Zwischen Narrativ und Praxis: Ein Plädoyer für praxisnahe Risikonarrative in der Smart-Speaker-Nutzung

Lukas Schmitz

Zusammenfassung

Der Beitrag untersucht, wie Nutzer:innen im häuslichen Alltag Risiken im Zusammenhang mit Smart Speakern sprachlich bearbeiten und einordnen. Auf Grundlage ethnografisch informierter Interviews wird gezeigt, dass dominante Risikonarrative zwar verfügbar sind, im Alltag jedoch häufig nicht als handlungsleitende Orientierung fungieren. Stattdessen werden Risiken ironisiert, externalisiert oder zeitlich entkoppelt, während situativ erfahrbare Störungen besonders unmittelbare praktische Konsequenzen nach sich ziehen. Der Beitrag argumentiert entsprechend, dass Risikonarrative nur dann handlungsbefähigend wirken können, wenn sie an konkrete Alltagssituationen anschlussfähig sind.

1. Einleitung

Digitale Sprachassistenten wie Amazon Alexa, Google Home/Nest oder Apples HomePod sind in den vergangenen Jahren zu einem verbreiteten Bestandteil häuslicher Arrangements geworden. Sie werden für einfache Tätigkeiten genutzt – etwa zur Informationsabfrage, zur Steuerung von Medien und smarten Geräten oder zur Organisation alltäglicher Abläufe. Gleichzeitig sind diese ‚Smart Speaker' aufgrund ihrer umfassenden Datenerfassung und -verarbeitung zu einem zentralen Gegenstand gesellschaftlicher Risikodiskurse geworden. Fragen des Datenschutzes, möglicher Überwachung oder der Kontrolle über personenbezogene Daten gehören zu den wichtigsten Bezugspunkten öffentlicher wie wissenschaftlicher Auseinandersetzungen mit diesen Technologien. Empirische Studien zeigen dabei wiederholt, dass Nutzer:innen diese Risiken durchaus wahrnehmen und benennen können (Abdi u. a. 2019; Malkin u. a. 2019), auch wenn nicht zwangsläufig Konsequenzen daraus gezogen werden.

Ein prominenter Bezugspunkt ist dabei das sogenannte Privacy Paradox, das ursprünglich im Kontext sozialer Netzwerke beschrieben wurde (Barnes 2006) und die Diskrepanz zwischen geäußerten Datenschutzbedenken und tatsächlichem Nutzungshandeln bezeichnet (vgl. Norberg u. a. 2007; Acquisti u. a. 2015). Neuere Arbeiten haben diese Diagnose jedoch auch kritisch diskutiert und darauf hingewiesen, dass Einstellungen und Verhalten im Bereich digitaler Privatheit nicht notwendigerweise konsistent zusammenfallen (Dienlin/Trepte 2015). Die damit verbundene Beobachtung, dass Einstellungen gegenüber Risiken nicht automatisch zu entsprechendem Verhalten führen, ist allerdings nicht auf digitale Technologien beschränkt, sondern wurde bereits in früheren Debatten etwa im Zusammenhang mit Umweltverhalten diskutiert (Stokols 1995). Weiter ausdifferenziert wurde unter dem Begriff des Privacy Cynicism darauf hingewiesen, dass scheinbar widersprüchliches Verhalten weniger auf Inkonsistenz als auf resignative oder distanzierte Haltungen gegenüber als unvermeidlich wahrgenommenen Datenpraktiken zurückzuführen sein kann (Hoffmann u.a. 2016; Lutz u. a. 2020). Diese Ansätze eint das Interesse an der Frage, wie Menschen mit bekannten Privatheitsrisiken umgehen und warum das Bewusstsein möglicher Risiken nicht ohne Weiteres in verändertes Handeln übersetzt wird.

Aus soziologischer Perspektive verweist dieses Spannungsverhältnis jedoch über individuelle Einstellungen hinaus. In modernen Gesellschaften werden Risiken grundsätzlich kulturell, medial und institutionell vermittelt (Beck 1986; Lupton/Tulloch 2002; Wilkinson 2010). Risiken erscheinen damit als abstrakte Gefährdungen, die zwar diskursiv präsent sind, sich jedoch nicht notwendig in konkrete Handlungssituationen übersetzen lassen. Im Feld digitaler Technologien verbinden sich solche abstrakten Risikodeutungen häufig mit Narrativen der Überwachung, der Intransparenz von Datenflüssen und asymmetrischer Machtverhältnisse, wie sie etwa im Zusammenhang mit dem Konzept des Überwachungskapitalismus diskutiert werden (Zuboff 2018). Dabei bleibt Überwachung zwar allgegenwärtig, zugleich aber räumlich und situativ schwer greifbar (Lyon 2007; 2018). In diesem Zusammenhang sprechen Bauman und Lyon (2013) von „flüchtiger Überwachung", um die diffuse und schwer lokalisierbare Form zeitgenössischer Überwachungspraktiken zu beschreiben. Der in diesem Beitrag verwendete Risikobegriff unterscheidet sich dabei von probabilistischen Risikodefinitionen, wie sie häufig in der klassischen Risikoforschung verbreitet sind. Dort wird Risiko oft als Kombination aus Eintrittswahrscheinlichkeit und potenziellem Schaden verstanden. Die im Kontext digitaler

Technologien diskutierten Risiken – etwa Überwachung, Datenweitergabe oder langfristige Profilbildung – entziehen sich jedoch zumeist einer solchen quantifizierbaren Bestimmung. Für Nutzer:innen bleibt meist unklar, wie wahrscheinlich bestimmte Ereignisse sind, wann sie eintreten könnten oder welche konkreten Folgen sie haben. Damit fehlt im Alltag häufig die Grundlage, Risiken überhaupt zuverlässig einzuschätzen oder gegeneinander abzuwägen. Risiken erscheinen daher weniger als kalkulierbare Gefährdungen, sondern als abstrakte Möglichkeitsräume, die primär über narrative und diskursive Deutungsmuster vermittelt werden. Empirische Studien zeigen entsprechend, dass abstrakte Datenschutz- oder Überwachungsrisiken häufig nur begrenzte praktische Konsequenzen für alltägliche Entscheidungen entfalten (Friedewald u. a. 2016; Degli Esposti/Santiago-Gomez 2015).

Charakteristisch für diese Risikonarrative ist eben ihr hoher Abstraktionsgrad. Sie operieren mit generalisierten Begriffen wie 'Big Data' oder 'Algorithmen', die nur begrenzt an konkrete Nutzungssituationen anschließbar sind. Die Beobachtung, dass Privatheit kontextabhängig bewertet wird (Nissenbaum 2010), motiviert die Frage, wie dieser Kontext in der alltäglichen Praxis konkret beschaffen ist – eine Frage, der der vorliegende Beitrag nachgeht. Aufbauend auf einem praxistheoretischen Theorierahmen wird der analytische Fokus auf die Ebene alltäglicher Praxis gelenkt. Im Zentrum steht nicht primär, was Nutzer:innen über Privatheitsrisiken denken, sondern wie Risiken im häuslichen Alltag sprachlich, situativ und praktisch bearbeitet werden. Während Ansätze wie das *Privacy Paradoxon* beschreiben, dass Risikoerkenntnis und Handeln nicht deckungsgleich sind, rekonstruiert dieser Beitrag, wie dieses Nicht-Passungsverhältnis im Alltag konkret bearbeitet wird und wie Risikonarrative beschaffen sein müssen, um diesem Umstand zu begegnen.

Auf Grundlage ethnografischer Hausbesuche und leitfadengestützter Interviews wird analysiert, welche narrativen und praktischen Formen der Risikobearbeitung im Alltag wirksam werden und welche nur begrenzte praktische Wirksamkeit entfalten. Das zentrale Argument dieses Beitrags lautet, dass Risiken im Zusammenhang mit Smart Speakern im Alltag zwar als kulturelle Narrative verfügbar sind, im praktischen Umgang mit den Geräten jedoch meist nur in bestimmten Situationen thematisiert und selten zu einer kontinuierlichen Orientierung des Handelns werden. Vielmehr sind sie zu verstehen als reflexiv abrufbares Deutungswissen, das nur in bestimmten Situationen tatsächlich handlungsrelevant wird. Diese Diagnose bildet die Ausgangsbasis für die anschließende Diskussion, unter welchen

Bedingungen Risikonarrative stärker an alltägliche Praxis anschlussfähig werden können.

Theoretisch verbindet der Beitrag Ansätze der soziologischen Risikoforschung, die Risiken als kulturell und diskursiv produzierte Ordnungen begreifen (Lupton/Tulloch 2002; Wilkinson 2010), mit praxistheoretischen Perspektiven, die den Vorrang routinisierter, materiell eingebetteter Handlungsvollzüge betonen (Reckwitz 2003; Schatzki 2002). Zunächst wird der theoretische Rahmen zu Risikonarrativen und ihrer begrenzten Anschlussfähigkeit an Alltagspraxis entwickelt (Kapitel 2). Anschließend werden zentrale Muster der Risikobearbeitung im Alltag der Smart-Speaker-Nutzung empirisch rekonstruiert (Kapitel 3). Abschließend wird diskutiert, welche Konsequenzen sich daraus für die Gestaltung handlungsbefähigender Risikonarrative im Kontext digitaler Technologien ergeben (Kapitel 4).

2. Theoretischer Rahmen

2.1 Risikonarrative als kulturelle Ordnungen

Risiko ist kein objektiver Zustand, sondern ein kulturell und diskursiv produziertes Konzept, das gesellschaftlich ausgehandelt, kommuniziert und bewertet wird (Lupton/Tulloch 2002; Wilkinson 2010). Risiken entstehen daher nicht allein aus technischen Eigenschaften, sondern aus narrativen und semantischen Ordnungen, die bestimmen, welche Gefährdungen als relevant gelten. Risikonarrative strukturieren damit Wahrnehmungen, Erwartungen und politische Problematisierungen, ohne notwendigerweise konkrete Handlungen anzuleiten.

In Bezug auf Smart Speaker etwa dominieren narrative Muster der Überwachung, der Intransparenz von Datenflüssen sowie der Einflussnahme durch sogenannte Big-Tech Unternehmen. Diese Narrative operieren mit Abstraktionen: mit der Vorstellung permanenter Abhörung, allgegenwärtiger Datenauswertung bis hin zum quasi-totalitären Zugriff durch staatliche oder wirtschaftliche Akteure (vgl. Abdi u. a. 2019; Maccario u. a. 2022). Solche Narrative sind kulturell weithin etabliert und medial wie alltäglich präsent, bleiben jedoch zumeist unscharf.

Und nicht zuletzt werden Risiken in modernen Gesellschaften zunehmend nicht mehr durch unmittelbare Erfahrung, sondern durch Expertenwissen, Medienberichte und institutionelle Diskurse vermittelt (Beck 1986; Luhmann 1991). Alles in allem erscheinen Risiken damit als kommu-

nikative Konstruktionen, die gesellschaftliche Aufmerksamkeit bündeln. Im vorliegenden Beitrag werden Risikonarrative als kulturell verfügbare Deutungsmuster verstanden, die Gefährdungen benennen, ihre Ursachen zuschreiben und implizite Handlungsrelevanz beanspruchen – ohne dass diese im Alltag notwendigerweise eingelöst wird. Es stellt sich also die Frage, unter welchen Bedingungen solche Narrative für alltägliche Handlungsvollzüge überhaupt anschlussfähig werden.

2.2 Praxistheoretische Perspektive auf Risiko und Alltag

Praxistheoretische Ansätze bieten einen analytischen Rahmen, um diese Frage zu präzisieren. Aus praxistheoretischer Sicht ist Handeln nicht primär das Ergebnis bewusster Abwägungen, sondern wird durch routinisierte Vollzüge, körperliche Gewohnheiten, materielle Arrangements und situative Anforderungen strukturiert (Reckwitz 2003). Wissen ist in dieser Perspektive stets in bestehende Praktiken eingefasst.

Für Risiken bedeutet dies, dass ihre praktische Wirksamkeit weniger von ihrer diskursiven Prominenz als von ihrer situativen Erfahrbarkeit abhängt. Heidenstrøm (2021) zeigt etwa, dass Risikoempfinden stark von der Logik konkreter Handlungssituationen geprägt ist: Bleiben Gefährdungen abstrakt, zeitlich oder räumlich entkoppelt, verlieren Risiken an praktischer Relevanz.

Die Nutzung von Smart Speakern – etwa das Stellen von Timern, das Abspielen von Musik oder das Steuern häuslicher Infrastruktur – ist zumeist in erleichterungs- oder komfortorientierte Praktiken eingebettet – diese Geräte werden gewissermaßen genutzt, um Erleichterung oder Unterhaltung zu gewährleisten (Xu u. a. 2022). Die Vorstellung, dass Sprachdaten weit entfernt verarbeitet, gespeichert oder weitergegeben werden, bleibt jedoch abstrakt und schwer zu verorten. Risiken erscheinen also nicht als Bestandteil der konkreten Nutzungssituation, sondern als externalisierte, zeitlich und räumlich entfernte Möglichkeitsräume.

Risikonarrative bleiben so im Alltag häufig nur begrenzt handlungswirksam: Sie adressieren Gefährdungen auf einer symbolischen und diskursiven Ebene, ohne an die Logiken, Routinen und materiellen Arrangements alltäglicher Praxis anschließen zu können. Die Frage nach der Wirksamkeit von Risikonarrativen ist damit weniger eine Frage individueller Einsicht oder Rationalität, sondern eine Frage ihrer praktischen Anschlussfähigkeit.

3. Risikobearbeitung im Alltag der Smart-Speaker-Nutzung

In der Empirie zeigt sich, dass Nutzer:innen Risiken im Zusammenhang mit Smart Speakern zwar regelmäßig thematisieren, diese Risiken jedoch nur selten zu einer grundlegenden Reorganisation der Nutzungspraxis führen.[1] Stattdessen lassen sich wiederkehrende Muster der sprachlichen und praktischen Bearbeitung identifizieren. Im Folgenden werden drei zentrale Muster rekonstruiert, in denen sich Ironisierung, semantische Unschärfe, institutionelles Vertrauen und situative Praxis in unterschiedlicher Weise verschränken.

3.1 Kontrollversuche und ihre Grenzen

In verschiedenen Interviews etwa berichten Nutzer:innen davon, dass sie versuchen, Kontrolle über den Smart Speaker herzustellen, indem sie Geräteeinstellungen anpassen oder Transparenzfunktionen nutzen. Diese Praktiken erscheinen als bewusste Versuche, Risiken zu bearbeiten, werden jedoch zugleich als brüchig und unzureichend erlebt.

So schildern Interviewte, dass sie Einstellungen zur Speicherung von Sprachaufnahmen vornehmen, zugleich aber doch zuweilen davon ausgehen, dass diese Eingriffe technisch jederzeit unterlaufen werden können: „Du kannst ja einstellen, ob sie speichert oder nicht. Ich hab die Speicherung ausgestellt, aber dann kommt irgendein Update, und dann ist es auf

1 Der Beitrag basiert auf 22 ethnografisch informierten Hausbesuchen mit leitfadengestützten Interviews zur Nutzung von Smart Speakern in deutschen Haushalten (2021–2024). Die Gespräche wurden aufgezeichnet, transkribiert und durch Beobachtungsprotokolle ergänzt. Der Zugang ist technografisch sensibilisiert (Kien 2008) und folgt einem interpretativen Vorgehen, das an Prinzipien der Grounded Theory anschließt (Corbin/Strauss 2008; Charmaz 2014; Bowen 2006). Gerade die Artikulation von Risiken im Interview macht sichtbar, wie Nutzer:innen Risiken narrativ einordnen, relativieren oder auf Distanz halten und welche Deutungsformen hierfür im Alltag verfügbar sind.
Die Haushalte wurden in Deutschland über öffentliche Aufrufe sowie ein Schneeballverfahren rekrutiert. Das Sample ist hinsichtlich Alter, Geschlecht, Bildungsstand, monatlichem Einkommen sowie städtischen und ländlichen Wohnkontexten heterogen zusammengesetzt. Die Datenerhebung fokussiert dabei auf aktuelle Nutzer:innen von Smart Speakern; Formen der Nicht-Nutzung oder des Abbruchs aufgrund von Risikobedenken sind entsprechend nicht Teil des Samples und stehen nicht im Fokus der Analyse. Die Daten wurden im Projekt „Disruptionen vernetzter Privatheit“ erhoben, das von 2021 bis 2025 an der TU Dresden durchgeführt wurde.

einmal wieder an. Dann denk ich mir halt auch: wieso dürfen die das einfach?“ (Transkript Hausbesuch 8)

Neben solchen Eingriffen werden vereinzelt auch Transparenzfunktionen genutzt, etwa akustische Signale, die anzeigen sollen, wann das Mikrofon aktiv ist: „Ich hab mir eingestellt, dass immer ein Ton kommt, sobald sich das Mikro einschaltet, also ich kann das dann schon nachvollziehen.“ (Transkript Hausbesuch 13)

Grundsätzlich bleibt das Vertrauen auf potenzielle Kontrolle der Risikofaktoren thematisch präsent und wird verschieden bearbeitet. Hier berichtet ein Forschungsteilnehmer, wie er seine Unsicherheit in Bezug auf ein mögliches Mithören kanalisiert, indem er eine neue Funktion des Anbieters nutzt:

> *„Stromlos! Das Mikro existiert dann nicht, wenn ich auf diesen Knopf drücke, Mikrofon aus, ist das Mikro stromlos stumm, es nimmt nichts mehr auf, gar nichts. Es ist erwiesen, ne? Das war bei denen, davor bei den Generationen nicht so. Konnteste stumm schalten, war aber trotzdem noch aktiv.“* (Transkript Hausbesuch 5)

Doch auch wenn solche Funktionen zu einer situativen Bearbeitung empfundener Risiken führen, verweist das Material eher auf ein Muster symbolischer Kontrolle. Wissen über Kontrolloptionen und Transparenz ist vorhanden und wird teilweise genutzt, entfaltet jedoch keine dauerhaft stabile handlungsleitende Wirkung – vielmehr bleibt der Umgang mit Privatheitsfragen pragmatisch (Schmitz 2024). In vielen Fällen erzeugen solche Praktiken weniger eine tatsächliche Risikoreduktion als vielmehr ein Gefühl symbolischer Kontrolle: Die Existenz von Einstellungen oder Abschaltoptionen vermittelt Handlungsfähigkeit, ohne dass damit notwendigerweise eine verlässliche Kontrolle über Datenverarbeitung verbunden ist. Risiko wird nicht vermieden, sondern pragmatisch verwaltet; die Nutzungspraxis bleibt weitgehend unverändert. In einigen Hausbesuchen zeigt sich zudem, dass selbst potenzielle Schritte zur Risikobearbeitung nicht unternommen werden; beim gemeinsamen Sichten der Steuerungsapp der Smart Speaker wurde etwa deutlich, dass die Privatsphäre-Einstellungen zumeist kaum verwaltet oder gar nicht genutzt wurden.

3.2 Ironisierung, Unschärfe und Narrative institutioneller Sicherheit

Ein zweites Muster betrifft die sprachliche Rahmung von Risiken. Risiken werden zwar benannt, jedoch häufig ironisiert, semantisch unscharf gehalten oder durch gegenläufige Sicherheitsnarrative entschärft. Diese Strategien tragen dazu bei, Risiken semantisch präsent zu halten – insbesondere in der Interviewsituation – ohne daraus tiefgreifende Veränderungen der Nutzungspraxis abzuleiten.

In den Interviews reagieren Nutzer:innen auf Fragen nach Überwachung oder Datenmissbrauch häufig mit Ironie oder sarkastischer Distanz. Ironie markiert dabei keine Unkenntnis, sondern eine bewusste Entschärfung: Das Risiko wird anerkannt, zugleich aber seiner Dringlichkeit beraubt.

Diese Distanzierung wird durch eine auffällige Unschärfe der Risikokategorien verstärkt. Nutzer:innen vermischen unterschiedliche Gefährdungsvorstellungen – Datenauswertung und -weitergabe, Monetarisierung oder Überwachung – ohne diese klar auf konkrete Nutzungshandlungen zu beziehen. Eine eindeutige Zuordnung von Handlung und verbundenem Risiko bleibt aus. Risiko erscheint dadurch diffus und ist so schwer in alltägliche Entscheidungslogiken integrierbar.

Ergänzend werden Risiken häufig durch Sicherheitsnarrative relativiert. Verweise auf Datenschutzgesetze oder nationale Regulierungsrahmen dienen als implizite Entlastung: „Wenn man nach China guckt, da würde man sich andere Gedanken machen. Aber in Deutschland ist man, glaub ich, gut aufgehoben. (lacht)“ (Transkript Hausbesuch 2)

Damit wird Verantwortung für den Umgang mit Risiken externalisiert. Risiko bleibt zwar thematisch präsent, erscheint jedoch nicht als Aufgabe der Nutzer:innen selbst, sondern als Angelegenheit staatlicher oder institutioneller Kontrolle. In Kombination mit zeitlichen Verschiebungen – etwa der Verlagerung möglicher Gefährdungen in eine unbestimmte Zukunft – verlieren Risiken weiter an aktueller Handlungsrelevanz, wenngleich sie durchaus reflektiert werden: „Man weiß halt auch nie, was die Zukunft bringt. Vielleicht interessiert sich irgendwann doch jemand dafür, was du vor 20 Jahren gemacht hast.“ (Transkript Hausbesuch 8)

Ironisierung, semantische Unschärfe und institutionelles Vertrauen wirken hier zusammen als narrative Entlastungsmechanismen, die es ermöglichen, Smart Speaker weiter routiniert zu nutzen, ohne Risiken in der Praxis nachhaltig zu begegnen.

3.3 Fehlfunktionen als Handlungsmotivation

Während abstrakte oder strukturelle Risikonarrative häufig keine tiefgreifende Reorganisation alltäglicher Praxis auslösen, werden Situationen, in denen der Smart Speaker konkret und unmittelbar die Nutzung stört, jedoch als handlungsrelevant erlebt. Im Material zeigen sich technische Fehlfunktionen als besonders verdichtete Situationen unmittelbarer Intervention.

So wird davon berichtet, dass Mikrofone deaktiviert oder Geräte abgeschaltet werden, weil der Smart Speaker wiederholt ohne erkennbaren Anlass reagiert: „Bei der einen war's tatsächlich ein Fehler, dass die die ganze Zeit losging. Deswegen hab' ich dann das Mikro ausgeschaltet." (Transkript Hausbesuch 5)

Im Unterschied zu abstrakten Datenschutz- oder Überwachungsrisiken greifen solche Situationen unmittelbar in den Nutzungsvollzug ein und eröffnen zugleich klar identifizierbare Handlungsmöglichkeiten. In diesen Situationen wird Risiko nicht als abstrakte Überwachungsgefahr verhandelt, sondern wird als spürbare Störung im Alltag bearbeitet. Die Reaktion ist dabei praktisch motiviert: Ziel ist es, die Irritation zu beenden. Aktiv werden Nutzer:innen vor allem dann, wenn die Störung zeitlich, räumlich und situativ dicht an die Nutzungspraxis gekoppelt ist. Besonders dort, wo Risiken konkret erfahrbar werden, verdichten sie sich zu unmittelbarer Handlungsrelevanz. Nutzer:innen bearbeiten Risiken im Zusammenhang mit Smart Speakern durchaus aktiv, doch die artikulierten Risikonarrative und Kontrollpraktiken entfalten nur selten praktische Wirkung. Ironisierung, semantische Unschärfe und institutionelles Vertrauen neutralisieren Risiken sprachlich und delegieren Verantwortung. Besonders intensive Eingriffe in die Nutzungspraxis entstehen dort, wo Risiken situativ als konkrete Störungen erfahrbar werden.

4. Diskussion: Das Passungsproblem zwischen Risikonarrativ und Alltagspraxis

Die empirischen Beispiele verdeutlichen ein Passungsproblem zwischen dominanten Risikonarrativen und der Bearbeitungsfähigkeit von Risiken in der alltäglichen Nutzungspraxis von Smart Speakern. Risiken werden zwar thematisiert, entfalten jedoch – aufgrund schwer nachvollziehbarer technischer Prozesse und fehlender Lokalisierbarkeit – nur begrenzte prak-

tische Wirksamkeit. Dies verweist weniger auf eine fehlende Sensibilität gegenüber Privatheitsfragen als vielmehr auf unterschiedliche Logiken von Risikodiskursen und Alltagshandeln.

Aus praxistheoretischer Perspektive bestätigt sich damit, dass Wissen und Handeln nicht automatisch gekoppelt sind (Reckwitz 2003). Während Risikonarrative auf einer abstrakten, gesellschaftlich geteilten Ebene operieren, sind alltägliche Praktiken körperlich, materiell und situativ eingebettet. In der konkreten Nutzung dominieren Anforderungen wie Zeitersparnis, Bequemlichkeit oder reibungslose Abläufe gegenüber abstraktem Wissen über Datenverarbeitung oder Überwachung. Risiken werden dabei nicht ignoriert, sondern häufig relativiert, ironisiert oder an institutionelle Akteure delegiert.

Risikonarrative erfüllen in diesem Zusammenhang eine wichtige symbolische Funktion: Sie strukturieren Aufmerksamkeit, benennen Gefährdungen und machen abstrakte Problemlagen kommunizierbar. Symbolische Wirkmächtigkeit ist jedoch nicht mit praktischer Handlungsrelevanz gleichzusetzen. Im Alltag führen Risiken häufig nicht zu einer grundlegenden Reorganisation der Nutzungspraxis, weil sie entweder schwer lokalisierbar oder nicht eindeutig an bestimmte Handlungssituationen gebunden sind.

Alltagspraxis wirkt somit als Selektions- und Entlastungszusammenhang, in dem Risiken nicht umfassend abgewogen, sondern situativ bearbeitet werden (Möller 2024). Ironisierung, semantische Unschärfe oder die Externalisierung von Verantwortung lassen sich dabei als alltagspraktische Strategien verstehen, Risiken semantisch präsent zu halten, ohne daraus konkrete Handlungen abzuleiten. Gleichzeitig lassen sich diese Strategien auch als Reaktionen auf eine Situation verstehen, in der Risiken für Nutzer:innen kaum abzuschätzen sind, da weder Eintrittswahrscheinlichkeiten noch konkrete Folgen überschaubar sind. Nutzer:innen handeln dabei nicht notwendigerweise irrational oder gleichgültig, sondern pragmatisch innerhalb der Logiken ihrer alltäglichen Praktiken. Technische Fehlfunktionen dagegen – etwa unerwartete Aktivierungen oder falsche Reaktionen des Systems – sind zeitlich konkret, räumlich eindeutig verort- und unmittelbar erlebbar. Anders als abstrakte Datenschutz- oder Überwachungsrisiken betreffen solche Fehlfunktionen nicht potenzielle zukünftige Schäden, sondern unmittelbar erfahrbare Störungen der Nutzungspraxis. Vor allem eröffnen sie klare Handlungsmöglichkeiten, etwa das Ausschalten des Geräts, das Deaktivieren des Mikrofons, das Überprüfen von Einstellungen oder eine veränderte Nutzungssituation. Praxisnahe Risikonarrative müssen daher

nicht zwingend Fehlfunktionen abbilden, wohl aber deren strukturelle Qualität nachahmen: Sie sollten eine kommunikative Irritation erzeugen, die den routinierten Nutzungsvollzug gedanklich unterbricht und so einen Moment der Aufmerksamkeit schafft, in dem Handeln wahrscheinlicher wird. Abstrakte Gefährdungsszenarien erzeugen diese Unterbrechung nicht – sie laufen am laufenden Alltag vorbei, ohne in ihn einzugreifen.

Aus diesen Befunden ergeben sich mehrere Konsequenzen für die Gestaltung von Risikonarrativen im Kontext digitaler Technologien. Die Analyse legt nahe, dass Risikokommunikation häufig wirkungslos bleibt, wenn sie sich auf abstrakte Gefährdungsszenarien beschränkt. Ein abstraktes Narrativ – dass etwa ein Smart Speaker kontinuierlich Daten sammelt und damit verschiedene Risiken verbunden seien – bleibt für viele Nutzer:innen schwer greifbar. Risiken werden im Alltag vor allem dann handlungsrelevant, wenn sie an konkrete Nutzungssituationen gebunden sind, räumlich und zeitlich lokalisierbar erscheinen und eine erkennbare Handlungsmöglichkeit eröffnen. Genau diese Eigenschaften fehlen vielen verbreiteten Risikonarrativen über digitale Überwachung. Praxisnähere Darstellungen würden daher konkrete Situationen beschreiben, in denen Daten entstehen und verarbeitet werden – etwa wie ein Sprachbefehl aufgezeichnet und an Server des Anbieters übertragen wird. Wirksamer wären Risikoinformationen vermutlich dann, wenn sie nicht außerhalb, sondern innerhalb der Nutzungssituation präsent werden – etwa durch Hinweise direkt am Gerät, die im Moment der Datenerhebung sichtbar machen, was mit Sprachaufnahmen geschieht.

Adressaten solcher Darstellungen sind insbesondere Akteure der Wissensvermittlung, etwa Medien, Verbraucherorganisationen, Bildungsinitiativen oder Datenschutzinstitutionen. In medialer Berichterstattung, Verbraucherinformationen oder Formen der Datenschutzkommunikation müssten Risiken daher stärker über konkrete Nutzungsszenarien vermittelt werden, die zeigen, wann Daten entstehen, wie sie verarbeitet werden und an welchen Punkten Nutzer:innen überhaupt Einfluss auf diese Prozesse nehmen können.

Gleichzeitig darf eine stärkere Praxisorientierung von Risikonarrativen nicht zu einer einseitigen Individualisierung von Verantwortung führen. Die Gestaltung transparenter und sicherer Technologien bleibt in erheblichem Maße eine Aufgabe von Plattformanbietern, Regulierung und institutionellen Akteuren. Narrative können daher nur einen Teil der Bearbeitung digitaler Risiken leisten und müssen durch strukturelle Maßnahmen ergänzt werden. Die Analyse zeigt damit insgesamt, dass das Problem we-

niger in mangelndem Risikobewusstsein der Nutzer:innen liegt, sondern in der begrenzten Anschlussfähigkeit abstrakter Risikonarrative an die Logiken alltäglicher Praxis. Praxisnahe Risikonarrative wären damit nicht nur eine kommunikative Verbesserung, sondern eine notwendige Bedingung dafür, dass Risikobewusstsein überhaupt handlungsrelevant werden kann.

Literatur

Abdi, Noura; Ramokapane, Kopo M.; Such, Jose M.; Rashid, Awais (2019): More than smart speakers: Security and privacy perceptions of smart home personal assistants. In: *Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, S. 451–466.

Acquisti, Alessandro; Brandimarte, Laura; Loewenstein, George (2015): Privacy and human behavior in the age of information. *Science*, 347(6221), S. 509–514.

Barnes, Susan (2006) *A privacy paradox: Social networking in the United States*, First Monday, 11(9).

Bauman, Zygmunt und Lyon, David (2013) *Daten, Drohnen, Disziplin: ein Gespräch über flüchtige Überwachung*. Berlin: Suhrkamp .

Beck, Ulrich (1986): *Risikogesellschaft. Auf dem Weg in eine andere Moderne*. Frankfurt a. M.: Suhrkamp.

Bowen, Glenn A. (2006): Grounded theory and sensitizing concepts. *International Journal of Qualitative Methods*, 5(3), 12–23.

Charmaz, Kathy (2014): *Constructing Grounded Theory*. London: Sage.

Corbin, Juliet; Strauss, Anselm (2008): *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Thousand Oaks, CA: Sage.

Degli Esposti, Sara und Santiago-Gomez, Elvira (2015): Acceptable Surveillance-Orientated Security Technologies: Insights from the SurPRISE Project, *Surveillance & Society*, 13(3/4), S. 437–454.

Dienlin, Tobias und Trepte, Sabine (2015): „Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors", *European Journal of Social Psychology*, 45, S. 285–297.

Friedewald, Michael, van Lieshout, Marc, Rung, Sven und Ooms, Merel (2016): The Context-Dependence of Citizens' Attitudes and Preferences Regarding Privacy and Security. In: S. Gutwirth, R. Leenes, und P. De Hert (Hrsg.) Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection. Dordrecht: Springer, S. 51–74.

Heidenstrøm, Nina(2021): The utility of social practice theory in risk research. *Journal of Risk Research*, 25(2), S. 236–251.

Hoffmann, Christian Pieter; Lutz, Christoph; Ranzini, Giulia. (2016). *Privacy Cynicism: A new Approach to the Privacy Paradox. Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(4), Article 7. https://doi.org/10.5817/CP2016-4-7

Kien, Grant (2008): Technography: Studying technology in everyday life. In: Eileen M. Trauth (ed.), *Qualitative Research in Information Systems*, S. 147–168. Hershey, PA: IGI Global.

Luhmann, Niklas (1991): *Soziologie des Risikos*. Berlin: de Gruyter.

Lupton, Deborah; Tulloch, John (2002). "Risk is part of your life": Risk epistemologies among a group of Australians. *Sociology*, 36(2), S. 317–334.

Lutz, Christoph; Hoffmann, Christian P.; Ranzini, Giulia (2020): Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media & Society*, 22(7), S. 1168–1187.

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

Lyon, David (2018): *The Culture of Surveillance: Watching as a Way of Life*. Cambridge: Polity Press.

Maccario, Guglielmo; Naldi, Maurizio (2022): Privacy in smart speakers: A systematic literature review. *Security and Privacy*, 6(1).

Malkin, Nathan; Deatrick, Joe; Tong, Allen; Wijesekera, Primal; Egelman, Serge; Wagner, David (2019): Privacy attitudes of smart speaker users. *Proceedings on Privacy Enhancing Technologies*, 2019(4), S. 250–271.

Möller, Johanna E. (2024): Situational privacy: theorizing privacy as communication and media practice. In: *Communication Theory*, Volume 34, Issue 3, August 2024, S. 130–142.

Nissenbaum, Helen (2010): *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

Norberg, Patricia A.; Horne, Daniel R.; Horne, David A. (2007): The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1), S. 100–126.

Reckwitz, Andreas (2003): Grundelemente einer Theorie sozialer Praktiken. *Zeitschrift für Soziologie*, 32(4), S. 282–301.

Schatzki, Theodore (2002): *The Site of the Social: A Philosophical Account of the Constitution of Social Life and Change*. University Park, PA: Penn State University Press.

Schmitz, Lukas (2024): „Da drück ich dann auf Mikro, wenn's hier mal um Dinge geht…" Kreative Privatisierung. Der Umgang mit Privatheitsansprüchen in der Smart Speaker-Nutzung. In: *Data Sharing – Datenkapitalismus by Default?* Hg. v. Michael Friedewald et al.. Baden-Baden: Nomos, S. 215-242.

Stokols, D. (1995) „The Paradox of Environmental Psychology", *American Psychologist*, 50, S. 821–837.

Wilkinson, Ian (2010). *Risk, vulnerability and everyday life.* London: Routledge.

Xu, Kun; Chan-Olmsted, Sylvia; Liu, Fanjue (2022): Smart speakers require smart management: Two routes from user gratifications to privacy settings. *International Journal of Communication*, 16, S. 192–214.

Zuboff, Shoshana (2018): *Das Zeitalter des Überwachungskapitalismus.* Frankfurt am Main: Campus Verlag.

Über den Autor

Lukas Schmitz, M.A.
promoviert an der TU Dresden zur praktischen Herstellung von Bequemlichkeit im häuslichen Alltag am Beispiel der Smart-Speaker-Nutzung und ist wissenschaftlicher Mitarbeiter im SCODI-Projekt an der Johannes-Kepler-Universität in Linz. Email: lukas.schmitz@jku.at