Teil V:
Narrative in Sicherheitsforschung, Resilienz und der Geburtshilfe

Zukunftsvisionen der Sicherheit: Resilienznarrative in der Sicherheitsforschung

Sophia Rossmann und Naomi Shulman[1]

Zusammenfassung

Dieser Beitrag untersucht Resilienznarrative in der deutschen Sicherheitsforschung und -politik, die zu einer wirkmächtigen Zukunftsvision der öffentlichen Sicherheit zusammenfließen. Diese Zukunftsvision, die wir mit Jasanoff und Kim als soziotechnisches *Imaginary* verstehen, drückt sich auf forschungsprogrammatischer und politischer Ebene im Ziel aus, gesellschaftliche Resilienz mithilfe technischer Sicherheitsinnovationen zu fördern. Dabei gelten Daten als unentbehrliche Grundlage für wirkungsvolle Sicherheitssysteme: Die Narrative zur gesellschaftlichen Resilienz gegenüber Bedrohungen und Gefahren zielen darauf ab, dass Individuen Verantwortung für das gesellschaftliche Wohl zeigen, indem sie Daten teilen. Zugleich sollen Individuen darauf vertrauen, dass soziotechnische Sicherheitssysteme verantwortungsvoll mit ihren Daten umgehen. Mittels einer Diskursanalyse untersuchen wir relevante politische Programme und Strategien sowie zwei empirische Fallbeispiele aus der Sicherheitsforschung und diskutieren, wie diese Datenschutz verhandeln. Anhand dieser Materialien zeigen wir auf, welche Merkmale des Resilienzbegriffs zur Konjunktur von Resilienznarrativen geführt und damit zu einem Wandel der Sicherheitskultur beigetragen haben. Schließlich verdeutlichen wir, dass das soziotechnische *Imaginary* der gesellschaftlichen Resilienz kritischer Diskussion und Reflexion nicht nur auf wissenschaftlicher, sondern auch auf politischer Ebene bedarf. Denn indem technische Innovationen als Dreh- und Angelpunkt von Sicherheitssystemen und damit von gesellschaftlicher Resilienz dargestellt werden, geraten soziale Fragen, die für die Zukunftsgestaltung der öffentlichen Sicherheit wesentlich sind, aus dem Blick.

1 Beide Autorinnen haben zu gleichen Teilen zum Artikel beigetragen; die Nennung erfolgt alphabetisch. Die Forschung wurde innerhalb des Projekts BeLIFE, unter der Leitung von Prof. Dr. Lars Gerhold (TU Braunschweig), gefördert. Wir danken Lasse Wennerhold, M.Sc. für die Interviews, die er konzipiert und mit den Projekten durchgeführt hat.

1. Einleitung

Der Bevölkerungs- und Katastrophenschutz zielt darauf ab, die öffentliche Sicherheit für Bürger:innen zu gewährleisten.[2] Die Beschäftigung mit den Bedingungen und Merkmalen der Sicherheit ist damit für die Politik und die Gesellschaft ein grundlegendes Thema. So ist Sicherheit, im Sinne des Schutzes vor Gefahren, nicht nur ein „Leitbegriff politischen Handelns", sondern bildet auch einen „umfassenden sozialkulturellen Orientierungshorizont" (Conze 2022, S. 12). Die Frage, was Sicherheit ausmacht, hängt davon ab, was eine Gesellschaft als Gefahren versteht und wie sie diese adressieren möchte. Dies unterliegt einem kontinuierlichen Aushandlungsprozess, der die gesellschaftliche „Sicherheitskultur" prägt (Daase 2010).

Ein wesentliches Spannungsfeld in diesem Aushandlungsprozess ist die Frage, wie Gesellschaften den Bedürfnissen der Privatheit und der Sicherheit begegnen und wie sie den verantwortungsvollen Umgang damit regeln (vgl. Riescher 2010). In diesem Beitrag geht es um Privatheit im Kontext der Datennutzung und somit vor allem um die „Fähigkeit und den Rechtsanspruch von Individuen und Gruppen, […] über die Verfügbarkeit von Informationen über die eigene Person (informational privacy) zu bestimmen" (Kruse/Schmitt 2021, S. 4). Privatheit betrifft nicht zuletzt die Herausforderungen der Macht (wer worüber entscheidet und welche Handlungsbefugnisse hat) und die Risiken, die aus der Machtausübung erwachsen. Es gilt, die Grenzen einer zum Zweck der öffentlichen Sicherheit ausgeübten Macht zu bestimmen und somit bspw. dem Machtmissbrauch oder der Überwachung vorzubeugen.

Diese grundsätzliche Spannung tritt in Debatten über die Verfügbarkeit, Generierung und Nutzung von Daten in der Sicherheitsforschung und -praxis zutage. Während datengetriebene Systeme als Handlungs- und Entscheidungsgrundlage im Bevölkerungs- und Katastrophenschutz dienen, wird im Umgang mit personenbezogenen Daten auch der Schutz und die Autonomie des Individuums zur praktischen Herausforderung.

Zentral für diese Debatten ist der Begriff der gesellschaftlichen Resilienz. Die Konjunktur von Resilienznarrativen lässt sich als Folge einer Ausweitung des gesellschaftlichen Sicherheitsverständnisses verstehen.

2 Rechtlich gesprochen bezieht sich „öffentliche Sicherheit und Ordnung" in ihrer Gesamtheit auf die gesetzlichen, staatlichen und gesellschaftlichen Ebenen, nämlich auf „den Schutz der geschriebenen Rechtsordnung, des Staates und seiner Institutionen und der individuellen Rechtsgüter der Bürger" (Alexy u. a. 2023).

Christopher Daase erläutert, wie sich das Sicherheitsverständnis aufgrund wachsender gesellschaftlicher Sicherheitsbedürfnisse und der Wahrnehmung zunehmend komplexer und vernetzter soziopolitischer Verhältnisse entlang verschiedener Dimensionen erweitert hat (2010, S. 142-148).[3] Indem sich die Dimensionen des Sicherheitsbegriffs verändern – und damit auch die gesellschaftliche Wahrnehmung dessen, was Sicherheit bedeutet und in welchen Bereichen sie eine Rolle spielt –, wandelt sich auch die Sicherheitskultur. Diese umfasst die gesellschaftliche Gefahrenbewertung sowie die als optimal gesehenen Mittel zur Gefahrenbekämpfung (Daase 2010, S. 140). In einer Gesellschaft, die sich aktuell weniger mit konkreten Bedrohungen als mit „unklaren und zukünftigen Risiken" beschäftigt, wächst ein Verlangen nach „proaktiver Sicherheits- oder besser: Risikopolitik" (ebd., S. 148). Seit dieser Beurteilung Daases sind gut fünfzehn Jahre vergangen. Betrachtet man die sicherheitskulturellen Entwicklungen in den letzten Jahren und blickt voraus, so zeichnet sich neben diesem Verlangen nach „proaktiver Risikopolitik" ein Streben nach einer Resilienzpolitik ab, die nicht nur von proaktiver Handlung, sondern auch von einer gesamtgesellschaftlichen Verantwortung für den Umgang mit Sicherheitsbedürfnissen gekennzeichnet ist.

In diesem sicherheitskulturellen Wandel entsteht jedoch auch ein „new security paradox" (Pavone u. a. 2016, S. 241), das insbesondere die Verschränkung von Technologien und Menschen betrifft: Gerade diejenigen Sicherheitslösungen, die auch technologische Überwachungsmechanismen einsetzen, produzieren eigene Risiken, die sich für Individuen bspw. in Form von Datenhoheitsverlusten und Einschränkungen der Privatheit bemerkbar machen (ebd.). Indem Technik zum Mittel wird, um personenbezogene Daten systematisch zu extrahieren oder gar zu erschaffen, sind nicht mehr nur Individuen Objekte der Überwachung, sondern Überwachung wird selbst zum System und betrachtet Kontexte, Muster und Verflechtungen (Marx 2002).

Vor dem Hintergrund dieser Herausforderungen begegnen Resilienznarrative Bedenken darüber, welche neuen Risiken und gesellschaftlichen Kosten die Praktiken der technologisierten Versicherheitlichung (vgl. Buzan u. a. 1998) mit sich bringen. Indem diese Narrative die gesamtgesellschaft-

3 Daase erwähnt hierbei (1) die Referenzdimension (Bezugspunkte der Sicherheit), (2) die Sachdimension (relevante Politikbereiche der Sicherheit), (3) die Raumdimension (sicherheitsbezogene geographische Ausdehnung) sowie (4) die Gefahrendimension (Gefahrenverständnis und Umgang mit Unsicherheiten) eines erweiterten Sicherheitsbegriffs (Daase 2010, S. 142-148).

liche Bewältigung zukünftiger Krisen und Katastrophen verheißen, drücken sie eine soziotechnische Zukunftsvision aus, in der alle Individuen dafür verantwortlich sind, ihren Beitrag zur Herstellung von Sicherheit und zur Resilienz des gesellschaftlichen Systems zu leisten. Dieser individuelle Beitrag besteht auch darin, Daten bereitzustellen, die als Grundlage sicherheitskritischer soziotechnischer Systeme dienen.

Im Folgenden analysieren wir, wie Narrative gesellschaftlicher Resilienz in transdisziplinären Diskursen über sicherheitskritische Technologien und Datenschutz wirken. Dabei beziehen wir uns auf ein Datenschutzverständnis wie es in der seit 2018 geltenden Europäischen Datenschutzgrundverordnung (DSGVO) dargelegt ist und als unmittelbar geltendes Recht in Deutschland Anwendung findet. Die DSGVO schützt die Grundrechte und Grundfreiheiten aller Personen (Art. 1 Abs. 2) und umfasst die Dimensionen des technischen Datenschutzes (Datensicherheit, IT-Sicherheit) und des individuellen Datenschutzes (Schutz der Privatsphäre und der Persönlichkeit, Recht auf informationelle Selbstbestimmung wie im Grundrecht verankert) (Wewer 2020).

Um die Wirkung von Resilienznarrativen in Diskursen zu Sicherheitstechnologien und Datenschutz zu untersuchen, nähern wir uns zuerst dem Begriff der gesellschaftlichen Resilienz als Ausdruck eines wirkmächtigen soziotechnischen *Imaginary* (Jasanoff/Kim 2009, 2015). Dann analysieren wir, wie dieses *Imaginary* einer sicheren Zukunft soziopolitisch gerahmt wird. Schließlich verdeutlichen wir anhand zweier Fallbeispiele, wie Narrative der Resilienz im soziotechnischen *Imaginary* des gesellschaftlichen Umgangs mit sicherheitskritischen Technologien eingebettet werden. Abschließend diskutieren wir die Ergebnisse vor dem Hintergrund der gegenwärtigen sicherheitskulturellen Dominanz von Narrativen, mittels derer dieses wirkmächtige soziotechnische *Imaginary* der gesellschaftlichen Resilienz zirkuliert: die Vision einer zukunfts- und handlungsfähigen Gesellschaft, die erkennt, dass Daten notwendige Informationsgrundlage aller Entscheidungen und Handlungen im Dienst der öffentlichen Sicherheit sind.

2. Eine Annäherung an den Begriff der gesellschaftlichen Resilienz

2.1 Resilienznarrative als Ausdruck soziotechnischer Imaginaries

Mit dem sozialwissenschaftlichen Konzept der *sociotechnical imaginaries* (Jasanoff/Kim 2009, 2015) lassen sich gesellschaftliche Zukunftsvisionen analytisch fassen. Jasanoff und Kim definieren soziotechnische *Imaginaries*[4] als „collectively held, institutionally stabilized, and publicly performed visions of desirable futures, animated by shared understandings of forms of social life and social order attainable through, and supportive of, advances in science and technology" (2015, S. 4). Kollektive *Imaginaries* sind relativ stabile, soziohistorisch gewachsene Phänomene, verknüpfen also Vergangenheit, Gegenwart und Zukunft sinnvoll miteinander, und sind in institutionellen Strukturen verankert. Sie geben Aufschluss darüber, was eine Gesellschaft als gut und erstrebenswert betrachtet und wie Wissenschaft und Technologie im Zusammenspiel mit Politik diese *Imaginaries* verwirklichen sollen.

Imaginaries sind somit auch performativ, da sie mögliche Zukünfte artikulieren, den politischen Willen für deren Umsetzung generieren und soziale Ordnung herstellen (Jasanoff/Kim 2009). So wird staatlich geförderte Wissenschaft und Technologieentwicklung von gesellschaftlich geteilten Zukunftsvisionen und politischen Zielen koproduziert. Gleichzeitig generieren wirkmächtige *Imaginaries* auch Pfadabhängigkeiten, indem sie manche *Imaginaries* plausibler als andere erscheinen lassen und so Aufmerksamkeit und Ressourcen in sich vereinigen (vgl. Wentland 2025).

Soziotechnische *Imaginaries* dienen uns als sensibilisierendes Konzept, um die Wirkmacht bestimmter Narrative zu analysieren, die die soziopolitische Kultur eines Landes prägen. Eine diskursanalytische Untersuchung dieser Narrative legt offen, welche potenziellen Zukünfte als möglich erachtet werden. Sozialwissenschaftliche Arbeiten haben bereits gezeigt, dass das Konzept der soziotechnischen *Imaginaries* ein produktives Instrument für die Sicherheitsforschung und die Analyse von Sicherheitskulturen ist (Binder 2022; Gerhold/Brandes 2021). So können beispielsweise nationale politische Strategien und Maßnahmen und staatliche Forschungsförderung eine Analysegrundlage bilden, um soziotechnische *Imaginaries* eines Landes herauszuarbeiten.

4 Der englische Begriff Imaginary wird auch im Deutschen verwendet (vgl. Wentland 2025).

2.2 Gesellschaftliche Resilienznarrative

Soziotechnische *Imaginaries* haben vielfältige Darstellungsformen, die materielle, performative und sprachliche Dimensionen miteinander verbinden. Im Folgenden werden wir zunächst auf die sprachliche Dimension eingehen, indem wir Narrative gesellschaftlicher Resilienz und resilienter Sicherheitssysteme in der deutschen Sicherheitsforschung als Ausdruck einer soziotechnischen Zukunftsvision lesen. Diese Narrative sind eng mit den materiellen und performativen Dimensionen verwoben, wie unsere empirischen Fallstudien zweier Sicherheitsforschungsprojekte zeigen.

Narrative sind öffentlich rezipierte Erzählungen, die identitäts-, ordnungs- und sinnstiftend wirken (vgl. Shulman 2024; Müller-Funk 2008; Hülk 2013). Sie verleihen soziotechnischen *Imaginaries* eine sprachliche Ausdrucksform, mittels derer diese zirkulieren und gefestigt werden. Narrative können auch deshalb gesellschaftliche Visionen darstellen, weil sie die Perspektiven einzelner Subjekte in einer kollektiven Erzählung aufgehen lassen (vgl. Breithaupt 2022, S. 186; Ächtler 2014, S. 258). So werden diese Narrative ein integraler Bestandteil politischer und gesellschaftlicher Diskurse und prägen die Sicherheitskultur.

Resilienznarrative sind im öffentlichen Diskurs um Sicherheitsfragen in den letzten Jahren sehr prominent geworden und werden als Inbegriff eines neuen, zukunftsweisenden systemischen Sicherheitsdenkens dargestellt. So schreibt die damalige Innenministerin Nancy Faeser in ihrem Vorwort zum Umsetzungsplan der Deutschen Strategie zur Stärkung der Resilienz gegenüber Katastrophen: „Das Ziel, unsere Resilienz umfassend zu stärken, steht für einen Paradigmenwechsel – vor allem weil wir nicht mehr nur in einzelnen Gefahrenkategorien und Zuständigkeiten denken“ (BMI 2024, S. 4). Der systemische Fokus gesellschaftlicher Resilienznarrative ist deshalb so wirkmächtig, weil er sowohl physische als auch ontologische Sicherheit verspricht. Denn eine resiliente Gesellschaft überlebt Krisen und Katastrophen nicht nur im materiellen Sinn, sondern bleibt in ihrem Wesen bestehen. Die ontologische Sicherheit einer Gesellschaft bezieht sich somit auf mehr als die Sicherung der Existenz; es geht vor allem darum, eine stabile kollektive Identität zu beschützen und zu bewahren (Kinnvall/Mitzen 2017, S. 4; vgl. Giddens 1991).

Gerade der Fortbestand der Gesellschaft – in ihrer kohärenten Identität – soll unter den destabilisierenden Bedingungen der Unsicherheit und des fehlenden Wissens über Zukunftsentwicklungen gewährleistet werden. Die Orientierung des Resilienzbegriffs auf Zukunftsgestaltung impliziert, dass

Resilienz zum erfolgreichen Umgang mit jedweder (auch unvorhergesehenen) Gefahr befähigt. Damit ermächtigt Resilienz auch in komplexen und unklaren Gefahrenlagen zur Handlung und wirkt einem Ohnmachtsgefühl entgegen. Dass Resilienz keinerlei Wissen über eine erwartbare Gefahr voraussetzt, unterscheidet den Begriff der Resilienz laut Terje Aven von dem des Risikos und erklärt die Wirkmächtigkeit von Resilienznarrativen (2019, S. 1196). Narrative der gesellschaftlichen Resilienz, die das soziotechnische *Imaginary* einer sicheren Zukunft mitbestimmen, können auch deshalb so überzeugend wirken, weil sie positive Konnotationen der Gestaltungsbefähigung in den Vordergrund rücken:

> Das Konzept der Resilienz liefert insgesamt weniger konkrete Handlungsanleitungen als ein allgemeines Rechtfertigungsmuster und Rationalitätsschema, das es erlaubt, Probleme entlang der Differenz verletzbar versus widerstandsfähig zu definieren und den negativen Beiklang von Risikodiskursen in die Positivsemantik von Entwicklungspotenzialen zu übersetzen. (Bröckling 2016, S. 400)

Somit verleihen Resilienznarrative selbst bereits ontologische Sicherheit und vermitteln normative Gewissheit, indem sie die Sicherung eines gesellschaftlichen Fortbestands mit der Überzeugung eines kollektiv für richtig und wichtig befundenen Ziels verbinden.

Aus soziopolitischer Perspektive gilt es deshalb zu beleuchten, wie Resilienznarrative die Pole der Verantwortungszuweisung und der Befähigung darstellen und rechtfertigen (vgl. Bonß 2015, S. 29-30). Denn gesellschaftliche Resilienz impliziert sowohl individuelle als auch kollektive Handlungsfähigkeit: Damit werden Bürger:innen als handelnde Subjekte in den Fokus gerückt und Verantwortung neu verteilt (Cavelty u. a. 2015, S. 7).

Diese Frage der Verantwortungszuweisung und -verteilung ist im Kontext der Datengenerierung und -nutzung besonders relevant. Denn Daten werden in den Resilienznarrativen der Sicherheitsforschung als unentbehrliche Grundlage für diejenigen sicherheitskritischen soziotechnischen Systeme dargestellt, deren Ziel es ist, die gesellschaftliche Resilienz zu fördern. So wird auch die Frage der Datennutzung mit der Frage verbunden, inwiefern das Individuum den Bestand des Kollektivs mitverantwortet und wie es zur gesellschaftlichen Resilienz beitragen kann und sollte. Allerdings bleibt weiterhin oft unbestimmt, was die individuelle Verantwortung für die kollektive Sicherheit genau bedeutet und wie sie zur gesellschaftlichen Resilienz beiträgt (Kaufmann 2014, S. 304). Ein Blick auf Narrative der

Resilienz in relevanten Programmen und Strategien der deutschen Politik und (Sicherheits)Forschung soll dies im folgenden Abschnitt verdeutlichen.

2.3 Programmatische und strategische Rahmungen der Narrative gesellschaftlicher Resilienz

In seinem Sicherheitsforschungsprogramm veröffentlicht das Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) seit 2007 alle fünf Jahre neue Rahmenprogramme der Forschungsförderung, die die zunehmende Zentralität von Resilienznarrativen aufzeigen. In den Anfangsjahren des Sicherheitsforschungsprogramms wurde die Frage der gesellschaftlichen Resilienz und ihr Bezug zur öffentlichen Sicherheit zwar bereits als vielversprechender Schwerpunkt verhandelt, aber inhaltlich noch nicht ausgefüllt (Thoma u. a. 2012, S. 41). In den seitdem vergangenen ca. 15 Jahren ist die gesellschaftliche Resilienz als gleichzeitige Voraussetzung und Auswirkung öffentlicher Sicherheitsbestrebungen zum Kern eines soziotechnischen *Imaginary* geworden, das Forschungspriorisierungen und Fördermittelvergaben mitbestimmt.

Dies macht sich auch in der Sicherheitsforschungsprogrammatik des BMFTR bemerkbar: Während das Rahmenprogramm der Jahre 2018 bis 2023 zwar bereits Resilienz als Kernthema in unterschiedlichen Lebensbereichen identifiziert, wird im aktuellen Rahmenprogramm für die Jahre 2024 bis 2029 die gesellschaftliche Resilienz Teil des Titels: „Forschung für die zivile Sicherheit – gemeinsam für ein sicheres Leben in einer resilienten Gesellschaft". Diese Formulierung verbindet eine wissenschaftliche Programmatik mit einem kollektiv-normativen *Imaginary* dessen, was „ein sicheres Leben" zukünftig ausmacht und wer dazu beitragen soll.

Das Rahmenprogramm soll die Verwirklichung übergeordneter sozio-politisch-strategischer Ziele unterstützen, insbesondere Ziele der Zukunftsstrategie Forschung und Innovation des BMFTR und der Deutschen Strategie zur Stärkung der Resilienz gegenüber Krisen und Katastrophen. Die Zukunftsstrategie Forschung und Innovation stellt soziotechnische Sicherheitslösungen als unabdingbar dar und wird Teil eines gesellschaftlich wünschbaren Sicherungsprozesses, in dem Menschen und Technologien zusammenarbeiten: „Für die zivile Sicherheit treiben wir die Entwicklung zukunftsfähiger Sicherheitslösungen an der Schnittstelle zwischen Mensch und Technologie voran" (Bundestag 2023, Drucksache 20/5710, S. 60). Dies veranschaulicht, wie soziotechnische Imaginaries nicht zuletzt durch „ac-

tive exercises of state power" geformt werden, die sich in Priorisierungen und Weichensetzungen äußern, beispielsweise in Mittelzuweisungen für Forschung und Entwicklung (Jasanoff/Kim 2009, S. 123). So wird die Forschung selbst zu einem Instrument, das soziotechnische *Imaginaries* etabliert und ausbaut: „National imaginations can penetrate the very designs and practices of scientific research and technological development" (ebd., S. 124).

Datenverfügbarkeit und -nutzung werden dabei als eine Grundbedingung für die gesellschaftliche Resilienz dargestellt. Daten gelten im Sicherheitskontext als notwendige „Basis für eine zielgerichtete Planung" und spielen über den gesamten Krisenzyklus hinweg – also vor, während und nach der Krise – „eine entscheidende Rolle" (Bundesministerium des Innern 2022, S. 30). Unter der Überschrift „Mutige und verantwortungsvolle Datenkultur" setzt sich die Deutsche Datenstrategie für „einen Kulturwandel hin zu mehr Datenbereitstellung und Datennutzung" ein (Bundesministerium für Digitales und Verkehr 2023, S. 33). Laut Strategie kann sich ein solcher Kulturwandel aus der gesamtgesellschaftlichen Überzeugung speisen, dass die Gewinne einer Datennutzung für das Allgemeinwohl die möglichen Risiken dieser Nutzung überwiegen: „Das Potential der Datennutzung kann nur voll ausgeschöpft werden, wenn Bürgerinnen und Bürger, Zivilgesellschaft, Wirtschaft, Wissenschaft und Staat die Vorteile der Datennutzung erkennen und Vertrauen in eine verantwortungsvolle Datennutzung entwickeln" (ebd.). Um das Vertrauen aller Akteur:innen in die verantwortungsvolle Datennutzung zu gewährleisten, gelte es, die Befolgung der relevanten rechtlichen Verordnungen des Daten- und Verbraucherschutzes zu garantieren, damit Individuen in allen digitalen Angelegenheiten „selbstständig, selbstbestimmt und sicher" agieren könnten (ebd.). Eben diese Vorstellung des gelungenen Zusammenspiels staatlicher Kontroll- und Sicherheitsmechanismen einerseits und menschlicher Entscheidungs- und Handlungsfähigkeit andererseits ist kennzeichnend für die Narrative der Resilienz, wie sie auch in unserer Fallstudie zum Ausdruck kommen.

3. Fallstudie: Die Förderrichtlinie SifoLIFE

Im Folgenden wollen wir verdeutlichen, wie Narrative der Resilienz und das aus ihnen erwachsende soziotechnische *Imaginary* einer sicheren Zu-

kunft in zwei Projekten zum Ausdruck kommen, die im Rahmen der SifoLIFE-Förderrichtlinie des BMFTR forschen. SifoLIFE fördert die „Demonstration innovativer Sicherheitslösungen in der Praxis".[5] Die fünf in der jetzigen zweiten Phase geförderten Projekte sind über ganz Deutschland verteilt und erproben ihre Lösungen für komplexe Krisenszenarien, die in ihren jeweiligen Kommunen plausible Gefahren darstellen.

In den SifoLIFE-Projekten sollen unterschiedliche Dimensionen der Resilienz – technisch, sozial, psychosozial und kommunal – gestärkt werden. Technische Innovationen sollen Informations-, Kommunikations- und Entscheidungsprozesse unterstützen. Die soziale Dimension stellt auf die Kompetenzen und Kapazitäten der Menschen ab: Die Bevölkerung soll in Krisensituationen handlungsfähig sein, und diese Handlungsfähigkeit kann durch das Bewusstsein für sicherheitsrelevante Themen sowie die individuelle und gesellschaftliche Vorbereitung auf Krisensituationen gestärkt werden. Die psychosoziale Dimension der Resilienz umfasst, wie Menschen Unsicherheiten, Bedrohungen und akute Krisen und Katastrophen sowie ihre eigene Handlungsfähigkeit wahrnehmen, und ob sie beispielsweise staatlichen Institutionen, politischen Entscheidungen und den Strukturen und Prozessen der Krisenbewältigung vertrauen. Schließlich sollen diese drei Dimensionen in der kommunalen Dimension der Resilienz in räumlich verorteten Gemeinschaften Ausdruck finden, indem sie das Verantwortungsgefühl der Menschen stärken und Engagement in Form von Selbsthilfe und gegenseitiger Hilfe fördern.

Wie artikulieren sich Narrative gesellschaftlicher Resilienz in Diskursen über sicherheitskritische Technologien und Datenschutz, aus denen sich ein soziotechnisches *Imaginary* zur Bewältigung zukünftiger Sicherheitsherausforderungen speist? Um dieser Frage nachzugehen, analysieren wir zwei der fünf SifoLIFE-Projekte. Wir untersuchen, wie diese Projekte die Nutzung von Technologien, einschließlich Fragen der Datenverarbeitung und des Datenschutzes, verhandeln und wie sie deren Rolle in der Herstellung öffentlicher Sicherheit darstellen. Ein besonderes analytisches Augenmerk gilt der Frage, wie die Projekte das Verhältnis zwischen Akzeptanz und Akzeptabilität diskutieren. Während Akzeptanz darauf verweist, dass einer Technologie empirisch und faktisch zugestimmt wird, setzt der philosophische Ansatz der Akzeptabilität auf die ethische Abwägung vor der eigentlichen Nutzung und suggeriert, dass technische Lösungen an

5 https://www.sifo.de/sifo/de/projekte/querschnittsthemen-und-aktivitaeten/sifolife/sifolife_node.html.

die Wünsche und Normen einer Gesellschaft angepasst werden müssen (Grunwald 2005).

Wir haben zwei Projekte ausgewählt, die jeweils anders gelagerte Ziele verfolgen: Das Projekt RESCUE-MATE hat einen stärkeren Fokus auf die Gesamtbevölkerung einer Großstadt, während das Projekt A.D.L.e.R. soziotechnische Lösungen für vulnerable Personen in ihren jeweiligen Wohnsituationen entwickelt, die auch Auswirkungen für die öffentliche Sicherheit haben. Diese verschiedenen Zielsetzungen erlauben auf analytischer Ebene zu vergleichen, wie Datengenerierung und -nutzung im Sicherheitskontext des Kollektivs und des Individuums gedacht wird.

Als Grundlage für die empirische Analyse dienen die jeweiligen Projektanträge sowie vier Interviews mit Projektpartnern, die zwischen August und November 2024 geführt wurden. Diese Dokumente haben wir diskursanalytisch ausgewertet (Keller 2001), um zu ergründen, wie die Projekte Risiken der Datengenerierung, -verarbeitung und -nutzung vor dem Hintergrund des Datenschutzes verhandeln. In einem zweiten Schritt haben wir unsere Analyse konzeptionell vertieft, indem wir soziotechnische *Imaginaries* als sensibilisierendes Konzept verwendet haben, um die induktiv gewonnenen Erkenntnisse zu kontextualisieren.[6]

4. Datennutzung für die gesellschaftliche Resilienz in SifoLIFE

Datengenerierung und -nutzung gilt in der Sicherheitsforschung als wesentliche Bedingung gesellschaftlicher Resilienz, da Daten eine unentbehrliche Informationsgrundlage für Entscheidungen und Handlungen bieten. Allerdings wirft diese Entwicklung die eingangs gestellte Frage auf, wie entsprechende Forschungsprojekte das Spannungsfeld zwischen Privatheit und öffentlicher Sicherheit ausloten. Wie werden Datengenerierung, -nutzung und -verarbeitung sowie insbesondere die damit verbundenen Risiken in den beiden Fallstudien narrativ verhandelt?

6 Da die Projektanträge nicht öffentlich sind, wird in der Analyse nur aus den Interviews zitiert.

4.1 Zwischen den Privatheitsansprüchen des Individuums und der Sicherheit der Gesellschaft

4.1.1 Das Projekt RESCUE-MATE

Das Projekt „RESCUE-MATE – Dynamische Lageerstellung und Unterstützung für Rettungskräfte in komplexen Krisensituationen" basiert auf dem Szenario einer Sturmflut in Hamburg. Eine Vorabstudie des Projekts, in der Behörden und Organisationen mit Sicherheitsaufgaben sowie Bürger:innen befragt wurden, zeigt, dass der Datenaustausch in Krisenlagen als größte Herausforderung wahrgenommen wird. Deshalb erprobt das Projekt derzeit ein soziotechnisches System, das Daten aus verschiedenen Quellen generiert, sammelt, auswertet und zusammenführt. Projektziel ist es, diese Daten zu nutzen, um ein dynamisches Lagebild in Echtzeit zu entwickeln und so ein Frühwarnsystem für das Sturmflutszenario und andere Krisenlagen zu etablieren. Damit will das Projekt die Entscheidungsfähigkeit von Rettungskräften in Krisen- und Katastrophensituationen optimieren und Evakuierungsmaßnahmen verbessern.

Das Projekt nutzt verschiedene Datenquellen und -typen, die es in einem dynamischen Lagebild zusammenführt: 1) statistische Daten; 2) Sensordaten, die durch Verkehrskameras, Terminalkameras und Umgebungssensoren sowie aus Sensorik zur Polder- und Deichüberwachung und Drohnen generiert werden. Die Drohnen nutzen KI-Technologie, um zur Lageaufklärung beizutragen und bspw. ertrinkende Menschen in Gewässern zu lokalisieren; 3) Informationen aus dem TETRA-Funk der Behörden, der mithilfe von KI ausgewertet wird; und 4) Social-Media-Daten, die ebenfalls mithilfe von KI ausgewertet werden. Dazu zählen Hinweise von Bürger:innen aus sozialen Netzwerken sowie Daten, die von Detektionsalgorithmen generiert werden, indem diese soziale Nachrichtenquellen automatisiert durchsuchen und analysieren und beispielsweise Informationen zu beschädigten Einrichtungen aus Bildern extrahieren. Zusätzlich zur Bündelung der Datenströme in einem Lagebild entwickelt das Projekt eine App, die Informationen bidirektional zwischen der Plattform und Rettungskräften sowie Bürger:innen vermittelt und Daten von diesen Akteur:innen gewinnt und ins System einspeist.

Das entwickelte Lagebild soll in die Arbeit des zentralen Krisenstabs der Innenbehörde integriert werden, aber auch anderen wichtigen Akteuren im Krisenfall (wie Feuerwehr, Polizei, Hafenpersonal, den Bezirken oder Fachbehörden wie der Umweltbehörde) zur Verfügung gestellt werden.

Während in anderen Forschungsprojekten bereits ähnliche Technologien entwickelt wurden, läge die Innovation des Projekts in der automatisierten Datenverarbeitung und der systemischen Zusammenführung verschiedener, teilweise bereits existierender Daten.

4.1.2 Datenschutz als technische Herausforderung

Im Projekt sind Daten, die im öffentlichen Raum generiert und von Nutzenden ins System eingebracht werden, Dreh- und Angelpunkt der Entwicklung des Lagebilds und der App. Der Datenaustausch in Krisen- und Katastrophenfällen wird als zentrales Element gesehen, um öffentliche Sicherheit herzustellen und so zur gesellschaftlichen Resilienz beizutragen. Gleichzeitig muss dieses System datenschutzkonform sein und so die Sicherheit personenbezogener Daten garantieren.

Das Projekt verhandelt Datenschutz primär entlang seiner technischen Dimension. Konkretere Reflexionen zur technischen Ausgestaltung des soziotechnischen Systems zeigen sich beispielhaft beim Thema Datenverschlüsselung. So beschreibt ein Mitarbeiter der Universität Hamburg die eigene Arbeit wie folgt:

> Interviewpartner: Ich habe Daten, [...] die müssen datenschutzfreundlich erhoben werden und dann müssen sie sicher und datenschutzfreundlich geteilt und verarbeitet werden und das ist ein ganz klassisches, ich sage mal, Verteilte-Systeme-IT-Sicherheitsproblem […].
> Interviewer: Und wenn Sie jetzt über Datenschutz sprechen, dann stelle ich mir das so vor, […] [dass es] um technischen Datenschutz [geht], also: Wie muss ich ein Computersystem bauen, damit da keine Daten abgegriffen werden?
> Interviewpartner: Genau. Oder wie analysiere ich Daten richtig, sodass man hinterher nicht so viel mehr herauslesen kann, über das, was man nicht herauslesen sollte? (Interview RM_UH)

Der Interviewpartner betont die Notwendigkeit, Daten sicher zu erheben und „datenschutzfreundlich" zu verarbeiten. Zum einen lässt sich diese technische Auslegung des Datenschutzes damit begründen, dass der Projektpartner im Bereich verteilter Systeme und IT-Sicherheit arbeitet. Zum anderen spiegelt diese Auslegung das Projektverständnis wider: Sicherheit bedeutet hier, sichere technische Systeme zu bauen, die wiederum physische Sicherheit produzieren.

Eine zweite Dimension von Datenschutz zeigt sich in der Umsetzung rechtlicher Datenschutzbestimmungen in der Datenplattform des Lagebilds. So beschreibt ein Interviewpartner der Hamburger Innenbehörde die technische Umsetzung rechtlicher Konformität als eine der zentralen Herausforderungen der Datenverarbeitung:

> … [Die Integration verschiedener Daten in eine Datenplattform] ist natürlich auch ein technisches Problem, weil man muss ja sozusagen die Daten erst mal alle reinkriegen. [...] Das ist ja auch ein Informatik-Thema, um dann in einem Rechte-Rollen-Konzept, sage ich jetzt mal, diese Daten auch wieder auszugeben. Und zwar an den, der sie braucht, beziehungsweise der sie haben will und der auch eine Berechtigung dafür hat. (Interview RM_IB)

Der datenschutzkonforme Umgang mit Daten wird hier vor allem als „Informatik-Thema" und damit als technische Problemstellung beschrieben. Dabei muss sichergestellt werden, dass die Datenplattform nur Daten an Personen ausspielt, die die dafür erforderlichen Rechte besitzen. So soll die rechtliche Dimension von Datenschutz – wer darf auf bestimmte Daten zugreifen – technisch umgesetzt werden. Dieser Ansatz führt dazu, dass teilweise unvollständige Daten ausgewertet werden müssen, wie der Interviewpartner der Universität Hamburg darlegt:

> Da haben wir so ein bisschen die Genauigkeit für den Datenschutz und für die dezentrale Datenhaltung geopfert. Also man hat weniger Sichtbarkeit dadurch, aber man hat damit aber auch die Akzeptanz erhöht, dass die [Anwender:innen] überhaupt bereit sind, Daten zu teilen. (Interview RM_HH)

Durch die Möglichkeit, bestehende Daten nur in einer bestimmten Form dezentral zu teilen (z. B. teilweise anonymisiert), erhofft sich das Projekt, die Akzeptanz für das System zu steigern und die Bereitschaft zu erhöhen, dass Anwender:innen wie Polizei oder Hilfsorganisationen ihre Daten dem System bereitstellen.

Risiken der Datennutzung und -verarbeitung werden im Projekt vor allem bezüglich der technischen Umsetzung von Datenschutz artikuliert, also Systeme zu bauen, die datenschutzkonform sind. Diese technische Umsetzung inklusive rechtlicher Datenschutzvorgaben wird gleichzeitig als Grundlage für die soziale Akzeptanz des Systems verhandelt.

Die Schaffung sozialer Akzeptanz des Systems wird auch an anderer Stelle als erstrebenswertes Ziel formuliert. Bürger:innen werden in das

Vorhaben einbezogen, indem das System öffentlich demonstriert und seine Mehrwerte vermittelt werden. Das Projekt strebt an, Vorbehalte gegenüber technischen Innovationen abzubauen, wie sie beispielsweise beim Einsatz von Drohnen erwartet werden. Während mit (potenziellen) Anwender:innen im Projekt verhandelt wird, welche Daten wie geteilt werden, bleibt die Beteiligung der Bevölkerung derzeit auf die Informationsphase beschränkt. Bürger:innen werden über die Nutzen des Systems informiert, aber bisher nicht als aktive Akteur:innen in die Ausgestaltung der Technologie einbezogen, was ein niedriges Level an Partizipation (Arnstein 1969) suggeriert. Folglich kann das Projekt zwar zur potenziellen Akzeptanz beitragen, jedoch bleibt das Potenzial für Akzeptabilität neuer Technologien und partizipative Gestaltung bislang ungenutzt..

4.1.3 Daten als Grundlage der gesellschaftlichen Resilienz: die intendierte Anwendung

Ziel der soziotechnischen Lösung des Projekts RESCUE-MATE ist es, die gesellschaftliche Resilienz zu steigern und Sicherheit herzustellen. Zum einen soll das Lagebild mit seinem Frühwarnsystem es ermöglichen, Krisen und Katastrophen vorausschauend zu antizipieren und so schneller und effizienter zu reagieren. Zum anderen soll die Lösung im Krisenfall Menschen dabei unterstützen, sich selbst zu helfen. Dazu soll die App einen entscheidenden Beitrag leisten.

Der Interviewpartner der Universität Hamburg sieht in der App einen Beitrag zur Steigerung der gesellschaftlichen Resilienz, weil die per App vermittelten Informationen in einer Gefahrensituation zur Selbsthilfe befähigen:

> … damit man auch den Bürger dazu in die Lage versetzt, so ein Bild über seine lokale Lage zu bekommen und zum Beispiel zu sehen, welche Rettungswege sind denn jetzt zum Beispiel verstopft, soll ich mich nicht bewegen. […] und dann selber in der Situation die richtigen Schlüsse ziehen zu können. (Interview RM_UH)

Diese durch technische Innovation ermöglichte Selbsthilfefähigkeit ist wichtiger Bestandteil eines Narrativs der gesellschaftlichen Resilienz. Es zeigt sich weiter, dass Resilienz nicht nur als erstrebenswertes Ziel gilt, sondern über die Anforderungen einer Sicherung der Existenzgrundlage hinausgeht:

> Diese Datensammlung, Aufbereitung, Entscheidungsunterstützung, das ist das, was wir im Projekt machen, was auch der Erhöhung der Sicherheit der Personen im Hamburger Raum, Sicherheit ist vielleicht zu kurz gefasst, ich benutze immer gerne den Begriff Resilienz auch so mal im technischen Kontext. Wir wollen im Prinzip die Widerstandsfähigkeit Hamburgs erhöhen, um auf unvorhergesehene Situationen reagieren zu können und dazu gehört es, umfassendes Wissen zu haben, vielleicht auch Vorhersagen treffen zu können, wie entwickelt sich der Wasserstand, das kann man bei einer Sturmflut übrigens sehr gut, das ist alles gut vorhersagbar, […] aber was man nicht weiß, ist, wie dann die Verkehrswege aussehen, wie sich die Personen verhalten werden in so einem Fall und dazu hilft diese […] situation awareness, die wir schaffen wollen. (Interview RM_UH)

Der Interviewpartner entscheidet sich für Resilienz als Begriff, der für ihn über den der Sicherheit hinausgeht. Er unterstreicht die systemische Dimension des Resilienznarrativs, welche das Vorhersagbare (quantifizierbare Daten) mit dem Unvorhersehbaren (menschlichem Verhalten) vereint und ersteres zur Grundlage nimmt, um mit letzterem umgehen zu können. Dabei wird klar, dass Resilienz auch deshalb als sicherheitsproduzierend verstanden wird, weil sie als Fähigkeit gilt, unter Bedingungen des Nichtwissens mit zukünftigen kritischen Entwicklungen umzugehen:

> [I]n meinem technischen Kontext ist Sicherheit eine Subdisziplin von Resilienz, […] zum Beispiel in meinem Kontext [wäre] Sicherheit, ich kann sicher kommunizieren, ohne dass irgendwer es abhört und Resilienz wäre dann auch, ich kann mich einstellen auf unvorhergesehene Veränderungen, also da passiert was und mein System wird geflutet mit Anfragen oder die Leute wollen alle raus aus dem Gebiet und ich kann mich darauf einstellen und kann da so ein bisschen nachsteuern, beispielsweise. (Interview RM_UH)

Während sich Sicherheit in dieser Charakterisierung auf relativ statische Größen in einer spezifischen Situation bezieht, soll Resilienz den Umgang mit dynamischen und nicht absehbaren Entwicklungen ermöglichen. Das soziotechnische *Imaginary* der Resilienz als Umgang mit Gefahren kreist auch in diesem Interview um die Frage der Verantwortung:

> Sicherheit [ist] eher etwas, wo der Staat vielleicht proaktiv was tut und dann eben Resilienz, eben diese Challenge-Toleranz, also sich auf unvorhergesehene Herausforderungen einstellen zu können, wo der Staat

> vielleicht ein bisschen was tut, damit die Bürger hinterher selber agieren können oder sich selber helfen können. (Interview RM_UH)

Der Interviewpartner unterscheidet hier zwischen einem Sicherheitsverständnis, das staatliches Agieren in den Mittelpunkt stellt und einem Resilienzverständnis, das aus dem Zusammenspiel von Staat und Gesellschaft erwächst. Indem technische Systeme wie die App Bürger:innen befähigen, in Krisenlagen zu handeln und sich selbst zu helfen, ist das Ziel der Herstellung von Sicherheit nicht mehr nur Aufgabe des Staats, sondern bindet die gesamte Gesellschaft ein.

Bei der Analyse der Fallstudie wird deutlich, dass technische Innovation als unausweichlich gilt, um zukünftigen Krisen und Katastrophen wie Sturmfluten zu begegnen und so die Bevölkerung besser schützen zu können. Im Projekt sollen technische Innovationen Sicherheit produzieren, indem sie anhand multipler Datenquellen den Überblick über komplexe Großschadenslagen schaffen. Dieser systemgenerierte Überblick gilt als wesentliches Element der angestrebten gesellschaftlichen Resilienz, weil er alle im Krisenfall Betroffenen verknüpft und ihre Handlungsfähigkeit fördert. Während Individuen dieser Datengewinnung nicht explizit zustimmen können, sollen sie die Notwendigkeit solcher Innovationen zum Wohle des Kollektivs dennoch verstehen und akzeptieren. Somit ist die Frage der Befähigung und der daraus entstehenden Verantwortung im Umgang mit Datenteilung und -nutzung für die öffentliche Sicherheit wesentlich und wird fortlaufend verhandelt.

4.2 Zwischen Privatheit und Sicherheit des Individuums

4.2.1 Das Projekt A.D.L.e.R.

Das zweite Fallbeispiel, das Dortmunder Projekt „A.D.L.e.R. – Automatisiertes Detektions-, Melde- und Leitsystem für Rettungskräfte", beschäftigt sich mit der Frage, wie man Rettungsketten neu denken kann, um sie effizienter und zielgerichteter zu gestalten. Der Fokus liegt auf vulnerablen Personen, wie älteren Menschen oder Menschen mit Beeinträchtigungen, denen Selbstständigkeit und das Alleinwohnen ermöglicht werden soll. Gleichzeitig sollen die eingesetzten Technologien die Effizienz der Einsatzkräfte steigern, da das System weniger Fehlalarme, einen gezielteren Ressourceneinsatz und schnellere Einsätze verspricht.

Als technische Innovation steht das Smart Home im Mittelpunkt, das registrieren soll, wenn Hausbewohner:innen sich akut in einer lebensbedrohlichen Lage befinden. Ein mögliches Szenario ist ein Küchenbrand. Das Smart Home soll durch seine technische Vernetzung Familienmitglieder, die Nachbarschaft sowie – im Falle einer Notfallmeldung – die Leitstelle der Feuerwehr informieren, die weitere Maßnahmen in die Wege leiten können. Hierfür werden verschiedene Daten gesammelt, die Aufschluss über die gesundheitliche Konstitution der Hausbewohner:innen sowie die Situation vor Ort geben können. Dazu zählen 1) ein Mehrkriterienmelder, der beispielsweise Brände in der Küche detektieren kann; 2) ein Präsenzmelder; 3) Verbindungssysteme, Hubs, die miteinander kommunizieren; 4) Daten aus Smart Mobility und 5) smarte *Wearables* wie eine Smartwatch, die Vitalfunktionen messen kann. In einem Steuerungselement laufen diese lokal gespeicherten Datenströme diverser Sensoren zusammen, werden verarbeitet und setzen gegebenenfalls Ereignismeldungen ab.

Eine weitere Funktion des Systems ist eine smarte Beleuchtung. So sollen Einsatzkräfte mittels Lichtsignalen vor und im Haus sofort erkennen, in welcher Wohnung sich die hilfebedürftige Person befindet. Die Wohneinheiten verfügen, wenn gewollt, über ein elektrisches Türschloss, das sich dezentral öffnen lässt und den Einsatzkräften Zutritt zur Wohnung erlaubt. Durch die eingesetzten Technologien sollen so überlebenswichtige Minuten gespart werden, um den Bewohner:innen im akuten Krisenfall zu helfen.

4.2.2 Datenschutz als Aushandlung psychosozialer Bedürfnisse

Im Projekt sind Daten, die im privaten Raum generiert werden, die Grundlage für das soziotechnische System. Der Datenaustausch zwischen Smart Home und Rettungsstelle wird im Spannungsfeld zwischen selbstbestimmtem Wohnen und individueller Datensouveränität verhandelt.

Das Projekt diskutiert die Risiken der Datengenerierung und -verarbeitung des Smart-Home-Systems vor allem vor dem Hintergrund ihrer psychosozialen Dimension. Datenschutz wird weniger als die Entwicklung eines sicheren technischen Systems verhandelt, sondern vielmehr als Grundrecht – als Schutz der persönlichen Freiheit und Selbstbestimmung. So wird auch die Ausgestaltung des Systems und die technische Umsetzung von Datenschutzvorgaben immer wieder in Bezug zum Wohlbefinden der Nutzenden gesetzt. Zentrales Beispiel hierfür ist die Frage nach den Speicherorten – lokal oder cloud-basiert. Beide Optionen könnten datenschutzkonform umgesetzt werden. Dennoch verbindet eine Mitarbeiterin

der Lebenshilfe Dortmund die Entscheidung zwischen cloud-basierten und lokalen Speicherorten mit den Anforderungen des Datenschutzes:

> [W]as macht man mit Datenschutz, […] um dann nur im Notfall das weiterzugeben und nicht alle Daten, die werden nicht nachhaltig aufgezeichnet, sondern [in dem Moment] erfasst, verarbeitet und dann erkennt das System, aha, kann weg, aha, muss ich weitergeben. (Interview ADLeR_LH)

Die Interviewpartnerin betont, dass durch die lokal arbeitenden Systeme Daten nicht gespeichert, weitergegeben und -verarbeitet werden. Dies solle Ängsten der Nutzenden vor Überwachung entgegenwirken:

> [Zum System] gehört auch eine Anwesenheitsinfrarotdetektion, wo man auch sagen kann, naja, kann ja ein Punkt für den Datenschutz oder so für sein eigenes Gefühl sein, wenn jetzt irgendwer auf eine Cloud zugreifen könnte und gucken kann, wann bin ich denn da und wann bin ich nicht da, dass man die Sicherheit hat, dass das nicht passieren kann. (Interview ADLeR_LH)

Die Möglichkeit, Daten lokal zu speichern, wird hier nicht nur als technische Aufgabe betrachtet, um gemäß der DSGVO eine verschlüsselte und zweckgebundene Datenverarbeitung zu gewährleisten, sondern auch als ein Umgang mit Daten verstanden, der Privatheit suggeriert. Das Projekt bevorzugt eine lokale Lösung, da angenommen wird, dass eine Cloud ein größeres Unbehagen bei Nutzer:innen auslösen würde.

Ein zentraler Bestandteil des Projekts ist es, Vertrauen in die Smart-Home-Technologien und die integrierte Datennutzung zu schaffen, um die Akzeptanz der Nutzenden sowie der Angehörigen, die oftmals mitentscheiden dürfen, zu steigern. Der Nexus aus Akzeptanz und Vertrauen ist ein in den Interviews immer wieder vorkommendes diskursives Element. Datenschutz wird wiederholt als Frage des eigenen Wohlgefühls mit der Technologie und des Vertrauens in diese reflektiert. So argumentiert ein Projektmitarbeiter des Instituts der Feuerwehr Dortmund:

> Natürlich ist das ein Zielkonflikt, die Selbstbestimmung wird nur erreicht, indem man sich mehr überwachen lässt, ist aber in dem Sinne für uns was, wo wir sagen, gut, die Alltagsüberwachung, in Anführungszeichen, ohne die geht es nicht und ist zumutbar natürlich aus unserer sicherheitsorientierten Perspektive, dass wir sagen, es macht Sinn. […] Aber das ist eben ein Thema, wo wir sagen, es hat auch Konsequenzen

> für den Nutzenden, die vielleicht weniger schön sind oder worauf man sich einlassen muss. Wo wir aber sagen würden, bitte tu das, weil es gibt die Vorteile, [dass den Nutzenden im akuten Krisenfall schneller und effizienter geholfen werden kann]. (Interview ADLeR_FW)

Dieses Zitat verdeutlicht, in welchem Spannungsverhältnis die Chancen und Risiken des technologischen Systems (die Ermöglichung von Selbstständigkeit vs. die potenzielle Überwachung) stehen. Zudem zeigt es, dass die Frage, ob ein technisches System schützt oder überwacht – ob es Sicherheit herstellt oder gefährdet – auch eine Frage der subjektiven Wahrnehmung ist. Der Mitarbeiter räumt ein, dass die Bewohner:innen nachvollziehbare Abwägungen anstellen, ob sie ihre Möglichkeit zum selbstbestimmten Alleinleben oder ihre Privatheit priorisieren, indem sie sich nicht „überwachen" lassen. Doch stellt er letztlich den Einsatz der Technologie als rationale und praktisch bessere Entscheidung dar.

Indem man sich auf das System einlässt, übernimmt man Verantwortung für sich und seine Mitmenschen und wird gleichzeitig befähigt, selbstständig im eigenen Zuhause zu leben. Die Interviewpartnerin der Lebenshilfe erklärt, „Da geht es um Risikoabwägung, um Selbstreflexion und letztendlich zu erkennen, dass mein eigenes Risiko ja auch meine Selbstständigkeit vielleicht auch beeinträchtigt" (Interview ADLeR_LH). Dieser Prozess der Risikoabwägung und der Selbstreflexion soll dazu führen, dass die Nutzenden die Sicherheit im Alltagsleben als wichtigeres Gut erkennen:

> [I]ch entscheide mich dafür, mich mit der Feuerwehr in dieses soziotechnische System zu begeben, dass man da auch Vertrauen entgegenbringt, dass diese Lösung funktioniert und dass da eben auch kein Missbrauch mit den Daten usw. passiert [...] die Entscheidung für die eigene Sicherheit was zu tun, aber auch das Vertrauen entgegenzubringen in das System und auch die Menschen, die dann letztendlich damit arbeiten und dann die Hilfe leisten. (Interview ADLeR_FW)

Auch hier ist Risikobewusstsein eng mit dem Vertrauen in die Technologie und deren Betreiber:innen verwoben. Zugleich soll die Integration des soziotechnischen Systems im Heim des Individuums das soziale Gefüge der Gemeinschaft und somit die gesellschaftliche Resilienz stärken.

Die Mehrwerte des soziotechnischen Systems werden nicht einfach unidirektional kommuniziert, sondern die potenziellen Nutzer:innen können selbst entscheiden, welche Teilkomponenten des Smart-Home-Systems sie in ihre Wohnung integrieren möchten. Das Projekt klärt bei Informations-

veranstaltungen über Möglichkeiten und Risiken der Smart-Home-Technologien auf und gibt Einblicke in die Speicherung, Nutzung und Verarbeitung der Daten. Dies soll den Nutzer:innen ermöglichen, eine informierte Entscheidung zu treffen, welche persönlichen Daten sie teilen möchten und welche Sensoren sie zu nutzen gewillt sind. Diese modularen Möglichkeiten bieten den Nutzer:innen Selbstbestimmungsmöglichkeiten, da sie die Kontrolle über die Erhebung ihrer Daten haben. Gleichzeitig hängt der Einsatz des Sicherheitssystems von der Akzeptanz der Nutzer:innen ab, wie auch beim Fallbeispiel des Projekts RESCUE-MATE. Allerdings verspricht die Möglichkeit der modularen Zusammenstellung im Vergleich nur ein etwas gesteigertes Level an Beteiligung, da Nutzende bisher nicht in den Prozess der Datengenerierung, -übermittlung und -nutzung und die Ausgestaltung des Systems einbezogen sind.

4.2.3 Zwischen Verantwortung und Vertrauen: Resilientes Individuum, resiliente Gesellschaft?

Auch im zweiten Fallbeispiel zeigen die Überlegungen der Interviewpartner:innen zu den psychosozialen und technischen Dimensionen des Sicherheitssystems, dass technische Innovation als unausweichlich gilt, um Menschen mit Beeinträchtigungen zu ermöglichen, selbstständig und selbstbestimmt in ihrem Zuhause zu leben. Akzeptanz für die soziotechnische Lösung soll hier allerdings nicht nur durch Aufklärung und Vertrauensherstellung geschaffen werden, wie im ersten Projekt, sondern auch durch individuelle Risikoabwägung und Einbindung der Nutzenden in die praktische Verwendung des Systems.

Resilienz, als Übernahme individueller Verantwortung für die Herstellung von Sicherheit und gleichzeitiges Vertrauen in Sicherheitssysteme, zeigt sich auch in diesem Projekt als wirkmächtige soziotechnische Zukunftsvision. Auch hier soll das technische Sicherheitssystem die Resilienz in Form von Handlungsfähigkeit fördern, indem vulnerable Individuen zur Selbstständigkeit ermächtigt werden. Diese Ermächtigung des Individuums erzeugt auch auf gesellschaftlicher Ebene Resilienz, indem in der Diskussion über den Umgang mit Risiken alle die Notwendigkeit anerkennen, dass die Herstellung von Sicherheit eine geteilte Aufgabe des Staates und der Gesellschaft ist.

Das Projekt stellt die Förderung der Selbstständigkeit und die gleichzeitige Forderung einer Mitwirkung an der Herstellung gesellschaftlicher Sicherheit als zukunftsträchtigen Umgang mit Risiken und Gefahren dar. So

erklärt die Interviewpartnerin von der Lebenshilfe, es liege in der Verantwortung der Gesellschaft, die resilienzerzeugenden Potenziale von daten- und technikgetriebenen Sicherheitslösungen für alle – und besonders für vulnerable – Menschen aufzuzeigen:

> Man wohnt alleine mit über 80, aber da muss man vielleicht tatsächlich mal über Risiken sprechen und vielleicht [...] werden die nicht mehr so reflektiert oder sind nicht mehr so bewusst. Aber welche Angebote gibt es denn eigentlich, damit die Zielgruppe erreicht wird und auch etwas dafür getan wird, dass sie wieder ein bisschen mehr selbst befähigt wird? Ich glaube, das ist auch eine Verantwortung, die man als Gesellschaft oder in Form dann von Dienstleistern in der sozialen Arbeit erbringen kann. (Interview ADLeR_LH)

Doch gerade die Vorstellung der Handlungsfähigkeit, die zugleich Ziel und Merkmal der Resilienz in gängigen soziotechnischen Narrativen ist, geht im Projekt in einem Streben nach Sicherheit auf, welches das Agieren von Mensch und Technik gleichsetzt und austauschbar werden lässt. So erklärt die Mitarbeitende der Lebenshilfe, Ziel des Projektsystems sei es, „Sicherheit für die Klienten [herzustellen], dass sie in Notfällen handlungsfähiger sind oder halt das System für sie handelt" (Interview ADLeR_LH). Die Fragen, wer oder was in soziotechnischen Sicherheitssystemen handelt, wie menschliche und technologische Interdependenzen in Zukunftsvisionen der resilienten Gesellschaft erscheinen und wie sie normative Forderungen nach Verantwortung und Vertrauen prägen, erfordern kritische Diskussion und (Selbst)Reflexion – in der Sicherheitsforschung, der Gesellschaft und der Politik.

5. Fazit

Wir haben beide Fallbeispiele auf die Frage hin untersucht, wie sich das Spannungsverhältnis zwischen der Privatheit des Individuums und der öffentlichen Sicherheit in Forschungsprojekten zum Bevölkerungs- und Katastrophenschutz entfaltet. In den Fallbeispielen wird die Beziehung zwischen Individuum und Kollektiv und ihrer jeweiligen Aufgabe in der Förderung und Forderung gesellschaftlicher Resilienz unterschiedlich dargestellt. In beiden Fällen gilt der Umgang mit Daten jedoch als Mittel der Verantwortungsübernahme für die Beteiligung an der Herstellung einer resilienten Gesellschaft. Im Projekt RESCUE-MATE dient die Datennutzung

als Informationsgrundlage eines soziotechnischen Systems für kollektive Sicherungsprozesse. Im Projekt A.D.L.e.R. wird die Datennutzung zum Ausdruck des idealen Zusammenspiels zwischen einem technischen System und einem Individuum, das seine Daten teilt, um selbstbestimmt und sicher alleinzuleben.

Wir haben gezeigt, wie Narrative der gesellschaftlichen Resilienz in der aktuellen Sicherheitsforschung verhandelt werden und so das soziotechnische *Imaginary* der resilienten Gesellschaft und einer sicheren Zukunft artikulieren und festigen. In den Projekten werden technische Innovationen als unabdingbare Mittel dargestellt, die es einer Gesellschaft ermöglichen, sich auf Krisen vorzubereiten und sie zu bewältigen. Die Nutzbarmachung und Zusammenführung verschiedener Daten in technischen Systemen wird zur Kernkomponente einer resilienten Gesellschaft, die auf unvorhergesehene und komplexe Gefahren reagieren kann und allzeit handlungsfähig ist. Dies ist die Vision eines Bevölkerungs- und Katastrophenschutzes, der auf einer datengetriebenen, technischen Lösung – einem *technological fix* – fußt, dabei aber auch auf menschliches Vertrauen in Technologie und die gesellschaftliche Akzeptanz technischer Sicherheitssysteme angewiesen bleibt.

Damit schreibt sich ein soziotechnisches *Imaginary* fort, das in Anbetracht der gesellschaftlichen Wahrnehmung zunehmender Unsicherheiten und multipler Krisen zum Wandel der Sicherheitskultur beigetragen hat. Subjekte und gesellschaftliche Gruppen sollen Verantwortung für ihre Sicherheit übernehmen, indem sie Daten mit soziotechnischen Systemen teilen. Gesellschaftliche Resilienz wird dadurch erhöht, dass möglichst viele Daten generiert und genutzt werden, um mit Unsicherheiten besser umgehen zu können. So wird in Resilienznarrativen die Frage der Datenteilung und -nutzung von einer persönlichen Entscheidung zwischen den Risiken, die jeweils mit der Datenteilung bzw. -nutzung für Privatheit und Sicherheit einhergehen, zu einer Entscheidung zwischen eigenen Bedürfnissen und dem Wohl der Gesellschaft. Dabei bleiben Aushandlungen der Risiken, die für das Individuum und das Kollektiv aus der Datenverarbeitung entstehen, auf Fragen der technischen Datensicherheit und der rechtlich konformen Verwendung von Daten beschränkt. Diese Tendenz, Maßnahmen im Bevölkerungs- und Katastrophenschutz zu technokratisieren, birgt allerdings auch Fallstricke.

Es geht nicht darum, diese technikzentrierte Zukunftsvision per se abzulehnen. Nach der Analyse der Fallbeispiele stellt sich jedoch die Frage, ob eine Auseinandersetzung mit Datenschutz als technische, rechtliche und

psychosoziale Herausforderung ausreicht, um die Spannungen zwischen Privatheit und öffentlicher Sicherheit in ihrer Tragweite zu erkennen und zu adressieren. Denn indem in den Narrativen der Sicherheitsforschung datengetriebene technische Systeme als Kernelement innovativer "Sicherheitslösungen" und damit als Treiber gesellschaftlicher Resilienz dargestellt werden, geraten soziopolitische Fragestellungen aus dem Blick. Doch es gilt, diese Fragen ebenso ernst zu nehmen und kritisch zu reflektieren. So sollte erörtert werden, auf welcher Grundlage Individuen und Kollektive Entscheidungen treffen, wessen Zukünfte wie verhandelt werden, welche Zukünfte eine Gesellschaft als erstrebenswert erachtet und welche Interessen und Akteurskonstellationen dabei unberücksichtigt bleiben oder miteinander konkurrieren. Eine solche Betrachtungsweise könnte die Akzeptabilität von Innovationen stärker in den Blick nehmen, anstatt allein Akzeptanz für starre technische Systeme zu schaffen. Es ist also wichtig, die Risiken und Chancen einer solchen Vision zu verhandeln und mit allen Stakeholder:innen zu diskutieren – nicht zuletzt mit Entscheidungsträger:innen aus der Politik.

Literatur

Ächtler, Nina (2014): Was ist ein Narrativ? Begriffsgeschichtliche Überlegungen anlässlich der aktuellen Europa-Debatte. *Kulturpoetik*, 14(2), S. 244–268.

Alexy, Lennart; Fisahn, Andreas; Hähnchen, Susanne; Mushoff, Tobias und Trepte, Uwe (2023): Sicherheit und Ordnung, öffentliche. In: Lennart Alexy, Andreas Fisahn, Susanne Hähnchen, Tobias Mushoff und Uwe Trepte (Hg.): *Das Rechtslexikon. Begriffe, Grundlagen, Zusammenhänge*. Bonn: J.H.W. Dietz Nachf.

Arnstein, Sherry R. (1969): A ladder of citizen participation. *Journal of the American Planning Association*, 35(4), S. 216–224.

Aven, Terje (2019): The Call for a Shift from Risk to Resilience: What Does it Mean? *Risk Analysis*, 39(6), S. 1196–1203. doi:10.1111/risa.13247.

Binder, Clemens (2022): Forschung und Innovation als Sicherheitspolitik? Die Politik der Entwicklung von Sicherheitstechnologien in der Europäischen Union. . Wien: Österreichisches Institut für Internationale Politik (oiip). URL: https://nbn-resolving.org/urn:nbn:de:0168-ssoar-85196-4 (besucht am 13.05.2026).

Bonß, Wolfgang (2015): Karriere und sozialwissenschaftliche Potenziale des Resilienzbegriffs. In: Martin Endreß und Andrea Maurer (Hg.): *Resilienz im Sozialen*. Wiesbaden: Springer, S. 15–31.

Breithaupt, Fritz (2022): *Das narrative Gehirn. Was unsere Neuronen erzählen*. Berlin: Suhrkamp.

Bröckling, Ulrich (2016): Gut angepasst? Belastbar? Widerstandsfähig? Resilienz und Geschlecht. In: Roland Anhorn und Marcus Balzereit (Hg.): *Handbuch Therapeutisierung und Soziale Arbeit*. Wiesbaden: Springer VS, S. 391–408.

Bundesministerium für Digitales und Verkehr, Bundesregierung (2023): Fortschritt durch Datennutzung. Strategie für mehr und bessere Daten für neue, effektive und zukunftsweisende Datennutzung. https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Publikationen/Digitale-Welt/fortschritt-durch-datennutzung.htmlhttps://www.bmv.de/nationale-datenstrategie.de

Bundesministerium für Forschung, Technologie und Raumfahrt (2024): Forschung für die zivile Sicherheit – gemeinsam für ein sicheres Leben in einer resilienten Gesellschaft Rahmenprogramm der Bundesregierung 2024–2029. URL: https://www.sifo.de/sifo/shareddocs/Downloads/bmbf-programm/sicherheitsforschungsprogramm_24.pdf?__blob=publicationFile&v=4 (besucht am 13.05.2026)

Bundesministerium für Forschung, Technologie und Raumfahrt (2023): Zukunftsstrategie Forschung und Innovation. https://www.bmftr.bund.de/SharedDocs/Downloads/DE/2022/zukunftsstrategie-fui.html (besucht am 13.05.2026)

Bundesministerium des Innern, Bundesregierung (2024): Umsetzungsplan der deutschen Strategie zur Resilienz gegenüber Katastrophen. URL: https://www.publikationen-bundesregierung.de/pp-de/publikationssuche/umsetzungsplan-resilienz-2299098 (besucht am 13.05.2026)

Bundesministerium des Innern, Bundesregierung (2022): Deutsche Strategie zur Stärkung der Resilienz gegenüber Katastrophen. Umsetzung des Sendai Rahmenwerks für Katastrophenvorsorge (2015–2030) – Der Beitrag Deutschlands 2022–2030. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/BMI22017-resilienz-katastrophen.pdf?__blob=publicationFile&v=3 (besucht am 13.05.2026)

Bundesregierung (2023): Nationale Datenstrategie der Bundesregierung – Weiterentwicklung Fortschritt durch Datennutzung – Strategie für mehr und bessere Daten für neue, effektive und zukunftsweisende Datennutzung. BT Drucksache 20/8260. URL: https://dserver.bundestag.de/btd/20/082/2008260.pdf (besucht am 13.05.2026)

Buzan, Barry; Wæver, Ole und de Wilde, Jaap (1998): *Security: A New Framework for Analysis*. Boulder: Lynne Rienner.

Conze, Eckart (2022): Dynamiken der Sicherheit. *Aus Politik und Zeitgeschichte*, 32-33, S. 10–15.

Daase, Christopher (2010): Der Wandel der Sicherheitskultur – Ursachen und Folgen des erweiterten Sicherheitsbegriffs. In: Peter Zoche, Stefan Kaufmann und Rita Haverkamp (Hg.): *Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken*. Bielefeld: transcript, S. 139–158.

Dunn Cavelty, Myriam; Kaufmann, Mareile und Søby Kristensen, Kristian (2015): Resilience and (In)Security: Practices, Subjects, Temporalities. *Security Dialogue*, 46(1), S. 3–14.

Giddens, Anthony (1991): *Modernity and Self-Identity*. Stanford: Stanford University Press.

Grunwald, Armin (2005): Zur Rolle von Akzeptanz und Akzeptabilität von Technik bei der Bewältigung von Technikkonflikten. *TATuP-Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis*, 14(3), S. 54–60.

Hülk, Walburga (2013): Narrative der Krise. In: Uta Fenske, Walburga Hülk und Gregor Schuhen (Hg.): *Die Krise als Erzählung. Transdisziplinäre Perspektiven auf ein Narrativ der Moderne*. Bielefeld: transcript, S. 113–132.

Jasanoff, Sheila und Kim, Sang-Hyun (2009): Containing the Atom. *Minerva*, 47(2), S. 119–146.

Jasanoff, Sheila und Kim, Sang-Hyun (2015): *Dreamscapes of Modernity*. Chicago: University of Chicago Press.

Kaufmann, Stefan (2015): Resilienz als Sicherheitsprogramm. In: Martin Endreß und Andrea Maurer (Hg.): *Resilienz im Sozialen*. Wiesbaden: Springer, S. 295–312.

Keller, Reiner (2001): *Wissenssoziologische Diskursanalyse*. Wiesbaden: Springer VS.

Kinnvall, Catarina und Mitzen, Jennifer (2016): Ontological Securities in World Politics. *Cooperation and Conflict*, 52(1), S. 3–11.

Kruse, Andreas und Schmitt, Eric (2021): Digitale Technologie und Gestaltung des Alterns – Notwendigkeit ethischer Diskurse. *EthikJournal*, 7(2), S. 1–24.

Marx, Gary T. (2002): What's New about the "New Surveillance"? *Surveillance & Society*, 1(1), S. 9–29.

Müller-Funk, Wolfgang (2008): *Die Kultur und ihre Narrative*. Wien und New York: Springer.

Pavone, Vincenzo; Santiago Gomez, Elvira und Jaquet-Chifelle, David-Olivier (2016): A Systemic Approach to Security. *Democracy and Security*, 12(4), S. 225–246.

Riescher, Gisela (2010): *Demokratische Freiheit und die Sicherheit des Leviathan*. Baden-Baden: Nomos.

Shulman, Naomi (2024): Krisenzeiten. Wie ein soziopolitisches Krisennarrativ Zukunft entwirft. Eine Analyse am Beispiel der ersten „Rede zur Zeitenwende. iF-Schriftenreihe (02/24). Institut Futur, Fachbereich Erziehungswissenschaft und Psychologie, Freie Universität Berlin. http://dx.doi.org/10.17169/refubium-43055

Thoma, Klaus; Hiller, Daniel; Leismann, Tobias und Dree, Birgit (2011): A German Perspective on Security Research. In: Klaus Thoma (Hg.): *European Perspectives on Security Research. acatech DISKUTIERT*. Berlin und Heidelberg: Springer, S. 27–43.

Wentland, Alexander (2025): Zukunftsbilder und Imaginaries der Mobilität. In: Weert Canzler, Juliane Haus, Andreas Knie und Lisa Ruhrort (Hg.): *Handbuch Mobilität und Gesellschaft. Sozialwissenschaftliche Verkehrs- und Mobilitätsforschung.* Wiesbaden: Springer VS, S. 267–279.

Wewer, Göttrik (2020): Datenschutz. In: Tanja Klenk, Frank Nullmeier und Göttrik Wewer (Hg.): *Handbuch Digitalisierung in Staat und Verwaltung*. Wiesbaden: Springer VS, S. 193–204.

Über die Autoren

Dr. Sophia Rossmann
ist Wissenschafts- und Technikforscherin an der Freien Universität Berlin und Leiterin des Forschungsforums Öffentliche Sicherheit. Ihre Forschungsschwerpunkte sind u. a. Praktiken der Wissensproduktion und des Wissenstransfers, Politics of Future-Making und Science-Policy-Interface im Feld des Bevölkerungs- und Katastrophenschutzes. E-Mail: sophia.rossmann@fu-berlin.de

Dr. Naomi Shulman
ist Zukunftsforscherin und Kulturwissenschaftlerin an der Technischen Universität Braunschweig und Leiterin des Forschungsforums Öffentliche Sicherheit. In ihrer Forschung untersucht sie u. a. Sicherheitskulturen und -diskurse, Zukunftsvisionen der Sicherheit sowie Praktiken des Wissenstransfers und der Transdisziplinarität. E-Mail: naomi.shulman@tu-braunschweig.de