Sicherung sozialer Nachhaltigkeit durch Technologie? Eine qualitative Studie zu technischen Assistenzsystemen im Bereich Cybersicherheit

Mario Anastasiadis, Hektor Haarkötter, Kathrin Keller, Mariana Ochoa Moreno

Abstract

Cybersecurity und aktuelle Desinformation zählen zu den derzeit kritischen Bereichen im Kontext der Nutzung des Internets. Die hier dargestellte Forschung ist Teil der wertegebundenen Entwicklung zweier technischer Online-Assistenzsysteme, die vulnerablen Gruppen konkret helfen sollen. Die Forschung ist im technikethischen Kontext des Value Sensitive Design verortet und daher durch qualitativ-explorative Begleitforschung flankiert, deren Ergebnisse in Bezug auf Migrant:innen hier in Teilen präsentiert werden. Dabei stehen die Bedarfe und Erwartungen der Proband:innen sowie ihre Aussagen zu Vertrauen in Technologie, Institutionen und Medien im Zentrum.[1]

1. Ausgangslage

Nach Angaben des Cybersicherheitsmonitors des Bundesamts für Sicherheit in der Informationstechnik (BSI) sind die Bundesbürger:innen erheblich von Cybergefahren betroffen. Zugleich mangele es ihnen an Bewusstsein sowie wirksamen Instrumenten und Kompetenzen zu ihrer Abwehr (BSI 2024: 17). Dies betrifft „von Verwaltungsbehörden über KMU bis hin zu den einzelnen Bürgerinnen und Bürgern" die Gesellschaft als Ganzes, so Claudia Plattner, Präsidentin des BSI (Plattner 2023: 5). Nach Angaben des Bundesministeriums des Innern und für Heimat gehören zu dieser hybriden Bedrohungslage „Desinformation, Cyberangriffe auf staatliche Stellen und Unternehmen, Spionage und Industriespionage, Diebstahl von geistigem Eigentum, wirtschaftliche Einflussnahme, [...] Sabotage von Kritischen Infrastrukturen und Einflussnahme auf freie Wahlen." (BMI o.J.) dazu. Somit ist auch die zweite hier wesentliche Dimension, nämlich politische Desinformation als Teil einer umfassenderen Sicht auf die derzeitige

1 Die Studie wurde im Rahmen zweier vom Bundesministerium für Bildung und Forschung (BMBF) geförderter Forschungsprojekte zu Cybersicherheit (Projekt CrossComITS) sowie Desinformation (Projekt NEBULA) durchgeführt. Die Autor:innen sind gleichberechtigte Verfasser:innen dieses Beitrags.

https://doi.org/10.5771/9783748940616-305 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Bedrohungslage identifiziert. Auf diese Entwicklungen reagiert auch die Wissenschaft, da förderpolitisch erkannt wurde, dass die Entwicklung technischer Assistenz-Systemen sowie die Stärkung von Wissen und Kompetenzen wichtig sind. Die hier dargestellten Projekte stehen in eben dieser Logik.

Im Bereich Cybersicherheit (Projekt CrossComITS) geht es um die Vermittlung von IT-Security-Kompetenzen für vulnerable Gruppen durch ein technisches Assistenzsystem in Form einer Sicherheitsplattform, auf der relevantes Wissen mit Hilfe von Sicherheitsmittler:innen weitergegeben werden soll. Im Bereich Desinformation (Projekt NEBULA) werden ein Online-Assistenzsystem zur algorithmischen Detektion von Desinformation entwickelt und somit Kompetenzen gestärkt. In beiden Projekten wird zu den vulnerablen Gruppen von Jugendlichen, Rentner:innen und Migrant:innen geforscht. Die Technologieentwicklung ist in beiden Projekten durch Begleitforschung (Interview-Studien) flankiert, aus der hier Ergebnisse der Studie mit Migrant:innen präsentiert werden. Dazu werden Cybersicherheit und Desinformation erörtert, Hinweise zur Vulnerabilität und zur Reduktion des Digital Divide als normativem Zielwert gegeben sowie eine Verortung im technikethischen Paradigma des Value-Sensitive-Design (Hillerbrand 2021) begründet. Dann werden ausgewählte empirische Studienergebnisse dargestellt und diskutiert.

2. Kritische Dimensionen der Internet-Nutzung

Für Cybersicherheit und Desinformationen als kritische Dimensionen des digitalen Alltags werden nachfolgend grundlegende Konzepte vorgestellt und wesentliche Bedingungsfaktoren skizziert.

2.1 Cybersicherheit

Cybersicherheit hat in den letzten Jahren erheblich an Bedeutung gewonnen. Daher geht ein holistisches Verständnis über die rein technische Betrachtung hinaus und erfordert die Berücksichtigung sozialer und politischer Dimensionen auf Makro-, Meso- und Mikroebene (Schünemann 2023). Die digitale Vernetzung sowie die Anonymität des Internets tragen zur Komplexität der Bedrohungslage bei. Häufig sind organisierte Hackergruppen kaum zu identifizieren oder gar dingfest zu machen. Zugleich sind

https://doi.org/10.5771/9783748940616-305 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

ihre Motive so vielfältig wie die von ihnen eingesetzten Technologien (BKA 2024: i). Der Begriff „hybride Cyberbedrohungen" wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) geprägt und beschreibt komplexe digitale Bedrohungen. Dies bedroht nicht nur Institutionen (etwa durch Denial-of-Service Operationen oder Hack-und-Leak-Angriffe). Sie werden auch bei politischen Konflikten eingesetzt, etwa um die Sicherheit von Staaten zu untergraben oder politische Instabilität zu fördern (BKA 2024; BMI o.J.; BSI 2024). Cybersicherheit umfasst auf der Mikroebene etwa die Sicherheit privater Geräte oder den Schutz vor Cyberkriminalität. Alltägliche Praktiken wie die Nutzung von Lokalisierungsdiensten oder die Erstellung von Online-Profilen erzeugen Datenspuren. Durch *Social Engineering* oder *Phishing* sind Hackern hier viele Möglichkeiten gegeben (Schünemann 2023). Die informationelle Selbstbestimmung sowie die digitale Souveränität der Menschen können hierdurch beeinträchtigt werden (Albers 2005; Bettinger/Reißmann 2022; Friedewald et al. 2017). Dies betrifft insbesondere vulnerable Bürger:innen.

2.2 Desinformation

Spätestens seit der US-Wahl 2016 sind Fake News zu einem viel beachteten Problem politischer Kommunikation geworden (Haarkötter 2021), für die mittlerweile meist der Begriff der Desinformation verwendet wird (Zimmermann/Kohring 2018). Für Allcott und Gentzkow (2017) sind dabei die Intentionalität und der (mögliche) Täuschungseffekt wesentliche Definitionskriterien. Desinformationen sind demnach intentional gefälschte Nachrichten, die nachprüfbar falsch sind und Menschen irreführen können – ein Verständnis, das auch im vorliegenden Zusammenhang gültig ist. Die Relevanz von Desinformationen lässt sich durch die Betrachtung sozialer Medien weiter verdeutlichen. Soziale Medien und Messenger-Dienste haben zur Entstehung digitaler Öffentlichkeiten geführt, über deren deliberative Güte zumeist kritisch geurteilt wird (Seeliger/Sevignani 2021). Zudem haben sie zu einer kommunikativen Ermächtigung politischer Akteure geführt, die Desinformation als politisches Mittel einsetzen (Keller 2023). Zudem ist staatliche Desinformationen als Mittel politischer Propaganda ein wichtiger Faktor geworden (Broschart 2024). So sind im Internet ganze Nachrichtenwelten für alternatives Wissen und Desinformation entstanden.

https://doi.org/10.5771/9783748940616-305 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

3. Vulnerabilität und Reduktion des Digital Divide

Wie nachfolgend erörtert, sind Angehörige vulnerabler Gruppen Ausgangspunkt der vorliegenden Studie. Für sie treten die Reduktion digitaler Spaltung und die Vermittlung von Medienkompetenzen als normative Zielwerte einer technikethischen Technologieentwicklung deutlich hervor.

3.1 Vulnerabilität

Menschen mit niedriger Bildung (Glenski et al. 2018), Ältere (Shresta/Spezzano 2019), Jugendliche (Seo et al. 2020) und Migrant:innen (Ruokolainen/Widén 2020), erleben in vielen Lebensbereichen Benachteiligungen (Gomolla 2017). Dies gilt auch für die digitale Sphäre. Die Handlungsfelder Cybersicherheit und Desinformation stellen für sie somit besondere Herausforderungen dar.

3.2 Reduktion des Digital Divide und Kompetenzvermittlung als Zielwerte

Es wird deutlich, dass die Reduktion des sog. Digital Divide (Van Dijk 2020) für Angehörige vulnerabler Gruppen hochrelevant ist. In der Forschung zum Digital Divide werden drei Ebenen unterschieden: (1) der 1st-level divide (Access), der Unterschiede beim materiellen Zugang in den Blick nimmt, (2) der 2nd-level divide (Literacy), der Ungleichheiten bei digitalen Fähigkeiten und daraus resultierende Unterschiede in der Nutzungsqualität adressiert sowie (3) der 3rd-level divide (Agency),der auf Unterschiede in den Ergebnissen, die sich aus der Nutzung von Informations- und Kommunikationstechnologien bezogen auf Lebenschancen ergeben, abhebt. Eine Verringerung des Digital Divide findet sich auch als wesentliches Elemente in den Sustainable Development Goals der Vereinten Nationen und wird dort als Parameter sozialer Nachhaltigkeit adressiert (Valdez/Javier 2021). Soziale Nachhaltigkeit wird in diesem Zusammenhang nicht im engeren Sinne als umweltbezogene Kategorie verstanden, sondern als Dimension selbstbestimmter, gelingender gesellschaftlicher Partizipation. Daneben ist die Stärkung von Medienkompetenz ein Ziel, das Funiok (2020) bezüglich Cybersicherheit und Desinformation konkretisiert. Zum einen ist dies der sichere Umgang mit Daten. Zum anderen sind dies kritische Informations- und Nachrichtenkompetenzen. Die Förderung von

https://doi.org/10.5771/9783748940616-305 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Informations- und Medienkompetenzen ist somit ein Zielwert, um die Teilhabechancen „aller sozialen Gruppen am Selbstverständigungsprozess der Gesellschaft zu ermöglichen" (Röben 2013: 10). Migrant:innen sind unter den vulnerablen Gruppen sogar mehrfach betroffen, da sie auch Angehörige anderer vulnerabler Gruppen sein können (Schimany et al. 2012: 22). Für die vorliegende Untersuchung wird darum diese Gruppe besonders in den Fokus genommen. Die Ergebnisse der Studie können aber mutatis mutandis auch für Mitglieder der anderen Fokusgruppen gelten.

4. Zur Studie – Methodologie und Methodik

Die vorliegende Studie analysiert Muster der Sinngebungen und Praktiken von Migrant:innen in den Handlungsfeldern Cybersicherheit und Desinformation. Zudem sind ihre Erwartungen an die in Entwicklung stehenden Assistenzsysteme Gegenstand der Analyse. Ziel ist eine wertebasierte Technologieentwicklung. Die Studie verortet sich dazu im Kontext des Value Sensitive Design (VSD) (Hillerbrand 2021). Im VSD wird verantwortungsvolles Technologiedesign ins Zentrum gestellt (Heesen 2016). Dabei stehen Aspekte im Fokus, wie Ethik, Verantwortung, Gerechtigkeit oder kulturelle Sensibilität (Cipolla/Bartholo 2014). Auch können Parameter wie ökologische oder gesellschaftliche Implikationen in die Entwicklung einfließen. Mit Blick auf vulnerable Gruppen gilt das Gebot zur Neutralisierung von „Benachteiligungen insbesondere von Minderheiten, die Technikentwicklungen wissentlich, willentlich oder völlig unbeabsichtigt nach sich ziehen" (Hillerbrand 2021: 469). Um dies zu gewährleisten, umfasst VSD einen iterativen, dreiphasigen Prozess, in dem technische Designs im Dialog mit entsprechender Begleitforschung aus dem Bereich der empirischen Sozialforschung immer wieder angepasst werden können (Hillerbrand 2021): (1) die Konzeption, (2) die empirische Phase und (3) die technische Entwicklung. Die Studie ist innerhalb der Phasen 2 und 3 angesiedelt. Die Begleitforschung wurde mit teilstrukturierten Leitfaden-Interviews durchgeführt und ist methodologisch somit in der qualitativ-explorativen Sozialforschung verortet. Die Rekrutierung des Samples (Abb. 1) erfolgte anhand zweier Kriterien: (1) Vulnerabilität und (2) Migrationshintergrund.

https://doi.org/10.5771/9783748940616-305 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Abb. 1: Überblick über das Sample

P	w/m/d	Herkunft	Alter	Sprache	Dauer
P1	m	Afghanistan	80	DE	54:18
P2	w	Mexiko	33	DE	81:46
P3	m	Kamerun	42	DE	45:20
P4	m	Russland	37	DE	65:43
P5	w	Russland	23	DE	49:46
P6	m	Türkei	31	DE/ENG	62:09
P7	m	Bosnien-H.	24	DE	28:40
P8	w	Türkei	23	DE	37:35
P9	w	Tunesien	34	DE	47:56
P10	w	Russland	27	DE	49:48
P11	m	Italien	46	DE	28:59
P12	w	Russland	21	DE/ENG	62:03
P13	w	Italien	52	DE	42:49
P14	w	Portugal	43	DE	55:11
P15	m	Griechenland	60	DE	44:13
P16	w	Albanien	27	ENG	47:07

In Anlehnung an die Definition des Statistischen Bundesamtes (Statistisches Bundesamt o.J.), wurde ein Migrationshintergrund festgestellt, wenn Proband:innen selbst oder mindestens ein Elternteil nicht in Deutschland geboren wurden. Die Rekrutierung erfolgte in zwei Wellen: (1) über Institutionen aus dem Bereich der Migrationsarbeit[2] sowie über (2) Schneeballeffekte. So konnte ein Sample von n=16 rekrutiert werden. In deduktiver Hinsicht waren die Interviews in sechs Kategorien (K) vorstrukturiert (Abb. 2). Im Rahmen der Ergebnisdarstellung hier stehen jedoch vor allem Kategorie 6 sowie eine weitere induktiv auf Basis des Datenmaterials entwickelte Kategorie zu Vertrauen und Misstrauen im Fokus.

2 An dieser Stelle sei dem Bonner Institut für Migrationsforschung und Interkulturelles Lernen (BIM e.V.) sowie dem International Office der Hochschule Bonn-Rhein-Sieg für die Unterstützung gedankt.

https://doi.org/10.5771/9783748940616-305 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Abb. 2: Deduktive Kategorien im Überblick

K	Thema der Kategorie
K1	Wissen und Assoziationen zu Cybersicherheit und Desinformation
K2	Eigene und vermittelte Erfahrungen
K3	Medienrepertoire, Medienpraktiken, Medienkompetenzen
K4	Einschätzungen zur gesellschaftlichen Relevanz von Cybersicherheit und Desinformation
K5	Unterschiede und Gemeinsamkeiten Deutschland/Herkunftsland
K6	Bedarfe und Erwartungen bzgl. technischer Assistenzsysteme

Die Auswertung erfolgte in Anlehnung an die Grounded Theory (Strauss/Corbin 1996), wobei eine softwaregestützte Kombination aus deduktiven und induktiven Auswertungsschritten umgesetzt wurde.

5. Ergebnisse

Im vorliegenden Zusammenhang liegt der Fokus auf der Darstellung der Kategorie 6 (K6) sowie der in ihrem Rahmen induktiv entwickelten Subkategorien (SK) und Dimensionen (D). Zudem wird ein Schwerpunkt auf die induktiv entwickelte Querschnittskategorie (QK1) zu Vertrauen und Misstrauen gelegt.

5.1 Bedarfe und Erwartungen bezüglich technischer Assistenzsysteme

Im Rahmen der Analyse haben sich für K6 drei Subkategorien ergeben, anhand derer sich die zentralen Ergebnisse illustrieren lassen.

Abb. 3: K6 Bedarfe und Erwartungen bezüglich technischer Assistenzsysteme

SK6.1: Bedienbarkeit	D1: Einfachheit
	D2: Input-Output-Struktur
SK6.2: Form des Output/Feedback	D1: Verständlichkeit

https://doi.org/10.5771/9783748940616-305 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

	D2: Multilingualität
	D3: Visualität/Bild/Bewegtbild
SK6.3: Inhalt des Outputs/Feedbacks	D1: Informationsfunktion
	D2: Verifizierung/Richtigstellung
	D3: Warnfunktion
	D4: Instruktivität

Die SK6.1 umfasst Aussagen zur grundlegenden Bedienbarkeit. Nicht unerwartet ist dabei der Befund, dass die meisten Proband:innen betonen, die Bedienung solle einfach und nachvollziehbar sein (D1: Einfachheit). „Das muss einfach sein, effektiv, attraktiv […], gut und schnell" (P3). Eine weitere Erwartung bezog sich darauf, dass die Systeme sowohl eine unmittelbare Eingabe von Links, URLs oder Bildern (Input), ermöglichen sowie ein stets klar nachvollziehbares Ergebnis (Output/Feedback) liefern sollen (D2: Input-Output-Struktur). „Ich lese irgendeine Nachricht und kann ich das an diese App weiterleiten. Und die kann dann kontrollieren, […] ob das falsch ist oder nicht falsch ist" (P1). Wie Output/Feedback auf formaler Ebene beschaffen sein sollten bzw. welche Erwartungen dazu formuliert wurden, konstituiert die Subkategorie SK6.2. Hier wird geäußert, der Output solle verständlich sein (D1: Verständlichkeit). „Es […] sollte sehr verständlich sein. Sehr einfach, mit einfachen Wörtern, mit einfachen Instruktionen […]" (P4). Die Dimension Verständlichkeit hat im vorliegenden Fall eine für die Entwicklung bedeutsame Konsequenz, die in den Entwicklungsprozess konkret einfließen soll, nämlich, dass die Erwartung besteht, die Systeme sollten mehrsprachig sein (D2: Mulitilingualität). „Man muss auch Leute für mehrere Sprachen haben" (P1). Hinsichtlich der konkreten Form des Output/Feedback wird im Rahmen von D3: Visualität/Bild/Bewegtbild vielfach formuliert, dass vornehmlich visuelle Inhalte, wie Bilder und Videos gewünscht werden. Dabei zeigt sich auch, dass die gängigen Content-Formate der nutzungsstarken Social Media sich auf die Erwartungen an technische Assistenzsysteme auswirken. "[…] weil ich denke, ah, etwas, das nicht so ein Buch ist… ein PDF ist. Manchmal… ich bin gewohnt… „Ach, gibt es nicht ein TikTok dafür, [um] das zu erklären? Ein Video, […] dass es praxisnah ist" (P2). Insbesondere die Vorstellung lange Texte lesen zu müssen, wird kritisch gesehen. „[…] mit Bildern oder Videos. Nicht nur langweilige Texte über Cybersecurity. Die Leute schauen lieber auf Bilder.

https://doi.org/10.5771/9783748940616-305 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

[…] Wenn es kompliziert wird, dann wird es nicht genutzt“ (P4). Neben den Erwartungen an die formalen Aspekte des Outputs sind im Rahmen der Subkategorie SK6.3 Inhalt des Outputs/Feedbacks die Erwartungen bezüglich der inhaltlichen Ebene erfasst. Dabei werden vornehmlich vier Aspekte betont. Zum ersten wird erwartet, dass die Systeme grundlegende Informationen vermitteln sollten (D1: Informationsfunktion). „Ich glaube, die Lösung ist einfach, Menschen zu informieren und erzählen, was es ist und wie man sich sichern kann. Das ist, ich glaube, der beste Weg“ (P10). Dies wird dezidiert auch mit der Annahme verbunden, dass viele Nutzer:innen nicht ausreichend informiert sind, um Gefahren im Netz zu erkennen. „Yeah, I think, again, basic information is very important because it can make a big difference. Because most of the time, I think, the people who have no education about this or have no practice about that they are targeted on purpose” (P7). Zum zweiten wird im Rahmen von D2: Verifizierung/Richtigstellung formuliert, dass die technischen Assistenzsysteme eine Verifizierungsfunktion durch die Implementierung von Fakten und Quellenangaben gewährleisten sollen. Dies verweist deutlich auf den Fact Checking-Anspruch, den die Systeme einzulösen in der Lage sein sollten. „[…] es wäre auch gut, wenn sie dieses Video oder diesen Link in die App schicken können und […] wenn jemand das schon verifizieren kann. […] ein System, natürlich nicht eine Person“ (P6). Ähnlich argumentiert auch P9. „Also das wäre super, wenn ich eine App jetzt habe, das kann für mich checken, ob das richtig [ist] oder nicht, ob das stimmt oder nicht. Das macht die Sachen ein bisschen einfacher für Leute. Also brauche ich nicht so viel nachzugucken […]“ (P9). Auch wird formuliert, dass Desinformationen und wahre Informationen gegenübergestellt werden können. „Dann sie können da auch die falsche Version [gemeint ist eine Desinformation]” und natürlich auch die richtige Version schreiben und auch mit Bildern oder Videos und auch zum Beispiel, […] wenn ich etwas kontrollieren möchte […]“ (P6). Ein ganz wesentlicher Aspekt ist die Erwartung, die Systeme sollten den Zugang zu vertrauenswürdigen Inhalten und Quellen unterstützen. „Die App kann Quellen, die vertraulich sind, nennen […]“ (P5). Weitergehend wird die Erwartung formuliert, dass beide Systeme eine Warnfunktion vorhalten sollten, die auf akute Gefahrensituationen und aktuelle Desinformationen hinweist. „Über Cyberkriminalität […] Falschmeldungen und so weiter. […] Da kann diese App sich vorbereiten, damit die Zeit ist, es zu verhindern oder irgendwie Warnung geben“ (P1). Nicht zuletzt wurde im Rahmen von D3: Instruktivität die Erwartung formuliert, die Systeme sollten auch konkrete Handlungsanweisungen geben, etwa

https://doi.org/10.5771/9783748940616-305 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

bezüglich der Abwehr von Cybergefahren. „Ein Video mit „Achten Sie darauf. Sie müssen sich versichern, dass das eine echte Website ist, in die URL gucken" (P2). Ähnlich argumentiert P5. „Was ist einfachste Schritte, was könnten sie machen, um sicherer zu sein? Also, Instruktion sozusagen." Viele Aussagen verweisen implizit auf die Relevanz von Vertrauen und Misstrauen, weshalb dies nachfolgend dezidierter ausgearbeitet wird.

5.2 Querschnittskategorie Vertrauen und Misstrauen

In allen Interviews wurde die Relevanz von Vertrauen und Misstrauen deutlich, aus denen sich wichtige Hinweise auch auf die Erwartungen an Assistenzsysteme ableiten lassen, weshalb eine Querschnittskategorie (QK) Vertrauen und Misstrauen gebildet wurde.

Abb. 4: Querschnittskategorie 1 Vertrauen/Misstrauen

SQK1.1: Allgemein	D1: Lebensweltlich
	D2: Im Internet
SQK1.2: Assistenzsysteme	D1: Institutionelle Anbindung und Legitimität
	D2: Zertifizierung, Gütesiegel
SQK1.3: Herkunftsland/Deutschland	D1: Staatliche Einflussnahme in autoritären Systemen
	D2: Personenbezogene Daten in autoritären Systemen
	D3: Angst vor realweltlichen Folgen in autoritären Systemen
SQK1.4: Medien/Mediensystem	D1: Desinformation in autoritären Systemen
	D2: Erosion des Medienvertrauens in autoritären Systemen

Die erste Subkategorie beinhaltet in Dimension 1 generelle, auf die Lebenswelt insgesamt bezogene Aussagen. Dimension 2 umfasst Aussagen zum Internet, die zeigen, dass die Assoziationen der Befragten von Sicherheitsbedenken und Misstrauen geprägt sind. „I am absolutely certain that the

https://doi.org/10.5771/9783748940616-305 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

people who steal data, the hackers, they are improving their skills and I think there is no way for us to protect ourselves 100%" (P12). Das Bild vom Internet als Gefahrenraum wird in vielen Interviews betont. „Im Internet gibt es so viele Informationen. […] kann man gehackt werden. […] viele Menschen auf dieser Welt haben Angst in diesen Fallen zu ertappt zu sein" (P3). Im Rahmen der zweiten Subkategorie zu Vertrauen/Misstrauen in die Assistenzsysteme treten für die konkrete Entwicklung der Systeme sehr wichtige Punkte hervor. Es wird formuliert, dass die Systeme vertrauenswürdig sein sollen. „Hauptsache, […], dann kann ich dieser App vertrauen. Das ist ganz wichtig" (P9). Zugleich wird konkretisiert, wie solcherlei Vertrauen zustande kommen könnte. In Dimension 1 sind darum Aussagen zusammengefasst, die darauf verweisen, dass eine Anbindung an offizielle Institutionen, wie etwa staatliche Stellen und damit eine Legitimierung der Systeme, vertrauensbildend wirken würde. „Um zu vertrauen, ich brauche das… also das muss anerkannt von der Stadt sein. […] Ministerium. […] also ich würde es trauen nur, wenn es von der Stadt […] ist" (P6). Auch finden sich Aussagen, dass Forschungseinrichtungen und Universitäten vertraut wird. Zudem sollten die Systeme die Quellen angeben, mit denen sie operieren. Daher „müsste diese App selber Quellen angeben und wo sie herkommt, wer sie betreibt, dass man es nachprüfen kann. Dass es jetzt nicht irgendjemand [ist], der in seinem Keller sitzt und sich lustig was ausdenkt, […] sondern, dass da ein Institut dahinter steht für Medienforschung oder an der Universität, dass man dadurch seriöser erscheint" (P13). Neben der institutionellen Anbindung wird die Erwartung formuliert, die Systeme sollten Vertrauenswürdigkeit in Form einer Markierung deutlich machen, etwa in Form von Gütesiegeln oder Certified Accounts. „Und dann stelle ich mir vor, so wie bei Fairtrade […] oder wie bei der Eierpackung, so in einem kleinen Bild. […] das kann jeder in seine Website hinzufügen. Also, diese Häkchen von Twitter zum Beispiel damals, als sie gut funktioniert haben" (P2). Die dritte Subkategorie konkretisiert dies weiter, denn während viele Teilnehmer mit Blick auf deutsche Institutionen die Anbindung an diese als vertrauenssteigernd benennen, äußerten manche deutliche Vorbehalte gegenüber staatlichen Strukturen ihrer Herkunftsländer. Staatliche Stellen werden dabei vielfach mit der Regierung gleichgesetzt, der Misstrauen entgegengebracht wird. Dies zeigt sich vor allem bei Proband:innen aus autoritären Regimen (Dimension 1). „Okay, so first of all, for me being able to trust this app, it has to be written in bold font with capslock that this app is not funded by the government. That it is the independent organisations organised by some people who like to help in factchecking.

https://doi.org/10.5771/9783748940616-305 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Because if it's something about the government, It won't be factchecking. It's just going to be the government's side" (P12). Die zweite Dimension umfasst Befürchtungen zu personenbezogenen Daten in autoritären Regimen. „I can give the example of political situation in Russia. There was the team of Alexei Navalny. […] And they were collecting the data from the followers […]. It was also me and my family. And we gave them all our data, like name, surname, and I think the e-mail address, that was all. And one day, the ex-worker of their team published all this data publicly, because he was working in government […] for the Federal Security Office to arrest all these people and to threaten them. That's a good example of how politicians can play with data and why it's also very important not to share your data, even with guys you trust. […] And I know how valuable my data is for the Russian government. That is the huge consequence for people sharing their data" (P12). Diese Punkte korrespondieren mit Dimension 3, nämlich der Angst vor realweltlichen Folgen digitaler Handlungen. „Entweder die Leute können mich, […] meine Kreditkarte nutzen. […] noch schlimmer ist, dass jemand, der in der Nähe von mir wohnt mir etwas - ein Gefahr antun möchte, dass er weiß, wo ich wohne oder, dass man nicht mehr anonym ist" (P2). Die vierte Subkategorie beinhaltet Aussagen zur Rolle von Medien und Mediensystem in autoritären Systemen. Dabei wird die Annahme formuliert (Dimension 1), dass der Anteil von Desinformation weiter steigen wird. „Ich denke, das Problem [der Desinformation] wird größer. Der Staat, so wie ich das sehe, unternimmt nichts. Aus meiner Sicht ist öffentlich-rechtliche Medien… bleiben ohne Einfluss […] Und das Problem wird dann größer" (P4). Darüber hinaus wird deutlich, dass die Erfahrungen in autoritären Systemen zu einer erheblichen Erosion des Medienvertrauens (Dimension 2) führen, was insbesondere mit Blick auf politische Desinformationen deutlich wird. „Also ich gucke nicht so viel Nachrichten darüber, was in der Welt jetzt passiert, weil, ich kann nicht unterscheiden, was wahr ist und was nicht. […] Ich ärgere mich so, dass diese Medien… [Mein Papa] verliert seine Menschlichkeit und kann nichts dagegen tun […] das ist meine Familie und meine Freunde, sie sagen einfach […]: ich vertraue an nichts, jetzt können wir nichts trauen, wir können nicht wissen, was wahr ist und was nicht. Und das ist auch schade" (P5). Auch wenn ein technisches Assistenzsystem kaum den Anspruch haben kann, alle der hier illustrierten Punkte zu Vertrauen und Misstrauen aufzulösen, ist es gleichwohl wichtig, um diese Aspekte zu wissen und im Rahmen des Systems adressieren zu können.

https://doi.org/10.5771/9783748940616-305 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

6. Stand und Ausblick: Zur iterativen Schleife in CrossComITS und NEBULA

Die Ergebnisse geben Hinweise darauf, welche konkreten Erwartungen bezüglich technischer Assistenzsysteme in der Gruppe der Migrant:innen bestehen. Für die iterative Einspeisung dieser Ergebnisse in den technischen Entwicklungsprozess eröffnen sich dadurch Möglichkeiten, die Nutzbarkeit der Systeme zu verbessern und das Ziel der Kompetenzsteigerung zu erreichen. Dabei lassen sich Aspekte erkennen, die im Rahmen der konkreten Demonstratorentwicklung bereits in Umsetzung sind. Dazu gehören grundlegend eine gute und einfache Nutzbarkeit (Usabilty), die Input-Output-Struktur, die Verständlichkeit von Interface und Feedback insgesamt, die Multilingualität, die Informationsfunktion sowie die Möglichkeit auf Grundlage des Feedbacks, Inhalte zu verifizieren. Gleichwohl verweisen die Ergebnisse auf eine Reihe operativ nicht trivialer Konsequenzen bezüglich der konkreten Technologieentwicklung. So ist ein multimedial aufbereiteter Output deutlich entwicklungsintensiver als ein in der Hauptsache textbasiertes Feedback. Gleiches gilt für eine Warnfunktion sowie konkrete Instruktionen für spezifische Situationen, die eine situative Aktualität erfordern. Zu diesen Punkten werden im Rahmen der Demonstratorentwicklung derzeit verschiedene Varianten geprüft.

Darüber hinaus sind die hier dargestellten Ergebnisse durch Fragen nach Vertrauen und Misstrauen in Technologie, Internet, offizielle Institutionen, den Staat und das Mediensystem charakterisiert. Ein wichtiges Muster deutet sich darin an, dass während Institutionen des Herkunftslandes vielfach Misstrauen entgegengebracht wird, deutschen Institutionen durchaus Vertrauenswürdigkeit zugesprochen wird. Im Zuge dessen sehen viele der Proband:innen eine deutliche Markierung der institutionellen Anbindung des Assistenzsystems im Sinne eines Gütesiegels als wünschenswert an. Dies werden die entwickelten Systeme im Rahmen der Interface-Gestaltung konkret aufgreifen, um Reaktanzen zu verringen und Vertrauen zu stärken.

Derzeit befinden sich beide Demonstratoren in kontinuierlicher Entwicklung. Die Demonstratoren werden ab Herbst 2024 in qualitativen Folgestudien mit drei vulnerablen Gruppen (Jugendliche, Senior:innen und Migrant:innen) getestet. Die dann daraus gewonnen Erkenntnisse werden abermals in den iterativen Prozess der wertegebundenen Technologieentwicklung eingespeist, um so dem Ziel der Kompetenzsteigerung in den Bereichen Cybersicherheit und Desinformation sowie der Reduktion des Digital Divide als Parameter sozialer Nachhaltigkeit näher zu kommen, ganz so wie es die Sustainable Development Goals (SDG) der

https://doi.org/10.5771/9783748940616-305 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

UN definieren. In den SDGs sind die Reduktion des Digital Divide sowie die Stärkung von Medienkompetenzen als Querschnittskategorien zentral im Streben nach sozialer Nachhaltigkeit. Beide Aspekte werden demnach in einer Reihe von SDGs thematisiert, nämlich in SGD 4: Hochwertige Bildung, SGD 5: Geschlechtergleichstellung, SGD 8: Menschenwürdige Arbeit und Wirtschaftswachstum, SGD 9: Industrie, Innovation und Infrastruktur, SGD 10: Weniger Ungleichheiten, SGD 16: Frieden, Gerechtigkeit und starke Institutionen sowie SGD 17: Partnerschaften zur Erreichung der Ziele. Insbesondere in SGD 10 wird das Verständnis sozialer Nachhaltigkei konkretisiert und mit einer gewünschten Zunahme sozialer Gerechtigkeit, Fairness und Inklusion in Beziehung gesetzt. „The digital divide is of particular significance […] as it is a form of inequality that has the effect of compounding other forms of deprivation by denying access to an increasing range of opportunities in areas such as education, employment, and health" (Valdez/Javier 2020: 96). Um die Frage nach einer Zunahme sozialer Nachhaltigkeit im Sinne der Steigerung von Kompetenzen für eine gelingende Partizipation am gesellschaftlchen Diskurs konkret zu adressieren, kann das hier skizzierte iterative Value Sensitive Design um Aneignungsstudien ergänzt werden, die über die Prototypentestung hinausgehen, also die Frage stellen, wie und mit welchen Folgen die hier entwickelten Technologien in ihrer dann finalen Version von den Angehörigen der vulnerablen Gruppen tatsächlich genutzt und angeignet werden.

Literatur

Albers, Marion (2005): Informationelle Selbstbestimmung. Baden-Baden: Nomos. Online verfügbar unter doi:10.5771/9783845258638.

Allcott, Hunt/Gentzkow, Matthew (2017): Social Media and Fake News in the 2016 Election. In: Journal of economic Perspectives 31 (2), S. 211-36. Online verfügbar unter doi: 10.1257/jep.31.2.211.

Broschart, Steven (2024): Putins digitale Front und die Wahrheit dahinter. Wiesbaden: Springer

Bundeskriminalamt (BKA) (2024): Cybercrime - Bundeslagebild 2023. Wiesbaden. S. 27.

Bundesministerium des Innern und für Heimat (BMI) (o.J.): Hybride Bedrohungen und Desinformation. Bundesministerium des Innern und für Heimat. Zugriff am 10.7.2024a. Online verfügbar unter: https://www.bmi.bund.de/DE/themen/heimat-integration/wehrhafte-demokratie/abwehr-hybrider-bedrohungen/abwehr-hybrider-bedrohungen-node.html;jsessionid=665DD89045755ECBC4B753226F5225AC.live881 (Abfrage am: 14.08.2024).

https://doi.org/10.5771/9783748940616-305 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2024): Befragung zur Cybersicherheit 2024.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (o.J.): DDoS-Angriffe im Cyberraum. Bundesamt für Sicherheit in der Informationstechnik. Zugriff am 11.7.2024. Online verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/DDoS/ddos.html?nn=128786 (Abfrage am: 02.08.2024).

Cipolla, Carla/Bartholo, Roberto (2014): A Dialogical Approach to Socially Responsible Design. In: International Journal of Design 8 (2), S. 87-100.

van Dijck, José/Poell, Thomas/de Waal, Martijn (2018): The Platform Society. New York: Oxford University Press. Online verfügbar unter doi: 10.1093/oso/9780190889760.001.0001.

van Dijk, Jan (2020): The Digital Divide. Cambridge: polity.

Friedewald, Michael/Lamla, Jörn/Roßnagel, Alexander (Hg.). (2017): Informationelle Selbstbestimmung im digitalen Wandel. Wiesbaden: Springer Fachmedien Wiesbaden. Online verfügbar unter doi: 10.1007/978-3-658-17662-4.

Funiok, Rüdiger (2020): Verantwortliche Mediennutzung. Wünschenswerte Selbstverpflichtungen von Rezipient_innen und Nutzer_innen. In: Dies. (Hg.): Communicatio Socialis, 53 (2), S. 136-147. Online verfügbar unter doi: 10.5771/0010-3497-2020-2-136.

Glenski, Maria/Weninger, Tim/Volkova, Svitlana (2018): Propagation from Deceptive News Sources Who shares, How Mush, How Evenly, and how Quickly? In: IEEE Transactions on Computational Social Systems 5 (4), S. 1071-1082. Online verfügbar unter doi: 10.1109/TCSS.2018.2881071

Gomolla, Mechtild (2017): Direkte und indirekte, institutionelle und strukturelle Diskriminierung. In: Scherr, Albert/El-Mafaalani, Aladin/Yüksel, Gokcen (Hg.): Handbuch Diskriminierung. Wiesbaden: Springer VS, S. 133-155. Online verfügbar unter doi: 10.1365/s40702-020-00618-7.

Haarkötter, Hektor (2021): Wahrheit und Lüge im (außer-) journalistischen Sinne. In Schicha, Christian et al. (Hg.): Medien und Wahrheit. Medienethische Perspektiven auf Desinformation, Lüge und „Fake News". Baden-Baden: Nomos, S. 309-331.

Heesen, Jessica (Hg.). (2016): Handbuch Medien- und Informationsethik. Stuttgart: J.B. Metzler Verlag.

Hillerbrand, Rafaela (2021): Value Sensitive Design. In: Grunwald, Armin/Hillerbrand, Rafaela (Hg.): Handbuch Technikethik (2. aktualisierte und erweiterte Auflage) . Berlin: J.B. Metzler Verlag, S. 466-471.

Keller, Kathrin (2023): Nur die halbe Wahrheit?: Wie alternative Onlinemedien in der Coronapandemie berichten. Eine empirische Untersuchung. In Haarkötter, Hektor/ Nieland, Jörg-Uwe (Hg.): Agenda-Cutting. Wiesbaden: Springer Fachmedien, S. 157-173. Online verfügbar unter doi: 10.1007/978-3-658-38803-4_7.

von der Pfordten, Dietmar (2021): Gerechtigkeit. In: Grunwald, Armin/Hillerbrand, Rafaela (Hg.): Handbuch Technikethik (2., aktualisierte und erweiterte Auflage) . Berlin: J.B. Metzler Verlag S. 196-202.

Plattner, Claudia (2023): Vorwort. jährlich No. BSI-LB23/512.

https://doi.org/10.5771/9783748940616-305 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Röben, Bärbel (2013): Medienethik und die „Anderen“: Multiperspektivität als neue Schlüsselkompetenz. Wiesbaden: Springer Fachmedien Wiesbaden. Online verfügbar unter doi: 10.1007/978-3-531-19114-0.

Reißmann, Wolfgang/Bettinger, Patrick (2022): Editorial: Digitale Souveränität und relationale Subjektivität. In: Dies. (Hg.): Digitalität und Souveränität. Braucht es neue Leitbilder der Medienpädagogik? 2022/06, S. 1-2.

Ruokolainen, Hilda/Widén, Gunilla (2020): Conceptualising misinformation in the context of asylum seekers. In: Jansen, Bernard: Information Processing & Management, 57 (3), 102127. Online verfügbar unter doi: 10.1016/j.ipm.2019.102127.

Schimany, Peter/Rühl, Stefan/Kohls, Martin (2012): Ältere Migrantinnen und Migranten. Entwicklungen, Lebenslagen, Perspektiven. In BAMF (Hg.): Forschungsbericht 18. Nürnberg.

Schünemann, Wolf J. (2023): Cybersicherheit. In: Klenk, Tanja/Nullmeier, Frank/Wewer, Göttrik (Hg.): Handbuch Digitalisierung in Staat und Verwaltung . Wiesbaden: Springer Fachmedien Wiesbaden, S. 1-12. Online verfügbar unter doi: 10.1007/978-3-658-23669-4_17-2 .

Seeliger, Martin/Sevegnani, Sebastian (Hg.) (2021): Ein neuer Strukturwandel der Öffentlichkeit? (1. Auflage) . Baden-Baden: Nomos.

Seo, Hyunjin/Blomberg, Matthew/Altschwager, Darcey/Tien Vu, Hong (2020): Vulnerable Populations and Misinformations: A Mixed-Methods Approach to Underserved Older Adults. In: Online Information Assessment, New Media Soc. Online verfügbar unter doi: 10.1177/1461444820925041.

Shrestha, Anu/Spezzano, Francesca (2019): Online misinformation: From the deceiver to the victim . Vancouver: ASONAM‘19. S. 847-850.

Statistisches Bundesamt (DESTATIS) (o.J.): Migrationshintergrund. Zugriff am 29.08.2024. Online verfügbar unter: https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bevoelkerung/Migration-Integration/Glossar/migrationshintergrund.html (Abfrage am: 07.08.2024).

Strauss, Anselm L./Corbin, Juliet M. (1996): Grounded Theory. Grundlagen qualitativer Sozialforschung. Weinheim: Psychologie Verlags Union.

Valdez, Violet/Javier, Samantha (2021): Digital Divide: from a Peripheral to a Core Issue for All SDGs. In Reduced Inequalities. Springer International Publishing, S. 88-101. Online verfügbar unter doi: 10.1007/978-3-319-95882-8_107.

Zimmermann, Fabian/Kohring, Matthias (2018): ‘Fake News‘ als aktuelle Desinformation. Systematische Bestimmung eines heterogenen Begriffs. In: Medien & Kommunikationswissenschaft 66 (4). Baden-Baden: Nomos, S. 526–541.

https://doi.org/10.5771/9783748940616-305 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY