alltagskommunikation über Instant-Messenger, die Informationssuche über Google, die Selbstdarstellung in sozialen Netzwerken, die Unterhaltung über Audio- und Videoplattformen sowie Transaktionen im Netz längst zur Gewohnheit geworden und bei den Befragten fest im Alltag integriert. Im Rahmen der Selbstauskunft wird deutlich, dass in diesen Bereichen den besonders häufig genutzten Anwendungen zum Teil ein großes Vertrauen entgegen gebracht wird, was den Datenschutz anbelangt. Selbst diejenigen, die angeben sich möglicher Datenschutzrisiken bewusst zu sein und auf ihre Privatsphäre zu achten, geben bei regelmäßig genutzten Angeboten besonders viele und zum Teil sehr sensible Daten von sich preis. Ein 28-Jähriger bemerkt: „Auch wenn das dem widerspricht, was ich vorhin gesagt habe. Zu den sensiblen Daten zählt auch, wo man sich aufhält und was man da macht und das kann man auf WhatsApp auch alles rausfiltern. Aber man empfindet das da irgendwie nicht so drastisch." (Facciorusso, 2017, S. 69).

Insgesamt zeigt sich, dass Angebote, deren Nutzen sich bewährt hat, meist automatisch wiederverwendet und datenschutztechnisch nicht permanent neu geprüft werden. Demnach beeinflussen besonders die *Erfahrung* und das daraus gewonnene *Vertrauen* die Habitualisierung der Onlinenutzung (Facciorusso, 2017). Ein 26-Jähriger, der im Vergleich zu den anderen Befragten viel zum Datenschutz im Allgemeinen weiß, erklärt zum Beispiel: „Gmail ist so der Account, wo sage ich mal die ganzen wichtigen privaten Dinge durchgehen, weil es da noch in Ordnung ist. [...] Da hatte ich bisher keine Probleme." (ebd.).

Zudem zeigt sich die kognitive Passivität bzw. habitualisierte Onlinenutzung auch darin, dass bestimmte Angebote häufig ohne konkretes Ziel und rein zur *kognitiven Entlastung* genutzt werden. So berichtet eine 24-Jährige, dass sie oft online ist, um „die Welt außen rum zu vergessen. Einfach nur durchswitchen [...] nicht groß nachdenken. Sondern sich

einfach mit etwas beschäftigen, wo man den Kopf jetzt nicht so sehr benutzen muss.“ (ebd., S. 71).

3.2 Die Privacy Calculus-Theorie

Auch ein zweiter Forschungsstrang, die sogenannte *Privacy Calculus-Theorie* befasst sich mit möglichen Faktoren, die das Privatsphäreverhalten der Nutzer beeinflussen. Hier wird angenommen, dass Menschen in einer Art Risiko-Nutzen-Kalkulation Vor- und Nachteile gegeneinander abwägen, die mit der Datenpreisgabe im Netz verbunden sind. Überwiegen demnach die Vorteile, so sind diese trotz der wahrgenommenen Risiken bereit, den Verlust ihrer Privatsphäre in diesem Bereich zu akzeptieren (Trepte et al., 2017; Kokolakis, 2017; Li, Sarathy, & Xu, 2010; Blumberg, Möhring, & Schneider, 2009). Überwiegen die Risiken sind diese nicht zur Datenpreisgabe bereit.

Während das Paradoxon also postuliert, dass die Sorgen und Ängste der Menschen keinen Effekt auf deren Privatsphäreverhalten im Netz haben, argumentiert der Privacy Calculus-Ansatz, dass diese sowie die mit der Datenpreisgabe verbundenen Vorteile durchaus das Verhalten beeinflussen (vgl. Dienlin, 2019). Das Selbstoffenbarungsverhalten im Netz wird hier also nicht als paradox gesehen, sondern als Ergebnis einer rationalen bzw. bewussten Entscheidungsfindung.

Der Effekt von Sorgen auf das Nutzungsverhalten zeigt sich in Form von individuellen *Handlungsstrategien zum Schutz der Privatsphäre* (Facciorusso, 2017). Demnach ließe sich erklären warum Menschen online Angebote nutzen, obwohl sie damit Risiken für ihre Privatsphäre verbinden. Zum einen wird der damit verbundene Nutzen höher als das Risiko bewertet und zum anderen versuchen die Nutzer den Risiken (in ihrem Ermessen) entgegen zu wirken. So können sie zum Beispiel darauf achten, besonders wenig Daten von sich preiszugeben bzw. nur solche zu offenbaren, die für das Funktionieren des Dienstes tatsächlich notwendig sind oder mit dessen Missbrauch sie (theoretisch) leben könnten. Daten können zudem unvollständig, anonymisiert oder unkorrekt angegeben werden, um einer Identifikation vorzubeugen. Auch technische Maßnahmen wie das Anpassen von Datenschutz-Einstellungen, Löschen von Cookies, Installieren von Anti-Virusprogrammen können dem Nutzer ein Gefühl der Kontrolle über seine Privatsphäre geben (Blumberg, Möhring, & Schneider, 2009). Das bewusste Zurückhalten der Daten bzw. die Nichtnutzung stellt die wohl konsequenteste Strategie zum Schutz der Privatsphäre dar.

Bei der Kosten-Nutzen-Analyse gibt es Faktoren, die die *Wahrnehmung von Risiken minimieren* können (Facciorusso, 2017). Das *Vertrauen* bezieht sich vor allem auf die institutionelle Ebene (Konzerne und Regierungen). So zeigen die Ergebnisse von Facciorusso (2017), dass einige Befragte bei Anbietern wie Amazon, Google, Apple oder Facebook darauf vertrauen, dass ihre dort hinterlegten Daten vor Missbrauch geschützt oder ihre Daten an Dritte nicht weitergegeben werden (ebd.). Ein 19-Jähriger, der sehr viele datenschutzkritische Angebote nutzt und freiwillig viele Daten von sich preisgibt, erläutert zum Beispiel: „Und was auch dazu führt, dass ich nur Apple-Produkte benutzte ist, dass ich Apple ver-

traue, weil sie auch bei Stiftung-Warentest für Sicherheit und Privatsphäre auf den Top-Plätzen sind.“ Während häufig genutzten Plattformanbietern vertraut wird, wird eher in anderen Nutzern (auf Facebook) die größte Gefahrenquelle gesehen, wenn es um die Verletzung der Privat-sphäre geht (ebd., S. 61f.; siehe auch Schenk et al., 2012). Auch die Faktoren Informationsasymmetrie, habitualisierte Onlinenutzung (hier spielt Vertrauen auch eine Rolle) und kognitive Wahrnehmungsverzerrung (Kapitel 3.2), können die wahrgenommenen Risiken auf Seiten der Nutzer senken.

Zum anderen gibt es Faktoren, die die *Wahrnehmung von Risiken maximieren* können. So berichten Befragte aufgrund von *negativen Erfahrungen* bestimmte Daten von sich online nicht mehr preiszugeben bzw. bestimmte Dienste nicht mehr zu nutzen (Facciorusso, 2017). Eine 19-Jährige erklärt etwa auf Facebook jahrelang Opfer von Hasskommentaren gewesen zu sein und dort seither die Preisgabe bestimmter Inhalte zu vermeiden. Umgekehrt räumen die meisten Teilnehmer ein, sensible Daten trotz bestehender Risiken oft von sich preis-zugeben bzw. bestimmte Dienste zu nutzen, weil sie damit bisher weder direkt noch indirekt negativen Erfahrungen gesammelt haben: „Vielleicht weil mir noch nichts passiert ist. Also dass mein Account gehackt wurde oder so. Ich weiß jetzt auch von noch niemandem, dem so was in der Art mal passiert wäre.“ (ebd., S. 61). Demnach scheinen besonders die negativen Erfahrungen der Befragten deren Risikowahrnehmung und die Wahrscheinlichkeit von Handlungsstrategien zu erhöhen. Auch Debatin und Kollegen (2009) haben in einer Studie zur Facebook-Nutzung bereits zeigen können, dass Nutzer, deren Privatsphäre dort schon einmal verletzt wurde, eher dazu neigen, ihre Privatsphäre-Einstellung zu ändern.

Um das Selbstoffenbarungsverhalten von Nutzern anhand des Kosten-Nutzen-Kalküls zu verstehen, muss hier ein weiterer wichtiger Punkt beachtet werden. So lassen sich *individuelle Stufen des Privaten* differenzieren, die ebenfalls das Verhalten beeinflussen (siehe hierzu auch Paine et al., 2007; Livingstone, 2008; Schenk et al., 2012; Wolff, 2013; Turow et al., 2015; Marwick und Hargittai, 2018). Facciorusso (2017) greift dies im sogenannten *Schalenmodell der Privatsphäre* auf, das ohne Anspruch auf Vollständigkeit zu erklären versucht, wie die unterschiedliche Datenpreisgabe von Menschen im Netz zustande kommt. Denn die Ergebnisse ihrer Studie zeigen: Es kann sich zum einen je nach Person (P) und Kontext unterscheiden, welche Daten als privat gelten (P 1: Gehalt ist privat; P 2: Gehalt ist nicht privat). Zudem können die von einer Person als privat erachteten Daten unterschiedlich gewichtet werden (P 1: Gehalt und Kontostand sind privat, Kontostand ist privater als Gehalt).

Dem Modell nach ist jeder Mensch von einer Sphäre umgeben, die in Schalen abgestuft bis in das Innerste einer Person reicht – den *Kern der Privatsphäre*. Gibt jemand private Daten von sich preis, gilt: (1.) Mit dem zugeschriebenen Grad an Privatheit der Daten steigt bzw. sinkt das Bedürfnis nach deren Schutz und Kontrolle. Demnach muss in der Risiko-Nutzen-Kalkulation eines Individuums der Nutzen mit zunehmendem Privatheitsgrad der Daten steigen, damit es diese bewusst preisgibt. (2.) Somit kann es auch Daten geben, die gegenüber einer Kalkulation immun sind, da das Individuum diese nahe am Kern des Priva-

ten verortet. Das heißt unabhängig von den damit verbundenen Vorteilen werden diese Daten nicht bewusst preisgegeben. (3.) Nahe am Kern werden vor allem jene Daten verortet mit deren Preisgabe das Individuum negative Folgen wie etwa monetäre, physische oder psychische Schäden befürchtet, besonders wenn dadurch ein Imageschaden verursacht werden kann. Während monetäre Schäden insgesamt eher als reparabel bewertet werden, gelten vor allem physische, besonders aber psychische Schäden als irreparabel.

3.3 Der Resignationsansatz

Um das scheinbar paradoxe Privatsphäreverhalten besser zu verstehen, soll ein weiterer Forschungsstrang vorgestellt werden, der hier Resignationsansatz genannt wird. Denn neben den Privatsphäre-Sorgen und den mit der Daten-preisgabe verbundenen Vorteilen gibt es auch weitere Faktoren, die das Verhalten der Nutzer erklären können.

Die Kommunikationswissenschaftler Joseph Turow und Kollegen befragen in einer repräsentativen Telefonumfrage (2015) amerikanische Internetnutzer ab 18 Jahren zu deren Verhalten im Onlinehandel und kritisieren in diesem Kontext das Kosten-Nutzen-Argument. Demnach sei die Behauptung der Konzerne falsch, dass die Mehrheit der Amerikaner Informationen über sich preisgibt, weil für sie die damit verbundenen Vorteile überwiegen. Die Studie zeigt, dass die meisten Amerikaner ihre Daten kontrollieren wollen, gleichzeitig aber davon überzeugt sind, dass dies nicht möglich ist. So zeigt sich, dass mehr als die Hälfte der Befragten, die sich in einem Szenario bereit zeigen ihre Daten über ihr Einkaufsverhalten für einen Rabatt preiszugeben (selbst wenn sie wissen, dass sich daraus Rückschlüsse auf deren Konsumverhalten, Lebensstil, Gesundheitszustand, Demografie oder Ethnie ziehen lassen), Resignation empfinden wenn es um die Kontrolle ihrer Daten geht. Entgegen bisheriger Annahmen zeigt sich zudem, dass die Bereitschaft der Datenpreisgabe nicht mit einem Mangel an Wissen erklärt werden kann. Denn die Befragten, die am meisten über die Datenschutzpraktiken im Online-Handel wissen, neigen eher zur Resignation, weil sie ihre Bemühungen für sinnlos halten. Daher gehen die Autoren davon aus, dass die Datenpreisgabe der Amerikaner weniger aufgrund der Vorteile im Sinne eines Kosten-Nutzen-Kalküls erfolgt, sondern vielmehr aufgrund eines resignierten Verhaltens.

Eine ähnliche Haltung zur Privatsphäre wird in der Online-Forschung unter den Begriffen *Privacy Fatigue* (Keith et al., 2014; Choi, Park und Jung, 2017), *Privacy Cynicism* (Hoffmann, Lutz und Ranzini, 2015) oder auch *Online Apathy* (Hargittai und Marwick, 2016) untersucht.

Choi, Park und Jung (2017) lehnen den Begriff *Privacy Fatigue* an bestehende Fatigue-Theorien an. Demnach ist Fatigue ein subjektives unangenehmes Gefühl der Müdigkeit, das in einem Rückzug münden kann. Ein entscheidendes Merkmal bei Menschen mit Ermüdung ist die Unfähigkeit, Entscheidung treffen zu können, vor allem dann wenn sie bei ihrer Entscheidungsfindung mit mehr Dingen zu tun haben, als sie im Entscheidungsprozess bewältigen können. So können Nutzer etwa von den Optionen möglicher Datenschutzeinstellungen überwältigt sein und auch Schwierigkeiten haben das Verwaltungssystem für den

Datenschutz als solches zu verstehen. Entscheidend ist, dass Onliner mit Privacy Fatigue den Aufwand bei der Entscheidungsfindung minimieren wollen und daher dazu neigen, den einfachsten Weg zu wählen, indem sie zum Beispiel die Standardoption der Datenschutz-Einstellung akzeptieren. In einer Online-Befragung von 324 südkoreanischen Internetnutzern (im Alter von 20 bis 59 Jahren) zeigen die Autoren, dass Privacy Fatigue einen größeren Einfluss auf das Verhalten der Nutzer hat als deren Privatsphäresorgen. Während Menschen mit einem hohen Grad an Privatsphäre-Sorgen eher dazu neigen Maßnahmen zum Schutz ihrer Privatsphäre zu ergreifen, neigen Menschen mit einem hohen Grad an Privacy Fatigue eher dazu, nichts zum Schutz ihrer Daten zu unternehmen. Der Bildungsgrad der Befragten war insgesamt überdurchschnittlich hoch.

Mit dem Begriff *Privacy Cynicism* beschreiben Hoffmann, Lutz und Ranzini (2015) eine Haltung, demnach Nutzer Unsicherheit, Ohnmacht und Misstrauen empfinden, wenn es darum geht wie Plattform-Anbieter mit privaten Daten umgehen. Dies führt zu Zynismus bzw. zu einem weniger vorsichtigen Umgang mit den Daten im Netz. Denn auch wenn Nutzer den Anbietern nicht vertrauen und Bedrohungen für ihre Privatsphäre wahrnehmen, rechtfertigen sie ihre Nutzung mit der Überzeugung, dass es außerhalb ihrer Macht liegt ihre Daten effizient zu schützen. Die Autoren interpretieren diese Haltung als kognitiven Bewältigungsmechanismus, der es vor allem Nutzern mit niedriger Kompetenz und Selbstwirksamkeit erlaubt, die Vorteile eines gewünschten Dienstes ohne kognitive Dissonanz zu nutzen. Das Konzept untermauern die Autoren empirisch mithilfe von Fokusgruppen-Diskussionen (insgesamt 96 Teilnehmer), die nach dem Sinus-Milieu rekrutiert wurden. Ein interessantes Ergebnis, das in der Diskussion jedoch nicht erneut aufgegriffen wird: Ein hoher Grad an Bildung scheint nicht zwangsläufig zu weniger Zynismus zu führen. So berichten auch erfahrene Nutzer von der Machtlosigkeit die Daten online schützen zu können.

Hargittai und Marwick (2016) befragen mithilfe von Fokusgruppen-Gesprächen insgesamt 40 Teilnehmer zwischen 19 und 35 Jahren zur Nutzung sozialer Netzwerke. Die Ergebnisse zeigen, dass sich die Nutzer um ihre Privatsphäre sorgen, im Sinne einer Kosten-Nutzen-Logik die Preisgabe ihrer Daten abwägen und dort sogar mehr oder weniger wirksame Strategien zum Schutz der Privatsphäre anwenden. Zudem drücken die Nutzer ein Gefühl von Apathie aus, indem die Verletzung der Privatsphäre als unvermeidlich und die Nicht-Nutzung sozialer Netzwerke als keine Option betrachtet wird, da die damit verbundenen Nachteile als zu hoch gelten. Dennoch wenden die Nutzer diverse kreative Handlungsstrategien an, wohlwissend dass diese ihre Daten nicht ausreichend schützen, was die Autoren als „resigned pragmatism" beschreiben (S. 3752). Wenn Nutzer also verstehen, dass sie ihre Daten nicht ausreichend kontrollieren können, ziehen sie sich beim Teilen der Daten auf bestimmte Weise zurück (Selbstzensur, vgl. hierzu auch Chilling Effect, Kapitel 2.2). Die Autoren interpretieren das Verhalten als „pragmatic response" auf die vernetze soziale Umgebung der Nutzer, derer sie sich nicht entziehen können (ebd.).

Auch Facciorusso (2017) identifiziert Resignation als einen wichtigen Faktor, der auf das Verhalten zu wirken scheint. Auch dort berichten die Teilnehmer von einem *Gefühl der Machtlosigkeit* ihre Daten nicht schützen zu können, einer *Unsicherheit* nicht zu wissen

was mit den Daten genau geschieht sowie von einem *Konformitätszwang* sich der Datenpreisgabe aus beruflichen und privaten Gründen in der Regel nicht entziehen zu können. So berichtet ein Befragter: „Ich bin bei WhatsApp weg und habe gesagt: Nein, ich will es nicht mehr nutzen. Ging gar nicht. [...] Ich war raus in meinem Kreis. Also habe ich mir im Endeffekt wieder WhatsApp installiert, weil jeder gemeckert hat und das ging mir dann irgendwann auf den Sack." (ebd., S. 76). Auch an anderer Stelle berichten Nutzer einem sozialen Druck ausgesetzt zu sein: „Sonst dürftest du [...] quasi kaum Dinge machen, die alle anderen machen. [...] Du gehörst dann halt nicht zu dem Strom, der mitschwimmt." (ebd.; siehe auch *wahrgenommene subjektive Norm* bei Dienlin, 2019). Auch hier stellt der Verzicht aufgrund zu hoher Nachteile für viele *keine Alternative* dar, besonders bei häufig genutzten Anwendungen. Viele Nutzer berichten daher von einem Gefühl der Resignation, das sich zum einen in Form eines bewussten Zurückhaltens der Daten aber auch in der Preisgabe der Daten äußern kann. Interessant ist zudem, dass auch hier das *Wissen* zum Datenschutz mit Resignation zu korrelieren scheint: So berichten vor allem diejenigen resigniert zu sein, die viel über die Hintergründe und Möglichkeiten der Datenerfassung und -verwertung wissen.

4. Privatsphäre 2.0 – (noch) kein Ende in Sicht.

Das scheinbare Ende der Privatsphäre bestimmt seit längerem die breite Debatte und spannt sich zwischen den beiden Extremen „totale Überwachung" als Befürchtung auf der einen und „totale Transparenz" als Forderung auf der anderen Seite auf. Neben Regierungen und IT-Konzernen scheint eine zunehmende Gefahr vom Nutzer selbst auszugehen, indem dieser immer mehr onlinebasierte Angebote nutzt und Zeit im Netz verbringt. Nutzern wird in dem Zusammenhang oft ein mangelndes Problembewusstsein im Umgang mit ihren Daten im Netz nachgesagt (Horn, 2013; Wewer, 2013; Bolz, 2012). Wäre der mutmaßliche Wandel hin zu einer „privacy is no longer a social norm"-Kultur tatsächlich vollzogen, so dürften diese kein Problem mit der Offenlegung ihrer privaten Daten haben. Studien zeigen jedoch, dass Menschen ihre Privatsphäre wichtig ist und sie sich um ihren Schutz sorgen, gleichwohl sie online Daten von sich preisgeben, die diese gefährdet (Barnes, 2006; Trepte/Masur und Pape, 2015; Turow et al., 2015; Facciorusso, 2017; Marwick und Hargittai, 2018).

Ziel des Beitrags war es daher herauszufinden, wie sich solch ein scheinbar widersprüchliches Privatsphäreverhalten im Netz erklären lässt. Um sich einer Antwort zu nähern wurden hier drei Bereiche aus der Privatsphärenforschung vorgestellt, die sich mit dem Nutzerverhalten online befassen.

Das ***Privacy Paradox*** beschreibt die Diskrepanz, dass sich Menschen um den Schutz ihrer Privatsphäre sorgen und gleichzeitig online jede Menge private Daten von sich preisgeben. Die Privatsphäresorgen der Nutzer scheinen also keinen Effekt auf deren tatsächliches Verhalten im Netz zu haben. Neben Studien, die das Phänomen bestätigen, gibt es auch zunehmend jene, die es wiederlegen bzw. postulieren, dass es in seiner Extremform so nicht existiert (Dienlin, 2019). So konnten Baruh und Kollegen (2017) in einer ersten Meta-

Studie zum Paradox zeigen, dass vermehrte Sorgen um die Privatsphäre auch mit einem durchschnittlich vorsichtigeren Umgang mit den Daten einhergehen.

Zudem kann der Widerspruch, der durchaus existieren kann, anhand diverser Faktoren erklärt werden, wovon drei exemplarisch vorgestellt wurden. So existieren bei den Nutzern sehr oft *(1.) Informationsasymmetrien*, die eine rationale Entscheidungsfindung bzgl. der Datenpreisgabe erschweren bzw. unmöglich machen. Denn viele Nutzer sind sich den Hintergründen und Möglichkeiten der Erfassung, Analyse und Verwertung ihrer Daten und damit den Risiken einer Preisgabe nicht bzw. nur zum Teil bewusst. Gründe für den Mangel an Wissen können sowohl die Komplexität und Abstraktheit des Themenfelds sein, die sehr oft dazu führt, dass sich Nutzer im Sinne einer Kosten-Nutzen-Kalkulation gegen den Aufwand der Wissensaneignung und für den unmittelbare Nutzen entscheiden. Und auch wenn Nutzern Informationen zur Verfügung stehen, so kann es sein, dass sie diese nicht auf ihren Fall auslegen und damit nicht verstehen können.

Es können bei den Nutzern zudem *(2.) kognitive Wahrnehmungsverzerrungen* bestehen, die erklären, dass der Prozess der Entscheidungsfindung nicht immer anhand logisch-rationaler Regeln stattfindet. So stufen viele den unmittelbaren Vorteil, der ihnen durch die Nutzung des jeweiligen Dienstes entsteht höher ein als die damit verbundenen Langzeitrisiken für die Privatsphäre (*Optimism Bias*). Zudem glauben auch viele, dass eher andere durch ihr Onlineverhalten den Schutz ihrer Privatsphäre gefährden (*Third Person Effect*). Besonders verbreitet ist auch die Annahme, dass man durch die Datenerfassung nichts zu verbergen und damit auch nichts zu verlieren habe (*Nothing to Hide*). Hier argumentieren Nutzer, dass es online keine Daten gibt, die (gesetzlich) gegen sie verwendet werden und damit ihr Image beschädigen können. Gegnern und Kritikern der Datenerfassung wird hingegen latent unterstellt, dass diese etwas zu verbergen haben. Diese Haltung bewerten Adorjan und Ricciardelli (2018) als Anpassung an eine Debatte, in der der Schutz der Privatsphäre fast unmöglich und die hohe Eigenverantwortung den Nutzer zu überfordern scheint.

Auch die *(3.) habitualisierte Online-Nutzung* bestimmter Angebote und ein damit einhergehendes *Vertrauen* können zusätzlich erklären, warum Bedenken relativiert und das Verhalten nicht angepasst werden. Angebote, die regelmäßig genutzt werden und deren Nutzen sich bewährt hat, werden meist automatisch bzw. routiniert wiederverwendet und datenschutz-technisch nicht permanent neu geprüft. Da Routinen allgemein von geringem kognitiven Aufwand und Non-Selektivität gekennzeichnet sind, können diese zu einem unkritischeren bzw. unvorsichtigeren Umgang mit den Daten im Netz führen. Haben Nutzer allerdings direkt oder indirekt *negative Erfahrungen* mit einem bestimmten Angebot erfahren, kann sich dies auf die Habitualisierung auswirken.

Auch der ***Privacy Calculus-Ansatz*** befasst sich mit möglichen Faktoren, die das Verhalten von Internetnutzern beeinflussen. Der Ansatz geht davon aus, dass Menschen in einer Art Risiko-Nutzen-Kalkül die Vor- und Nachteile der Datenpreisgabe gegeneinander abwägen. Überwiegen die Vorteile, so sind diese trotz Sorgen bereit, ihre Daten preiszugeben und die Gefährdung ihrer Privatsphäre zu riskieren. Im Gegensatz zum Privacy Paradox lautet hier also das Argument, dass die Sorgen sowie die mit der Datenpreisgabe verbunde-

nen Vorteile das Verhalten der Nutzer beeinflussen können. Der Effekt der Sorgen kann sich in Form von *Handlungsstrategien zum Schutz der Privatsphäre* äußern (Facciorusso, 2017). So können Nutzer etwa technische Maßnahmen ergreifen, sparsam mit ihren Daten umgehen oder auch ein Angebot nicht nutzen. Innerhalb der Kosten-Nutzen-Analyse gibt es zudem Faktoren, die die *Wahrnehmung von Risiken minimieren* (Vertrauen, Informationsasymmetrien, kognitive Wahrnehmungsverzerrung, habitualisierte Onlinenutzung) sowie *maximieren* können (negative Erfahrungen) (ebd.). Wichtig ist zudem, dass es zum Teil große Unterschiede geben kann, welche Daten der Einzelne als privat empfindet und wie stark er die als privat erachteten Daten gewichtet. Diese Kategorisierung und Gewichtung ist nicht starr, sondern kann sich je nach Kontext und Erfahrung der Nutzer verändern (siehe *Schalenmodell der Privatsphäre*).

Zuletzt wurde der ***Resignationsansatz*** vorgestellt. So berichten Nutzer oft von einem Gefühl der Machtlosigkeit, weil sie glauben ihre Daten online nicht schützen zu können, auch dann nicht, wenn sie dort Maßnahmen zum Schutz anwenden. Zudem frustriert viele nicht wirklich zu verstehen, was mit ihren Daten genau gemacht wird.

Dieses Gefühl von Unsicherheit, Misstrauen und Machtlosigkeit wird in der Online-Forschung unter den Begriffen *Privacy Fatigue* (Keith et al., 2014; Choi, Park und Jung, 2017), *Privacy Cynicism* (Hoffmann, Lutz und Ranzini, 2015) oder auch *Online Apathy* (Hargittai und Marwick, 2016) aufgegriffen. So können diese Gefühle zu einem Ermüdungszustand führen, der es Nutzern unmöglich macht rational Entscheidungen bzgl. der Privatsphäre zu treffen, vor allem dann, wenn viele Faktoren zu beachten sind (Choi, Park und Jung, 2017). In solchen Situationen neigen Nutzer dann eher dazu, den kognitiven Aufwand zu minimieren und den einfachsten Weg zu gehen (ebd.).

Diese Ermüdung bzw. Resignation kann in zwei Richtungen verlaufen: Im bewussten Zurückhalten der Daten bzw. Selbstzensur (vgl. Hargittai und Marwick, 2016; Facciorsso, 2017) oder der Datenpreisgabe (vgl. Turow et al., 2015; Choi, Park und Jung, 2017; Facciorusso, 2017). Eine Studie zeigt sogar, dass Resignation einen größeren Effekt auf das Nutzerverhalten hat als die Privatsphäresorgen. Demnach führt ein hoher Grad an Sorgen eher zu Handlungsstrategien zum Datenschutz als ein hoher Grad an Resignation (Choi, Park und Jung, 2017). Weiterhin ist eine erhöhte Bereitschaft der Datenpreisgabe laut manchen Studien nicht zwingend mit einem Mangel an Wissen zu erklären. Demnach neigen Nutzer, die viel zum Datenschutz wissen und im Grunde über die Werkzeuge einer (annähernd) akkuraten Kosten-Nutzen-Kalkulation verfügen, eher zur Resignation (vgl. Facciorusso, 2017) und zur Preisgabe ihrer Daten (Turow et al., 2015).

Ziel des Beitrags war es weiterhin, sich der Antwort auf die Frage zu nähern, in welchem Verhältnis das Privatsphäreverhalten der Internetnutzer zur Debatte um das Ende der Privatsphäre zu bewerten ist.

Zunächst ist zu sagen, dass die Debatten um das Ende von etwas im Grunde immer darauf hindeuten, dass man sich kritisch mit dem aktuellen Zustand des „Endenden" auseinandersetzt (bzw. fordert, dass etwas Neues beginnt). Bei der Endismus-Debatte um die Privatsphäre geht es also um die Frage, welchen Wert Privatsphäre für uns hat und ob wir diesen

Wert erhalten wollen – sprich, wie wir heute und vor allem in Zukunft als Gesellschaft leben möchten. Diese Frage betrifft jeden Einzelnen und muss im demokratischen Sinne von unten nach oben (und nicht umgekehrt) erarbeitet und im Kollektiv beantwortet werden. Denn auch wenn die Privatsphäre für die Freiheit des Individuums und die Existenz einer demokratischen Gesellschaft von existenzieller Bedeutung ist, so ist ihre Existenz nicht in Stein gemeißelt, sondern wurde stets an den Kontext gesellschaftlicher Entwicklungen angepasst und daher auch immer wieder neu gedacht. Wie viele Freiheiten muss sie daher von jeder Generation neu hinterfragt und erkämpft werden (Rosenberg, 1969)

Zuckerbergs Behauptung also, dass Privatsphäre eine soziale Norm sei, „that has evolved over time" (Zuckerberg zitiert nach Kirkpatrick, 2010) ist insofern richtig, als es sich hier um kein starres, sondern um ein historisch-kontextual bedingt dynamisches Konzept handelt. In diesem Zusammenhang dann aber zu behaupten, dass sich die Menschen damit *wohl fühlen* immer mehr Daten von sich preiszugeben, muss mit Blick auf die hier vorliegenden Ergebnisse in Frage gestellt werden. Argumentationen wie diese zielen im Grunde nur darauf ab, eine wirtschaftlich motivierte Lüge zu etablieren und zu legitimieren, bis sie sich „wahrgelogen" hat.[7] Nutzer sollen glauben, dass sie nichts zu verbergen haben und die Privatsphäre besser der totalen Transparenz als neuem Ideal weicht. Sie sollen in ihrer Rolle als Inhalte generierende Nutzer glauben, echte Teilhabe zu haben und dadurch an Macht zu gewinnen.

Das ist in vielerlei Hinsicht durchaus richtig und soll hier nicht als völlig bedeutungslos abgetan werden. Doch Konzernen wie Facebook, Google und Co. geht es weniger um den Machtzuwachs Einzelner als darum, einen möglichst großen und verifizierbaren Datensatz zu generieren, der für Zwecke, die wir nicht (wirklich) kennen, mit Mitteln, die wir weder sehen, verstehen noch kontrollieren können, genutzt und verwertbar gemacht wird. Damit bestehen in Wahrheit Machtasymmetrien stärker denn je und die größten Profiteure des beschworenen Paradigmenwechsels wären kommerzielle (aber auch politische) Interessensvertreter, die den Datenlieferern keine echte Teilhabe ermöglichen.

Der Beitrag konnte zeigen, dass Nutzer ihre Privatsphäre als schützenswert erachten und ihre Daten im Netz sehr gerne kontrollieren möchten. Es zeigt sich, dass sie dies im Rahmen ihrer Möglichkeiten auch in Form diverser Handlungsstrategien in der Regel auch tun. Damit dies noch optimaler erfolgt, müssen Nutzer insgesamt mehr aufgeklärt und in ihrer Medienkompetenz gestärkt werden. Denn bewusst zu handeln heißt auch anders handeln zu können (zumindest theoretisch). Zum anderen, und hier schließt sich der Beitrag der

7 Die Bemerkung bezieht sich auf den Sozialphilosophen Günther Anders und seine kritische Haltung zum Fernsehen. Demnach wird dem Empfänger der Fernsehinformation Objektivität vorgetäuscht, indem man ihn im Glauben lässt, über abwesende Informationen verfügen zu können. Dies gibt ihm ein Gefühl von Machtzuwachs, obwohl er der eigentlichen Urteilsarbeit enthoben wird: „Das Fernsehbild gibt vor, das Abbild der Realität zu sein und wird so zum Vorbild für gerade diese Realität. Das führt zu dem Bumerang-Effekt. Der Mensch richtet sich nach dem Abbild der Wirklichkeit und die Realität wird auf diesem Wege zu diesem verzerrten Abbild. Auf einmal stimmt, was im Fernsehen zu sehen ist: Die Lüge hat sich wahr-gelogen." Anders zitiert nach Liessmann (2002), S. 92.

Auffassung von Trepte und Kollegen an, muss ein positives Verständnis von Privatsphäre etabliert werden, um auf Systemebene mehr Handlungsfähigkeit zu erhalten.

Es konnte aber auch gezeigt werden, dass Nutzer die oben beschriebene Machtasymmetrie wahrnehmen und aufgrund dessen zum Teil resignieren, was ebenfalls deutlich macht, dass sie das von den Konzernen propagierte Ideal nicht teilen. Dabei ist es besonders bedenklich, wenn die Resignation der Nutzer dazu führt, dass diese ihre Daten nicht bewusst zurückhalten, sondern im Gegenteil weniger vorsichtig mit ihren Daten umgehen. Dass Nutzer hier kapitulieren und sich ihrer Autonomie beraubt und nicht (im Sinne des Kalkül-Ansatzes) als wirkliche „Entscheider" sehen, muss in das Bewusstsein der Politik drängen.

Trotz der hohen gesellschaftlichen Relevanz, die die Debatte hat, scheint vor allem der Ansatz der Resignation als Erklärung für die Selbstoffenbarung der Nutzer empirisch noch nicht hinreichend gefasst und theoretisch noch nicht ausreichend systematisiert. Für weitere Studien könnte daher von Interesse sein, ob und wie sich der Resignationsansatz mit dem Privacy Calculus-Modell verbinden lässt. Vor dem Hintergrund, dass Transparenz und vor allem Medienkompetenz als wichtige Mittel gesehen werden um Internetnutzer für einen bewussteren Umgang mit ihren Daten zu sensibilisieren, wäre zudem wichtig zu erfahren, inwiefern sich die Zunahme von Information und Wissen tatsächlich auf deren Verhalten auswirkt. Führt Aufklärung zwingend zu einem vorsichtigen Umgang mit den eigenen Daten im Netz (im Sinne des Privacay Caclulus) oder kann dadurch sogar bei manchen Nutzern eher ein resigniertes Verhalten in Richtung Datenpreisgabe verstärkt werden? Interessant wäre hier, inwiefern sich resignierte Nutzer (bzw. Situationen) voneinander unterscheiden, die ihre Daten eher bewusst zurückhalten oder eher preisgeben (bzw. in denen Nutzer resigniert sind). Interessant wäre auch das dem Nothing-to-Hide-Argument zugrunde liegende Motiv genauer zu untersuchen und zu prüfen, ob sich hinter dieser ausgedrückten Gleichgültigkeit eine pragmatische Anpassung im Sinne Adorjans und Ricciardellis (2018) verbirgt. Zudem kann auch der Frage nachgegangen werden, inwiefern ein wahrgenommener Autonomieverlust im Netz einen destabilisierenden Einfluss auf unsere Autonomie im Gesamten hat, also auf all jene Bereiche, in denen selbstbestimmtes Denken, Entscheiden und Handeln von Bedeutung sind.

Literatur

ABELS, Heinz (2019): Einführung in die Soziologie. Band 2: Die Individuen in ihrer Gesellschaft, 5. Auflage. Wiesbaden: Springer VS.

ACQUISTI, Alessandro und GROSS, Ralph (2006): Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In: Danezis, George und Golle, Philippe (Hrsg.): Privacy Enhancing Technologies. Berlin und Heidelberg: Springer (Lecture Notes in Computer Science, 4258), S. 36-58.

ADORJAN, Michael und RICCIARDELLI, Rosemary (2018): A new Privacy Paradox? Youth Agentic practices of privacy. Management despite 'Nothing to Hide' online. Pre-publication accepted version, forthcoming in Canadian Review of Sociology, February 2019. Verfügbar unter: https://prism.ucalgary.ca/bitstream/handle/1880/107108/Adorjan%20%26%20Ricciardelli%20-%202019%20-%20a%20new%20privacy%20paradox.pdf?sequence=1&isAllowed=y [31.10.2018].

ALTMANN, Irwin (1975): The Enviromet and Social Behaviour. Monterey: Brooks/Cole.
BARNES, Susan B. (2006): A privacy paradox: Social networking in the United States. In: First Monday, 11 (9). Verfügbar unter: http://firstmonday.org/article/view/1394/1312 [31.10.2018].
BARUH, Lemi/ SECINTI, Ekin und CEMALCILAR, Zeynep (2017): Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. In: Journal of Communication, 2017, S. 26-53.
BATES, Alan P. (1964): Privacy – A Useful Concept? In: Social Forces, Vol. 42, Nr. 4, S. 429-434.
BLUMBERG, Kerstin/ MÖHRING, Wiebke und SCHNEIDER, Beate (2009): Risiko und Nutzen der Informationspreisgabe in Sozialen Netzwerken. In: Zeitschrift für Kommunikationsökologie und Medienethik, 11 (1), S. 18-24.
BOLZ, Norbert (2012): Das Internet als Katalysator für den Wandel von Sprache und Kultur. In: Biber, Christoph (Hrsg.): Digitale Demokratie. Berlin: GDA.
BOSESKY, Pino und BRÜNING, Christoph (2014): Verständnis und Schutz von digitaler Privatheit im nationalen Recht. In: Hill, Hermann und Schliesky, Utz (Hrsg.): Die Neubestimmung der Privatheit. Baden-Baden: Nomos (Verwaltungsressourcen und Verwaltungsstrukturen, 26).
BRAUN, Max und TREPTE, Sabine (2017): Privatheit und informationelle Selbstbestimmung: Trendmonitor zu den Einstellungen, Meinungen und Perspektiven der Deutschen. Stuttgart: Universität Hohenheim.
BROWN, Barry und SELLEN, Abigail (2001): Exploring Users' Experiences of the Web. In: First Monday, 6 (9). Verfügbar unter: http://firstmonday.org/ojs/index.php/fm/article/view/882/791 [20.10.2018].
BUCHMANN, Johannes (2013) (Hrsg.): Internet Privacy. Options for adequate realisation (acatech STUDIE). Heidelberg (u.a.): Springer Verlag.
BURGOON, Judee K. (1982): Privacy and communication. In: Burgoon, Michael (Hrsg.): Communication Yearbook 6. Beverly Hills: Sage, S. 206-249.
BVerfG 65, 1 – Volkszählungsurteil. Verfügbar unter: http://www.servat.unibe.ch/dfr/bv 065001.html [1.10.2018].
DAVISON, Phillips W. (1983). The third-person effect in communication. In: Public Opinion Quarterly, 47 (1), S. 1-15.
DEBATIN, Bernhard et al. (2009): Facebook and online privacy: Attitudes, behaviors, and unintended consequences. In: Journal of Computer-Mediated Communication, 15, 2009, S. 83-108.
DIENLIN, Tobias (2019): Das Privacy Paradox: Eine Analyse aus psychologischer Perspektive. In: Specht, Louisa/ Werry, Susanne und Werry, Nikola (Hrsg.): Handbuch Datenrecht und Digitalisierung. Berlin: Erich Schmidt Verlag. Im Erscheinen.
DIVSI (2014): Kinder, Jugendliche und junge Erwachsene in der digitalen Welt. Eine Grundlagen-studie des SINUS-Instituts Heidelbergs im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI). Hamburg: DIVSI.
DWYER, Catherine/ HILTZ, Starr Roxanne und PASSERINI, Katia (2007): Trust and privacy concerns within social networking sites: A Comparison of Facebook and Myspace. Verfügbar unter: http://csis.pace.edu/~dwyer/research/DwyerAMCIS2007.pdf [30.10.2018].
ECKART, Christel (2001): Erfahrungen des Selbst – Kulturen des Widerspruchs. Kassel: Manuskript.
EICHENHOFER, Johannes (2017): Privatheit und Transparenz in der Demokratie. In: Forschungsjournal Soziale Bewegungen. Analysen zur Demokratie in der Zivilgesellschaft 30 (2017), S. 133-142.
ELLISON, Nicole et al. (2011): Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environment. In: Trepte, Sabine und Reinecke, Leonard (Hrsg.): Privacy Online. Berlin und Heidelberg: Springer Verlag, S. 19-31.
FACCIORUSSO, Dominique (2013): Google – The World Brain. Was passiert wenn die ganze Welt zum Index wird? Zur Entwicklung, Auswirkung und Bedeutung von Google für unsere Informationsgesellschaft. Heidelberg: Bachelorarbeit Johannes Gutenberg Universität Mainz.

FACCIORUSSO, Dominique (2017): "Privacy is no longer a social norm." – Eine qualitative Befragung junger Erwachsener über das Verständnis von und die Einstellung zur Privatsphäre im Internet. Heidelberg: Masterarbeit Johannes Gutenberg-Universität Mainz.

FREES, Beate und KOCH, Wolfgang (2018): ARD/ZDF-Onlinestudie 2018: Zuwachs bei medialer Internetnutzung und Kommunikation. In: Media Perspektiven, Heft 09, 2018, S. 398-413.

GIDDENS, Anthony (1984): The constitution of society: outline of the theory of structuration. University of California Press.

GRÄF, Dennis/ HALFT, Stefan und SCHMÖLLER, Verena (2011): Privatheit. Formen & Funktionen. Passau: Karl Stutz.

GRIMM, Petra und KRAH, Hans (2014): Ende der Privatheit? Eine Sicht der Medien- und Kommunikationswissenschaft. Verfügbar unter: http://www.digitaleethik.de//showcase//2014/11/Ende_der_Privatheit_Grimm_Krah.pdf [31.10.2018].

HENNE, Benjamin (2014): Methoden zur Schaffung von Bewusstsein über persönliche Informationen als notwendige Voraussetzung für den Schutz der Privatsphäre. Hannover: Veröffentlichte Dissertation der Gottfried Wilhelm Leibniz Universität Hannover.

HORN, SILVIO (2013): Facebook – Gefahr oder Chance? In: Hill, Hermann/ Martini, Mario und Wagner, Edgar (Hrsg.): Facebook, Google und Co. Chancen und Risiken. Baden-Baden: Nomos (Verwaltungsressourcen und Verwaltungsstrukturen, 23), S. 151-175.

HOTTER, Maximilian (2011): Privatsphäre. Der Wandel eines liberalen rechts im Zeitalter des Internets. Frankfurt a.M.: Campus Verlag.

KIRKPATRICK, Marshall (2010, 10.01.): Facebook's Zuckerberg Says The Age of Privacy Is Over. In: New York Times. Verfügbar unter: http://www.nytimes.com/external/readwriteweb/2010/01/10/10readwriteweb-facebooks-zuckerberg-says-the-age-of-privac-82963.html [31.10.2018].

KLINGER, Ulrike (2018): Aufstieg der Semiöffentlichkeit: Eine relationale Perspektive. Publizistik, 63(2), S. 245-267.

KOKOLAKIS, Spyros (2017): Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. In: Computers and Security, Vol. 64, S. 122-134.

KURZ, Constanze und RIEGER, Frank (2011): Die Datenfresser. Wie Internetfirmen und Staat sich unsere Daten einverleiben und wir die Kontrolle darüber zurückerlangen. Bonn: S. Fischer Verlag.

KUZMANOVIC, Bojana (2016): Optimistischer Fehlschluss als Beispiel für systematische Verzerrung in der Entscheidungsfindung. In: Ach, Johann/ Lüttenberg, Beate und Nossek, Alexa (Hrsg.): Neuroimaging und Neuroökonomie. Grundlagen, ethische Fragestellungen, soziale und rechtliche Relevanz. Berlin (u.a.): LIT Verlag (Münsteraner Bioethik-Studien, 14), S. 5-19.

LAMP, Erich (2009): Die Macht der Öffentlichen Meinung – und warum wir uns ihr beugen. Über die Schattenseite der menschlichen Sozialnatur. München: Olzog.

LI, Han/ SARATHY, Rathindra und XU, Heng (2010): Understanding situational online information disclosure as a privacy calculus. In: Journal of Computer Information Systems. Verfügbar unter: https://faculty.ist.psu.edu/xu/papers/jcis.pdf [30.10.2018].

LIESSMANN, Konrad Paul (2002): Günther Anders: philosophieren im Zeitalter der technologischen Revolutionen. München: Verlag C.H. Beck.

LIVINGSTONE, Sonia (2008): Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. In: New Media & Society, 10 (3), S. 393-411.

MARTHEWS, Alex und TUCKER, Catherine E. (2015): Government Surveillance and Internet Search Behavior. Verfügbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564 [10.10.2018].

MARWICK, Alice und HARGITTAI, Eszter (2018): Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. In: Information, Communication & Society. Verfügbar unter: http://www.tiara.org/wp-content/uploads/2018/05/Marwick_Hargittai_2018_Nothing-to-hide-nothing-to-lose.pdf [31.10.2018].

NOELLE-NEUMANN, Elisabeth (1979): Öffentlichkeit als Bedrohung. Beiträge zur empirischen Kommunikations-forschung. Hrsg. Von Jürgen Wilke, 2., durchges. Auflage. Freiburg und München: Alber Broschur Kommunikation.

NORBERG, Patricia/ HORNE, Daniel und HORNE, David (2007): The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. In: Journal of Consumer Affairs, Volume 41, Issue 1, S. 100-126.

PAINE, Carina et al. (2007): Internet users' perceptions of ‚privacy concerns' and ‚privacy actions'. In: International Journal of Human-Computer Studies, 65 (6). Amsterdam: Elsevier, S. 526-536.

PENNEY, Jon (2016): Chilling Effects: Online Surveillance and Wikipedia Use. In: Berkeley Technology Law Journal, Vol. 31, 1, S. 117- 182.

RIEGER, Jörg (2014): Die intuitive Verarbeitung von nicht genau erfassbarer Information: Eine experimental-ökonomische Untersuchung von Einflussfaktoren auf den 'Statistischen Menschen'. Berlin: Logos Verlag.

RITTER, Martina (2008): Die Dynamik von Privatheit und Öffentlichkeit in modernen Gesellschaften. Wiesbaden: VS Verlag für Sozialwissenschaften.

RÖSSLER, Beate (2001): Der Wert des Privaten. Frankfurt a.M.: Suhrkamp.

ROSENBERG, Jerry M. (1969): The Death of Privacy. Random House.

SAUTER, Theresa (2014): Öffentlichmachung privater Subjekte im Web 2.0: Eine Genealogie des Schreibens als Selbsttechnik. In: Österreichische Zeitschrift für Soziologie, 39 (1), S. 23-40.

SCHIEDERMAIR, Stephanie (2012): Der Schutz des Privaten als internationales Grundrecht. Tübingen: Mohr Siebeck (Jus Publicum: Beiträge zum Öffentlichen Recht, 216).

SCHWEIGER, Wolfgang (2007): Theorien der Mediennutzung: Eine Einführung. Wiesbaden: VS-Verlag für Sozialwissenschaften.

SEUBERT, Sandra (2012): Der gesellschaftliche Wert des Privaten. In: Datenschutz und Datensicherheit, 2012 (2). Wiesbaden: Springer Verlag, S. 100-104.

SEUBERT, Sandra (2017): Das Vermessen kommunikativer Räume. Politische Dimensionen des Privaten und ihre Gefährdung. In: Forschungsjournal Soziale Bewegungen. Analysen zur Demokratie in der Zivilgesellschaft 30 (2017), S. 124-132.

SEUBERT, Sandra und HELM, Paula (2017): Privatheit und Demokratie. In: Forschungsjournal Soziale Bewegungen. Analysen zur Demokratie in der Zivilgesellschaft 30 (2017), S. S. 120-124.

SEUBERT, Sandra und NIESEN, Peter (2010): Die Grenzen des Privaten. Baden-Baden: Nomos.

SOLOVE, Daniel J. (2007): ‚I've got nothing to Hide,' and other misunderstandings of privacy. In: San Diego Law Review, Vol. 44. GWU Law School Public Law Research Paper No. 289, S. 745-772.

SPIEKERMANN, Sarah/ GROSSKLAGS, Jens und BERENDT, Bettina (2001): E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus actual Behavior. In: Proceedings of the 3rd ACM conference on Electronic Commerce. New York: ACM, S. 38-47.

STARK, Birgit/ MAGIN, Melanie und JÜRGENS, Pascal (2017): Ganz meine Meinung? Informationsintermediäre und Meinungsbildung – Eine Mehrmethodenstudie am Beispiel von Facebook. LfM, 2017 (LfM-Dokumentation, Band 55).

STRUKTURWANDEL DES PRIVATEN (2018): Ergebnisse. Verfügbar unter: https://strukturwandeldesprivaten.wordpress.com/projekt/ergebnisse/ [31.10.2018].

TADDICKEN, Monika (2011): Selbstoffenbarung im Social Web. In: Publizistik, 56 (3), S. 281–303.

TADDICKEN, Monika (2013): The "privacy paradox" in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. In: Journal of Computer-Mediated Communication, 19, 248–273.

THIMM, Caja (2013): Digitale Lebenswelten. Zur Mediatisierung sozialer Beziehungen. In: Eumann, Marc et al. (Hrsg.): Medien, Netz und Öffentlichkeit. Impulse für die digitale Gesellschaft. Essen: Klartext Verlag.

THOMAS, Emerson I. (1970): The System of Freedom of Expression. New York: Vintage Books.

TREPTE, Sabine et al. (2017): A Cross-Cultural Perspective on the Privacy Calculus. In: Social Media + Society, S. 1-13.

TREPTE, Sabine und DIENLIN, Tobias (2013): Privatsphäre im Internet. In: Porsch, Torsten und Pieschl, Stephanie (Hrsg.): Neue Medien und deren Schatten. Mediennutzung, Medienwirkung und Medienkompetenz. Göttingen: Hogrefe, S. 53-80.

TREPTE, Sabine und MASUR, Philipp (2020): Need for Privacy. In: Zeigler-Hill, Virgil und Shackelford, Todd K. (Hrsg.): Encyclopedia of personality and individual differences. London.

TREPTE, Sabine und REINECKE, Leonard (2009): Sozialisation im Social Web: Eine Forschungsagenda zu den Wirkungen des Web 2.0. In: Zeitschrift für Kommunikationsökologie und Medienethik, 11 (1), S. 35-39.

TREPTE, Sabine/ MASUR, Philipp und PAPE, Thilo (2015): Privatheit im Wandel? Eine repräsentative Umfrage und eine Inhaltsanalyse zur Wahrnehmung von Privatheit in Deutschland. Universität Hohenheim.

TUFEKCI, Zeynep (2008): Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. In: Bulletin of Science Technology Society, 28 (1), S. 20-36.

TUROW, Joseph/ HENNESSY, Michael und DRAPER, Nora (2015): The Tradeoff Fallacy. How Marketers are misrepresenting American Consumers and opening them up to exploitation. Verfügbar unter: https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf [31.10.2018].

WARREN, Samuel D. und BRANDEIS, Louis D. (1890/1984): The Right to Privacy. The Implicit Made Explicit. In: Schoeman, Ferdinand David (Hrsg.): Philosophical Dimension of Privacy: An Anthology. Cambridge (u.a.): Cambridge University Press, S. 75-103.

WEIß, Ralph (2008): Das mediale entblößte Ich – verlorene Privatheit? In: Jurczyk, Karin und Oechsle, Mechthild (Hrsg.): Das Private neu denken – Erosionen, Ambivalenzen. Leistungen. Münster: Verlag Westfälisches Dampfboot, S. 175-191.

WESTIN, Alan F. (1967): Privacy and Freedom. New York: H. Wolff.

WEWER, Göttrick (2013): Die Verschmelzung von privater und öffentlicher Sphäre im Internet. In: Ackermann, Ulrike (Hrsg.): Im Sog des Internets. Öffentlichkeit und Privatheit im digitalen Zeitalter, S. 53-70.

WHITE, Gregory L. (1975): The Chilling Effects of Surveillance: Deindividuation and Reactance. Verfügbar unter: https://pdfs.semanticscholar.org/02d4/d1957a29ff94431af21007743438e3c75f0f.pdf [10.10.2018].

WORMS, Christoph und GUSY, Christoph (2012): Verfassung und Datenschutz – das Private und das Öffentliche in der Rechtsordnung. In: Datenschutz und Datensicherheit, 2012 (2). Wiesbaden: Springer Verlag, S. 92-99.

ZUCKERBERG, Mark (2010, 24.05.): From Facebook, Answering Privacy Concerns with New Settings. In: Washington Post. Verfügbar unter: http://www.washingtonpost.com/wpdyn/content/article/2010/05/23/AR2010052303828.html [1.11.2018].