Zeitschrift für
Semiotik
Band 40 • Heft 1-2 (2018)
Seite 63-82
Stauffenburg Verlag Tübingen

„Alexa, kann ich dir vertrauen?“ Sprachassistenten als Wegbereiter der gläsernen Privatsphäre

Anne Diessner, Lisamarie Haas und Carina Konopka, Eberhard Karls
Universität Tübingen

Summary. For some years now, language assistants have been making their way into everyday lives of many people. The intelligent personal assistants integrated in smartphones and special speakers seem to make the life of those who use them easier. At the same time, however, they open up possibilities for interfering with the privacy of users. Companies collect large amounts of sometimes sensitive personal data for improved functionality and marketing. This calls into question the traditional understanding of privacy. This article discusses the technical functioning of language assistants, elaborates on the transformation of privacy, and problematizes the new helpers concerning their relationship to the users' privacy, using Amazon's Alexa as an example.

Zusammenfassung. Seit einigen Jahren halten Sprachassistenten Einzug in den Alltag zahlreicher Menschen. Die intelligenten persönlichen Assistenten, die in Smartphones und speziellen Lautsprechern integriert sind, scheinen vorrangig das Leben ihrer Nutzer zu erleichtern. Gleichzeitig eröffnen sie jedoch Möglichkeiten des Eingriffs in die Privatsphäre der Nutzer. Unternehmen sammeln große Mengen teils sensibler persönlicher Daten für eine verbesserte Funktionalität und Marketing. Damit wird das traditionelle Verständnis von Privatheit infrage gestellt. Der vorliegende Artikel erörtert die technische Funktionsweise von Sprachassistenten, arbeitet die Transformation der Privatsphäre heraus und problematisiert die neuen Helfer am Beispiel von Amazons Alexa im Hinblick auf ihr Verhältnis zur Privatsphäre der Nutzer.

1. Einführung

Amazons Alexa, Apples Siri, Microsofts Cortana und Google Assistant – das Gespräch mit einem Sprachassistenten gehört für Millionen von Konsumenten zur täglichen Routine. Die sprachgesteuerten Systeme sind in Smartphones und bestimmten Lautsprechern integriert und sollen als soge-

nannte intelligente persönliche Assistenten eine Erleichterung in vielen Lebensbereichen darstellen (vgl. Lenz-Kesekamp und Weber 2018: 18; López u.a. 2018: 241). Der vorliegende Artikel möchte Sprachassistenten im Rahmen der ‚Surveillance Studies' untersuchen (vgl. z.B. Lyon 2007). Dabei soll ihre Auswirkung auf die Privatsphäre beleuchtet und Amazons Sprachassistent Alexa beispielhaft in den Fokus gestellt werden. Es soll aufgezeigt werden, inwiefern Sprachassistenten ein weiterer Schritt in Richtung einer gläsernen Privatsphäre sind und weshalb diese einen nachhaltigen Schutz benötigt.

Der erste Teil bietet zunächst eine Einführung in die grundlegenden Funktionsweisen digitaler Sprachassistenten. Amazons Alexa wird hierbei als Beispiel dienen. Auf Grundlage des theoretischen Hintergrunds werden Sprachassistenten metaphorisch als Dienstboten des 21. Jahrhunderts bezeichnet. Die Metapher wird im Weiteren ausgeführt, um das heuristische Potenzial des Vergleichs für die weitere Argumentation der Arbeit nutzen zu können. Bereits in früheren Epochen zeigte sich der Wunsch der Menschen nach einem bequemen Leben, indem unliebsame Aufgaben anderen übertragen wurden. Mit der Nutzung heutiger Sprachassistenten verhält es sich ähnlich. Dennoch unterscheiden sich diese digitalen Dienstboten in einigen Aspekten fundamental von ihren analogen Vorfahren. Ziel der Dienstbotenmetapher ist es also, das Problembewusstsein für die neuen, digitalen Dimensionen von Dienstboten zu schärfen, da diese gravierende Auswirkungen auf die Privatsphäre der Nutzer haben können. Der zweite Teil widmet sich sodann der Problematisierung von Risiken der neuen Technologien für die Privatsphäre. Zunächst werden die theoretischen Grundlagen und der Wert der Privatsphäre beleuchtet, um anschließend den Einfluss von Amazons Alexa auf die Privatsphäre der Nutzer stellvertretend für Sprachassistenten zu diskutieren: Besteht die Gefahr, dass Alexa einen Beitrag zum vollständigen Verlust jeder Privatheit leistet und zur Transformation in eine Überwachungsgesellschaft beiträgt? Der dritte Teil stellt die Ergebnisse der Arbeit resümierend nebeneinander und bietet einen Ausblick auf das zukünftige Verhältnis von Sprachassistenten zur Privatsphäre.

2. Digitale Sprachassistenten als Dienstboten des 21. Jahrhunderts

Zu Beginn werden die Grundlagen eines theoretischen Verständnisses digitaler Sprachassistenten gelegt, auf welchen die weiteren Ausführungen aufbauen. Hierzu bietet dieser Abschnitt zunächst einen allgemeinen Überblick über die Funktionsweise von Sprachassistenten, um anschließend Amazons Alexa als konkretes Beispiel einzuführen. Außerdem parallelisiert dieser Abschnitt Sprachassistenten mit Dienstboten. Der Vergleich soll zu einem tieferen Verständnis der Privatsphärenproblematik führen, die den Schwerpunkt dieses Aufsatzes bildet. Bereits vorab sei angemerkt, dass Sprachassistenten als Teil einer weitreichenden technisch-digitalen Ent-

wicklung zu verstehen sind und die Machtverhältnisse zwischen den Großkonzernen und ihren Kunden eine andere Dimension einnehmen, als zwischen dem Adel und den analogen Dienstboten. Dennoch bringt der Vergleich einen Mehrwert hinsichtlich der Fragestellung dieser Arbeit.

2.1 Theoretischer Hintergrund digitaler Sprachassistenten

Im Jahr 2011 wurde der erste Sprachassistent unter dem Namen *Siri* im Rahmen der Vorstellung des iPhone 4S lanciert. Handelte es sich in der Anfangszeit noch um einen amüsanten Zeitvertreib, kann heute aufgrund der enormen technischen Fortschritte tatsächlich von einem intelligenten Assistenten im Alltag die Rede sein (vgl. Lenz-Kesekamp und Weber 2018: 19; Hoy 2018: 81). Derzeit gehören neben Apples Siri außerdem Google Assistant, Microsofts Cortana und Amazons Alexa zu den bekannten Produkten. Sprachassistenten sind definiert als „eine Software, die die menschliche Sprache interpretieren und über synthetisierte Stimmen interagieren kann" (Lenz-Kesekamp und Weber 2018: 18; vgl. auch Hoy 2018: 81). Diese Software ist in Smartphones und speziellen Lautsprechern (sogenannte ‚Smart Speaker') integriert.

Sprachassistenten liegt die Technologie des ‚Natural Language Processing' (NLP) zugrunde. NLP befasst sich mit der Verarbeitung der natürlichen Sprache, dem „Verstehen sowie der Semantik von Wörtern und Sätzen, der Klassifizierung von Texten, der korrekten Aussprache und Betonung sowie der Syntaxanalyse und der Beantwortung von Fragen" (Lenz-Kesekamp und Weber 2018: 19). Die Sprache ist der einzige Mediator zwischen dem Menschen und der Maschine. Es fehlen Nutzerschnittstellen wie Touchpads und Computermäuse. Deswegen ist auch von ‚Voice-First'-Geräten die Rede, die den intelligenten Assistenten über Hardware verfügbar und ansprechbar machen. Solche Geräte setzen die sogenannte ‚Zero-User-Interface'-Strategie um. Die grundlegende Idee hierbei ist, dass eine Interaktion, Kommunikation bzw. Transmission nicht offensichtlich durch das Gerät vermittelt wird. Das Gerät tritt vielmehr in den Hintergrund, um eine möglichst natürlich wirkende Benutzerschnittstelle zu gewährleisten. Der Dienst soll sich also bestmöglich in den Kontext der Nutzer einfügen (vgl. Bedford-Strohm 2017: 486–487; siehe auch López u.a. 2018: 241). Lenz-Kesekamp und Weber (2018: 19) nennen deshalb als Ziel digitaler Sprachassistenten, „eine möglichst weitreichende Kommunikation auf Augenhöhe zwischen Mensch und Computer per Sprache zu schaffen". Den Untersuchungen von López u.a. (2018) zufolge variiert das Gefühl von Natürlichkeit bei der Nutzung verschiedener Sprachassistenten. Im Test schnitt der Google Assistant am besten hinsichtlich des Natürlichkeitsgefühls bei der Interaktion mit Nutzern ab (vgl. ausführlich López u.a. 2018: 241–242).

Zur Konkretisierung der Funktionsweise von Sprachassistenten wird im Folgenden ein genauerer Blick auf Amazons Alexa geworfen. Der US-ame-

rikanische Online-Versandhändler Amazon ist ein Vorreiter im Gebiet der Sprachassistenten. Mit dem Namen Alexa wird seit 2014 das ‚Gehirn' der Gerätelinie Echo bezeichnet. Es handelt sich dabei um intelligente Smart Speaker mit integrierter Sprachsteuerung, die schätzungsweise 5,9 % der deutschen Internetnutzer verwenden. In den USA lag der Durchschnittswert 2018 bei etwa 15,4 % (vgl. Lenz-Kesekamp und Weber 2018: 19). Mittlerweile gibt es mehrere Produktvarianten des Smart Speakers, die sich im Grunde lediglich in der Lautsprechergröße unterscheiden: Amazon Echo, Echo Dot, Echo Plus, Echo Spot, Echo Show und andere Alexa-Geräte. Im Falle von Echo Spot und Echo Show weisen die Geräte zusätzlich ein Display auf.[1]

Die Funktionsweise der Smart Speaker beruht auf der soeben beschriebenen Technologie des NLP. Alle Echo-Geräte sind mit einer intelligenten Spracherkennungssoftware über ein Microphone-Array ausgestattet, das permanent aktiv eingeschaltet sein muss. Ein integriertes technisches Modul ermöglicht die Verbindung zum Internet und somit auch die Übermittlung der Sprachdaten an die Amazon Cloud. Das festgelegte Aktivierungswort lautet ‚Alexa'. Wird dieses sogenannte ‚wake word' vernommen, wird der Sprachbefehl oder die Frage des Nutzers aus den Umgebungsgeräuschen herausgefiltert und aufgenommen (z.B. ‚Alexa, schalte das Licht ein'). Die Audiodatei wird an die Amazon Cloud geschickt und in einen Text umgewandelt. Dieser Text wird entsprechend interpretiert und je nach Anfrage mit einem bestimmten ‚Skill' verknüpft. Der Lautsprecher gibt die Sprachausgabe des Assistenten aus und ermöglicht damit den Dialog mit den Nutzern (vgl. Bedford-Strohm 2017: 487; Lenz-Kesekamp und Weber 2018: 19; Hoy 2018: 82). Aufgrund der fortschreitenden Entwicklungen im Bereich der natürlichen Spracherkennung ‚versteht' der Sprachassistent auch diverse Formulierungen ein- und desselben Sprachbefehls, um zum gewünschten Ergebnis zu gelangen (vgl. Hoy 2018: 82–83). Es entsteht somit eine hybride Kommunikationsgemeinschaft zwischen Mensch und Maschine, die sich zunehmend in Richtung einer symmetrischen Verständigung entwickelt (vgl. Roser 2018: 250–251). Lenz-Kesekamp und Weber (2018: 21) nehmen eine Einteilung der Alexa Skills in folgende Kategorien vor:

- ‚Built In Skills': Auf dem Gerät bereits vorinstallierte Skills (z.B. die Ausgabe von Zeit);
- ‚Customs Skills': Externe Skills, die via Aktivierungswort den Dialog mit Usern ermöglichen;
- ‚Smart Home Skills': Skills zum Bedienen entsprechender automatisierter Anwendungen im Haushalt;
- ‚Flash Briefing Skills': Skills, die dem Nutzer schnelle vordefinierte Informationen bieten.

Diese Einteilung passt zu der Beobachtung, dass sich die Sprachassistenten verschiedener Entwickler einige Basisfunktionen teilen, sich jedoch in

weiteren Funktionalitäten (oder eben Skills) unterscheiden (vgl. López u.a. 2018: 241). Hoy (2018: 81, 93) nennt folgende Basisfunktionen, die via Sprachbefehl von allen digitalen persönlichen Assistenten ausgeführt werden können:

- Das Versenden und Vorlesen von Textnachrichten und E-Mails, das Tätigen von Anrufen;
- Die Beantwortung einfacher Informationsfragen (z.B. ‚Wie spät ist es?', ‚Wie wird das Wetter heute?');
- Das Einstellen von Timern und Weckern, Kalendereinträge tätigen;
- Erinnerungen setzen, Listen anlegen, einfache mathematische Berechnungen ausführen;
- Die Medienwiedergabe von verbundenen Diensten wie iTunes, Netflix, Spotify steuern;
- Die Bedienung von ‚Internet-of-Things'-Geräten wie Thermostate, Lichter, Alarmanlagen;
- Witze und Geschichten erzählen.

Weitere Funktionen können je nach Anbieter hinzugefügt werden. Die besagten Skills sind offen für Drittentwickler. Viele Medienhäuser, Unternehmen oder private Entwickler bieten sie an. Im Falle von Amazon werden die Skills nach einem Zertifizierungsprozess im Skill-Store veröffentlicht und für die Nutzer von Amazons Alexa verfügbar gemacht. Das Prinzip des Skill-Stores ähnelt dabei vom Prinzip dem App-Store für Smartphone-Anwendungen (Bedford-Strohm 2017: 487; Lenz-Kesekamp und Weber 2018: 20–21; vgl. auch Hoy 2018: 83). Wirtschaftlich betrachtet entwickeln sich Sprachassistenten damit zu einem neuen, vielversprechenden Touchpoint für die Kundenkommunikation von Unternehmen (dazu ausführlich Lenz-Kesekamp und Weber 2018: 18–19, 21). Amazons Alexa ist derzeit mit den meisten Drittentwickler-Erweiterungen auf dem Markt präsent (vgl. Bedford-Strohm 2017: 487; Hoy 2018: 84).

Alexa soll, wie alle Sprachassistenten, vorrangig der Erleichterung des Alltags der Nutzer dienen. Sprachassistenten gehören also wie die meisten Digitalisierungsstrategien zum neuzeitlichen Effizienzdenken und zum Dogma einer immer zeit- und kosteneffizienteren Bedürfnisbefriedigung (vgl. Bedford-Strohm 2017: 489–490, 492; zu zukünftigen Nutzungsweisen vgl. Hoy 2018: 85–86).

2.2 Die metaphorische Rückkehr der Dienstboten

Alexa als ein Helfer im Alltag legt einen Vergleich mit traditionellen Dienstboten nahe (vgl. zur Idee auch Zurawski 2014; Bartmann 2016; Krajewski 2010 zum Zusammenhang zwischen Medien und Dienern). Ein solcher Vergleich bietet das heuristische Potenzial, das Verhältnis von Sprachassistenten zu Privatsphäre und Überwachung aus einer anderen Perspektive

zu ergründen. Um das Verständnis und die Problematisierung des Themas zu veranschaulichen, sollen im Folgenden einige Parallelen von Sprachassistenten und Dienstboten aufgezeigt werden.

Als Blütezeit des analogen Dienstbotenwesens gilt in Westeuropa das 19. und beginnende 20. Jahrhundert. Dienstboten waren im Haushalt wohnende angestellte Dienstkräfte, die verschiedene Arbeiten in der Haus- und Landwirtschaft übernahmen. Es handelte sich um eine äußerst inhomogene Berufsgruppe mit einer steilen innerberuflichen Hierarchie. Dienstboten waren rechtlich eingebunden in den Haushalt ihrer Arbeitgeber und hatten ihren Anordnungen in stiller Unterwürfigkeit Folge zu leisten. Genügsamkeit, Anpassungsfähigkeit und die Bereitschaft zur Unterordnung waren daher gern gesehene Fähigkeiten von Dienstboten (vgl. Budde 1999: 149–175; Maurer 1995: 162). Die Eingebundenheit in den Haushalt und die idealtypischen Charaktereigenschaften der Dienstboten spiegeln sich in heutigen Sprachassistenten wider. Durch die Umsetzung der oben beschriebenen ‚Zero-User-Interface'-Strategie werden Sprachassistenten möglichst natürlich und unauffällig wirkend in den Kontext der Nutzer integriert. Die Geräte sind so programmiert, dass sie willenlos die Befehle der Nutzer ausführen und rund um die Uhr verfügbar sind. Ein Blick auf die Geschichte des Dienstbotenwesens zeigt, dass auch bei ihnen lange Arbeitszeiten bis zu 16 Stunden täglich nicht unüblich waren. Die Willkür der Dienstherrschaft entschied über den Arbeitsbeginn und das -ende. Bedienstete sollten lediglich die ihnen aufgetragenen Aufgaben möglichst unbemerkt erledigen (vgl. Budde 1999: 160–161; Maurer 1995: 177).

Eine weitere Parallele von Sprachassistenten und analogen Dienstboten besteht in der heutigen Ansprache. Die Ansprache digitaler Sprachassistenten erfolgt stets mit weiblichen Vornamen, im Falle von Amazon handelt es sich um den Frauennamen Alexa (vgl. Roser 2018: 250). Ab Ende des 19. Jahrhunderts kann eine zunehmende Feminisierung des Dienstbotenwesens ausgemacht werden, die sich heute fortzusetzen scheint (vgl. Budde 1999: 153–156). Bedford-Strohm (2018: 492) führt für die Nutzung weiblicher Figuren als Profilierung des Produktcharakters von Sprachassistenten ebenso historische Gründe an. Laut der klassischen Rollenverteilung wurden Frauen oftmals als Helferinnen angesehen. Darüber hinaus sollten jedoch auch technisch-pragmatische Gründe berücksichtigt werden: Frauenstimmen weisen oftmals eine bessere akustische Verständlichkeit auf und werden als freundlicher wahrgenommen (vgl. Bedford-Strohm 2018: 492). Das Anstellen von Dienstboten zeugte bereits früher von Reichtum und einem höheren Sozialprestige und hatte mithin eine Art Repräsentationscharakter in der Gesellschaft (vgl. Maurer 1995: 169, 174–175). Heutzutage kann in einigen Sprachassistenten z.B. in Form teurerer Smart Speaker durchaus weiterhin ein soziales Abgrenzungsmerkmal ausgemacht werden. Dennoch handelt es sich bei heutigen Dienstboten eher um eine Art Massenware, zumal in nahezu jedem Smartphone ein Sprachassistent integriert ist und Smart Speaker in einigen Ausführungen bereits relativ kostengünstig zu erhalten sind (vgl. Hoy 2018: 81).

Ein letzter Aspekt deutet ein möglicherweise problematisches Verhältnis von Dienstboten zur Privatsphäre an: Die früheren Dienstboten lebten im Haushalt ihrer Herrschaft. Aufgrund des engen Zusammenlebens lernten sie ihre Arbeitgeber genau kennen, denn sie bekamen von morgens bis abends die Geschehnisse und Gespräche im Haushalt mit. So waren Herrschaften auf die Loyalität ihrer Dienstboten angewiesen. Es sind Fälle des sozial gemischten Umgangs oder gar Freundschaften zwischen Dienstboten und Herrschaften überliefert. Doch nicht selten entwickelte sich eine Atmosphäre des Misstrauens und des Unverständnisses. Dies zeigt sich auch daran, dass das neugierige Dienstmädchen, das beispielsweise durch das Schlüsselloch äugt oder an der Tür lauscht, ein beliebtes zeitgenössisches Motiv in der Malerei darstellte (vgl. Budde 1999: 170–171; Maurer 1995: 168–169, 185). Schon in früheren Zeiten bemerkte man neben all den Vorzügen durchaus auch die Schattenseite von Dienstboten hinsichtlich der Privatsphäre. Bei Amazons Alexa und weiteren Sprachassistenten nehmen diese Bedenken allerdings ganz neue Dimensionen an, wie im nächsten Kapitel erläutert wird. Dabei gilt es nämlich trotz aller Parallelen und ähnlichen Mustern zu früheren Zeiten vor allem eins im Hinterkopf zu behalten: Amazons Alexa kann zwar stellvertretend als digitaler Nachkomme der Dienstboten im 21. Jahrhundert bezeichnet werden, doch Alexa ist kein Mensch, wie es die früheren Dienstboten waren. Alexa ist eine Maschine, die sich weder durch ein Gewissen noch durch ein Gefühl für Loyalität auszeichnet. Hinter den Anwendungen stehen in erster Linie wirtschaftliche Interessen großer Konzerne wie Amazon.

An dieser Stelle lässt sich festhalten, dass Sprachassistenten wie Amazons Alexa durch ihre vielfältigen Funktionen durchaus in der Lage sind, den Alltag ihrer Nutzer bequemer zu gestalten. Sprachassistenten spiegeln den stetigen technischen Fortschritt in der natürlichen Sprachverarbeitung wider. Es hat sich gezeigt, dass die Dienstbotenmetapher das Verhältnis der heutigen Nutzer von Sprachassistenten zu ihren Geräten passend beschreiben kann. Die digitale Dimension hat jedoch tiefgreifende Auswirkungen auf die Privatsphäre. Den vielen Erleichterungen im Alltag, die Sprachassistenten ihren Nutzern auf der einen Seite bieten, steht auf der anderen Seite ein Eindringen Dritter in die Privatsphäre gegenüber. Die Dienstbotenmetapher verdeutlicht diese Ambivalenz auf eine prägnante Weise – früher wie heute ist Komfort an die Preisgabe der Privatsphäre gebunden. Das folgende Kapitel widmet sich genauer den Veränderungen im Hinblick auf die Privatsphäre, die durch die Nutzung von Sprachassistenten entstehen.

3. Transformationen der Privatsphäre

In Zeiten der Digitalisierung lässt sich im Spannungsfeld von Sicherheit, Freiheit, Persönlichkeitsrecht, technischen Möglichkeiten und wirtschaftlichen Interessen eine kontroverse Debatte über die Privatsphäre beobach-

ten. Ziel dieses Kapitels ist es, das Problemfeld zu umreißen und die Nutzung von Sprachassistenten darin einzuordnen. Essentiell erscheint darüber hinaus die Frage, welchen Wert Privatheit hat und warum sie überhaupt als schützenswert angesehen wird.

3.1 Privatsphäre und Big Data

Die Debatte um die Privatsphäre ist seit Jahren präsent und wurde dabei sehr kontrovers geführt. Dabei finden sich zahlreiche Subdiskurse, weshalb zunächst eine Eingrenzung vorgenommen werden muss. In der Diskussion geht es häufig um das Verschwimmen der Grenze zwischen Privatsphäre und Öffentlichkeit durch die sogenannten sozialen Netzwerke. Dabei zeigt sich eine paradoxe Haltung: Einerseits äußern Nutzer Wertschätzung für Privatsphäre, geben jedoch andererseits freiwillig private Informationen preis (vgl. Steinbicker 2019: 88). Dieses Missverhältnis sei nicht in der Verantwortung von Nutzern, sondern in den Verhältnissen zu sehen, stellt Steinbicker fest: „Sie werden vor die Wahl gestellt zwischen der unbedingten Wahrung ihrer Privatsphäre und der – mit Preisgabe privater Informationen, also Offenheit verbundenen – Entfaltung ihrer Subjektivität“ (Steinbicker 2019: 88–89).

Einen Schritt weiter geht es nun in der Entwicklung zum ‚Internet of Things‘, das verschiedene Geräte und Dienste mit dem Internet verknüpft. Die Preisgabe privater Informationen dient dabei nicht mehr der Entfaltung von Subjektivität, sondern Komfort und Konsum. Denn für digitale Dienstboten wie Alexa sind Informationen über den Nutzer die Grundlage ihrer Funktionsweise. Steinbicker betont, „je personalisierter die Geräte und Systeme in ihren Hilfestellungen für die Lebensführung werden sollen, je mehr Informationen von und über uns benötigen sie“ (Steinbicker 2019: 84–85). Dabei sei die Spracheingabe nicht nur wichtig, um uns zu verstehen, sondern ebenso zur stetigen Verbesserung der Interpretation.

Darüber hinaus sind die individuellen Nutzerdaten für Konzerne wie Google, Facebook und Amazon wirtschaftlich höchst bedeutsam. Die Unternehmen sammeln diese im Hintergrund, um ein immer differenzierteres Profil anlegen zu können, das in der Folge personalisierte Werbung ermöglicht. Umschrieben wird dieses Sammeln und Verknüpfen von Nutzerdaten häufig als ‚Big Data‘. Obgleich der Internetnutzer in der Regel weiß, dass Daten von ihm gesammelt werden, kann er das Ausmaß meist nicht absehen oder kontrollieren, wie Baumann ausführt: „Unsere digitalen Existenzen weiten sich im virtuellen Raum ungeheuerlich aus, denn bei jeder digital mediatisierten Aktivität werden personenbezogene Daten gesammelt und gespeichert, oft in fremden Staaten“ (Baumann 2015: 7). In dieser Entwicklung hin zu einer immer umfassenderen Beobachtung der Internetnutzung sieht Baumann daher die eigentliche Bedrohung der Privatheit. Denn diese Beobachtung könne Individuen nun auch in Zusammenhängen entblößen, in denen Privatsphäre bislang nicht zur Disposition

gestanden habe: Bezog sich die Debatte über Privatsphäreverletzungen bislang auf individuelles Verhalten, z.B. in Online-Netzwerken oder TV-Shows wie *Big Brother*, müssten mittlerweile technologische und ökonomische Interessen berücksichtigt werden, da gesammelte Metadaten gänzlich neue Rückschlüsse auf den Nutzer zuließen (vgl. Baumann 2015: 17). Auch Stempfhuber und Wagner sehen in der unübersichtlichen Rekombination von Daten, dem ‚Profiling', die größte Herausforderung:

> Dabei stellen die User diese Daten schlichtweg durch ihren Gebrauch des Internets zur Verfügung, die dann ohne konkrete Fragestellung aufgezeichnet und weiter verwertet werden – sei es für Zwecke staatlicher Kontrolle, sei es für Marketingaspekte (Stempfhuber und Wagner 2019: 7).

Genau in diesem Spannungsfeld der Interessen verortet Baumann (2015: 7) die Gefahr für die Privatsphäre: Dem Internet folgten Markt und Staat gemeinsam mit ihren Gewinn- und Herrschaftsinteressen. Die Privatsphäre sei dabei nur hinderlich und werde daher unterlaufen, obgleich sie bislang eine wesentliche Rolle für die Machtbalance zwischen Individuum, Staat und Wirtschaft gespielt habe.

In der Folge stehen sich zwei konträre und wenig zielführende Perspektiven gegenüber, wie Stalder (2019) beschreibt. Auf der einen Seite finden sich die sogenannten ‚Post-Privacy'-Befürworter. Diese sehen als Folge des Verschwindens der Privatsphäre neue Toleranz und Offenheit. Radikale Transparenz schafft demnach die illusionäre Art der Selbstdarstellung ab, garantiert Meinungsfreiheit, deckt Ungerechtigkeiten auf und führt zu einem besseren Miteinander. Stalder zufolge verkenne ‚Post-Privacy' allerdings neue Formen der Diskriminierung. Auf der anderen Seite stehen Skeptiker, die das Ende des freien Denkens postulieren. Doch auch diese düstere Prognose „ist steril, denn in der Verkennung der neuen Möglichkeiten der Autonomie, verkommt sie zur reaktionären Nostalgie, die sich nach den klaren Verhältnissen von Autorität und Unterwerfung sehnt" (Stalder 2019: 108). Im Bemühen um eine objektivere Betrachtungsweise der Thematik scheint es sinnvoll, sich auf die Kernthemen zu besinnen und zunächst deutlich zu machen, welchen Wert Privatheit überhaupt beanspruchen kann.

3.2 Privatsphäre als schützenswertes Gut

Bevor ein Blick auf die Debatte um Privatsphäre in Zeiten der Digitalisierung möglich ist, sollte Privatheit definiert werden und ihre Einordnung als schützenswertes Gut begründet werden.

Eine historische Annäherung zeigt, dass die private und die öffentliche Sphäre schon seit vielen Jahrhunderten untrennbar miteinander verbunden sind. Der Begriff „Privatheit" stammt aus dem Lateinischen. Abgeleitet vom Verb „privare", was ‚berauben' bedeutet, bezeichnete „privatus"

den Bürger, der sich nicht politisch betätigte. Er war der öffentlichen Beobachtung entzogen bzw. beraubt (vgl. Schaar 2007: 15–16). Privatsphäre in der heutigen Bedeutung und ihr Gegenstück, die moderne Öffentlichkeit, haben sich vor allem in der bürgerlichen Gesellschaft herausgebildet. Das Bürgertum hegte den Wunsch, die individuellen Verhältnisse und Vorlieben den Einblicken Dritter zu entziehen, um so ein öffentliches Handeln überhaupt erst möglich zu machen (vgl. Schaar 2007: 16). Ohne Privatheit kann es also keine freie Öffentlichkeit geben, zumal die Privatsphäre als Raum des individuellen Rückzugs als eine Voraussetzung der freien Meinungsbildung gilt (vgl. Schaar 2007: 15–16). Im Laufe der Geschichte zeigt sich: „Je ‚öffentlicher' die Öffentlichkeit wurde, je größer also der Radius der veröffentlichten Informationen wurde, desto dringender wurde der Schutz der Privatheit" (Schaar 2007: 17).

Doch Privatheit ist nicht allein als Gegenstück zu Öffentlichkeit bedeutsam. Verletzungen der Privatsphäre betreffen in erster Linie das Individuum, das erscheint auf den ersten Blick logisch. Allerdings ist es für eine wissenschaftliche Auseinandersetzung mit dem Thema notwendig, rationale Gründe für die individuelle Bedeutsamkeit von Privatsphäre zu erkennen. Baumann (2015) untermauert seine Forderung nach Privatheit als Menschenrecht daher mit drei grundlegenden Interessen: Würde, Freiheit bzw. Autonomie und Gleichheit. Beobachtung im weitesten Sinne kann je nach Kontext eine Verletzung der Würde bedeuten, die nicht nur von der subjektiven Bewertung des Beobachteten abhängt, sondern genauso auch durch Außenstehende erkennbar sein kann. Ein viel diskutiertes Beispiel ist hier die TV-Sendung *Big Brother*: Zwar entscheiden sich die Kandidaten bewusst für die konstante Kameraüberwachung, als Zuschauer empfindet man jedoch etwa Aufnahmen unter der Dusche als entwürdigend für die gefilmte Person. Beobachtung stellt weiterhin eine Einschränkung der menschlichen Freiheit und Autonomie dar, da bei Entscheidungen unter Beobachtung Fremdbestimmung immer eine Rolle spielt. Schließlich schützt Privatsphäre vor Diskriminierung, da sie gesellschaftliche Ungleichheiten verdeckt, die nicht für das Gemeinwohl notwendig sind (vgl. Baumann 2015: 14–15).

Beate Rössler setzt sich in ihrer Monographie *Der Wert des Privaten* intensiv mit der Frage auseinander, welche Bedeutung Privatheit für das Individuum hat. Um definitorisch nicht von Begriffen wie „Öffentlichkeit" abhängig zu sein, schlägt sie einen anderen Ansatz zum Verständnis von Privatheit vor: „[A]ls privat gilt etwas dann, wenn man selbst den Zugang zu diesem ‚etwas' kontrollieren kann. Umgekehrt bedeutet der Schutz von Privatheit dann einen Schutz vor unerwünschtem Zutritt anderer" (Rössler 2001: 23). Legt man diese Definition zugrunde, zeigt sich deutlich, dass zwischen Privatsphäre und ‚Big Data' ein unübersehbarer Zusammenhang besteht: Der Nutzer hat keine Kontrolle darüber, wer welche Daten sammelt und damit Zugang dazu hat – ‚Big Data' stellt somit per se eine Verletzung der Privatsphäre dar. Damit ist jedoch weiterhin nicht geklärt, warum Privatsphäre schützenswert sein sollte. Rössler begründet dies in erster

Linie mit der Autonomie des Menschen. Privatheit in drei Differenzierungen ist dabei Teil des Rechts auf Selbstbestimmung: die Privatheit der Daten (informationell), private Entscheidungen und Handlungen (dezisional) und die Privatheit der Wohnung (lokal) (vgl. Rössler 2001: 25). Dass kein Fremder ohne Einladung die eigene Wohnung betreten darf oder dass Entscheidungen persönlicher Natur nicht mit jedem geteilt werden, leuchtet schnell ein. Der Wert informationeller Privatheit, um die es vorrangig bei der Diskussion um ‚Big Data' geht, ist dagegen weniger offensichtlich. Rössler meint mit dem Begriff die Kontrolle über die Informationen der eigenen Person gegenüber anderen. Im Grunde bedeutet dies, dass eine Person einschätzen kann, wie andere über sie denken bzw. was sie über sie wissen:

> [D]er Schutz informationeller Privatheit ist deshalb so wichtig für Personen, weil es für ihr Selbstverständnis als autonome Personen konstitutiv ist, (in ihren bekannten Grenzen) *Kontrolle über ihre Selbstdarstellung* zu haben, also Kontrolle darüber, wie sie sich wem gegenüber in welchen Kontexten präsentieren, inszenieren, geben wollen, als welche sie sich in welchen Kontexten verstehen und wie sie verstanden werden wollen (Rössler 2001: 209; Hervorhebung im Original).

Wird jemand heimlich abgehört oder beobachtet, herrscht sowohl eine kognitive als auch eine voluntative Asymmetrie zwischen Beobachtern und Beobachteten, was bedeutet, dass die Personen nichts von der Beobachtung wissen und diese auch nicht wollen. Diese Asymmetrie ist ebenfalls bei ‚Big Data' gegeben. Zwar wissen die meisten Nutzer über die Datensammlung Bescheid, können das Ausmaß und die Weiterverbreitung jedoch nicht erfassen. In der Regel wollen Nutzer das Vorgehen nicht explizit, sie nehmen es lediglich aufgrund der gebotenen Gratifikation hin (vgl. Rössler 2001: 204).

Informationelle Privatheit ist dabei nicht nur ein intrinsisches Bedürfnis, sondern bildet die Voraussetzung für das Ausüben von Autonomie (vgl. Rössler 2001: 203). Ganz grundsätzlich stellen die neuen Informationstechnologien aus zwei Gründen ein Problem dar: Einerseits, weil sie gegen den Willen von Personen ‚entprivatisieren' und andererseits, weil sie zu einer Bereitschaft der Reduktion des Privaten führen können. In der Konsequenz verliert die Privatsphäre an Bedeutung:

> Dies trifft dann jedoch nicht nur die Idee eines gelungenen – selbstbestimmten – Lebens, sondern auch die Idee der liberalen Demokratie: die nämlich auf autonome und sich ihrer Autonomie bewusste und diese schätzende Subjekte angewiesen ist (Rössler 2001: 218).

Neben der Autonomie des Individuums sieht Matzner (2017) die Dimension sozialer Beziehungen als relevant für Privatsphäre an. Er möchte daher mit dem Begriff der relativen Privatheit Rösslers Ansatz weiterführen und auf die Beziehungsebene ausweiten (vgl. Matzner 2017: 79). Relevant sind

hier besonders die sozialen Rollen, die Personen in alltäglichen Kontexten einnehmen. Privatheit wird in diesem Zusammenhang verstanden als Moderator für die Ausgestaltung dieser Rollen:

> Privatheitsnormen moderieren, welche Erscheinungsweisen eine Rolle beim Kuratieren dieser Erscheinung und deren Wahrnehmung durch andere spielen können. Sie moderieren die Art und Weise, wie wir werden können, wer wir sind, indem sie verschiedene Erscheinungen in verschiedenen Situationen auseinanderhalten (Matzner 2017: 88).

Der Wert von Privatheit besteht folglich nicht nur in einer individuellen autonomen Entscheidung. Vielmehr geht es darum „die Freiheit zu schützen, bestimmte Personen sein oder werden zu können" (Matzner 2017: 90). Im sozialen Gefüge wird diese Entscheidung nicht unabhängig getroffen, sondern im Zusammenspiel mit anderen als Aushandlungsprozess. Insgesamt „schützt Privatheit grundsätzlich die Freiheit zur Veränderung, die Freiheit eine andere Person werden zu können und damit auch die Pluralität menschlichen Lebens" (Matzner 2017: 92).

3.3 Sprachassistenten als Bedrohung für die Privatsphäre

Wie genau haben Sprachassistenten nun einen Einfluss auf die Privatsphäre ihrer Nutzer? Alexa hat viele Funktionen, die eine positive Auswirkung auf den Alltag haben. Die Kommunikation mit verschiedenen Diensten muss nicht mehr manuell ausgeführt werden, sondern kann durch gesprochene Sprache stattfinden. Der Nutzer muss sich nicht mehr bewegen, denn der Sprachbefehl reicht aus, selbst für kleine Aufgaben wie die Regelung der Lautstärke. Die Nutzung von Sprachassistenten ist bequem und vereinfacht einige Handlungen im Alltag. Begeisterte Nutzer würden sagen, dass die positiven Aspekte der Nutzung überwiegen und negative Aspekte weniger stark ins Gewicht fallen. Negative Auswirkungen der Nutzung sprachbasierter Assistenten existieren jedoch ebenso und sollen in diesem Kapitel genauer betrachtet werden.

3.3.1 Technische Angreifbarkeit von Alexa durch Dritte

Ein zentraler Aspekt, der die Nutzung von Amazons Alexa problematisch macht, ist die Angreifbarkeit der Sprache. Studien, wie die der Michigan State University und der Chiao Tung University in Taiwan (2018) zeigen, dass Angriffe auf die Sicherheit von Alexa möglich sind und welches Ausmaß diese annehmen können. Alexa reagiert, sobald sie ihr Aktivierungswort erkennt. Es gibt jedoch keine Einstellung, dass nur der Besitzer des Geräts einen Befehl senden kann. Jede Person, die das Aktivierungswort ausspricht und einen validen Sprachbefehl äußert, kann eine Funktion von

Alexa starten. Die Spracheingabe ist nicht personalisiert. Da das Gerät im Normalfall innerhalb geschlossener, privater Räume steht, ist ein Eingriff durch fremde Personen eher unwahrscheinlich. Trotzdem kann beispielsweise ein Gast ebenfalls Befehle an Alexa richten. Da Alexa fast ausschließlich durch menschliche Sprache gesteuert wird, jedoch keine physische Person anwesend sein muss, ist die Sprachsteuerung angreifbar (vgl. Ali u.a. 2018: 1). Es ist also auch möglich, dass eine Person außerhalb der Wohnung einen Sprachbefehl an Alexa richten kann. Alexa nimmt laut der Studie von Ali u.a. nur Sprachbefehle innerhalb von acht Metern auf (vgl. Ali u.a. 2018: 4). Dies bedeutet, dass sich eine Person innerhalb dieses Radius' befinden muss. Ein geöffnetes Fenster ist jedoch eine Möglichkeit, wie der Sprachbefehl an Alexa gerichtet werden kann, auch von außerhalb des Raumes, in dem sie sich befindet. Eine weitere Möglichkeit dafür sind Geräte mit Lautsprechern, die Sprachbefehle äußern können. Über einen laufenden Fernseher oder das Radio können so ebenfalls Sprachbefehle an Alexa gerichtet werden. Außerdem könnten die Geräte durch Hacker gesteuert werden. Ali u.a. (2017) schlagen vor, eine sensorische Technologie einzuführen, die misst, ob sich eine physische Person innerhalb des Raumes befindet. So könnte man sicherstellen, dass andere Geräte oder Personen außerhalb des Raumes nicht unbeaufsichtigt mit Alexa kommunizieren können.

Alexa und die verknüpften Skills an sich können also durch dritte Personen angegriffen werden. Zusätzlich können aber noch weitere Anwendungen durch Dritte attackiert werden, wenn der Sprachassistent beispielsweise mit ‚Smart-Home-Devices' verknüpft ist. Wenn jemand durch das Fenster Alexa auffordert, das ‚Smart-Lock' der Haustüre zu öffnen, kann die dritte Person sich Zugang zum Haus verschaffen. Dieses Beispiel zeigt, welches Ausmaß die Angreifbarkeit des Kommunikationsweges mit dem Sprachassistenten annehmen kann.

Eine Studie der Firma Syss (2017) zeigt ebenfalls, dass Anwendungen, die auf dem ‚Internet of Things' basieren, leicht angegriffen werden können. Das ‚Internet of Things' kann als „Kommunikation zwischen intelligenten Geräten ohne aktives Zutun des Menschen" (Schreiber und Straßheim 2017: 623) bezeichnet werden. Mit der Vision von allgegenwärtigen ‚intelligenten' Umgebungen geht die Angst vor einer umfassenden Überwachung des Einzelnen durch den Staat und die Wirtschaft sowie vor Missbrauch durch Kriminelle einher (vgl. Langheinrich 2007: 233). Wie bereits beschrieben, können so verknüpfte intelligente Systeme durch Dritte gesteuert werden:

> Befindet sich nun das Smartphone […] im Haus und ist ein Sprachassistent aktiv, reicht ein gekipptes Fenster aus, um sich die Haustüre öffnen zu lassen. […] Hierbei ist allein der Befehl ausschlaggebend, der Sprachassistent ist nicht fähig, Menschen anhand ihrer Stimme zu unterscheiden (Schreiber und Straßheim 2017: 625).

Außerdem kann ein Angreifer durch Manipulation des Datenverkehrs die Software kontrollieren. Da Sprachassistenten nur mithilfe des Internets und einer Verknüpfung mit der Cloud funktionieren, können sich Angreifer über die gespeicherten Daten Zugang zum System verschaffen, zum Beispiel über veraltete Software (vgl. Schreiber und Straßheim 2017: 624). Weil sie keinen internen Speicher besitzen, werden alle Anfragen, Befehle oder Informationen allgemein direkt in der Cloud gespeichert. Daraus entsteht ein „erhöhtes Sicherheitsrisiko, weil Angreifer nur einen zentralen Punkt, nämlich den in der Cloud angesiedelten Server des Anbieters, attackieren müssen, um zu einer Vielzahl von Systemen Zugang zu erhalten" (Schnurer 2015: 24). Die Angreifbarkeit der Technik hinter Alexa ist also definitiv gegeben. Welche Motive oder welchen Nutzen ein Angreifer hat, den Sprachassistenten über Sprache oder die Software zu manipulieren, kann unterschiedlicher Natur sein.

Warum ist es nun aber problematisch, wenn ein Sprachassistent wie Alexa attackiert wird? Einerseits gibt es die Möglichkeit, dass eine fremde Person Zugang zu den privaten Räumen des Nutzers erlangt. Wie in Kapitel 3.2 beschrieben, ist aber auch die informationelle Privatheit der Personen eingeschränkt, wenn solche Sicherheitslücken bestehen. Andererseits kann eine fremde Person in die Kommunikation mit dem Gerät eingreifen und möglicherweise Anwendungen starten, die nachteilig für den Nutzer sind.

3.3.2 Preisgabe privater Daten aus Bequemlichkeit und die Folgen

Daten, die Alexa von ihren Nutzern speichert, können ebenfalls durch solche externen Angriffe missbraucht werden. Gleichzeitig haben die Anbieter der Sprachassistenten jederzeit Zugriff auf diese Daten und nutzen sie für Werbezwecke und die Verbesserung ihrer Dienste. Schnurer thematisiert ‚Big Data' als Nebenprodukt der Bequemlichkeit, die Anwendungen wie Sprachassistenten ermöglichen: „Auch hier erkaufe ich mir also Bequemlichkeit in Form von Spracheingabe und immer besser auf mich zugeschnittene Ergebnisse mit Daten und Informationen, die ich dem jeweiligen Anbieter zur Nutzung überlasse" (Schnurer 2015: 24). Die digitalen Dienstboten ermöglichen es, viele Aktionen und Kommunikationen stark zu erleichtern. Durch die Nutzung dieser Geräte im privaten Raum lässt man aber auch die jeweiligen Anbieter mit hinein in die eigene Privatsphäre:

> Der Preis für diese Bequemlichkeit ist ganz eindeutig die Aufgabe unserer Privatheit im klassischen Sinne. Unser Leben wird von privaten Unternehmen in einem Maße durchleuchtet und erfasst, von dem Geheimdienste nur träumen können – und das mit unserer fleißigen Mithilfe (Schnurer 2015: 28).

In ihren Privatsphärebestimmungen sind die Nutzungsvereinbarungen streng geregelt und auch gesetzlich vorgeschrieben. Da die Standardein-

stellung die Speicherung aller Daten zulässt, muss der Nutzer selbst aktiv werden. Auch die Aufzeichnung aller Vorgänge, die über Alexa getätigt werden, wird erst auf Initiative des Nutzers gelöscht.

Unternehmen wie Amazon, Google oder Facebook brauchen große Mengen an Daten, um ihren Service zu verbessern und um Werbung so anzubieten, dass sie auf den einzelnen Nutzer zugeschnitten ist. Bei dem Sprachassistenten Alexa handelt es sich um ein Gerät, das sich in der privaten Wohnung befindet und dort immer in Bereitschaft ist, Sprachbefehle entgegenzunehmen. Aufgrund ihrer Technik müssen Sprachassistenten die ganze Zeit mithören. Die Unternehmen versichern zwar, dass die Sprachaufnahme erst nach Nennung des Aktivierungswortes startet, doch hier besteht ein großes Potenzial für Datendiebstahl und andere Angriffe (vgl. Hoy 2018: 85). Alexa kann also spätestens sobald das Aktivierungswort ausgesprochen wird, private Gespräche mithören und intime Themen, Vorlieben oder Gewohnheiten erfahren. Darin zeigt sich eine große Parallele zu den analogen Dienstboten. Dienstboten hatten, wie in Abschnitt 2 beschrieben, einen direkten Zugang zum privaten Raum ihrer Geschäftsgeber und konnten dort an intime und private Informationen gelangen. Der Nutzen war – wie bei den digitalen Dienstboten auch – trotzdem groß und schien zu überwiegen. Die Loyalität der Dienstboten wurde vorausgesetzt. Die Loyalität eines technischen Gerätes, in diesem Falle Alexa, wird von den Nutzern ebenfalls vorausgesetzt. Dies beinhaltet ebenfalls die Loyalität eines wirtschaftlichen Unternehmens mit finanziellen Interessen an der Nutzung des Produkts. Prinzipiell ist diese Loyalität in den Privatsphäre-Einstellungen von Amazon abgesichert und es ist für das Unternehmen nicht nützlich, dieses Vertrauen der Kunden zu verletzen. Dies würde dem wirtschaftlichen Interesse ebenfalls schaden. Viel wichtiger ist diese Thematik aus der Perspektive des Nutzers. Welchen Einfluss hat die freiwillige Preisgabe solcher privaten und intimen Informationen auf die Privatsphäre? Die Nutzer von Sprachassistenten[2] geben nebenbei persönliche Daten her, um diese Geräte nutzen zu können. Datenpreisgabe ist also die Zugangsschwelle, die überschritten werden muss, um teilhaben zu können.

Das Vertrauen, das die Nutzer Firmen wie Amazon entgegenbringen, ist hierbei ähnlich groß wie das Vertrauen, das man engen Freunden oder Familienmitgliedern entgegenbringt. Intimste Themen können von Alexa erfasst, gespeichert und mit anderen Daten verknüpft werden. Durch die Skills, die Alexa nutzt, können ebenfalls Dritte auf diese Daten zugreifen. Sie müssen es sogar, um überhaupt Anfragen verarbeiten zu können. Mithilfe von Suchanfragen und Sprachbefehlen an Alexa können Amazon oder Google von privaten Informationen erfahren, wie beispielsweise einer Schwangerschaft oder auch von bestimmten Vorlieben. Die Daten sind also preisgegeben und können hinterher zwar wieder gelöscht werden, verarbeitet wurden die Daten dann jedoch bereits. Schnurer fordert daher einen bewussteren Umgang mit den persönlichen Daten: „Wir müssen lernen, wirklich Privates privater zu halten als bisher. Wir müssen ein Bewusstsein dafür entwickeln, wie schnell wir wo Datenspuren hinterlassen“ (Schnurer 2015: 28).

Dienstboten, die einen Zugang zu den privaten Räumen ihrer Arbeitgeber hatten, erlangten das Vertrauen durch ihre Loyalität. Sie waren außerdem Ansprechpartner bei persönlichen Fragen ihrer Arbeitgeber. Bei technischen Geräten wie Alexa fällt der menschliche Charakter, der Dienstboten auszeichnet, weg. Dadurch, dass das Gerät aber mit einer menschenähnlichen Stimme spricht, wird wiederum Intimität erzeugt. In einer Studie der Universität Hohenheim, durchgeführt von Trepte und Masur (2015), wurden 2.824 Personen befragt, worüber sie besonders besorgt sind, wenn es um ihre Privatheit im Internet geht. 75 Prozent der Befragten sind sehr besorgt, dass sie keinen Einblick haben, was mit ihren Daten geschieht. In derselben Studie wurde aber auch gefragt, ob die Nutzer wissen, dass sie ihre personenbezogenen Daten einsehen können. Nur 44 Prozent der Befragten wussten davon. In der Studie geht es um das Internet im Allgemeinen und die Privatheit im Wandel.

Eine Studie des Marktforschungsinstituts Rheingold (Buggert 2017) befragte Nutzer von Alexa speziell zu ihrer Einstellung gegenüber der Technologie. Die Studie ist mit qualitativen Interviews durchgeführt worden und deshalb nicht repräsentativ, kann aber trotzdem ein Stimmungsbild wiedergeben. In der Studie wurden 20 Personen im Alter zwischen 20 und 75 Jahren befragt und parallel Erfahrungsberichte in sozialen Medien ausgewertet. Die Befragten werten Alexa als ihren persönlichen Zugang zur Technik der Zukunft und der Besitz eines sprachgesteuerten Assistenten wird als Statussymbol betrachtet. Gleichzeitig hat Alexa Auswirkungen auf das Machtgefühl ihrer Nutzer: „Bei den Nutzern ist die Hoffnung groß, dass sich mit Alexa eine neue Ära der Allmacht eröffnet“ (Buggert 2017: o. S.). Diese Macht zeichnet sich besonders dadurch aus, dass die Nutzer ohne viel Aufwand auf alle möglichen Anwendungen zugreifen können. Sie können Befehle geben und sich so ohne Widerspruch Wünsche erfüllen oder Aufgaben abnehmen lassen. Außerdem ruft Alexa durch die Kommunikation über Sprache ein Gefühl der Geborgenheit hervor (vgl. Buggert 2017). Hier zeigt sich, dass die sprachliche Ebene der Kommunikation und die Personalisierung des Geräts Auswirkungen auf die Emotionen der Nutzer haben können. Die Nutzer sind es gewohnt, dass ihre Kommunikationspartner menschlich sind und fühlen sich deshalb bei Sprachassistenten eher geborgen, wenn sie menschliche Züge haben. Paradoxerweise gaben die Befragten jedoch auch an, dass Alexas Funktionen in ihnen Angst vor dem Kontrollverlust in Bezug auf Abhängigkeit und Fremdbestimmung hervorrufen. Dies wird besonders auf den Verlust der Kontrolle über die persönlichen Daten und freien Entscheidungen bezogen:

> Sie fürchten mit Alexa buchstäblich in einen Zustand der Hörigkeit zu geraten. Vordergründig machen sich diese Befürchtungen oft daran fest, dass Alexa und damit Amazon einen rund um die Uhr abhören. Nichts ist mehr privat. ‚Amazon wird zur Datenkrake, die mich kategorisiert und alles von mir weiß.‘ Hintergründig ist mit der Hörigkeit aber auch die Furcht vor dem völligen persönlichen Kontrollverlust verbunden (Buggert 2017: o. S.).

Die Verbraucherzentrale (2017) warnt ebenfalls vor den Gefahren, die potenziell durch die Nutzung eines Sprachassistenten wie Alexa für die persönliche Privatsphäre entstehen können. Darüber hinaus können auch die Persönlichkeitsrechte von Gästen oder Familienmitgliedern verletzt werden, wenn diese sich im Raum befinden und Alexa aktiv ist.

Zusammengefasst lässt sich also sagen, dass besonders die leichtfertige Hergabe von privaten Informationen an ein Wirtschaftsunternehmen problematisch ist. Die aufgezeigten Sicherheitslücken müssen bei der Nutzung von digitalen Assistenten mitbedacht werden, genau wie die Interessen, die Unternehmen an den gewonnenen Daten haben. Der ehemalige Datenschutzbeauftragte (2003 bis 2013) der Bundesregierung Peter Schaar betont die Rolle des Nutzers in dieser Thematik:

> So darf nicht vergessen werden, dass durch die stetige Erhebung, Speicherung, Übermittlung und Auswertung persönlicher Daten den Betroffenen zunehmend die Kontrolle darüber entgleitet, wer was über sie weiß. Wenn der Einzelne die Verfügungsmacht über die von ihm preisgegebenen Informationen verliert, ist sein Recht auf informationelle Selbstbestimmung im Kern bedroht (Schaar 2007: 50).

Damit spricht Schaar konkret die Bedrohung der Privatsphäre und die darin enthaltenen Werte an. Informationelle Selbstbestimmung und die Kontrolle über persönliche und private Daten werden aufgegeben. Die Zerstreuung von Daten führt dazu, dass der Einzelne diese nicht mehr überblicken kann und so die Kontrolle darüber verliert, wer welche Daten über ihn gespeichert hat. Außerdem wird die Datenhergabe in unterschiedlichen Kontexten (Sprachassistenten, Soziale Netzwerke, Online Shopping, usw.) zu einer Notwendigkeit, die nur durch Verzicht vermieden werden kann. Je öfter persönliche Daten angegeben werden, desto mehr verlieren sie an Bedeutung. Psychologisch gesehen wird mit ihrer Degradierung zur Nebensächlichkeit die Schwelle des Widerstands bei den Nutzern geringer.

4. Konklusion

Sprachassistenten können als Wegbereiter der gläsernen Privatsphäre angesehen werden, wie dieser Artikel exemplarisch anhand von Amazons Alexa erörterte. Durch ihre vielfältigen Funktionen stellen die intelligenten persönlichen Assistenten einerseits eine Erleichterung in vielen Lebenssituationen dar. Dabei lassen sie sich in vielerlei Hinsicht mit Dienstboten des 18. bzw. 19. Jahrhunderts parallelisieren. Die heutige digitale Dimension der Dienstboten hat jedoch andererseits tiefgreifende Auswirkungen auf die Privatsphäre: Sprachassistenten haben durch ihre Funktionsweise technische Sicherheitslücken, die von Angreifern genutzt werden können, um sich Zugang zu den privaten Räumen der Nutzer zu verschaffen. Damit wird die lokale Privatheit gefährdet. Der größere Einfluss digitaler Dienstboten wie Alexa liegt jedoch bei der informationellen Privatheit der Nutzer.

Durch die großen Datenmengen, die ein Sprachassistent speichern und weitervermitteln muss, sind auch viele persönliche und intime Daten im Umlauf. In der Cloud werden sie vom Anbieter zwar geschützt, befinden sich trotzdem außerhalb der Kontrolle der Nutzer selbst. Den Firmen, die Sprachassistenten anbieten, wird also großes Vertrauen entgegengebracht. Dieses Vertrauen bezieht sich einerseits darauf, dass mit den Daten vertrauensvoll umgegangen wird und keine Überwachung des privaten Raums der Nutzer stattfindet. Andererseits vertrauen die Nutzer darauf, dass die Anbieter ihre Daten nicht verlieren oder verkaufen. Obwohl dieses Vertrauensverhältnis durch die Privatsphärebestimmungen geregelt ist, gibt der Nutzer die Kontrolle über seine persönlichen Daten und Informationen ab.

Obgleich einige Post-Privacy-Anhänger in einer gläsernen Privatsphäre die Chance für mehr Toleranz und Transparenz sehen, hat sich gezeigt, dass Privatheit als schützenswertes Gut anzusehen ist. Denn Privatheit ist erstens für die individuelle Autonomie des Menschen konstitutiv, da ein selbstbestimmtes Leben nur möglich ist, wenn jede Person frei entscheiden kann, was andere über sie wissen. Dabei handelt es sich zweitens um einen Aushandlungsprozess, dessen Ergebnis die Repräsentation einer Person in einem sozialen Kontext ist. Privatheitsnormen fungieren hier als Moderator. Schließlich ist drittens Privatheit unerlässlich, um eine funktionierende gesellschaftliche Öffentlichkeit zu schaffen. Privatheit kann somit als essentiell für eine demokratische und freiheitliche Gesellschaft gesehen werden.

Daraus ergibt sich die Notwendigkeit, die Privatsphäre nachhaltig zu schützen (vgl. Schaar 2007: 237). Einerseits liegt die Verantwortung für die persönlichen Daten der Nutzer zwar bei den Firmen, die sie verwenden. Insgesamt sollten Politik, Wirtschaft und Wissenschaft mit technischen Möglichkeiten verantwortungsvoll umgehen (vgl. Schaar 2007: 221). Doch das Verantwortungsbewusstsein für die eigenen Daten muss andererseits beim Nutzer der Sprachassistenten selbst beginnen: „[Die Privatsphäre] wird mehr denn je davon abhängen, welchen Wert unsere Gesellschaft diesem Gut beim Abwägen gegenüber Bequemlichkeit, Effizienz und Sicherheit zuweisen wird“ (Langheinrich 2007: 233).

Anmerkungen

1 Laut Amazons Produktseite, abgerufen von https://www.amazon.de/b?ie=UTF8&node=12775495031 [Letzter Zugriff am 24.02.2019].

2 Nicht nur die Nutzer von Sprachassistenten geben ihre Daten preis, auch Nutzer des Internets im Allgemeinen oder Besitzer von Kundenkarten tun dies. Hier soll aber der Fokus auf die Nutzer von Sprachassistenten gelegt werden.

Literatur

Ali, Kamran, Xinyu Lei, Chi-Yu Li, Alex X. Liu, Guan-Hua Tu und Tian Xie (2017). The Insecurity of Home Digital Voice Assistants – Amazon Alexa as a Case Study. URL: https://arxiv.org/pdf/1712.03327.pdf [Letzter Zugriff am 07.03.2019].

Bartmann, Christoph (2016). *Die Rückkehr der Diener. Das neue Bürgertum und sein Personal.* München: Carl Hanser.

Baumann, Max-Otto (2015). *Privatsphäre als neues digitales Menschenrecht?: Ethische Prinzipien und aktuelle Diskussionen.* Hamburg: Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI).

Bedford-Strohm, Jonas (2017). Voice First? Eine Analyse des Potentials von intelligenten Sprachassistenten am Beispiel Amazon Alexa. *Communicatio Socials* 4, 485–494.

Budde, Gunilla-Friederike (1999). Das Dienstmädchen. In: Ute Frevert und Heinz-Gerhard Haupt (eds). *Der Mensch des 19. Jahrhunderts.* Frankfurt a.M. und New York: Campus, 148–175.

Buggert, Sebastian (2017). Pilotstudie. Wie Alexa die geheimen Wünsche ihrer Nutzer erfüllt. URL: http://www.rheingold-marktforschung.de/pilotstudie-alexa/ [Letzter Zugriff am 06.03.2019].

Hoy, Matthew B. (2018). Alexa, Siri, Cortana, and More. An Introduction to Voice Assistants. *Medical Reference Service Quarterly* 37, 1, 81–88.

Krajewski, Markus (2010). *Der Diener. Mediengeschichte einer Figur zwischen König und Klient*. Frankfurt a.M.: Fischer.

Langheinrich, Marc (2007). Gibt es in einer total informatisierten Welt noch eine Privatsphäre? In: Friedemann Mattern (ed.). *Die Informatisierung des Alltags. Leben in smarten Umgebungen.* Berlin und Heidelberg: Springer, 207–264.

Lenz-Kesekamp, Vera und Tony Weber (2018). Alexa Skills. Welche Chancen und Risiken sind damit verbunden? *Wirtschaftsinformatik & Management* 6, 18–25.

López, Gustavo, Luis Quesada und Luis A. Guerrero (2018). Alexa vs. Siri vs. Cortana vs. Google Assistant. A Comparison of Speech-Based Natural User Interfaces. In: Isabel L. Nunes (ed.). *Advances in Human Factors and System Interactions.* Cham: Springer, 241–250.

Lyon, David (2007). *Surveillance Studies. An Overview.* Malden: Polity Press.

Matzner, Tobias (2017). Der Wert informationeller Privatheit jenseits von Autonomie. In: Steffen Burk, Martin Hennig, Benjamin Heurich, Tatiana Klepikova, Miriam Piegsa, Manuela Sixt und Kai Erik Trost (eds.). *Internetrecht und Digitale Gesellschaft: Band 10. Privatheit in der digitalen Gesellschaft.* Berlin: Duncker & Humblot, 75–93.

Maurer, Michael (1995). Dienstmädchen in adeligen und bürgerlichen Haushalten. In: Gotthard Frühsorge, Rainer Gruenter und Beatrix Freifrau Wolff Metternich (eds.). *Gesinde im 18. Jahrhundert.* Hamburg: Felix Meiner, 161–187.

Roser, Andreas (2018). Warum sprechen Menschen mit Maschinen? *Wissenschaft & Praxis* 69, 5–6, 249–256.

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

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

Schnurer, Georg (2015). Selbst vermessen – fremd gesteuert? Konsequenzen der totalen Vernetzung. *Information – Wissenschaft & Praxis*, 67, 1, 22–28.

Schreiber, Sebastian und Alexander Straßheim (2017). IoT-Penetrationstest. *Datenschutz und Datensicherheit* 41, 10, 623–627.

Stalder, Felix (2019). Autonomie und Kontrolle nach dem Ende der Privatsphäre. In: Martin Stempfhuber und Elke Wagner (eds.). *Praktiken der Überwachten: Öffentlichkeit und Privatheit im Web 2.0.* Wiesbaden: Springer Fachmedien, 97–110.

Steinbicker, Jochen (2019). Überwachung und die Digitalisierung der Lebensführung. In: Martin Stempfhuber und Elke Wagner (eds.). *Praktiken der Überwachten: Öffentlichkeit und Privatheit im Web 2.0.* Wiesbaden: Springer Fachmedien, 79–96.

Stempfhuber, Martin und Elke Wagner (2019). Einleitung. In: Martin Stempfhuber und Elke Wagner (eds.). *Praktiken der Überwachten: Öffentlichkeit und Privatheit im Web 2.0.* Wiesbaden: Springer Fachmedien, 1–13.

Trepte, Sabine und Philipp K. Masur (2015). Privatheit im Wandel. Eine repräsentative Umfrage zur Wahrnehmung und Beurteilung von Privatheit (Bericht vom 18. Juni 2015). Stuttgart: Universität Hohenheim. URL: https://www.uni-hohenheim.de/fileadmin/einrichtungen/psych/Team_MP/Berichte/Bericht_-_Privatheit_im_Wandel_2014-06-18.pdf [Letzter Zugriff am 06.03.2019].

Verbraucherzentrale (2017). Amazon hört zu: „Echo“ jetzt auch in hiesigen Wohnzimmern. URL: https://www.verbraucherzentrale.de/aktuelle-meldungen/digitale-welt/amazon-hoert-zu-echo-jetzt-auch-in-hiesigen-wohnzimmern-13149 [Letzter Zugriff am 06.03.2019].

Zurawski, Nils (2014). Geheimdienste und Konsum der Überwachung. In: *APuZ* 64, 14–19.

Anne Diessner, Lisamarie Haas und Carina Konopka
Eberhard Karls Universität Tübingen
Institut für Medienwissenschaft
Wilhelmsstr. 50
D-72074 Tübingen
E-Mail: klaus.sachs-hombach@uni-tuebingen.de