

Teil III:
Riskante Narrative: Auswirkungen von Risikonarrativen

Riskante Narrative um das Smart Home: risikoreiche Motive und Nutzungskonstellationen vernetzter Sensoren in Haushalten.

Andreas Bischof, Franziska Baum, Tanja Lehmann

Zusammenfassung

Der Beitrag untersucht Smart-Home-Technologien als Teil diskursiver Risikonarrative und zeigt, wie dominante Erzählungen von Komfort, Sicherheit und Sorge Privatheitsrisiken verschleiern und Verantwortung individualisieren. Smart Homes werden als individuelle Konsumententscheidung und als Lösung für Alltagsentlastung und Schutz gerahmt, während Machtasymmetrien gegenüber Plattformanbietern sowie innerhalb von Haushalten weitgehend unsichtbar bleiben. Auf Basis einer qualitativen Interventionsstudie mit sensorgestützter Datenerhebung in Haushalten analysieren wir alltagspraktische Deutungen und Aushandlungen von Kontrolle, Privatheit und Verantwortung. Die Ergebnisse zeigen, dass Risiken gegenüber datenverarbeitenden Plattformen häufig als unvermeidbar akzeptiert werden, während Macht- und Kontrollverhältnisse innerhalb von Haushalten – etwa durch ungleiche Zugriffs- und Administrationsrechte auf Smart-Home-Systeme – kaum problematisiert werden. Der Beitrag versteht Smart-Home-Narrative dabei als diskursive Deutungsangebote, über die spezifische Subjektpositionen hervorgebracht werden und sich asymmetrische Macht- und Kontrollverhältnisse im privaten Raum stabilisieren. Rekonstruiert werden drei riskante Subjektpositionen, die mit spezifischen Verwundbarkeiten, Machtasymmetrien und Verantwortungsüberlastungen einhergehen: das Subjekt als „Datenopfer“, das sich angesichts übermächtiger Plattformstrukturen als handlungsunfähig erlebt, das Paar aus souveränem Administrator und abhängiger Partnerin sowie die sorgende Überwacher:in. Insgesamt verdeutlicht der Beitrag, dass Smart-Home-Narrative zur Stabilisierung asymmetrischer Machtverhältnisse im privaten Raum beitragen.

1. Einleitung

Das Zuhause gilt als besonders schützenswerter privater Raum, gerät jedoch mit der zunehmenden Verbreitung von Smart Home-Technologien unter Druck. Im Kontext des Bandes interessieren uns Risikonarrative über das Smart Home dabei in ihrer diskursiven Scharnierfunktion: Sie verbinden gesellschaftliche Wertvorstellungen und Rollenbilder mit den Handlungsmöglichkeiten der Nutzer:innen (2.). Bevor wir diese Aneignungen und Aushandlungen im Feld untersuchen, rekonstruieren wir die Metanarrative des smarten Wohnens. Die stabilsten Narrative sind von zwei Versprechen geprägt: Komfort und Sicherheit. Wir diskutieren diese Narrative und darin enthaltene Versprechen sowie ihre Implikationen für Risiken der Nutzung (3.).

Im Zentrum steht die Frage, welche Sicherheits-, Privatheits- und Kontrollvorstellungen in welchen Konstellationen von Akteur:innen und alltagsweltlichen Smart-Home-Settings tatsächlich wirksam werden. Um den Blick auf die riskanten Narrative und Akteurskonstellationen der tatsächlichen Smart-Home-Nutzung richten zu können, ist eine besondere Forschungsanlage nötig. Denn in Befragungen werden Narrative leicht reproduziert – das tatsächliche Handeln, privatsphäre-kritische Praktiken und Asymmetrien innerhalb von Haushalten werden indes weniger leicht sichtbar. Dies ist bspw. als „Privacy Paradox“ benannt worden: Eine grundsätzliche Ablehnung von Datenauswertung aus dem Zuhause wird zwar von vielen für wichtig und schützenswert gehalten, dies übersetzt sich jedoch nicht unbedingt in Konsumpraxen und Privatsphäre schützendes Verhalten (Gerber et al. 2018).

Aufbauend auf einer qualitativen Interventionsstudie, in der Teilnehmende Zugang zu Daten einer niedrigschwelligen Smart-Home-Sensorik erhielten und anschließend in reflektierenden Einzel- und Gruppengesprächen befragt wurden, wird aufgezeigt, welche Narrative und daraus abgeleitete Subjektpositionen von Smart-Home-Nutzer:innen aufgegriffen, zurückgewiesen, ignoriert oder transformiert werden. Wir zeigen und diskutieren typische Motive und Konstellationen im Hinblick auf Risiken. Erkennbar wird, wie das Smart Home und das damit einhergehende Privatheitsrisiko – insbesondere die Überwachung und Nachvollziehbarkeit von Tagesabläufen – über Narrative wie Komfort und Bequemlichkeit, Sicherheit und Kontrolle sowie das Wohlbefinden Angehöriger legitimiert wird. Die Frage nach Risiken wird dabei von den teilnehmenden Anwender:innen in zwei Richtungen ausgeblendet: Gegenüber den anbietenden Plattformkonzernen

wie z. B. Amazon fühlen sich die Nutzer:innen machtlos und bereits ausgeliefert: Wenn das Smartphone und Social Media schon alles wissen, warum die Convenience des Smart Homes ablehnen? Die Kontroll- und Machtpositionen *innerhalb* des Haushalts werden darüber hinaus fast nicht problematisiert. Konträr zum etablierten Narrativ der Bedrohung von außen geht hier ein Risiko von Mitbewohner:innen oder Vermieter:innen aus, die das Smart Home installieren und kontrollieren. Wir leiten am Ende der Diskussion drei typische, riskante Subjektpositionen ab: das Subjekt als „leichtfertiges Datenopfer“, das Paar aus souveränem Administrator und abhängiger Partnerin, sowie die sorgende Überwacher:in (4.).

Im Hinblick auf Risikonarrative wird dabei deutlich, dass die dominanten Smart-Home-Narrative tatsächliche Risiken der Nutzung verschweigen und Verantwortung individualisieren. In der Aneignung der Technik im Alltag durch Anwender:innen führt das zu Spannungsfeldern, in denen sich riskante Machtasymmetrien institutionalisieren (5.). Der Schutz des Smart-Home-Systems nach außen wird im Sinne der gängigen Sicherheitsnarrative befolgt, die internen Machtasymmetrien ausgeblendet.

2. (Risiko-)Narrative als Subjektpositionen

Narrative können soziologisch als Deutungsangebote verstanden werden, die Akteur:innen Orientierung bei der Bewertung und Gestaltung ihres Handelns bieten. Sie übernehmen eine Scharnierfunktion zwischen gesellschaftlichem Diskurs und der Praxis im Alltagsleben von Personen, indem sie diskursive Deutungen in alltagspraktische Orientierungen übersetzen. Narrative können im Kontext des Bandes zum Beispiel als die prägenden Vorstellungen von Risikobewertungen verstanden werden, die für Nutzer:innen und Betroffene beim Einsatz von digitaler Technik handlungsleitend sind.

Willy Viehöver (2001: 182, 2012a/b) etablierte den Begriff des Narrativs im Anschluss an die wissenssoziologische Diskursanalyse Kellers und beschreibt Narrative als Spezialdiskurse mit einem gewissen Spin oder einer Storyline (Keller 2005: 230). Sie formen eine kohärente Erzählung, die Orientierung im Alltag bietet. Narrative enthalten bzw. etablieren konkrete *Subjektpositionen*, also normative ideale Verhaltensweisen, wie bspw. das unternehmerische Selbst, das selbstverantwortlich seine Arbeitskraft erhält (Bröckling 2007; Bührmann 2012). Gerade vor dem Hintergrund eines digitalen Wandels werden neue Subjektpositionen wie das digitale Selbst

bzw. sich vermessende Selbst (Jarrett 2016; Lupton 2016; Mau 2017; Nosthoff/Maschewski 2019) beschrieben. Narrative rund um das Smart Home beinhalten also Subjektpositionen und damit Orientierungs- und Identifikationsangebote im Umgang mit einem zunehmend digitalen Zuhause. In diesem Sinne wirken Narrative nicht deterministisch, sondern bieten Subjektpositionen als Orientierungs- und Identifikationsangebote an, zu denen sich Akteur:innen in ihrem Handeln positionieren können.

Die narrativ vermittelten Subjektpositionen bieten allerdings keine fertigen Lösungen im Sinne von korrekten Umgangsweisen bei spezifischen Problemen, sondern sind vielmehr widersprüchliche Anforderungen an das Subjektwerden und Subjektsein in einer digitalisierten Welt. Sie ermöglichen es, einem bestimmten Ideal nachzueifern, und so konkreten „Rollen-, Identitäts- und Lebensführungsmodellen, die in Subjektpositionen konstituiert werden“ (Bosančić 2014: 92), zu folgen. Subjektpositionen sind dabei häufig affektiv aufgeladen (ebd.: 118). Sie lösen ein bestimmtes Begehren aus, sie auszufüllen – oder auch nicht. So gelten bestimmte Männlichkeitspositionen bspw. als besonders erstrebenswert, andere Positionen werden emphatisch abgelehnt (Anti-Subjekte). Das Zusammenspiel aus hegemonial-erstrebenswerten Idealen und Anti-Subjekten lässt Subjektpositionen entstehen (ebd.: 127). Narrative können alle drei Ebenen von Subjektpositionen ansprechen, indem sie spezifische Probleme identifizieren, bestimmte Problemursachen und Lösungen thematisieren, positive und negative Konsequenzen antizipieren und legitimierende Leitbilder und Prinzipien als wesentlich definieren (Viehöver 2012b: 178, 180). Im Kontext des Smart Home zeigen sich diese Narrative oft unvollständig: Sie greifen reale Probleme, Konsequenzen und Lösungen nur eingeschränkt auf, was zu einer Diskrepanz zwischen narrativem Lösungsversprechen und tatsächlicher Nutzung führt. Die Aufgabe datenbasierter Forschung ist es, die empirische Lücke zwischen der Identifikation von solchen narrativen Lösungsversprechen und ihrer tatsächlichen Manifestation und Auswirkung auf der Mikroebene zu untersuchen (Bührmann 2012, Bosančić 2014). Aus der Identifikation von typischen Subjektpositionen rund um das Smart Home ergibt sich also die Frage, wie die Subjekte auf die Anforderungen reagieren und sie in ihr digitales Alltagsleben integrieren.

Subjektpositionen werden durch Narrative vermittelt und bieten Orientierungsangebote, wie sich handelnde Personen in einem digitalen Alltag positionieren und identifizieren können. In diesem Sinne verstehen wir Narrative als typisches Medium der Subjektivierung, die über Storys bzw. Storylines Anforderungen an Subjekte enthalten, bestimmte Rollen einzu-

nehmen. Dabei erzeugen unterschiedliche und gegenläufige Debatten auch widersprüchliche Subjektpositionen. So kann eine Subjektposition die Normalisierung von Überwachung enthalten, eine andere die Ablehnung von Überwachung. Es liegt also an den Subjekten selbst, sich mit der einen oder der anderen zu identifizieren bzw. diese auszufüllen und ggf. neu miteinander zu verknüpfen. Hinsichtlich der verfügbaren Narrative und Subjektpositionen rund um das Smart Home fragen wir deshalb danach, welche Vorstellungen und Narrative von Risiken für Nutzer:innen und Betroffene handlungsleitend werden.

3. Metanarrative um das Smart Home

Zunächst muss also untersucht werden, unter welchen diskursiven Bedingungen und mit welchen Narrativen Smart-Home-Produkte in die Gesellschaft kommen. Anschließend an das Konzept der Subjektivierungsanalyse (Bosančić 2014) wollen wir zunächst klären, welche kulturell dominanten Erzählmuster sich um das Smart Home feststellen lassen, bevor wir untersuchen, wie diese sich im Feld im Hinblick auf Risiken auswirken (vgl. 4.). Dabei wurden die beiden Metanarrative Komfort und Sicherheit ausgewählt, da sie in der Literatur und in der Analyse von Industriebereichen, Marketingtexten und Zukunftsvisionen am prominentesten herausstechen (Jasanoff/Kim 2009). Gegenstand dieses Kapitels sind die „Metanarrative“ um Smart Homes, also großformatige, relativ stabile, hegemoniale Deutungsangebote, die die gesellschaftlich geteilte Idee des weitgehend unsichtbar computerisierten Zuhauses prägen. Es sei vorab betont, dass diese Metanarrative nicht die tatsächliche Nutzung oder die Erfahrungen von Nutzer:innen widerspiegeln, sondern analytische Konstrukte darstellen. Dazu greifen wir auf Befunde aus kritischen Analysen von Industrie-Berichten, Marketing-Texten und Zukunftsvisionen zurück, die als „sociotechnical imaginaries“ (Jasanoff/Kim 2009) technische Machbarkeit mit gesellschaftlich Wünschenswertem verknüpfen.

3.1 Das Smart Home als Komfort-Versprechen

Die Essenz des Smart Homes als *Annehmlichkeitsstruktur*, die Teil alltäglicher Routinen ist, bringt das berühmt gewordene „Sal-Szenario“ von Weiser (1991) auf den Punkt. Weisers Artikel hat das Feld des „Ubiquitous

Computing“ entscheidend geprägt. Weiser entwirft in seinem über 21.000-mal zitierten Text eine fiktionale Alltagssituation um eine weiblich gelesene Figur namens Sal, die in einer vernetzten (ubiquitous) Welt lebt:

Beim Aufwachen merkt Sal, wie ihr Wecker — aufmerksam geworden durch Unruhe im Schlaf — ihr bereits Kaffee gebrüht hat und nun leise fragt: „Kaffee?“ — und sie murmelte nur „Ja.“ Beim anschließenden Frühstück liest Sal ihre Zeitung, markiert mit einem elektronischen Stift eine interessante Textstelle — und der Stift sendet das Zitat automatisch an ihr Büro. Auf dem Weg zur Arbeit blickt sie in den Rückspiegel, der sie über Verkehrsverhältnisse informiert und ihr ein neues Café in der Nähe zeigt. Sie wechselt auf die Autofahrt, um einem Stau zu entgehen. Beim Betreten ihres Büros melden sich die Systeme automatisch an — Sals Alltag, ihr Arbeitsplatz und alle anderen Aufenthaltsorte sind nahtlos in das vernetzte System eingebettet. (Synopsis nach Weiser 1991, S. 102-104; Übers. d. Autor:innen)

Die thematischen Kerne des Szenarios sind unsichtbare, pro-aktive Systeme, die den Kontext wahrnehmen und in ein Narrativ der Vertrautheit und des Komforts eingebettet sind. Komfort wird hier nicht nur funktional, sondern auch affektiv verstanden: als eine durch Vertrautheit, Unsichtbarkeit und Selbstverständlichkeit hergestellte Bequemlichkeit der Techniknutzung. Weisers Artikel wirkt im Zeitalter der Smartphones und des Internet of Things rückblickend wegweisend, andererseits hat er die Realisierung der dargestellten Fiktion auch vorangetrieben. Kinsley (2011) analysiert, wie das Szenario sowohl als Prognose, Fiktion als auch als handlungsleitende Vision zugleich fungiert, und wie Elemente davon in späteren Forschungsarbeiten aufgenommen wurden. Wie Bell und Dourish (2007) zeigen, wurde Weisers Vision das dominante Narrativ in der UbiComp-Community. Sie diskutieren, dass viele Forschungspfade in diesem und verwandten Feldern stark von der Annahme beeinflusst sind, dass diese nahe Zukunft schon unmittelbar bevorstehe – und dadurch erst ermöglicht wurden.

Auf den ersten Blick wirkt das Sal-Szenario unproblematisch und kommensurabel, schließt es doch direkt an typische Alltagserfahrungen von Angestellten an. Aylett und Quigley (2015) heben allerdings hervor, dass das Szenario keineswegs eine neutrale Zukunftsvision darstellt, sondern normative Konstruktionen beinhaltet, die Homogenität, Komfort und eine bestimmte Lebensweise voraussetzen. Um an Weiser selbst anzuschließen: Wenn smarte Technologien sich in „the fabric of everyday life“ einweben sollen, lässt sich kritisch fragen, welcher Alltag dabei eigentlich vorausge-

setzt wird. Aylett und Quigley kritisieren, dass die Darstellung sozial und ökonomisch stark voraussetzungsreich ist: Sie unterstellt eine gehobene Mittelklasse-Position, gut ausgebaute Infrastruktur, technikaffine Nutzer:innen und eine soziale Umgebung, in der permanente Vernetzung gewünscht ist und ohne Konflikte oder Machtasymmetrien funktioniert. Die normative Schlagseite der Vision zeigt sich vor allem darin, dass Sichtbarkeiten und Privatheit im Szenario meist als gelöst vorausgesetzt werden — u. a. durch technische Lösungen wie Verschlüsselung oder Pseudonyme — während Fragen sozialer Ungleichheit, Zugänglichkeit und Kontrollverhältnisse gar nicht thematisiert werden. Sal ist eine idealtypische, privilegierte Wissensarbeiterin, für die das Paradigma des allgegenwärtigen, aber unsichtbaren Computers zum Komfort- und Effizienzideal gerinnt. Die Vision adressiert also jene, deren Alltag als normal vorausgesetzt und deren Bedürfnisse als normative Basis einer zukünftigen digitalen Umwelt verstanden werden. Diese Vision als wünschenswert zu deuten, unterschlägt aber Diversität in ökonomischen, kulturellen Strukturen und insbesondere Konstellationen des Zusammenlebens über Einpersonenhaushalte hinaus.

Dass Sal als alleinlebend und unabhängig dargestellt wird, passt zu den jüngeren Smart-Home-Narrativen, die vor allem Individualität und Personalisierung betonen (Dahlgren et al. 2021). Smart-Home-Services werden durch Werbung und Darstellungen in Industriekommunikation nicht nur als individuelle Kaufentscheidung vermarktet, sondern als Antwort auf den Wunsch, Produkte und Dienste exakt auf individuelle Präferenzen zuzuschneiden, um Komfort, Kontrolle und Wahlfreiheit zu maximieren (ebd.). Das Smart Home wird also nicht nur als Technik zur Steuerung des Haushalts gesehen, sondern als Plattform für Individualisierung, Identitätsausdruck, und Lifestyle. Strüver (2023) analysiert Smart-Home-Produkte wie Amazons Sprachassistenten Alexa in einer plattform-ökonomischen Perspektive als propagierte „Komfort-Infrastruktur“ für Nutzer:innen. In dieser Perspektive sind Systeme wie Alexa ein Knotenpunkt, über den der Konsum von Smart-Home-Technologien erleichtert und verstetigt wird — denn wer einmal auf Alexa setzt, tritt in ein System ein, in dem viele Geräte, Dienste und Interaktionen nur über diese Plattform sinnvoll funktionieren. Personalisierung trägt wesentlich zum wahrgenommenen Komfort bei, da sich mit zunehmender Nutzung Präferenzen, Routinen und Abhängigkeiten ausbilden, die einen Plattformwechsel unattraktiv machen. Komfort entsteht, weil Systeme Nutzungspräferenzen lernen und Situationen antizipieren, die auf detaillierten Profilen des Alltags- und Nutzungsverhaltens basieren.

Zusammenfassend lässt sich festhalten, dass das Smart Home auf einem Metanarrativ der Convenience, also Komfort und Bequemlichkeit, basiert, das in einer Steigerung des individuellen Nutzens bei hoher Personalisierung besteht, und sich durch eine hohe Alltagsintegration auf eine umfassende Individualisierung bis hin zum Identitätsausdruck auszeichnet: Das hegemonial-erstrebenswerte Ideal zeichnet smarte Subjekte, die smarte Geräte benutzen (Coleman 2018).

3.2 Das Smart Home als Kontroll-Versprechen

Neben Komfort und Alltagsentlastung bilden Narrative über Sicherheit und Schutz einen zweiten Kern der Metaerzählungen um das Smart Home. Zahlreiche Produkte werden mit dem Versprechen vertrieben, durch schnelle Benachrichtigungen Schutz vor äußeren Einflüssen wie Einbruch, Hochwasser oder Feuer zu bieten, oder durch Kameras Personen und Tiere in der Wohnung zu überwachen. Wie Stark und Levy (2018) gezeigt haben, legt dieser diskursive Mechanismus Smart-Home-Technologien über Fürsorge und Schutz vor Risiken nahe, wobei aus der alltäglichen Nutzung Überwachungspraktiken entstehen, die nicht explizit markiert werden. Im Begriff des „surveillant consumer“ verbinden die Autor:innen Konsum, Betreuung und Risikoabwehr zu einer neuen Subjektposition: Nutzer:innen kaufen Überwachungstechnologien ein, überwachen ihrerseits Familienmitglieder, Haustiere oder Objekte, wobei die resultierende Überwachung nicht als Eingriff, sondern als Ausdruck von Verantwortlichkeit und Fürsorge interpretiert wird. Sicherheit und Schutz werden durch vernetzte Kameras in Produkten wie Türklingeln oder Kinderspielzeug zu konsumierbaren Werten. Wieso sollten verantwortungsvolle Eltern kein Interesse daran haben zu wissen, was ihre Kinder gerade tun, wenn sie diese so vor Gefahren schützen könnten? Die Subjektposition der sorgenden Eltern legitimiert die Überwachung als Ausdruck von Fürsorge und Verantwortung.

Im Anschluss daran zeigen neuere empirische Arbeiten zu Smart-Home-Geräten deutlich, wie stark Sicherheit und Schutz in praktischen Nutzungskontexten als zentrale Rahmungen fungieren. Studien zu Innenraum-CCTV (u. a. Tan et al. 2022; Liu 2024) belegen, dass Smart-Home-Überwachung als Sorgepraxis – „watching over“ – verstanden wird. Heimkameras dienen dazu, Kinder, Haustiere oder ältere Angehörige „im Blick zu behalten“, Einbruch zu verhindern oder die heimische Ordnung abzusichern. Nutzer:innen entwickeln sich so zu häuslichen Sicherheitsmanager:innen,

die Ereignisse im Haus überwachen, Daten interpretieren und über Zugriff und Sichtbarkeit entscheiden. Der Schutz- und Sicherheitsdiskurs verschiebt Überwachung dadurch in einen moralisch legitimierten Raum. Gleichzeitig zeigt die Vergleichsstudie von Percy-Campbell et al. (2024), dass Nutzer:innen häufig über Risiken informiert sind, diese jedoch angesichts versprochener Kontrolle und Komfort ausblenden oder hinnehmen.

Zudem machen Studien mit Fokus auf intime Überwachung (Rogers et al. 2023; Dereymaeker et al. 2024) sichtbar, dass diese Schutz-Narrative innerhalb von Haushalten ungleich wirken und neue Machtpositionen hervorbringen. Wer Zugriff auf Geräte und Apps hat – oft Eltern, Partner:innen oder technisch versiertere Haushaltsmitglieder – gerät nicht nur in die Position des Beobachtens, sondern erhält auch die Fähigkeit, Verhalten zu regulieren oder zu sanktionieren. Das Smart Home dient damit als soziale Infrastruktur, in der Sorge und normierende Überwachung ineinander übergehen. Das Narrativ des sicheren, auch in Abwesenheit zu beschützenden Heims überdeckt die Tatsache, dass immer auch Grenzziehungen, Hierarchien und Erwartungen aktiviert werden.

Zusammenfassend zeigt sich, dass solche Narrative das Bild des Hauses als Schutzraum abrufen und den Nutzer:innen eine Ressource bieten, um persönliche Sicherheit durch Überwachung herzustellen – die „sorgende Überwacher:in“ wird zur Leitfigur.

3.3 Fazit: Dominante Smart-Home-Narrative verschieben Risiken der Nutzung

Komfort und Kontrolle, die Metanarrative rund um das Smart Home, verschieben und normalisieren Risiken der Nutzung. In ihnen sind die Wahlfreiheit und Handlungsfähigkeit der Einzelnen überbetont, und mögliche Ungleichheiten, Machtgefälle sowie resultierende Konflikte zwischen unterschiedlichen Akteur:innen ausgeblendet. Dieser Befund lässt sich auf zwei Ebenen anschaulich zeigen: Einerseits wird das Risiko der systemischen Differenz zwischen den Technikanbietern und deren vollumfänglichen Zugriff auf Datenströme und den Nutzenden in den Narrativen des Smart Homes nahezu völlig individualisiert. Andererseits wird durch die starke moralische Aufladung von sozialen Rollen wie bspw. Eltern mit Kontrolle zum Schutz umgehen sollen, eine privatheits-sensitive Diskussion zwischen unterschiedlichen Betroffenen in einem Haushalt mit Smart-Home-Technik erschwert. Dies kann die Wahlfreiheit einschränken und zu

Handlungsunfähigkeit führen, da Diskussionen zwischen Betroffenen über Privatheitsfragen erschwert werden.

Grundlegend wird die Verantwortung für den Umgang mit Smart-Home-Technik und den damit einhergehenden Risiken primär denjenigen zugeschrieben, die entsprechende Systeme erwerben und installieren. Das Smart Home erscheint als eine individuelle Kaufentscheidung mit Verantwortung, obwohl die tatsächliche Verantwortung für sichere Systeme bei Herstellern und Plattformanbietern liegt. Auf der systemischen Ebene haben die Käufer:innen daher auch die Verantwortung, die von ihnen genutzten Systeme gegenüber unbefugten Zugriffen – etwa durch Hacker, betrügerische Akteur:innen oder Plattformkonzerne – abzusichern. Die Hersteller und Vermittler von Services, Plattformkonzerne wie Meta oder Küchenhersteller wie Miele, werden dagegen in den dominanten Komfort- und Kontrollnarrativen nicht als verantwortliche Akteure sichtbar, sie sind als Träger möglicher Risiken weitestgehend unsichtbar. Wie Strüver für die vernetzende und ermöglichende Rolle von Amazons Alexa feststellt: Smart-Home-Technologie koppelt das Versprechen von mehr Selbstbestimmung an mehr Konsum, Daten-Exposition und Kontrolle durch die Plattform. Die Rückseite der Komfort-Infrastruktur ist eine Verwertungs-Infrastruktur (Strüver 2023).

Dahlgren et al. (2021) haben diesen Zusammenhang als *techno-hedonistische Imaginationslogik* bezeichnet und das Risiko identifiziert, dass dadurch andere Werte wie Privatheit, Autonomie, soziales Geflecht, Verantwortung und Nachhaltigkeit vernachlässigt werden. Die Metanarrative von Komfort und Kontrolle basieren auf der Vorstellung eines rationalen, technisch versierten, selbstbestimmten Individuums, das sämtliche Entscheidungsmöglichkeiten nutzen will. Diese Annahme übersieht Macht-, Geschlechter-, Altersunterschiede – und vor allem Dynamiken im Haushalt. Während Sal allein lebt, sind in der empirischen Wirklichkeit Partner:innen, Kinder oder Eltern, Besucher:innen sowie Dienstleister:innen im Haushalt von den Folgen der Datenverarbeitung durch Smart-Home-Geräte betroffen.

Befunde aus Konsument:innenbefragungen stützen die Lesart der Risikoverschiebung bzw. -verschleierung, zeichnen aber auch unterschiedliche Umgangsweisen der Nutzer:innen damit nach. Eine vergleichende Auswertung von 68 einschlägigen Studien zu Smart-Home-Nutzung (Percy-Campbell et al. 2024) hat festgestellt, dass viele Nutzer:innen mit den wahrgenommenen Vorteilen wie einem erhöhten Gefühl der Sicherheit zufrieden sind. Darüber hinaus zeigten die meisten Studien bei den Nutzer:innen

nur ein begrenztes Verständnis für die Praktiken der Datenerfassung oder des Datenschutzes, was dennoch mit einer hohen Nutzung korrelierte. Einige Nutzer:innen zeigen Coping-Strategien, indem sie Datenschutzrisiken bewusst akzeptieren, um Komfort und Sicherheit zu erhalten.

Hier setzt unsere Studie an, die untersucht, welche Privatheits-relevanten Praktiken in Haushalten rund um SmartHome-Daten existieren und wie Nutzer:innen auf Daten und Implikationen ihrer Daten reagieren sowie moralisch akzeptable Nutzungsweisen aushandeln.

4. Motive und Nutzungskonstellationen der Smart-Home-Nutzung in Haushalten

Für die Erforschung und Bewertung von Risikonarrativen sowie für die übergeordneten Fragen nach Freiheit und Selbstbestimmung bei der Smart-Home-Nutzung ist aus einer soziologisch informierten Sicht zu berücksichtigen, dass die Praktiken, Orte und Kontexte der *tatsächlichen Nutzung* vernetzter Alltagsgegenstände und digitaler Dienste eigensinnig, situativ und bisweilen widersprüchlich sind, etwa weil Haushalte unterschiedlich ausgestattet sind oder Nutzer:innen Geräte unterschiedlich einsetzen. Zwar lassen sich Narrative um das Smart Home und die damit implizierten Risiken anhand der kulturell geteilten Vorstellungen vom Smart Home untersuchen (vgl. 3.), gleichwohl verbleibt die Umsetzung der darin enthaltenen Subjektpositionen und die tatsächliche Praxis in der häuslichen Sphäre der Nutzung weitgehend unerforscht, da sie sich situativ, eigensinnig und teilweise widersprüchlich vollzieht und sich damit klassischen Befragungs- oder Beobachtungsmethoden nur schwer zugänglich macht.

Grundlage unserer Studie ist die Annahme, dass Nutzungs- und Sensordaten aus dem häuslichen Umfeld *sozial situiert* sind, das heißt, sie entstehen stets unter spezifischen lokalen Bedingungen und werden zugleich im Lichte des Alltagswissens der Nutzer:innen und damit innerhalb bestehender sozialer und moralischer Ordnungen interpretiert und bewertet (Fischer et al. 2016; Tolmie et al. 2016). Daten etwa zur Luftfeuchtigkeit im Kinderzimmer oder aus automatisierten Türschließsystemen sind bereits aufgrund ihres Entstehungskontexts sensibel – insbesondere innerhalb von Haushalten, da hier private Lebensbereiche und persönliche Routinen betroffen sind (Richter et al. 2018; Kurze et al. 2020).

Die bisherigen Methoden der Risikobewertung zum Smart Home (wie Information-Security-Risikoanalysen, Technology-Acceptance-Model-

le oder Normen und Standards) sind vielgestaltig, erfassen aber insbesondere diese konkrete soziale Situierung von Smart-Home-Geräten unzureichend. Während sich Einstellungen, Erwartungen und Informationsdefizite zu Smart-Home-Technologien durch klassische Erhebungsformen wie Umfragen erfassen lassen, entziehen sich jene Risiken und Implikationen, die erst im alltäglichen Gebrauch entstehen. Unser Vorgehen verfolgt daher einen kombinierten Ansatz aus lebensweltlicher Intervention mit begleitender Datenerhebung.

4.1 Wie im Smart Home forschen?

Aus der bisherigen Darstellung ergibt sich, dass der Einblick in Privatheitsrelevante Praktiken im Umgang mit Smart-Home-Produkten methodisch und technisch nicht trivial ist, da diese Praktiken stark situativ, in privaten Räumen eingebettet und teilweise unsichtbar stattfinden. Viele Nutzer:innen wissen nicht, welche Daten sie produzieren, ob und wo diese gespeichert bzw. weitergegeben und ausgewertet werden. Außerdem sind die Daten und Datenströme selbst der Wissenschaft i. d. R. nicht zugänglich und verbleiben bei den Anbietern. Im vom BMFTR geförderten Verbundprojekt *Simplications* begegnen wir dieser Herausforderung durch einen qualitativ-explorativen, mehrstufigen Ansatz, der Elemente der Cultural-Probe-Methoden (Köpferl et al. 2024) mit Gruppendiskussionen (Kurze et al. 2020) verbindet.

Die Studie beginnt mit einer Feldphase in Haushalten, die über zehn bis vierzehn Tage angelegt ist. In diesem Zeitraum wird in jedem Haushalt ein selbst entwickeltes *Sensorkit* (Kurze et al. 2025) installiert, das typische Umweltparameter anhand vermeintlich einfacher Sensoren im Zuhause erfasst. Technisch handelt es sich dabei um ein in sich geschlossenes System aus mehreren einfachen Sensoren für Temperatur, Bewegung, Licht und Luftfeuchtigkeit, das um Sensoren für Luftqualität und Lautstärke erweitert wurde. Die Sensoren sind über Bluetooth Low Energy oder WLAN mit einem Raspberry Pi verbunden, der die Messdaten kontinuierlich erfasst und lokal in einer Datenbank speichert. Die Teilnehmenden erhalten ein Tablet, über das sie innerhalb des Haushalts auf Visualisierungen der erfassten Sensorwerte zugreifen und diese eigenständig explorieren können. Die Installation des Sensorkits erfolgt beim ersten Hausbesuch gemeinsam mit den Forschenden. Neben der technischen Einrichtung wird ein erstes Interview geführt, in dem Erwartungen, bisherige Erfahrungen mit Smart-

Home-Technik und erste Assoziationen zu Sensordaten und Privatheit thematisiert werden. Parallel dazu halten die Forschenden erste Beobachtungen zum Haushalt, zu räumlichen Gegebenheiten und zur Platzierung der Sensoren in Feldnotizen fest. Den Teilnehmenden wird für jeden Tag der etwa zehn- bis vierzehntägigen Laufzeit ein Aufgabenheft in Anlehnung an Tagebuchmethoden zur Verfügung gestellt, das sie dazu einlädt, die dargestellten Daten mit konkreten Alltagsereignissen in Beziehung zu setzen, Beobachtungen zu notieren und im Verlauf der Studie auch die Position einzelner Sensoren zu verändern. Auf diese Weise wird das Sensorkit als Cultural Probe (Berger et al. 2018; Köpferl et al. 2024) eingesetzt: Es soll nicht primär „objektive“ Messwerte liefern, sondern situierte Reflexionen und Erzählungen über Daten, Alltag und Privatheit anregen. Am Ende der Feldphase wird das Sensorkit im Rahmen eines weiteren Hausbesuchs wieder abgebaut. Ein Abschlussgespräch dient dazu, Erfahrungen mit dem Kit, die Wahrnehmung der erhobenen Daten sowie mögliche Irritationen oder Konflikte zu erfassen. Die Kombination aus kontinuierlicher Datenerhebung, alltäglicher Exploration durch die Teilnehmenden und begleitenden Gesprächen erzeugt ein reiches, multimodales Datenkorpus aus Sensorzeitreihen, schriftlichen Selbstkommentaren und qualitativen Protokollen.

Etwa zehn Tage nach der Demontage des Sensorkits werden Teilnehmende aus jeweils zwei bis drei Haushalten zu einer *datenbasierten Gruppendiskussion im Format „Daten-Raten“* eingeladen. Für diese Sitzungen bereitet das Forschungsteam anonymisierte Auszüge der aufgezeichneten Sensorwerte vor (z. B. Zeitreihen zu Licht, Bewegung oder Lautstärke), die bewusst so ausgewählt werden, dass sie typische, aber potenziell sensible Alltagssituationen widerspiegeln. Im Gruppensetting werden diese Datenausschnitte gemeinsam betrachtet und diskutiert. Die Teilnehmenden werden aufgefordert, zu rekonstruieren, welche Ereignisse die Daten wahrscheinlich repräsentieren, welchem Haushalt sie zuzuordnen sind und welche Schlussfolgerungen Dritte aus solchen Daten ziehen könnten.

Das Format knüpft direkt an das in früheren Projekten entwickelte Guess-the-Data-Verfahren (Kurze et al. 2020) an, mit dem gezeigt werden konnte, dass Personen aus einfachen Smart-Home-Sensordaten nicht nur eigene Routinen, sondern auch das Verhalten anderer Haushaltsmitglieder rekonstruieren und für „laterale“ Überwachung nutzen können. Die Sitzungen werden als moderierte Gruppendiskussionen durchgeführt, in denen neben der Deutung der Daten auch normative Bewertungen, wahrgenommene Risiken sowie Ideen für alternative Gestaltungen thematisiert

werden. Die Teilnahme wurde – im Sinne einer Anerkennung des zeitlichen Aufwands – finanziell entschädigt.

Methodologisch ist die Studie im Feld einer partizipativen, interpretativen Mensch-Computer-Interaktion verortet, die Smart-Home-Sensorik nicht nur als technische Infrastruktur, sondern als Bestandteil sozialer Praktiken und Machtverhältnisse versteht. Die Teilnehmenden fungieren nicht bloß als „Datenlieferant:innen“, sondern als Ko-Interpret:innen der eigenen Daten – sowohl in der individuellen Exploration des Sensorkits als auch im kollektiven Deuten im „Daten-Raten“. Indem die Methode die Teilnehmenden dazu anregt, eigene und fremde Daten zu interpretieren, wird implizites Alltagswissen über vermeintlich „harmlose“ Sensorwerte sichtbar. Damit verfolgt das Studiendesign eine doppelte Zielsetzung: Zum einen sollen empirisch die Bedeutungszuschreibungen, Risikoabwägungen und möglichen machtförmige Praktiken im Umgang mit Sensordaten rekonstruiert werden; zum anderen wirkt das Forschungssetting selbst als Aufklärungs- und Reflexionsformat, das ein Bewusstsein für die Sensibilität solcher Daten und mögliche Schutzstrategien schärft.

Die Teilnehmenden wurden über Zeitungsanzeige, digitale Verteiler und soziale Medien zur Teilnahme aufgefordert. Die Studie fand im Raum Chemnitz und Umgebung statt, umfasste 18 Haushalte und wurde in zwei Feldphasen im Frühjahr 2024 (F1) und Frühjahr 2025 (F2) erhoben. Das Sample besteht insgesamt aus acht Paaren über 60 Jahren, zwei Müttern mit Kindern und Partner, fünf alleinlebenden Männern im mittleren Alter (teilweise verpartnert), einer WG aus zwei männlichen Personen unter 30 Jahren, einem jungen Paar unter 30 Jahren sowie einer alleinlebenden Frau über 60 Jahren. Bei den vornehmlich älteren Paaren (+60 Jahre) findet sich typischerweise ein männlicher Partner, der über eine berufliche Nähe zur IT-Branche verfügt und bereits ein eigenes Smart-Home-System betreibt. In 12 der 18 Haushalte waren smarte Geräte wie Alexa, Thermomix bis hin zu komplexen Smart-Home-Systemen vorhanden.

Zu den Limitationen der Studie gehört erstens ihre kontextuelle und sozialräumliche Spezifik: Die Erhebung in 18 Haushalten im Raum Chemnitz bildet lokale Altersverteilungen, Milieus und Deutungsrepertoires ab, und erlaubt nur eingeschränkt Rückschlüsse auf andere Regionen oder noch stärker diversifizierte Haushaltsformen. Zweitens ist die Stichprobe strukturell selektiv: Die Rekrutierung über Anzeigen, Verteiler und soziale Medien begünstigt tendenziell teilnahmebereite, reflexionsaffine und technisch aufgeschlossene Personen. Dadurch können geschlechts- und generationsspezifische Macht- und Zuständigkeitsordnungen zwar sichtbar wer-

den, zugleich bleiben aber andere Konstellationen (z. B. stark konflikthafte Arrangements oder Haushalte ohne „Gatekeeper“) unterrepräsentiert. Drittens erzeugt das Studiendesign selbst Reaktivität und Interventionseffekte: Das Sensorkit als Cultural Probe, die Visualisierungen am Tablet sowie das Daten-Raten zielen explizit auf Irritation, Reflexion und Re-Interpretation; damit werden Praktiken nicht nur beobachtet, sondern mit hervorgebracht, wodurch die Trennlinie zwischen Alltagsroutine und Forschungssituation analytisch zu markieren ist. Viertens bleibt der Zugriff auf die tatsächlichen Datenökologien kommerzieller Smart-Home-Plattformen begrenzt: Das lokale, geschlossene Sensorkit bildet zwar alltägliche Situierungen nach, kann aber die proprietären Datenflüsse, Inferenzlogiken und Plattformkopplungen realer Smart-Home-Ökosysteme nur indirekt adressieren. Schließlich ist auch das „Daten-Raten“ als Gruppensetting potenziell normativ gerahmt (z. B. durch Moderation, Anonymisierungsentscheidungen und soziale Erwünschtheit), sodass weniger die „objektive“ Reichweite von Überwachung rekonstruiert wird als vielmehr jene sozial geteilten Plausibilitäten und moralischen Bewertungen, die Teilnehmende im kommunikativen Vollzug herstellen.

Gleichwohl ist das Vorgehen in besonderer Weise aussagekräftig, weil es die Untersuchung von Risiken konsequent auf der Ebene sozialer Praxis und situierten Sinnverstehens verankert – also dort, wo sowie Narrative von Komfort und Bequemlichkeit sowie Sicherheit und Kontrolle alltagsweltlich relevant werden. Gerade die Kombination aus kontinuierlicher Datenzeitreihe, teilnehmend generierten Selbstkommentaren und rekonstruktiven Gesprächen ermöglicht eine methodische Triangulation, die nicht auf „wahre“ Verhaltensmessung zielt, sondern auf die Analyse, wie Daten zu Ereignissen, Personen und Verantwortlichkeiten in Beziehung gesetzt werden. Die bewusst interventionistische Anlage ist dabei ein Erkenntnis-mittel: Jene meist impliziten Deutungs-routinen, Normalitätsannahmen und Grenzziehungen, die in rein beobachtenden oder standardisierten Designs häufig unsichtbar bleiben, werden so explizit. Besonders hervorzuheben ist zudem die partizipative Ausrichtung, weil Teilnehmende als Ko-Interpret:innen ihrer Daten auftreten und damit nicht nur Einstellungen berichten, sondern Interpretationspraktiken demonstrieren – einschließlich der Fähigkeit, aus vermeintlich „harmlosen“ Umweltdaten soziale Szenen zu rekonstruieren und normativ zu bewerten. In diesem Sinne liefert die Studie weniger repräsentative Häufigkeiten als analytisch generalisierbare Einsichten in Mechanismen (z. B. laterale Überwachung, Aushandlung von Zuständigkeiten, moralische Ökonomien der Privatheit), die über den

Einzelfall hinaus anschlussfähig sind und die Lücke zwischen abstrakten Risikonarrativen und konkreter häuslicher Datenpraxen empirisch belastbar schließen.

4.2 Risikoreiche Motive und Nutzungskonstellationen

4.2.1 Narrative, die Smart Home-Nutzung motivieren

Wir konnten in unseren Fällen die beiden Metanarrative von Komfort und Bequemlichkeit sowie Sicherheit und Kontrolle insbesondere in den Motivationen und Rechtfertigungen eines moralisch sinnvollen Smart-Home-Einsatzes wiederfinden. Allerdings mit interessanten Spezifika, warum und von wem Smart-Home-Produkte angeschafft werden, und worauf sich Kontrolle, insbesondere im Kontext von Mietwohnungen, bezieht. Zudem lässt sich mit der Frage nach dem „Smarten Altern“ ein Spezialfall beobachten, der die Subjektposition der eigenverantwortlichen Vorsorge und der „sorgenden“ Überwachung durch Angehörige vereint.

Komfort und Effizienzkontrolle durch das Smart Home

Die Teilnehmenden, die bereits smarte Geräte bzw. Systeme nutzen, sind meist männliche Personen, die aus einem IT-affinen Beruf stammen und sich auch in der Freizeit gern einem Technikprojekt widmen. Als wesentlicher Motivator im Sample hat sich Energieeffizienz erwiesen. Dafür werden sowohl selbst konfigurierte Smart-Home-Systeme auf Open-Source-Basis eingesetzt als auch Systemlösungen im Ökosystem eines Herstellers.

„Also, es ist der Komfortgewinn und es ist auch tatsächlich die Kosteneinsparung. (...) Auch mit diesem Home-Away-System, also, dass es halt merkt, ob das Handy anwesend ist oder nicht und dann heizt es halt gar nicht erst, obwohl man da eine Routine einprogrammiert hat.“ (FIT7, Aufbau, Pos. 73)

Außerdem werden Lichtsteuerung und weitere digitale Zugänge für eine leichtere Bedienbarkeit von Geräten im Haushalt geschaffen. So beschreibt etwa ein Teilnehmer, warum und wie er den Zugang zur Garage mit seinem Smartphone verbunden hat:

„Weil manchmal diese komische Funkfernbedienung nicht ging, da habe ich noch über Homematic IP auch so einen Taster halt gebaut. (...)“

Und man kriegt eine Nachricht, wenn das Garagentor auf oder zugeht.“ (F1T8m, Aufbau, Pos. 174)

Während tech-affine Nutzer das Smart Home als Projekt betrachten, das in einer Digitalisierung von Routinen besteht, nutzen weniger tech-affine Nutzende eher fertige, standardisierte Produkte ohne tiefergehende Anpassung. Bei ihnen steht das Komfortversprechen im Vordergrund, bspw. Licht ohne Schalter bedienen zu können oder Medienwiedergabe zu steuern:

„Zum Fernsehen gucken, zum Musik hören, sehr praktisch, aber ich ruf dann auch gerne so Einkaufslisten zu, find ich äußerst praktisch.“ (F2T1, Aufbau, Pos. 18)

Bei den teilnehmenden Frauen ist die energieüberwachende Form der Nutzung eher selten. Sie nutzen Smart-Home-Systeme mit und werden besonders hinsichtlich ihrer Alltagsaufgaben und der Benutzbarkeit der Schnittstellen eingebunden. So zeigt sich etwa, dass nicht nur der Stromverbrauch der Waschmaschine getrackt wird, sondern eine Meldung auf dem Smartphone der Partnerin erfolgt, wenn diese keinen Strom mehr verbraucht, also die Wäsche fertig ist. Dieser Bezug zu Haushaltstätigkeiten ist – wenn auch stereotyp – vorherrschend: Smarte Geräte in der Alltagswelt der weiblichen Teilnehmer:innen sind vor allem Küchengeräte wie der Thermomix. Auch in der Nutzung des Sensorkits zeigen sich geschlechtsspezifische Unterschiede. Frauen nutzen es u. a. zu Lautstärkemessungen (nicht zu laut sein) und annotieren in den Sensordaten Tätigkeiten wie Kochen, Essenszeiten und Schlafenszeiten der Kinder.

Insgesamt überwiegt die Vorstellung vom Smart Home als Unterstützung. Gerade Teilnehmerinnen, die selbst noch keine Smart-Home-Produkte besitzen, werten diese teilweise als „Luxus“ (F2T9, Pos. 109), den man sich anschaffen könnte, wenn man mal mehr Geld oder ein Eigenheim besäße.

Kontrolle von richtigem und falschem Lüften

Entlang der Frage von Eigentum der Wohnung zeigte sich in unserem Sample eine Spezifik des Kontroll-Narrativs besonders deutlich: Die Sensorkits wurden in fast jedem Haushalt von den Teilnehmenden zur Überwachung der Luftfeuchte und -qualität im Hinblick auf Schimmelbildung eingesetzt. Dabei haben sowohl Eigentümer:innen als auch Mieter:innen Luftfeuchtigkeitsmessungen vorgenommen, um Annahmen bezüglich eines

(vermeintlich) richtigen oder falschen Lüftungsverhaltens bzw. der Qualität der Bausubstanz zu überprüfen.

Das wurde insbesondere in den Gruppendiskussionen deutlich, die sich besonders eignen, um die kollektiv geteilte Bedeutung von Narrativen von Smart-Home-Produkten zu ermessen. Die Gespräche machen sichtbar, wie die in Kapitel 3 beschriebenen Narrativen – Komfort und Bequemlichkeit sowie Sicherheit und Kontrolle – von den Teilnehmenden interpretiert und in ihre Alltagspraxis übertragen und miteinander verbunden werden. Dabei zeigt sich, welche Rollen Normen, Deutungsschemata und kollektive Wissensbestände spielen. In allen sechs Diskussionen wurde deutlich, dass die Teilnehmenden eine starke normative Vorstellung von richtigem und falschem Lüftungsverhalten haben, die mit Verantwortlichkeiten und Anti-Rollen korrelierten:

„Die Leute müssen lernen zu heizen, [zu] lüften. Man bezahlt nicht mehr an Heizkosten. Wenn man diese Balance findet. Wir haben die gefunden. Schon 20 Jahre. Wir haben keinen Schimmel. [...] Und wenn ich jetzt die Luftfeuchtigkeit messe und nicht rausfinde, aha, ich muss mal was ändern. Da ist der Streit vorprogrammiert mit dem Vermieter.“ (F1T2w, DRI, Pos. 630)

An der Praxis des Lüftens haben sich in unserem Material Vorstellungen von Ordnung, Gesundheit und Moral verdichtet, wie in keiner anderen Frage. Einerseits wurde hierbei auf rationales, wissenschaftlich legitimates Handeln (Schimmelprävention, Energieeffizienz, Virenreduktion) verwiesen, andererseits aber auch Narrative von Reinheit, Klarheit und Disziplin verknüpft. Insbesondere die Rolle der nachlässigen Mieter:innen war moralisch aufgeladen: Entgegen den Messwerten (nicht) zu lüften, galt quer über die Haushalte als Zeichen von Nachlässigkeit oder sogar Rücksichtslosigkeit gegenüber Nachbar:innen und Eigentümer:innen. Sie erfüllt die Funktion eines Anti-Subjekts, das die eigene Positionierung legitimiert und stärkt. Die Subjektposition „verantwortungsbewusste Mieter:in“ selbst ließ sich wiederum sehr gut mit der Nutzung von Sensoren und Smart-Home-Produkten stützen und stärken: Wer ein Interesse an korrektem Lüften hat, kann Sensoren gegenüber nicht abgeneigt sein.

Darüber hinaus bezogen sich besonders die tech-affinen Männer mit eigenen Smart-Home-Systemen stark auf Sicherheitsnarrative, die auf autarker Nutzung basierten. Das Wissen, wo die eigenen Daten hingehen und gespeichert werden, galt ihnen als Garant für Sicherheit – im Gegensatz zu einer unkritischen Nutzung von beispielsweise Amazon Alexa.

„Ich habe auch bis jetzt alles vermieden, was in die Cloud geht oder so. Das habe ich immer alles ausgeschaltet. Oder wenn es nicht geht, habe ich es in der Fritzbox blockiert.“ (F1T8m, DR3 Pos. 460)

Sicherheit wird dabei vor allem als „Sicherheit nach außen“ verstanden. Einbrecher (auch im Sinne von Hacker:innen), Tech-Konzerne oder Geheimdienste wurden als Akteure benannt, vor denen sich geschützt werden müsse. Gerade Menschen mit DDR-Sozialisation wiesen dabei häufig darauf hin, dass dies im Zweifel immer vergeblich sei, wenn der unbedingte Wille zur Überwachung da sei, ob mit oder ohne Zugriff auf Smart-Home-Daten (F1T2m, DR1, Pos. 596). Eine Position, die wiederum denen mit weniger Zeit und Expertise ein Anknüpfen ermöglicht, die Risiken der Nutzung von plattform-basierten Systemen und deren Datensammlung ebenfalls auszublenden.

Smart Alter(n)

Bei älteren Menschen lassen sich Subjektpositionen erkennen, in denen Komfort und Sicherheit besonders stark miteinander verschränkt werden. Dass smarte Sensoren die Selbstständigkeit im Alter im eigenen Zuhause unterstützen könnten, wurde von allen Teilnehmenden der Studie geteilt – unabhängig von ihrer Technikaffinität oder bisherigen Smart-Home-Nutzung. Nur für ein älteres Paar war die Nutzung von Smart-Home-Geräten zur Kompensation von Defiziten allerdings bereits gelebte Realität. Von allen anderen wurde diese aber als sinnvolle Nutzung gewertet, der gegenüber sie aufgeschlossen sind – und für die es dann kaum einen Messwert gibt, der zu sensibel wäre. Dies betraf insbesondere Nutzungsszenarien, die Dritten die Möglichkeit eröffnen, im Notfall Nachricht oder Zugang zu erhalten – „Wenn etwas ist“, so die häufig reproduzierte Aussage. Die Wertung dieser Nutzung als angemessen dehnte sich aber weit über Notfall-Zugänge hinaus auf eine sehr selbstverständliche Form der alltäglichen Überwachung:

„Wenn ich jetzt vielleicht in der Familie jemand hätte, der nur noch schwer zu Hause zurechtkommt, wo man merkt, also wenn jetzt um achte oder neune oder zwölfte der Kühlschrank nicht auf – könnte was passiert sein. [...] Wenn ich jetzt jemanden habe, der unwahrscheinlich gerne kocht, und der heute nicht kocht, dann könnte man gucken.“ (DR1, F1T2w, Pos. 600)

Die in den entsprechenden Passagen diskutierten Beispiele beinhalteten vermehrt auch eine direkte Überwachung von Körperfunktionen durch vernetzte Sensoren, wie bspw. der Atmung. Im Kontext von smartem Altern wurde vermehrt der Einsatz von Sensoren in Szenarien und Räumen befürwortet, die die Befragten aber für die eigene Nutzung ausgeschlossen haben, wie z. B. im Bad oder Schlafzimmer.

4.2.2 Riskante Relationen im Smart Home

Aus dem Überblick über Narrative, die die Nutzung von Smart-Home-Produkten motivieren und legitimieren, lassen sich insbesondere zwei problematische Beziehungsformen zwischen Subjektpositionen diskutieren. Die eine verläuft innerhalb von Haushalten, die andere entlang der Datenflüsse aus den Haushalten zu Dritten.

Smarte Vernetzung aus Haushalten nach außen

In der Simplications-Studie zeigte sich, dass die Bewohner:innen bereits viel mehr smarte Technik benutzten, als ihnen in den Eingangsinterviews zunächst bewusst war. Typischerweise wurden Geräte wie „Amazon Alexa“ oder Saugroboter als vernetzt identifiziert, der SmartTV und Thermomix sowie die weitreichende Einbindung von mobilen Endgeräten wie Smartphones in die Steuerung von Haushaltsgeräten wurde allerdings selten erkannt und thematisiert. Diese Ebene der Vernetzung des Alltags, die ebenfalls mit allerhand Sensorik und Datenflüssen einhergehen, wurde als gegeben und unausweichlich wahrgenommen.

Eine Wahrnehmung von Risiken zeigt sich kursorisch am Beispiel von Re-Targeting, also dem Einspielen personalisierter Werbung, die an zuvor geführte Alltagsgespräche erinnert: „Es ist schon beängstigend teilweise.“ (DR2, FIT6m, Pos. 460). Hier entsteht das unangenehme Gefühl vor allem, weil zuvor gesuchte oder besprochene Themen durch die Werbung im Alltag wieder präsent werden – es findet keine technische Sprachüberwachung statt und Werbung wird nicht gezielt aus den Gesprächen generiert. Re-Targeting dient somit als Projektionsfläche für mögliche Risiken, die im Gespräch nicht weiter thematisiert wurden. Eine gesteigerte Gefahr fremder Überwachung wird hingegen vor allem mit komplexeren Sensoren wie Kameras, Mikrofonen oder am Körper getragenen Wearables assoziiert.

Die typischen Smart-Home-Sensoren werden als deutlich mittelbarer eingeschätzt und nicht als vergleichbar problematisch wahrgenommen.

Ein Spannungsverhältnis zeigt sich bei der Bewertung der Akteure, die Zugriff auf Daten haben könnten – und der Verantwortlichkeit des Schutzes davor: Während Nutzer:innen sich für verantwortlich halten, ihre Daten abzusichern, werden Plattformanbieter:innen oder andere Akteur:innen in den Narrativen kaum als Verantwortungsträger sichtbar. Produkthersteller, sowohl aus dem Consumer Electronics-Bereich als auch aus der Haushaltstechnik, genießen ein hohes Vertrauen. Gleichzeitig gibt es keine Vorstellung von konkreten Auswertungs- und Verwertungsszenarien, die über die Nutzung hinausgehen. Das Erstellen personalisierter Profile, der Handel damit und dessen mögliche Folgen für Verbraucher:innen sind den allermeisten Teilnehmer:innen nicht bewusst. Vielmehr wird die Ansicht geäußert, man könne diesen Bestrebungen ohnehin nichts entgegensetzen und sich dementsprechend auch nicht absichern. Gegenüber konkreter gedachter Dritten wie Hackern oder (unter Umständen) Vermietern bestehen wiederum normative Vorstellungen davon, dass deren Zugriff auf Smart-Home-Daten unrecht und verhältnismäßig sei. Interessant war hier im Kontext der Diskussion über das Lüften, dass das Teilen von Luftfeuchtheitswerten als besonders sensibel eingeschätzt wurde. Diese Daten seien zwar äußerst nützlich, würden jedoch am Ende lieber nicht mit Vermietern geteilt. Und zwar vor allem deshalb, weil die Daten einerseits auch anders (als im Sinne der Mieter:innen) interpretiert werden könnten, und andererseits auch viel mehr preisgeben könnten als nur das Lüftungsverhalten.

Vor diesem Hintergrund ergeben sich diametrale Nutzungsoptionen: Wer zentral auf Komfortnarrative abstellt, blendet die Risiken im Alltag tendenziell stärker aus, auch wenn sie im Zuge der Gruppendiskussion formulierbar sind. Die Alternative zu dieser pragmatischen Konsumentenhaltung ist, sich komplett zu verweigern. Dies erfolgt häufig bei fehlenden Skills (F2T2w) bzw. mit Hinblick auf den Aufwand (F1T1m).

Wer hingegen den Aufwand der Eigenverantwortung zur Herstellung von Sicherheit nicht scheut, setzt auf Open-Source-Systeme, was nicht nur erheblichen technischen Aufwand erfordert, sondern auch dazu führen kann, dass Kontrolle und Zugriffsmöglichkeiten ungleich verteilt sind.

Smarte Vernetzung innerhalb von Haushalten

Der eigene Haushalt wird als Vertrauensgemeinschaft wahrgenommen, mit der grundsätzlich erst einmal alles geteilt werden kann, jedoch im Hinblick auf die tatsächlichen vorliegenden Zugänge zu vorhandenen Daten auch nicht immer wird.

Die Risiken, Daten im eigenen Haushalt zu teilen und den Privatraum permanent über vernetzte Sensorik zu überwachen, werden bis auf einige Ausnahmen – Bäder und Schlafzimmer –, tendenziell als gering wahrgenommen. Zwar wird den Teilnehmenden bewusst, dass sich Tagesabläufe, Aktivitäten und Routinen sowie Besuch, also Personenzahl und Verhalten, aus den Daten ablesen lassen („man kann halt feinste Nutzerprofile damit halt anlegen“ (FIT7m, Aufbau, Pos. 65)), die Risikoeinschätzung ist aber gering. Gerade den älteren Personen fehlt es an einer konkreten Vorstellung davon, wie eine solche Datenmenge, wie sie sie selbst in nur zwei Wochen produziert haben, analysiert werden kann. Auch die Risiken der digitalen Kontrolle durch Angehörige und Partner:innen, die im Smart Home entstehen können, werden extrem unterschätzt.

Wie Fachverbände gegen Gewalt an Frauen immer wieder betonen, bestehen im Smart Home erhebliche Privatheitsrisiken der Überwachung und Kontrolle: Statistisch ist insbesondere für Frauen der eigene Haushalt der gefährlichste Ort (UNODC 2022; BKA 2025), wobei die Bedeutung und Prävalenz digitaler Gewalt massiv steigt (BKA 2025: 32). Unsere Erhebung bestätigt dies dahingehend, aufzuzeigen, wie schnell die Kontrolle über Daten im Haushalt aus der Hand gegeben wird. Die Überwachungs- und Kontrolloptionen durch den alleinigen Zugriff einer Person auf die Bewegungsdaten der anderen Haushaltsmitglieder sind massiv. Durch die typische Motivation als Technikhobby bzw. -projekt hat in Mehrpersonenhaushalten oft nur eine Person den Zugang zu den Daten. Im Sinne von Komfort wird darauf geachtet, dass Partner:innen, die keinen eigenen Zugriff auf das System haben, alternative Interfaces, bis hin zu vernetzten Tastern, zur Verfügung stehen und ein Nutzen für sie sichtbar wird. Tendenziell wurden weibliche Haushaltsmitglieder jedoch häufiger nur informiert oder nutzungstechnisch einbezogen, indem bestimmte Geräte oder Räume für sie spezifisch ein- oder ausgeschlossen werden. Dies wurde in Paarbeziehungen oft als „Vetorecht“ bezeichnet, auch wenn Aushandlungen manchmal durch Anschaffung und Installation umgangen werden: „Aber die Kameras habe ich halt einfach irgendwann hingehangen, und gesagt: Garten ist jetzt videoüberwacht. Punkt.“ (DR2, FIT6m, Pos. 915)

Welche AGBs dem Einsatz dieser Technik zu Grunde liegen, entscheidet und bestätigt häufig nur die installierende Person. Insofern besteht ein doppeltes Privatheitsrisiko aus der Abgabe der Verantwortung.

Ein weiteres Risiko, neben der Gefährdung der Privatheit der nicht-einbezogenen Haushaltsmitglieder, ergibt sich mit Blick auf die Kontrolle und Wartung der Smart-Home-Systeme. Gefragt, ob er Zugänge mit seiner Tochter teilen würde, antwortet ein Teilnehmer, dass er dafür gar keine Notwendigkeit sehe: „Sie hat ja gar nicht die VPN-Daten. Müsste ja, weil ich ja meine Daten in der Cloud habe, müsste dann die VPN-Verbindung dann doch bei ihr eingerichtet werden.“ (DR3, FIT8m, Pos. 533)

Der Aufwand, einen sicheren Zugriff für eine angehörige Person einzurichten, wird als zu hoch eingeschätzt. Das Risiko, Wissen über die Anlage und deren Einrichtung mit niemandem zu teilen und dadurch die Kontrolle zu verlieren, wird dabei nicht thematisiert bzw. nicht als bedenkenswert erkennbar. Vielmehr überstrahlt hier ein vermeintliches Sicherheits-Narrativ die Nutzung, das darauf setzt, immer in der Lage zu sein, das System selbst zu verwalten und wenig Zugangsoptionen zu schaffen.

4.3 Drei riskante Subjektpositionen im Smart Home

Unsere Daten zeigen, dass unter der Oberfläche der verbreiteten Metanarrative von Komfort und Sicherheit durchaus widersprüchliche und riskante Subjektpositionen für Nutzer:innen entstehen. Im Folgenden diskutieren wir drei davon.

Im Hinblick auf Privatsphäre als normative Anforderung, die Privatsphäre zu schützen, erzeugt das Smart Home Überforderung, Verantwortungsdruck und Ohnmachtsgefühle. Die Komfort- und Sicherheitsversprechen wirken dagegen so, dass wiederum das Nicht-Mitmachen bei datengetriebenen Handlungen wie dem Lüften sozial sanktionierbar wird. Handlungsoptionen zu individueller Privatsphäre sind wiederum kompliziert, versteckt oder mit Nachteilen und hohem Aufwand verbunden. Oftmals haben die Teilnehmenden dieses Ungleichverhältnis als individuelle Überforderung markiert, die wir als „Privacy Fatigue“ (Choi et al. 2018) interpretieren: Das Gefühl, dass die permanente Aufforderung, Einstellungen zu prüfen, Einwilligungen zu managen, AGBs zu lesen, Cookies abzuwählen usw. als zu viel und wirkungslos empfunden wird. Das lässt sich als Reaktion auf die Verantwortungsasymmetrie lesen, die Privatsphäre als Anforderung individualisiert, statt Macht von Plattformkonzernen und Regulierungsver-

sagen zu thematisieren. Die von den Teilnehmenden geäußerte Haltung „ohne die geht es nicht“ ist vor diesem Hintergrund kein plumper Zynismus, sondern eine Coping-Strategie: Sie reduziert kognitive Dissonanz und schützt vor der Erschöpfung, die aus Privacy Fatigue entsteht. Gleichzeitig stabilisiert sie aber genau die Machtverhältnisse, die sie kritisiert: Wenn es ohne Google, Apple und Amazon nicht geht, und die eh schon „global abrufen können“ (FIT6m, DR2, Pos. 891), erscheint Widerstand als sinnlos, Regulierung als Symbolpolitik und individuelle Praxis als lächerlich. Handlungsunfähigkeit wird zur Identität: *das Subjekt als „Datenopfer“*.

In den vorliegenden Deutungen von Smart-Home-Technik bestätigt sich die markante Individualisierung von Verantwortung, die primär bei denjenigen verortet wird, die Geräte kaufen, konfigurieren und „im Griff haben“ sollen (vgl. 3.3). Damit werden klassische „User-Tugenden“ – Informiertheit, Technikaffinität, Vernunft – zu einer normativen Erwartung an einzelne Subjekte, während andere betroffene Werte wie Privatsphäre, Autonomie, das soziale Gefüge im Haushalt, Verantwortungsasymmetrien und Nachhaltigkeit systematisch in den Hintergrund treten. Das technohedonistische Imaginativ, das beinhaltet über Smart Home „alles unter Kontrolle“ zu haben, wirkt dabei nicht nur als Verheißung von Komfort und Effizienzkontrolle, sondern produziert neue Verwundbarkeiten – auch für jene technisch versierten Personen, die das System managen (müssen) und dadurch zum zentralen Knotenpunkt von Zugang zu und damit auch Macht über Datenflüsse im Haushalt werden.

Gerade in Bezug auf Partnerinnen von „Tech-Nerds“ verschränken sich damit bekannte Narrative wie der „Wife Acceptance Factor“ (Aagard 2023) – Smart Home muss vor allem für die Partnerin „erträglich“ und „praktisch“ sein – mit einer stillschweigenden Verschiebung von Verantwortung: Von „überlassen“ bis hin zu „überwachen lassen“ reicht ein Kontinuum, in dem Haushalts-Infrastruktur (Heizung, Licht, Zutritt) digital vermittelt und dadurch asymmetrisch kontrollierbar werden.

Die Fokussierung auf äußere Risiken – Einbrecher, Hacks, „das Internet“ – blendet dabei Machtverhältnisse im eigenen Haushalt aus. Eine Subjektposition, die auf individualisierte Verantwortung mit delegierender Entlastung reagiert. Die Position „Mein Partner kümmert sich darum“, ist vor diesem Hintergrund ambivalent: Sie ist höchst nachvollziehbar im Angesicht von Care-Lasten und Entlastungsversprechen von Smart Home bzw. Smart Care für Frauen, erzeugt aber neue Risiken für digitale Gewalt, Überwachung und Abhängigkeit. So entsteht für Frauen als vulnerable Gruppe ein doppeltes Privatheits-Individualisierungs-Paradox: Um Smart

Home überhaupt sicher nutzen zu können, wäre eine Absicherung sowohl nach außen als auch nach innen (gegen missbräuchliche Nutzung durch Nahestehende) nötig, während der dominante Diskurs nur die äußere Bedrohung adressiert und zugleich die Verantwortung auf das Individuum – meist den technisch interessierten Partner – verschiebt. Die delegierte Verantwortungsübernahme erscheint damit als praktische Lösung, reproduziert aber jene Ungleichheits- und Risikostrukturen, die im Diskurs um digitale Sicherheit weitgehend unsichtbar bleiben. Im Interviewausschnitt – „meine Frau [...], die ihr iPhone liebt, aber ehrlich gesagt nicht zurechtkäme, wenn der Heizungsregler, der eben über den Router bei mir ist, ausfallen würde“ (DR6, F2T10m, Pos. 42) – wird deutlich, wie diese zwei riskanten Subjektpositionen ko-konstruiert werden: *der souveräne Administrator und die abhängige Partnerin*, die als entlastet und zugleich hilflos markiert ist.

Eine dritte riskante Subjektposition lässt sich als *sorgende Überwacher:in* fassen: Personen, die Smart Home und Smart Care vor allem aus Sorge um andere einsetzen – ältere Angehörige, Kinder, kranke Partner:innen – und dabei sowohl Risiken verursachen als auch „für andere“ zu tragen glauben. In Szenarien des „smarten Alterns“ oder einer „datafied motherhood“ werden erwachsene Kinder und Mütter zu aktiven Produzent:innen von Überwachungsinfrastrukturen: Sie installieren Baby-Cams, Ortungs-Apps oder Sturzsensoren oder richten Mähroboter und Sprachassistenten ein. Unter Risiko sind dabei jedoch vor allem die Überwachten – ältere Menschen und Kinder –, deren Alltag zunehmend durch automatisierte, teils adaptiv reagierende Systeme, Einschätzungen und Alarmer strukturiert wird. Die Sorge wird zunehmend technisch vermittelt und genau diese Vermittlung erzeugt neue Abhängigkeiten und Kontrollmöglichkeiten. Diese Sorge-Subjektposition ist zugleich eng mit einer Krise der sozialen Reproduktion verschränkt. Smart-Home- und Plattformdienste adressieren nicht nur überlastete Mütter und pflegende Angehörige, sondern auch alleinlebende (insbesondere jüngere) Männer, die Schwierigkeiten haben, die eigene Versorgung sicherzustellen: Essen wird per App bestellt, die Wohnung per Smart Home „verwaltet“. Plattformökonomie und Smart-Home-Technik ersetzen in gewisser Weise weiblich konnotierte Reproduktionsarbeit – Kochen, Organisieren, Erinnern, Kümern – und erzeugen dabei ein Gefühl von Selbstbestimmung durch Technikkontrolle: Man erscheint als souveräne Nutzer:in, die ihre Umgebung intelligent steuert, während man faktisch in Infrastrukturen eingebunden wird, die neue Abhängigkeiten schaffen. Theoretisch lässt sich diese dritte Subjektposition

als Internalisierung von Komfort- und Sicherheitsversprechen lesen: Das Versprechen von Sicherheit, Komfort und Entlastung wird zu einem moralischen Imperativ der Sorge („Wenn ich wirklich eine gute Mutter / ein verantwortungsvolles Kind / ein moderner Mann bin, dann nutze ich diese Technologien“). Daraus entstehen sorgend-überwachende Konsument:innen: als Konsument:in von Sicherheits- und Convenience-Produkten werden sie machtvollen Produzent:innen von Daten, die soziale Beziehungen strukturieren („Wer bestellt was?“, „Wer schaut wann auf die Baby-Cam?“, „Wer kontrolliert die Türkamera?“).

Mit der Perspektive auf Subjektpositionen wird sichtbar, dass Smart-Home-Produkte auch Beziehungsarbeit und Machtverhältnisse neu konfigurieren: Sorge wird privatisiert, technisiert und an Einzelne delegiert, während strukturelle Fragen – Care-Infrastruktur, Ungleichheit, Gewalt im Nahraum – unsichtbar bleiben. Gerade darin liegt die riskante Qualität dieser dritten Subjektposition: Sie fühlt sich verantwortlich und entlastet zugleich, stabilisiert aber durch ihre Praxis jene datengetriebenen und geschlechter- bzw. generationsspezifischen Machtordnungen, die sie eigentlich zu entschärfen hofft.

5. Fazit

Der Beitrag hat gezeigt, wie das Smart Home und die damit verbundenen Privatheitsrisiken über Narrative von Komfort, Sicherheit und Sorge legitimiert werden – und wie diese Narrative zugleich Risiken verschieben, individualisieren und unsichtbar machen. In der Analyse der Metanarrative wird deutlich, dass Smart Home als Lösung für die Krise der alltäglichen Reproduktionsarbeit inszeniert wird: als Komfort-Infrastruktur, die Hausarbeit, Organisation und Fürsorge automatisiert, sowie als Sicherheitsdispositiv, das das Zuhause nach außen absichert und für Angehörige „mitsorgt“. Damit werden jedoch gerade jene Machtverhältnisse ausgeblendet, die in der Plattformökonomie ebenso wie im Haushalt selbst wirksam sind.

Unsere empirische Studie konnte trotz der sozialräumlich und quantitativ begrenzten Reichweite sowie der unvermeidlichen Reaktivität eines interventionistischen Feldsettings zeigen, zu welchen Formen situierter Datenpraxen spezifische Konstellationen führen. Gerade die methodische Verschränkung von Sensordaten, reflexiver Exploration und datenbasierter Gruppendiskussion machte jene impliziten Deutungs- und Aushandlungs-

praktiken sichtbar, in denen Smart-Home-Risiken im Alltag überhaupt erst entstehen und sozial wirksam werden.

Die drei rekonstruierten Subjektpositionen – das Subjekt als „Datenopfer“, das Paar aus souveränem Administrator und abhängiger Partnerin sowie die sorgende Überwacher:in – sind analytisch besonders fruchtbar, weil sie die widersprüchlichen Anforderungen bzw. Zumutungen der Smart-Home-Nutzung nicht als bloße „Einstellungen“, sondern als sozial hervorgebrachte Selbst- und Fremdverhältnisse sichtbar machen; zugleich ist die Typologisierung selbst ein heuristisches Ordnungsmittel. Erstens sind die Subjektpositionen weniger stabile „Typen“ von Personen als situativ aktivierte Modi des Umgangs mit Daten, Verantwortung und Sorge, die je nach Anlass, Beziehungsdynamik oder verfügbaren Ressourcen wechseln können: Ein „Datenopfer“ kann – etwa in Momenten akuter Störung, bei Medienberichten über Hacks oder bei Konflikten im Haushalt – kurzfristig in eine Haltung des „souveränen Administrators“ übergehen (oder umgekehrt). Zweitens können andere Haushaltsformen (z. B. mehrsprachige oder migrantische Haushalte, prekäre Wohnlagen, queer-familiäre Arrangements, konflikthafte Trennungs- oder Gewaltkontexte, professionell betreute Wohnformen) weitere Subjektpositionen hervorbringen oder die Gewichtung der rekonstruierten Positionen verschieben. Drittens liegt der analytische Fokus dieser Studie auf Subjektpositionen entlang von Privatheit, Verantwortung und Sorge. Andere Achsen der Subjektivierung – etwa Konsum- und Statuslogiken, Nachhaltigkeitspraktiken, ästhetische und affektive Dimensionen von Technikbeziehungen oder arbeitsbezogene Rationalitäten (Homeoffice, Selbstoptimierung) – geraten daher eher am Rand in den Blick, obwohl sie in Smart-Home-Praxen ebenfalls strukturierend wirken können. Es handelt sich also nicht um eine abschließende Kartografie des Smart-Home-Subjekts, sondern um eine analytische Perspektive, deren Stärke darin liegt, plausible Mechanismen der Verantwortungsindividualisierung, der innerhäuslichen Machtasymmetrien und der technisierten Sorge sichtbar zu machen. Subjektpositionen sind hier als kontingente, überlappende und kontextsensitive Figurationen verstanden, die einen Beitrag zu Mechanismen der Verschiebung von Zuständigkeit, der Normalisierung von Überwachung und moralische Imperative der Sorge leisten, und damit auch über das konkrete Sample hinaus theoretisch anschlussfähig sind.

Die wichtigste Konsequenz aus dieser Perspektive ist, Smart-Home-Technologien nicht länger primär als Frage individueller „richtiger Nutzung“ zu adressieren, sondern als Teil soziotechnischer Infrastrukturen, in

denen Plattformmacht, Geschlechterverhältnisse, Generationenbeziehungen und digitale Gewalt zusammenspielen. Eine kritische Diskussion von Smart Home muss entsprechend situierte Haushalts-Konstellationen in den Blick nehmen – statt Verantwortung einseitig bei den einzelnen Nutzer:innen zu belassen.

Für den Ausblick implizieren die Befunde ein dreifaches Weiterarbeiten in Praxis, Politik und Forschung: Erstens braucht es eine breit angelegte, alltagsnahe Verbraucher:innenbildung, die nicht bei Technikkompetenz im engen Sinn stehen bleibt, sondern die Deutungs- und Aushandlungspraxen im Haushalt adressiert (wer konfiguriert, wer versteht, wer trägt Risiken, wer wird überwacht) und damit Privatheit als relationale, konflikthaft verteilte Ressource thematisiert. Zweitens verweisen die rekonstruierten Verantwortungsasymmetrien auf einen klaren Regulierungsauftrag: Wenn Privatheit und Sicherheit faktisch über AGBs, Einwilligungen und Standard-settings individualisiert werden, müssen Nutzungsbedingungen, Default-Einstellungen und Widerrufs- bzw. Opt-out-Optionen politisch stärker kontrolliert, vereinfacht und durchsetzbar gemacht werden – insbesondere dort, wo Drittbetroffenheit im Haushalt entsteht und „Zustimmung“ sozial nicht frei ausgehandelt werden kann. Drittens ist weitere empirische Erforschung notwendig, die sowohl sozial diversere Haushalte und konflikthafte Konstellationen einbezieht als auch die Kopplung häuslicher Praktiken mit Plattform- und Geräteökologien systematischer nachzeichnet: Gefragt sind Designs, die die situierte Sinnproduktion von Daten ernst nehmen, stärker vergleichend arbeiten (bspw. Milieus, Geschlechter- und Generationenordnungen) und die Wechselwirkungen von Alltagsroutine, Marktversprechen und Regulierung als dynamisches Feld untersuchen.

Literatur

- Aagaard, Line K. (2023). When smart technologies enter household practices: The gendered implications of digital housekeeping. *Housing, Theory and Society*, 40(1), S. 60–77.
- Aylett, Matthew P. und Quigley, Aaron J. (2015): The broken dream of pervasive sentient ambient calm invisible ubiquitous computing. *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*, S. 425–435.
- Bell, Genevieve und Dourish, Paul (2007): Yesterday's tomorrows: notes on ubiquitous computing's dominant vision. *Personal and ubiquitous computing*, 11(2), S. 133–143.

- Berger, Arne; Kurze, Albrecht; Totzauer, Sören; Storz, Michael; Lefeuvre, Kevin; Bischof, Andreas und Freiermuth, Mira (2018): Sensing Home: Designing an Open Tool That Lets People Collect and Interpret Simple Sensor Data from Their Homes. *i-com*, 17(2), S. 153–167.
- BKA/Bundeskriminalamt (2025). Bundeslagebilder - Geschlechtsspezifisch gegen Frauen gerichtete Straftaten 2024. Online unter: <https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/StraftatenGegenFrauen/StraftatengegenFrauenBLB2024.html?nn=237578> [letzter Zugriff: 12.12.2025].
- Bosančić, Saša (2014): *Arbeiter ohne Eigenschaften: Über die Subjektivierungsweisen angelernter Arbeiter* (Theorie und Praxis der Diskursforschung). Zugl.: Augsburg, Univ., Diss., 2012. Wiesbaden: Springer VS.
- Bröckling, Ulrich (2007): *Das unternehmerische Selbst: Soziologie einer Subjektivierungsform* (Suhrkamp Taschenbücher Wissenschaft, Bd. 1832). Frankfurt am Main: Suhrkamp.
- Bührmann, Andrea D. (2012): *Das unternehmerische Selbst: Subjektivierungsform oder Subjektivierungsweise?* In R. Keller, W. Schneider, W. Viehöver (Hrsg.), *Diskurs – Macht – Subjekt*. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 145–164.
- Choi, Hanbyul; Park, Jonghwa und Jung, Yoonhyuk (2018): The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81, S. 42–51.
- Coleman, Beth (2018): Smart Things, Smart Subjects: How the “Internet of Things” Enacts Pervasive Media. In J. Sayers (Hg.), *The Routledge Companion to Media Studies and Digital Humanities*. London: Routledge, S. 222–229.
- Dahlgren, Kari; Pink, Sarah; Strengers, Yolanda; Nicholls, Larissa und Sadowski, Jathan (2021). Personalization and the Smart Home: Questioning techno-hedonist imaginaries. *Convergence*, 27(5), S. 1155–1169.
- Dereymaeker, Julie; Schokkenbroek, Janneke M.; Martens, Marijn und De Wolf, Ralf (2024): Smarter homes, smarter surveillance? Exploring intimate surveillance practices in modern day households. *New Media & Society*, 27(11), S. 6119–6138.
- Fischer, Joel E.; Crabtree, Andy; Rodden, Tom; Colley, James A.; Costanza, Enrico; Jewell, Michael O. und Ramchurn, Sarvapali D. (2016): „Just Whack It on Until It Gets Hot“: Working with IoT Data in the Home. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, S. 5933–5944.
- Gerber, Nina; Gerber, Paul und Volkamer, Melanie (2018): Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. In: *Computers & Security*, 77, S. 226–261.
- Jarrettt, Kylie (2016): *Feminism, Labour and Digital Media. The Digital Housewife*. New York, London. Routledge.
- Jasanoff, Sheila und Kim, Sang-Hyun (2009): *Containing the atom: Sociotechnical imaginaries and nuclear power in the United States and South Korea*. Minerva, 47(2), S. 119–146.
- Keller, Reiner (2005): *Wissenssoziologische Diskursanalyse: Grundlegung eines Forschungsprogramms*. Wiesbaden: VS Verlag für Sozialwissenschaften.
- Kinsley, Samuel (2011): Anticipating ubiquitous computing: Logics to forecast technological futures. *Geoforum*, 42(2), S. 231–240.

- Köpferl, Karola; Lehmann, Tanja; Börner, Andy; Becker, Alexa; Berger, Arne; Bischof, Andreas und Kurze, Albrecht (2024): *Partizipative Ansätze in der Entwicklung smarter und privatsphärefreundlicher Technik für das Zuhause*. INFORMATIK 2024. Bonn: Gesellschaft für Informatik e.V., S. 823–828.
- Kurze, Albrecht; Bischof, Andreas; Totzauer, Sören; Storz, Michael; Eibl, Maximilian; Brereton, Margot und Berger, Arne (2020): Guess the Data: Data Work to Understand How People Make Sense of and Use Simple Sensor Data from Homes. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, S. 1–12.
- Kurze, Albrecht; Börner, Andy und Reuter, Christin. (2025): SensorKit: A Toolkit for Simple Sensor Data in Research, Education and Beyond. In Gesellschaft für Informatik e.V., *Mensch und Computer 2025 - Workshopband, Chemnitz, Deutschland*. Bonn: Gesellschaft für Informatik e.V.
- Liu, Na (2024). CCTV cameras at home: Temporality experience of surveillance technology in family life. *New Media & Society*, 27(6), S. 3699–3719.
- Lupton, Deborah (2016): *The quantified self: A sociology of self-tracking*. Cambridge, Malden, MA: Polity.
- Mau, Steffen (2017): *Das metrische Wir: Über die Quantifizierung des Sozialen*. Berlin: Suhrkamp.
- Nosthoff, Anna-Verena und Maschewski, Felix (2019): *Die Gesellschaft der Wearables: Digitale Verführung und soziale Kontrolle, Digitale Welten*. Berlin: NP & I.
- Percy-Campbell, Jessica; Buchan, Jacob; Chu, Charlene; Bianchi, Andria; Hoey, Jesse und Khan, Shehroz S. (2024): User Perception of Smart Home Surveillance: An Integrative Review. *Surveillance & Society*, 22(3), S. 304–324.
- Richter, Johanna; Bischof, Andreas; Kurze, Albrecht; Totzauer, Sören; Freiermuth, Mira; Storz, Michael; Lefevre, Kevin und Berger, Arne (2018): Machtförmige Praktiken durch Sensordaten in Wohnungen. *Mensch und Computer 2018-Tagungsband*. Bonn: Gesellschaft für Informatik e.V.
- Rogers, Michaela M.; Fisher Coleen; Ali Parveen; Allmark Peter und Fontes Lisa (2023): Technology-Facilitated Abuse in Intimate Relationships: A Scoping Review. *Trauma, Violence, & Abuse*, 24(4), S. 2210–2226.
- Stark, Luke und Levy, Karen (2018): The Surveillant Consumer. *Media, Culture & Society*, 40(8), S. 1202–1220.
- Strüver, Niklas (2023): Wieso eigentlich Alexa? Konzeptualisierung eines Sprachassistenten als Infrastruktur und Plattform im soziotechnischen Ökosystem Amazons. *kommunikation@gesellschaft*, 24(1), S. 1–33.
- Tan, Neilly H.; Kinnee, Brian; Langseth, Dana; A. Munson, Sean und Desjardins, Audrey (2022): Critical-Playful Speculations with Cameras in the Home. *CHI Conference on Human Factors in Computing Systems*. New Orleans, LA: ACM, S. 1–22.
- Tolmie, Peter; Crabtree, Andy; Rodden, Tom; Colley, James und Luger, Ewa (2016): “This has to be the cats”: Personal Data Legibility in Networked Sensing Systems. *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, S. 491–502.

- UNODC/United Nations Office in Drugs and Crime (2022). Gender-related killings of women and girls (femicide/feminicide): Global estimates of gender-related killings of women and girls in the private sphere in 2021 - Improving data to improve responses. Online unter: https://reliefweb.int/attachments/88159e3c-6c74-482c-a40a-1d3f8ec2367b/Femicide_brief_22Nov2022_final2.pdf [letzter Zugriff: 12.12.2025]
- Weiser, Mark (1991): The Computer for the 21 st Century. *Scientific American*, 265(3), S. 94–105.
- Viehöver, Willy (2001): Diskurse als Narrationen. In R. Keller, A. Hirsland, W. Schneider und W. Viehöver (Hrsg.), *Handbuch Sozialwissenschaftliche Diskursanalyse*. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 177–206.
- Viehöver, Willy (2012a): »Menschen lesbarer machen«: Narration, Diskurs, Referenz. In M. Arnold und W. Viehöver (Hrsg.), *Erzählungen im Öffentlichen. Über die Wirkung narrativer Diskurse* (Theorie und Praxis der Diskursforschung). Wiesbaden: Springer VS, S. 64–133.
- Viehöver, Willy (2012b): Öffentliche Erzählungen und der globale Wandel des Klimas. In M. Arnold, W. Viehöver (Hrsg.): *Erzählungen im Öffentlichen, Über die Wirkung narrativer Diskurse* (Theorie und Praxis der Diskursforschung). Wiesbaden: Springer VS, S. 173–215.

Über die Autoren

Jun Prof. Dr. phil. Andreas Bischof

ist Juniorprofessor für Soziologie mit Schwerpunkt Technik an der TU Chemnitz. Er forscht u. a. zur Digitalisierung von Alltagswelten wie Arbeit, Bildung oder dem Zuhause und entwickelt dabei partizipative und transdisziplinäre Zugänge, um die "black box" digitale Technik und ihre Implikationen mit Nutzer:innen zu öffnen. E-Mail: andreas.bischof@hsw.tu-chemnitz.de

M.A. Franziska Baum

ist Wissenschaftliche Mitarbeiterin im Projekt Simplications und forscht zu Subjektivierung und Sorgearbeit, Arbeits-Plattformen für Care-Aufgaben bzw. Digitalisierung von Sorgearbeit und Schnittstellen zwischen Sorgearbeit und Sensorik im eigenen Zuhause. E-Mail: franziska.baum@hsw.tu-chemnitz.de

Dr. phil. Tanja Lehmann

ist Wissenschaftliche Mitarbeiterin an der Juniorprofessur Soziologie mit Schwerpunkt Technik an der TU Chemnitz. Sie forscht u. a. zur Internetnutzung im Strafvollzug und zur Bedeutung/Implikationen von einfachen Sensordaten in der Kriminalistik. E-Mail: tanja.lehmann@hsw.tu-chemnitz.de

