Informierte Einwilligung, häusliche Altenpflege und soziale Robotik – Ein Konzept zur Konkretisierung der Zweckangabe bei Social-Compagnion-Robotern

Wulf Loh und Anne Wierling

Einleitung

Im Bereich sozialer Robotik, besonders mit Blick auf die häusliche bzw. Tagespflege älterer Menschen, ergeben sich eine Vielzahl von Schwierigkeiten hinsichtlich eines adäquaten Datenschutzes (Calo 2012). Dies gilt ganz speziell für die Möglichkeit der informierten Einwilligung seitens der Betroffenen in die Datenverarbeitung, da in diesem Bereich eine Vielzahl an Sensorik und Datenverarbeitung zum Einsatz kommt, gleichzeitig aber ältere Menschen aufgrund ihrer mangelnden Technikaffinität eine besonders vulnerable Gruppe darstellen (Ammicht Quinn 2019). In diesem Beitrag sollen Aspekte einer sowohl DSGVO-konformen als auch ethisch akzeptablen Einwilligungskonzeption erarbeitet werden (Behrendt et al. 2019). Grundlage dieser Konzeption ist die Überlegung, die rechtlich und ethisch notwendigen Informationen zur Einwilligung in die Datenverarbeitung möglichst leicht verständlich und konkret zu gestalten. Hierfür wird auf konzeptueller Ebene eine Matrix entwickelt, die die Bestimmung der Zweckangabe der Datenverarbeitung sowie den Informationsgehalt der Einwilligung mit der potenziellen Eingriffstiefe in die Privatsphäre und informationelle Selbstbestimmung der Betroffenen in Beziehung setzt (Privacy Interference Matrix). Daraus wird eine proportionale Relation zwischen Konkretheit der Zweckangabe und Eingriffstiefe abgeleitet: *Je tiefer der potenzielle Eingriff in die Privatsphäre und informationelle Selbstbestimmung, desto konkreter muss der Zweck angegeben werden, und desto größer muss der Informationsgehalt der Einwilligung sein*. Diese Relation wird in

W. Loh (✉)
Stuttgart, Deutschland
E-Mail: wulf.loh@izew.uni-tuebingen.de

A. Wierling
Hörstel, Deutschland
E-Mail: Anne.Wierling@uni-siegen.de

G. Richter et al. (Hrsg.), *Datenreiche Medizin und das Problem der Einwilligung*,
https://doi.org/10.1007/978-3-662-62987-1_8

verschiedenen Kategorien der Eingriffstiefe ausbuchstabiert, welche dann unterschiedliche Zustimmungsmodi nach sich ziehen. Als Ergebnis werden tentativ einige Möglichkeiten für Abstufungen der Zustimmung aufgezeigt.

1 Der Kontext des NIKA-Projekts

Im Projekt NIKA (BMBF 16SV7944) wird ein soziales Compagnon-Robotik-System entwickelt, das ältere Menschen im häuslichen Umfeld aktivieren und unterhalten soll. Unter anderem werden spielerisch Gedächtnistraining und Biographiearbeit umgesetzt. NIKA soll auf drei robotischen Plattformen realisiert werden (Pepper, MiRo, Roomba), die jeweils über unterschiedliche Sensorik verfügen und u.U. Hilfsgeräten wie Bildschirmen und Tablets bedürfen. Eines der primären Ziele des Projektes ist es, für jede robotische Plattform und Interaktionssituation jeweils adäquate "Interaktionspattern" (Borchers 2000; Kahn et al. 2008) zu entwickeln, die den jeweiligen Interaktionskontexten und -möglichkeiten gerecht werden. Diese Muster sollen verallgemeinerbar dargestellt und für zukünftige Anwendungskontexte operationalisierbar gemacht werden (Tidwell 2010; Pollmann 2019).

Je nach robotischem System verfügt NIKA über unterschiedliche Sensorik und Kommunikationsmöglichkeiten. Während bspw. der Roboter "Pepper" mittels Mikrofonen und Kameras Sprache, Gestik und Mimik verarbeiten kann, ist dies dem Staubsaugerroboter "Roomba" nicht möglich. In umgekehrter Kommunikationsrichtung verfügt "Pepper" über eine Sprachausgabe, "MiRo" und "Roomba" dagegen nicht. Dies wurde in der Projektplanung absichtlich so gewählt, um verschiedene Interaktionsmöglichkeiten zu testen und als Interaktionspattern zu beschreiben.

Für Datenschutzbelange gehen wir davon aus, dass jede robotische Plattform über mehrere Sensoren verfügt, die für eine dauerhafte Funktionalität konstant aktiv und aufnahmebereit sein müssen. Exemplarisch lässt sich dies am Roboter "MiRo" verdeutlichen: Er verfügt über sechs Sensoren (Stereokameras, Mikrofone, Berührungs- und Lichtsensor, Abstandssensor, sowie einen sogenannten Cliff-Sensor, der Treppen und Abgründe erkennt und so Stürze verhindert). Darüber hinaus ist NIKA mobil, kann sich also eingeschränkt in den Räumlichkeiten bewegen und mindestens gestisch (d. h. durch Körpersprache, die – je nach Freiheitsgraden – z. T. sehr rudimentär ausfallen kann) interagieren.

Da es sich bei dem geplanten Einsatzbereich sowohl um die ambulante Tagespflege als auch um Wohnungen des betreuten Wohnens handelt, ist NIKA u.U. auch im privaten Wohnumfeld unterwegs. NIKA legt Nutzer:innenprofile an und speichert hierfür persönliche Daten (Name, biometrische Daten wie Gesicht, Sprachprofil für individuelle Erkennung, Ergebnisse des Gedächtnistrainings) sowie Daten aus den individuellen Interaktionen, um auf Interaktionspräferenzen reagieren zu können (Arten der Ansprache, tägliche Routinen, präferierte Motivationsmodi).

2 (Medizin-)ethische Grundlagen der informierten Einwilligung

In einem Beitrag der New York Times (NYT) von 2019 wurden 150 Datenschutzrichtlinien großer Internetplattformen sowie der Internetauftritte von Großunternehmen in ihrer "readability" mit großen literarischen Werken verglichen (Litman-Navarro 2019). Dieser nicht ganz ernst gemeinte Vergleich ergab, dass die Zoom-, Ebay- und AirBnB-Datenschutzrichtlinien eine ähnlich hohe Lesekompetenz erfordern wie das erste Kapitel von Kants "Kritik der reinen Vernunft", während der Autor des NYT Textes zum Lesen der Datenschutzbestimmungen von AirBnB etwa doppelt so lang brauchte wie für besagtes Kant-Kapitel. Selbst wenn man dieses Experiment mit einem Augenzwinkern betrachtet, macht es dennoch deutlich, dass viele der Datenschutzrichtlinien Textkompetenzen auf Universitätsniveau erfordern. Es wird einmal mehr offenkundig, dass Datenschutzrichtlinien und AGBs "by lawyers for lawyers" gemacht sind.

Auch wenn dies vielleicht nicht sonderlich überraschend sein mag, steht es doch in krassem Gegensatz zu dem *Ideal der informierten Einwilligung*, wie es in der Medizinethik formuliert wurde (Dworkin, 1988; Maclean, 2009) und bspw. auch in Art. 4 Nr. 11 DSGVO anklingt:

> „Im Sinne dieser Verordnung bezeichnet der Ausdruck: […] ‚Einwilligung' der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist".

Der Art. 7 Abs. 2 S.1 DSGVO gibt vor, dass bei schriftlichen Einwilligungen „das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" erfolgen muss. Es sollten daher keine Fremdsprachen, Fremdwörter oder juristische Termini Verwendung finden, da andernfalls der entsprechende Teil der Einwilligung gemäß Art. 7 Abs. 2 S. 2 DSGVO nicht verbindlich wäre. Auch das European Data Protection Board (EDPB) weist in seinen neuen Guidelines zu Einwilligungen explizit darauf hin, dass die Einwilligung von einer Durchschnittsperson verstanden werden muss – und eben nicht nur von Anwälten (EDPB 2020).

Weitere Anforderungen an eine datenschutzkonforme Einwilligung ergeben sich unter anderem aus Art. 6 Abs. 1 lit.a iVm Art. 7 DSGVO. Zusätzlich müssen die Begriffsbestimmung des Art. 4 Nr.11 und ggf. die Vorgaben des Art. 8 (Minderjährige), Art. 9 Abs. 2 (sensible Daten), Art. 22 (automatisierte Entscheidungen) sowie Art. 49 (Übermittlung in Drittländer) der DSGVO für eine wirksame Einwilligung berücksichtigt werden. Da die DSGVO jedoch erst seit Mai 2018 gültig ist, liegen bisher nur wenige relevante Gerichtsurteile des EuGHs zur DSGVO vor, weshalb die auslegungsfähigen Anforderungen an eine informierte Einwilligung noch nicht endgültig geklärt sind.

Unabhängig von den rechtlichen Vorgaben hängt aus (medizin-)ethischer Perspektive das Bestehen einer solchen Einwilligung typischerweise von drei Kriterien ab, die die einwilligende Person erfüllen muss: 1. vollständige Information (epistemische Dimension), 2. angemessene Entscheidungsfähigkeit (kognitive Dimension) und 3. Freiwilligkeit (Dimension der tatsächlichen Wahl) (Dworkin 1988; Eyal 2011).

2.1 Epistemische Dimension

Um eine informierte Entscheidung über die Preisgabe persönlicher Daten treffen zu können, müssen die betroffenen Personen über vollständige Informationen verfügen. Dies beinhaltet drei Aspekte: (a) Wissen über die Fakten, die für die Entscheidung ausschlaggebend sind, und daher (b) Wissen über die Situation, d. h. welche Fakten überhaupt zum Tragen kommen, sowie (c) eine allgemeine "appreciation of the nature and significance of the decision" (Charland 2008) für die Person selbst und ihr Umfeld. In der Literatur zur informierten Zustimmung wird dies oft unter dem Begriff "understanding" (Charland 2008) gefasst. In Übereinstimmung mit Catherine Elgins jüngsten Überlegungen zu "Verstehen" charakterisieren wir "understanding" hier als:

> „an epistemic commitment to a comprehensive, systematically linked body of information that is grounded in fact, is duly responsive to reasons or evidence, and enables nontrivial inference, argument, and perhaps action regarding the topic the information pertains to." (Elgin 2017)

Gerade im Kontext der Datenverarbeitung bei robotischen Systemen wird dieses Verstehen häufig durch den Wunsch nach einer Mensch-Maschine-Interaktion unterlaufen, die eine "seamless interaction" (DIN EN ISO 9241-11 2018; DIN EN ISO 9241-110 2020) ermöglichen soll. Damit ist gemeint, dass die Interaktion möglichst viele habitualisierte Kommunikationsmuster verwenden soll, um intuitiv verständlich zu sein und so den „cognitive load" der Nutzer:innen gering zu halten (Drury et al. 2004). Dies zieht vielfach eine humanoide oder animoide Mimik, Gestik und allgemeine Kommunikationsgestaltung nach sich, da diese den Nutzer:innen bekannt ist und daher wenig Aufmerksamkeit erfordert. Im Ergebnis bleiben jedoch Informationen, derer die interagierenden Personen zu einer wohlinformierten Einwilligung in die Datenverarbeitung bedürfen, unthematisch, da diese den reibungslosen Interaktionsfluss stören und die interagierenden Personen zu Reflexion und bewusster Entscheidung zwingen würden.

Aus rechtlicher Perspektive wiederum werden diese sehr anspruchsvollen Forderungen aus dem (medizin-)ethischen Bereich für den Kontext der Einwilligung in die Datenverarbeitung im Wege eines gesetzgeberischen Kompromisses zwischen "vollständiger Information" und dem jeweiligen Aufwand für die datenverarbeitende Stelle umgesetzt. Art. 4 Nr. 11 DSGVO definiert, dass eine Einwilligung in informierter Weise abgegeben werden muss. Gemäß Erwägungsgrund 42 Satz 4 DSGVO setzt "in informierter Weise"

voraus, dass die Betroffenen mindestens wissen müssen, wer verantwortlich ist und für welche Zwecke die personenbezogenen Daten verarbeitet werden sollen. Im Gegensatz dazu fordern Artt. 13 und 14 DSGVO deutlich mehr Informationen, welche den Betroffenen bei der Verarbeitung von personenbezogenen Daten zur Verfügung gestellt werden müssen.

Werden die Daten direkt bei den Betroffenen erhoben (Art. 13 DSGVO), müssen der Name und die Kontaktdaten de:r Verantwortlichen, ggf. die Kontaktdaten de:r Datenschutzbeauftragten, die Zwecke der Verarbeitung, die Rechtsgrundlage für die Verarbeitung, ggf. die berechtigten Interessen, die Empfänger oder Kategorien von Empfängern und bei Übermittlung an ein Drittland das Vorhandensein eines Angemessenheitsbeschlusses bzw. geeignete Garantien als Informationen an die Betroffenen herausgegeben werden. Weitere Informationen, die erteilt werden sollten, sind die Speicherdauer, das Bestehen von Betroffenenrechten, die Widerrufbarkeit der Einwilligung, das Beschwerderecht bei einer Aufsichtsbehörde, die Verpflichtung zur Bereitstellung von Daten, automatisierte Entscheidungsfindung und Zweckänderungen. Nur wenn die Daten nicht direkt bei den Betroffenen erhoben werden, müssen die Betroffenen gemäß Art. 14 DSGVO über die betroffene Datenkategorie sowie über die Quelle, aus der die Daten stammen, informiert werden. Ferner ist er darüber zu informieren, ob die Datenquelle eine öffentliche ist.

Die Informationen, die im Rahmen der informierten Einwilligung erteilt werden müssen, sollten jedoch von denen, die im Rahmen des Artt. 13 bzw. 14 DSGVO bereitzustellen sind (den sogenannten Informationspflichten), unterschieden werden. Somit kann nach Meinung des EDPB eine informierte Einwilligung auch dann vorliegen, wenn nicht alle Informationen der Artt. 13 bzw. 14 in der Einwilligung erteilt werden. Den Informationspflichten kann bspw. auch im Rahmen der Datenschutzerklärung des Unternehmens nachgekommen werden, wodurch eine zusätzliche Aufführung dieser Informationen in der Einwilligung vermieden werden kann (EDPB 2020).

Die Informationen der Artt. 13 bzw. 14 DSGVO müssen gemäß EDPB nicht zwingend im Rahmen einer informierten Einwilligung gegeben werden. Jedoch fordert das EDPB die Angabe von mindestens de:r Verantwortlichen, dem Zweck der Verarbeitung, der Datenkategorie, der Widerrufbarkeit der Einwilligung, ggf. Informationen bzgl. automatisierter Entscheidungen und Informationen zu Risiken bei Datenübermittlung an ein Drittland ohne das Vorhandensein eines Angemessenheitsbeschlusses bzw. geeigneter Garantien (EDPB 2020).

Bis ein die Anforderungen präzisierendes Urteil durch den EuGH vorliegt, werden im Folgenden daher die Empfehlungen des EDPB berücksichtigt.

2.2 Kognitive Dimension

Zusätzlich zu vollständigen Informationen benötigen die Nutzer:innen robotischer Systeme bestimmte *Entscheidungsfähigkeiten*, um die Informationen, die sie erhalten,

für sich sinnvoll zu ordnen, mit ihren Präferenzen und Volitionen zweiter Ordnung in Einklang zu bringen (Frankfurt 1987) und nach ihnen zu handeln. Um dies zu gewährleisten, dürfen sie nicht getäuscht, durch psychomotivationale Anreize unangemessen manipuliert oder anderweitig kognitiv eingeschränkt werden, z. B. durch Ablenkung ihrer Aufmerksamkeit.

Die bisherigen Mensch-Maschine-Interaktionsdesigns stehen diesem Ziel zuweilen entgegen, da sie häufig versuchen, eine möglichst reibungslose, natürliche und intuitive Interaktion sicherzustellen. Gerade bei Nutzer:innen, die wenig technikaffin sind, können Anthropo- bzw. Zoomorphisierungstendenzen hervorgerufen werden (Darling 2017), also die intuitive "Vermenschlichung" bzw. "Tierähnlichkeit" von Robotern. Anders gesagt: Um die Interaktion möglichst intuitiv und mit geringer kognitiver Beanspruchung zu halten, werden häufig aus menschlicher bzw. tierischer Kommunikation bekannte Interaktionsmuster verwendet. Damit wird jedoch bei den Nutzenden oftmals recht effektiv der Eindruck erweckt, es handele sich um ein menschen- bzw. tierähnliches Gegenüber – mit allen Konsequenzen. Dies ist dann problematisch, wenn die Nutzer:innen implizit auf weitere menschen- bzw. tierähnliche Eigenschaften schließen, nicht gerechtfertigtes Vertrauen aufbauen, etc. (Turkle 2010; Scheutz 2012).

Aus rechtlicher Perspektive ist das Äquivalent zur kognitiven Dimension die *Einwilligungsfähigkeit* der Betroffenen. Dabei kommt es nicht auf die Geschäftsfähigkeit der Erklärenden im Sinne des BGB an. Vielmehr muss die betroffene Person einsichtsfähig sein, also in der Lage sein, die Bedeutung und Tragweite ihrer Einwilligung zu verstehen (Hauser et al. 2019). Fehlt diese Einsichtsfähigkeit ist eine gleichwohl erteilte Einwilligung unwirksam (Steinrötter 2020). Vorstellbar, aber nicht pauschal annehmbar, ist eine solche fehlende Einwilligungsfähigkeit beispielsweise bei Patient:innen in psychiatrischer Behandlung oder bei fortgeschrittener Demenz. Eine wirksame Einwilligung kann dann nur von einem gesetzlichen Vertreter der Betroffenen erteilt werden.

Zudem ist auch eine Altersgrenze in Bezug auf Minderjährige für die Annahme der Einsichtsfähigkeit relevant. Im Rahmen der DSGVO kann eine Person ab Vollendung des 16. Lebensjahres auch ohne die Zustimmung der Eltern zulässig in ein Angebot von Diensten der Informationsgesellschaft einwilligen, wenn das Angebot dem Kind direkt (Moos et al. 2018) unterbreitet wird.

2.3 Freiwilligkeit

Typischerweise hängt die Freiwilligkeit einer Entscheidung davon ab, dass sie nicht unter Manipulation bzw. Zwang stattfindet. Nur wenn die Einwilligung in die Datenverarbeitung auf der Grundlage von reflexiver Einsicht und aus rationaler Überzeugung getroffen wird, d. h. aufgrund des "zwanglosen Zwangs des besseren Arguments" (Habermas 2009), gilt sie als freiwillig. Ein solcher Begriff der Freiwilligkeit ist

untrennbar mit dem Ideal personaler Autonomie (Kant AA V; Parfit 1984; Korsgaard 2009) verbunden und findet seinen rechtlichen Ausdruck im Konzept der "volenti non fit iniuria" ("Dem Einwilligenden widerfährt kein Unrecht"). Dies ist die Grundlage für das gesamte Vertragsrecht und damit auch für die Einwilligung in die Datenverarbeitung.

In rechtlicher Hinsicht muss gemäß Art. 4 Nr. 11 DSGVO eine Einwilligung freiwillig erfolgen, wobei der Begriff der Freiwilligkeit nicht legal definiert ist und daher ausgelegt werden muss. Der EuGH nutzt für die Auslegung von Sekundärrecht vor allem Erwägungsgründe, um den Zweck einer Norm zu bestimmen: Gemäß Erwägungsgrund 42 S. 5 DSGVO soll nur dann von einer Freiwilligkeit der Einwilligung ausgegangen werden, wenn die Betroffenen "eine echte oder freie Wahl haben und somit in der Lage sind, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden". Von einer Zwangssituation kann gemäß Erwägungsgrund 43 S. 1 DSGVO ausgegangen werden, wenn zwischen de:r Verantwortlichen und den Betroffenen ein klares Ungleichgewicht besteht und es daher unwahrscheinlich erscheint, dass die Einwilligung freiwillig erteilt wurde. Vorstellbar, aber nicht pauschal annehmbar, ist ein solches Ungleichgewicht beim Verhältnis Ärzt:in – Patient:in oder Pflegekraft – pflegebedürftige Person.

Denkbar wäre auch, dass bei Angeboten von Monopolisten von einem Ungleichgewicht ausgegangen werden kann. Abhilfe könnte dann ein äquivalentes Alternativangebot der Verantwortlichen schaffen, ohne dass sich daraus Nachteile für die Betroffenen ergeben (aA Steinrötter 2020). Hier liegt noch erhebliches Auslegungspotenzial, das wir im Rahmen dieses Textes nicht weiterverfolgen können. Darüber hinaus könnte es gemäß Erwägungsgrund 43 S. 2 an der Freiwilligkeit einer Einwilligung fehlen, wenn das Trennungsgebot nicht eingehalten wurde. Dies ist anzunehmen, wenn pauschal eine einzige Einwilligung zu tatsächlich verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten erteilt werden muss. Das Nicht-Kopplungs-Gebot (Erwägungsgrund 43 S. 2 DSGVO) sieht für die Beurteilung der Freiwilligkeit vor, dem Umstand, ob durch die Einwilligung eine Verarbeitung legitimiert werden soll, die über das hinausgeht, was für die Vertragserfüllung erforderlich wäre, in größtmöglichem Umfang Rechnung zu tragen.

Wie wir bereits gesehen haben, sind viele Mensch-Technik-Interaktionen mindestens potenziell manipulativ, wenn sie auch zumeist nicht mit direkter Täuschung verbunden sind (Loh i.Ersch.). Während sich „Täuschung" hierbei auf das aktive Verbreiten von Falschinformationen als Teil einer Manipulationsstrategie bezieht, ist mit „Verdeckung" das Verbergen des Manipulationsversuchs selbst gemeint (Rudinow 1978; Susser et al. 2019). Wie sich an den oben genannten Beispielen ersehen lässt, beruht nicht jede Manipulation zwangsläufig auf Täuschungen (Gorin 2014; Wood 2014), im Gegenteil: Viele der Manipulationsstrategien kommen völlig ohne Lügen oder dem Verleiten zu fehlerhaften Annahmen aus. Manipulative Mensch-Technik-Interaktionen setzen jedoch u.U. auf eine Verdeckung der eigenen Manipulationsstrategie in Form von Anthropo- bzw. Zoomorphisierungen. Dies gilt insbesondere, wenn emotionale Trigger (große

Augen, Kindchenschema, Welpenhaftigkeit etc.) verwendet werden, um die Interaktion positiv zu gestalten bzw. die Nutzenden dazu zu bringen, bestimmte Dinge zu tun.

Neben manipulativen Eingriffen in die Freiwilligkeit, die immer auch entweder die epistemische oder kognitive Dimension mit betreffen, ergeben sich in Mensch-Technik-Ensembles oftmals auch designseitige Zwänge zur Einwilligung in die Datenverarbeitung. Dies ist bspw. dann der Fall, wenn ohne eine Einwilligung die Funktionalität der Technik gar nicht – oder nur sehr eingeschränkt – genutzt werden kann (Cavoukian 2011; O'Connor et al. 2017). Hier wird vonseiten der Entwickler:innen die Default-Option "vollständige Einwilligung in die konstante Datenverarbeitung" nicht in Zweifel gezogen, sodass eine Technikentwicklung mit abgestuften Datenverarbeitungsmodellen, u.U. in Form von "Kaskadenmodellen" (Loe et al. 2015; Rost et al. 2020, sowie Lösungsmöglichkeiten für verschieden abgestufte Einwilligungen, nach wie vor nicht standardmäßig in Betracht gezogen wird.

Besonders im medizinischen und Altenpflegekontext stellt dies die Freiwilligkeit vor große Herausforderungen. Strukturell sind hier Patient:innen bzw. Pflegebedürftige sehr viel stärker auf Technologien angewiesen, und selbst im Anwendungsfall von NIKA als Companion-Roboter geben viele Nutzende möglicherweise unter dem Druck von Angehörigen und Pflegekräften nach. Um diese Schwierigkeiten zu umgehen bzw. abzumildern, werden wir im Folgenden eine Matrix vorstellen, die die Intensität des Privatheitseingriffs proportional an die Definition des Zwecks und den Informationsgehalt der Einwilligung bindet und auf diese Weise die Datenautonomie wieder teilweise an die Nutzer:innen zurückgibt, auch wenn sie mglw. manipulative als auch unter erheblichem Druck zustande gekommene Einwilligungen in die Datenverarbeitung mit Blick auf Mensch-Roboter-Interaktionen nicht verhindern kann.

3 Intensity of Privacy Interference

Welche Informationen im Rahmen einer informierten Einwilligung erforderlich sind, ist noch strittig. Es gibt zwar Empfehlungen des EDPB zum Mindestinhalt einer "informierten Einwilligung", aber noch keine Entscheidungen des EuGHs diesbezüglich, die Klarheit schaffen könnten. Zudem muss der Zweck sowohl im Rahmen der Informationspflichten als auch der Einwilligung angegeben werden. Offen ist dagegen bisher, in welchem Umfang dies geschehen muss. Weder in den Leitlinien zur Einwilligung aus dem Jahr 2018 noch in der aktualisierten Version des EDPB aus 2020 sind detaillierte Angaben zur Konkretheit des Zwecks aufgeführt. Ist es ausreichend anzugeben, dass der „Roboter funktionieren muss" oder dass er „die Altenpflege unterstützen soll"? Solche sehr allgemeinen Angaben oder gar Blankett-Einwilligungen sind unzulässig (Der Bayerische Landesbeauftragte für Datenschutz 2018).

Gleichzeitig wird der Angabe des Zwecks auch an verschiedenen anderen Stellen innerhalb der europäischen Bürokratie eine besondere Wichtigkeit beigemessen. Bspw.

schreibt die EU Kommission in ihrem jüngsten Weißbuch zur Künstlichen Intelligenz, dass „eindeutige Angaben […] insbesondere über den Zweck, für den die Systeme bestimmt sind […] und über das erwartete Maß an Genauigkeit bei der Erreichung des angegebene Zwecks“ gemacht werden müssen (Europäische Kommission 2020). Aber auch in diesem Dokument wird nicht präzisiert, inwiefern eine Konkretisierung der Angabe des Zwecks im Rahmen der Einwilligung stattfinden kann.

3.1 Matrix-Kriterien

Eine denkbare Lösung wäre die Einteilung von einzelnen Datenverarbeitungsprozessen des Roboters in Kategorien. Auf diese Weise könnte die Datenverarbeitung mit der Stärke des Eingriffs in die Privatsphäre der Betroffenen in Beziehung gesetzt werden: Je stärker dieser Eingriff, desto konkreter muss die Angabe des Zwecks erfolgen und desto mehr Informationen müssen im Rahmen der Einwilligung erteilt werden. Zur Beurteilung der Eingriffsstärke wird das allgemeine Persönlichkeitsrecht (APR) herangezogen. Das APR wurde in richterlicher Rechtsfortbildung aus Art. 1 Abs. 1 GG und Art. 2 Abs. 1 GG abgeleitet. Eine Ausprägung des APR ist das Konzept der informationellen Selbstbestimmung, das vom Bundesverfassungsgericht im sogenannten Volkszählungsurteil 1983 als Grundrecht anerkannt wurde. Im Grunde sagt es aus, dass Betroffene bestimmen können müssen, wer, was, wann und wie lange über sie weiß.

Aus dem Recht auf informationelle Selbstbestimmung lassen sich einige Kriterien ableiten, die zur Beurteilung des Eingriffs in die Privatsphäre herangezogen werden können und im Folgenden vorgestellt werden. Die Betroffenen müssen bestimmen können wer (Empfänger), was (Datenkategorie, Sphärentheorie, Aggregation, Erhebungsumfang, Anonymisierung, machine learning), wann (Erhebungsdauer) und wie lange (Datenspeicherung) über sie weiß. Selbst wenn die rechtliche Grundlage für die Verarbeitung keine Einwilligung ist, so sind einige Elemente, die zur Messung der Intensität des Eingriffs in die Privatsphäre vorgeschlagen werden, erforderlich, um die Vorgaben der Artt. 13, 14, 30 und 32 DSGVO zu erfüllen. Im Rahmen von Artt. 13 und 14 DSGVO müssen Informationen bezüglich der Löschfristen, Datenkategorien sowie Empfänger bereitgestellt werden. Auch für die Umsetzung des Art. 30 DSGVO, das Erstellen des Verzeichnisses für Verarbeitungstätigkeiten, sind diese Informationen erforderlich. Art. 32 DSGVO soll ein dem Risiko der Verarbeitung angemessenes Schutzniveau sicherstellen, wobei unter anderem die Möglichkeit der (zumindest) Pseudonymisierung in Erwägung gezogen werden soll. Um entsprechende Risiken der Verarbeitung beurteilen zu können, muss auch die Verknüpfbarkeit der Daten berücksichtigt werden, da diese einen Einfluss auf die Qualität der Daten hat. Steigt die Qualität der Daten, so hat dies Einfluss auf die mögliche Schadenschwere, die im Rahmen der Risikobeurteilung mitzubedenken ist. Des Weiteren müssen der Umfang (bspw. Big Data/Erhebungsdauer/Speicherdauer) und

die Umstände der Verarbeitung (bspw. Anzahl der Empfänger) in die Risikobeurteilung einbezogen werden.

Damit alle Kriterien entsprechend berücksichtigt werden können, müssen die verschiedenen Optionen der Kriterien gewichtet werden, um diese dann zu einem Gesamtergebnis zu aggregieren (vgl. Abschn. 3.2.). Hier bestehen mehrere Möglichkeiten: Bspw. könnten die jeweiligen Gewichtungen einfach aufaddiert werden und so eine Indexzahl bilden, mithilfe derer eine Einteilung in verschiedene Kategorien der Zweckangabe erfolgen kann. Alternativ wäre auch eine Aggregation per Mindestscore denkbar, d.h. dass für bestimmte (oder u.U. auch alle) der oben genannten Kriterien Mindeststandards für die jeweiligen Kategorien gelten. Andere Aggregationsfunktionen sind vorstellbar, ebenso eine Kombination verschiedener Funktionen.

Da eine solche Gewichtung je nach Aggregation zu höchst unterschiedlichen Ergebnissen führen kann, bedarf es eines gesellschaftlichen Aushandlungsprozesses, an dessen Ende eine politische Entscheidung (im Rahmen geltender Datenschutzbestimmungen) steht. Aus diesem Grund enthalten wir uns im Folgenden konkreter Gewichtungs- und Aggregationsvorschläge.

3.1.1 Datenkategorie

Die DSGVO unterteilt personenbezogene Daten in drei Kategorien: allgemeine personenbezogene Daten, sensible personenbezogene Daten und Daten über strafrechtliche Verurteilungen und Straftaten. „Sensible Daten“ sind gemäß Art. 9 DSGVO personenbezogene Daten, in denen Informationen über ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit enthalten sind. Ebenfalls sensibel sind genetische Daten, sowie biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung. Artikel 10 DSGVO regelt Daten über strafrechtliche Verurteilungen und Straftaten. Alle anderen personenbezogenen Daten können als allgemeine personenbezogenen Daten bezeichnet werden. Auch pseudonymisierte Daten sind personenbezogene Daten. Sie ermöglichen zwar keine direkte Identifizierung einer Person, erfassen aber bspw. das Verhalten einer Person, um zum Beispiel personalisierte Werbung schalten zu können. Bei pseudonymisierten Daten kann es sich sowohl um allgemeine als auch um sensible personenbezogene Daten handeln.

Handelt es sich um sensible Daten, stellt die Datenverarbeitung einen größeren Eingriff in die Privatsphäre dar als die Verarbeitung von allgemeinen Daten. Mit einer solchen Verarbeitung können erhebliche Risiken für die Grundrechte und Grundfreiheiten des Betroffenen entstehen (Erwägungsgrund 51 DSGVO), woraus ein erhöhtes Schutzbedürfnis der inneren persönlichen Lebensbereiche folgt (Matejek und Mäusezahl 2019). Nach Maßgabe der DSGVO müssen für die Verarbeitung von sensiblen Daten daher höhere Anforderungen an die Einwilligung erfüllt sein, damit diese zulässig ist.

Es muss sich in einem solchen Fall um eine *ausdrückliche Einwilligung* handeln. Eine konkludente Erteilung der Einwilligung ist ausgeschlossen, und ein Hinweis auf mögliche, mit der Verarbeitung verbundene Risiken muss erfolgen. Bezogen auf die Angabe des Zwecks oder den Informationsgehalt der Einwilligung ergibt sich aus der DSGVO zwar kein Unterschied aus der Differenzierung zwischen allgemeinen und sensiblen Daten. Nichtsdestotrotz sollte der Eingriff in die Privatsphäre als größer eingestuft werden, wenn Gesundheitsdaten oder biometrische Daten (=sensible Daten) im Gegensatz zu Name und Adresse (=allgemeine Daten) verarbeitet werden.

Des Weiteren könnte auch eine, vom Standpunkt des geltenden Rechts aus nicht vorgesehene, Individualisierung der Zuordnung denkbar sein: Für den einen sind Bankdaten essentiell schutzbedürftig, für den anderen eher die Daten zu Lebensgewohnheiten. Trotzdem zählen sie zu den allgemeinen Daten und werden im Rahmen der DSGVO nicht als sensible Daten eingestuft. Vorstellbar für die Einwilligung wäre, dass die Betroffenen vor der Erteilung der Einwilligung eine Gewichtung der zu erhebenden Daten vornehmen können, unabhängig davon, ob die DSGVO diese Daten als sensibel einstuft oder nicht. Die: Verantwortliche könnte beispielsweise alle Datenkategorien auflisten und die: Betroffene markiert die Datenkategorien, die sie: als besonders schützenswert empfindet. Alle nicht markierten Daten würden im Folgenden wie allgemeine Daten behandelt; alle markierten Daten würden wie sensible Daten behandelt. Alle Einwilligungen, die sich auf die Verarbeitung alsbesonders schützenswert markierter Daten beziehen, bedürften dann einer konkreteren Zweckangabe und eines höheren Informationsgehalts.

Für die Erstellung der Matrix wird die Verarbeitung sensibler Daten und/oder für die Nutzer:in besonders schützenswerter Daten stärker gewichtet als allgemeine Daten bzw. Daten, die nicht von der Nutzer:in als besonders schützenswert markiert wurden. Neben der rein numerischen Gewichtung ist auch ein Mindeststandard vorstellbar, bei dem bspw. die Kategorie mit der geringsten Eingriffstiefe überschritten wird, sobald sensible Daten verarbeitet werden.

3.1.2 Sphärentheorie

Die Sphärentheorie ist eine allgemeine, vom BVerfG in bestimmten Fällen herangezogene Theorie zur Eingriffsgewichtung beim allgemeinen Persönlichkeitsrecht. Alternativ (oder parallel), könnte auch diese Theorie zur Beurteilung des Eingriffs in die Privatsphäre herangezogen werden. Anstatt verschiedene Datenkategorien anhand der Unterscheidung “sensibel/allgemein” zu treffen, werden hier die drei Sphären der Intim-, Privat- oder Sozialsphäre zur Kategorisierung verwendet. Hierbei fordert ein Eingriff in die Intimsphäre den konkretesten Zweck bzw. die Einteilung in die höchste Kategorie, da hier der Kern der Menschenwürde betroffen ist (gmds/GDD 2017). Betrifft der Eingriff hingegen die Sozialsphäre, wären die Angabe eines weniger konkreten Zwecks und weniger Informationen bzw. die Einteilung in eine niedrigere Kategorie ausreichend

(ebd.). Entsprechend der obigen Kategorisierung kann eine Verarbeitung mit Eingriff in die Intimsphäre in einer hohen Gewichtung resultieren, während der Eingriff in die Sozialsphäre gering gewichtet wird. Alternativ sind hier auch verschiedene Mindeststandard-Modelle denkbar.

3.1.3 Aggregation

Der Eingriff in die Privatsphäre hängt zudem von der Aggregation der zu verarbeitenden Daten in Verbindung mit der Anzahl der Datenquellen ab. Können Daten einer Quelle mit Daten einer anderen Quelle verknüpft werden, so stellt dies einen tieferen Eingriff in die Privatsphäre dar, als wenn nur Daten einer Quelle verarbeitet werden. Mit steigender Anzahl *verknüpfter Datenquellen* steigt auch der Eingriff in die Privatsphäre des Betroffenen.

Nicht relevant ist indes die bloße Anzahl an Datenquellen, da diese nur das Potenzial der Aggregation widerspiegeln, aber keine Auskunft zum tatsächlichen Aggregationsvorhaben zulassen. Erhebt NIKA beispielsweise Verhaltensdaten zur Nutzer:in (Quelle 1), müssen diese nicht zwangsläufig auch mit deren Patient:innenakte (Quelle 2) verknüpft werden. Soll dies nachträglich doch noch geschehen, so setzt dies in den meisten Fällen gemäß Art. 6 Abs. 4 DSGVO die Einholung einer neuen Einwilligung voraus. Zweck und Informationsgehalt der neuen Einwilligung könnten dann, unter Berücksichtigung des neuen Aggregationsvorhabens, mithilfe der Matrix entsprechend neu bewertet werden.

Ein schlichter Reinigungs-Roboter, dessen Einsatzbereich die Bodenreinigung ist, nutzt in der Regel weniger Sensorik als ein sozialer Roboter, dessen Einsatzbereich im Gesundheitswesen, z. B. der Altenpflege, liegt. Wie die Grafik von MiRo zeigt (Abb. 1), kommen hier allein sechs Sensoren zum Einsatz, die potenziell 24 Stunden am Tag,

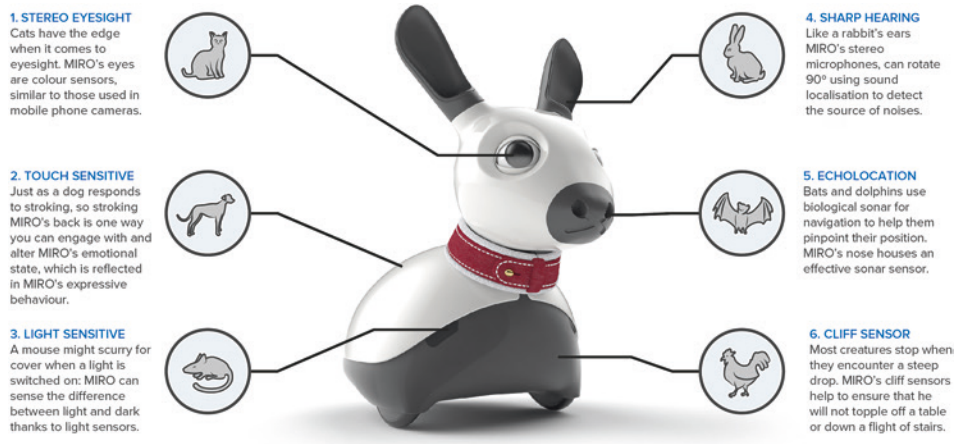

Abb. 1 MiRo's Sensoren (consequentialrobotics.com)

sieben Tage die Woche, Daten verarbeiten. Hier besteht ein weitaus höheres Potenzial zur Datenaggregation. Das Problem hierbei besteht vor allem darin, dass mehrere Datenpunkte ein genaueres Bild über die Lebensumstände und -gewohnheiten, Präferenzen und Überzeugungen, etc. der verdateten Personen (Nutzende und Dritte) ermöglichen. Zu berücksichtigen ist dabei auch, dass durch die Verknüpfung zweier allgemeiner Daten, wie beispielsweise Größe und Gewicht, schnell ein Gesundheitsdatum (BMI) werden kann. Die Verknüpfbarkeit der Daten sollte somit auch bei der Beurteilung der Datenkategorie beachtet werden.

Im Bereich der sozialen Robotik ist die Notwendigkeit der Personalisierung besonders hoch. NIKA muss zum einen in der Lage sein, Akteure in seinem Nahfeld zu erkennen (Bild-/Gesichtserkennung), um besondere Personen wie Nutzer:innen, Pflegekräfte und Angehörige durch die Verarbeitung von Videodaten zweifelsfrei zu identifizieren. Eine persönliche Ansprache der Nutzer:in ist nur möglich, wenn deren biometrische Daten mit ihrem Namen verknüpft werden. Dadurch wird die Privatsphäre der Nutzer:innen stärker beeinträchtigt als durch die des Reinigungsroboters, der mglw. nur Wärme- oder Laserdaten zur Abstandskontrolle verarbeitet.

Zum anderen soll NIKA in der Lage sein, Nutzer:innenprofile anzulegen. Neben der Kamera kann NIKA weitere Sensoren für die Gewinnung von Daten nutzen. Beispielsweise werden Mikrophone zur Spracherkennung eingesetzt, welche über die Erstellung eines Sprachprofiles auch zur Nutzer:innenidentifikation verwendet werden können. Wird dieses Sprachprofil mit anderen personenbezogenen Daten wie bspw. den visuellen biometrischen Daten, den Ergebnissen aus dem „Gedächtnistraining“, den von NIKA nebenbei aufgezeichneten täglichen Routinen oder aber den individuellen mit dem Roboter stattfindenden Interaktionen verknüpft und in einem Nutzer:innenprofil gespeichert, so besteht hier eine engmaschige Dokumentation des Privatlebens in den eigenen vier Wänden und damit ein erheblicher Eingriff in die Privatsphäre.

Eine Verarbeitung mit vielen verknüpfbaren Datenquellen fordert daher den konkretesten Zweck, in der Matrix operationalisiert durch starke Gewichtungen oder Mindeststandards. Betrifft die Verarbeitung hingegen nur eine Datenquelle ohne Verknüpfungsmöglichkeiten, ist die Angabe eines weniger konkreten Zwecks/weniger Informationen bzw. eine niedrige Gewichtung ausreichend.

3.1.4 Erhebungsdauer und -umfang (Big Data)

Für die Ermittlung der Eingriffstiefe ist weiterhin relevant, über welchen Zeitraum hinweg wie viele Daten erhoben werden. Eine Verarbeitung weniger Daten, die nur einmalig und für einen kurzen Zeitraum stattfindet, greift zumeist weniger tief in die Privatsphäre der Betroffenen ein als eine umfangreiche Verarbeitung, die über mehrere Jahre hinweg und rund um die Uhr stattfindet.

Ein Roboter im häuslichen Umfeld könnte den Gesundheitszustand einer Nutzer:in das ganze Jahr permanent überwachen und dabei sowohl Daten zu ihren sportlichen

Aktivitäten, Ernährung und Schlafgewohnheiten aufzeichnen. Im Gegensatz dazu analysiert ein Roboter im Krankenhaus ggf. nur für einen Tag die Bewegungsdaten der Patient:innen, um bei längerer Inaktivität eine Überprüfung des Gesundheitszustandes zu initiieren. Je länger der Roboter Daten über die Betroffenen erfasst, desto größer ist der Eingriff in deren Privatsphäre.

3.1.5 Speicherdauer

Erfasst der Roboter Daten über einen Zeitraum von bspw. 3 Jahren, könnte er diese Daten entweder 3 Jahre lang speichern oder aber auch nur eine Sekunde/Minute/Stunde/etc., um sie entsprechend auszuwerten. Je länger der Roboter etwas über die Nutzer:innen weiß, desto größer ist der Eingriff in die Privatsphäre. Die resultierende Punktzahl steigt daher mit der Speicherdauer.

3.1.6 Empfänger:innen (Anzahl)

Je mehr Datenempfänger:innen es gibt, desto mehr Personen erhalten potenziell Einblick in die personenbezogenen Daten. Mit jeder Empfänger:in steigt die Unsicherheit für alle verdateten Personen darüber, "wer was wann und bei welcher Gelegenheit über sie weiß" (BVerGE 65, 1). Entsprechend wird eine Verarbeitung in Abhängigkeit von der Anzahl der Empfänger:innen in der Matrix jeweils gewichtet.

3.1.7 Anonymisierung

Gibt es die Möglichkeit der Anonymisierung der Daten, so stellt die Verarbeitungstätigkeit ab dem Zeitpunkt der Anonymisierung keinen Eingriff in die informationelle Selbstbestimmung der Nutzenden mehr dar. Allerdings ist die Anonymisierung selbst bereits eine Datenverarbeitung, die u.U. einer Einwilligung und damit einer Zweckangabe bedarf. Dazu kommt die Möglichkeit der De-Anonymisierung, die mit zunehmender Datenverarbeitungsdauer, Anzahl der Datenquellen und -empfänger:innen exponentiell steigt (Narayanan und Shmatikov 2008; Li et al. 2020). Aus diesem Grund ist eine effektive Anonymisierung nicht einfach zu realisieren und zumindest aus juristischer Sicht nach wie vor umstritten (siehe Kapitel von Markus Spitz). Dies sollte sich unseres Erachtens auch bei der Erstellung der Matrix niederschlagen.

Keinen Unterschied sollte es machen, ob die Anonymisierung am Anfang oder erst am Ende einer über mehrere Jahre andauernden Erhebung geschieht. Es wird ein Verarbeitungsvorgang von Anfang bis Ende betrachtet und in der Matrix bewertet. Wird am Ende des Vorgangs eine Anonymisierung durchgeführt, so hat dies eine positive Auswirkung auf die resultierende Gewichtung bzw. Kategorie. Auch wenn die Anonymisierung also erst nach mehreren Jahren stattfindet, bleibt diese positive Auswirkung bestehen, da die drei Jahre nicht-anonymer Datenverarbeitung schon durch das Kriterium der Speicherdauer (und ggf. der Erhebungsdauer und des -umfangs) einen negativen Einfluss auf die resultierende Kategorie haben.

Ähnlich verhält es sich mit der Möglichkeit der De-Anonymisierung, die mit der Menge der Daten exponentiell steigt. Im Rahmen der jeweils relevanten Kategorien wie

“Aggregation/Datenquelle”, “Speicherdauer”, “Empfänger:innen” findet dieser Faktor Berücksichtigung. Da die Möglichkeit der De-Anonymisierung jedoch den meisten Nutzer:innen nicht ausreichend bewusst ist und die Gefahr einer De-Anonymisierung wie schon angedeutet mit zunehmender Speicherdauer, Anzahl der Datenquellen und -empfänger:innen exponentiell steigt, ist hier eine Diskontierung der Gewichtung des Kriteriums “Anonymisierung” über einem bestimmten Grenzwert zu überlegen. Damit könnten bspw. die positiven Gewichtungen einer Anonymisierung bei steigender Datenmenge und Verbreitung im gleichen Umfang herabgesetzt werden, in dem die Gefahr der De-Anonymisierung steigt.

Noch zu erörtern ist, ob auch die Art der algorithmischen Datenverarbeitung gerade mit Blick auf machine learning und tiefe neuronale Netze als eigenständiges Kriterium mit aufgenommen werden sollte. Leider können wir die Frage, inwieweit die Art und Quelle der Entscheidungsfindung (menschliche Entscheidungsträger:innen vs. automatisierte Entscheidungsmechanismen) einen Einfluss auf die Einwilligung in die Datenverarbeitung – und damit auf die Konkretheit der Zweckangabe – hat bzw. haben sollte, im Rahmen dieses Aufsatzes nicht weiterverfolgen.

3.2 Resultierende Zustimmungsmodi

Die Aggregation der Optionen innerhalb der einzelnen Kriterien kann dabei, wie oben schon angedeutet, mittels verschiedener Aggregationsfunktionen erfolgen. Einfache *numerische Gewichtungen* haben den Vorteil, dass hierbei die Kriterien untereinander vergleichbar werden. Je nachdem, wie mit welchen Werten die einzelnen Optionen eines Kriteriums gewichtet werden, entstehen so unterschiedliche Priorisierungen. Der Nachteil besteht darin, dass ein besonders gutes Rating in einer Kategorie ein sehr negatives Rating in einer anderen Kategorie aufwiegen kann. Somit ließe sich also z.B. die Datenerhebung besonders schützenswerter Daten durch eine geringe Anzahl an Datenquellen (besonders Sensoren) ausgleichen. Dies kann u.U. zu nicht wünschenswerten Ergebnissen führen.

Eine andere Aggregationsfunktion setzt bestimmte *Mindeststandards* für eine bestimmte Kategorie fest. So könnte bspw. beim Anlegen eines Nutzer:innenprofils nicht mehr Kategorie 2 erreicht werden. Umgekehrt könnte zum Erreichen von Kategorie 1 die Anonymisierung zwingend erforderlich sein. Diese Aggregationsfunktion hat den Vorteil, dass einzelne sehr erhebliche Eingriffe nicht durch andere positive Ergebnisse wieder wettgemacht werden können. Umgekehrt fehlt es dafür an der Vergleichbarkeit zwischen den einzelnen Kriterien. Daher plädieren wir für eine Kombination aus beiden Aggregationsmodellen. Andere Modelle sind natürlich möglich und Teil eines gesellschaftlich-gesetzgeberischen Aushandlungsprozesses.

Im Ergebnis führt die Aggregation der verschiedenen Kriterien zu einem Ergebnis, welches das jeweilige Datenverarbeitungssystem in eine bestimmte Kategorie (in unserem Bsp. K1-4) einteilt, die jeweils unterschiedliche Zweckangabebedingungen

sowie einen unterschiedlichen Informationsgehalt der Einwilligung nach sich zieht (Tab. 1):

In unserem Beispiel stellt Kategorie 1 einen geringen Eingriff in die Privatsphäre dar und fordert daher nur die Angabe de:r Verantwortlichen sowie die "einfache" Zweckangabe. Kategorie 2 stellt einen moderaten Eingriff in die Privatsphäre dar und fordert sowohl eine "einfache" Zweckangabe, Angaben zu:r Verantwortlichen und zur Datenkategorie als auch die wiederholte Einholung der Einwilligung. Kategorie 3 stellt einen hohen Eingriff in die Privatsphäre dar und würde neben einer konkreten Zweckangabe, der Angabe de:r Verantwortlichen, der Datenkategorie, des Widerrufsrechts der Einwilligung, die Wiederholung der Einwilligung noch ein Dialog-Verfahren erforderlich machen. Kategorie 4 stellt einen sehr hohen Eingriff in die Privatsphäre des Betroffenen dar und er fordert zusätzlich zu den schon genannten Bedingungen die Berücksichtigung der Rahmenbedingungen.

Eine *konkrete Zweckangabe* macht einen höheren Grad an Präzision und Konkretheit der Beschreibung erforderlich. Die Zweckangabe "zum Zweck der Nutzer:innenidentifikation" beispielsweise gibt keinen Aufschluss darüber, welche Daten verarbeitet werden, wie lange diese gespeichert werden, ob sie ggf. mehrfach ausgewertet werden, ob dafür die Bildung eines Nutzer:innenprofils vorgesehen ist und welche Risiken mit der Verfolgung des Zwecks einhergehen. Daher sollte bei der konkreten Zweckangabe auf eben diese Punkte eingegangen werden: Es sollte angegeben werden, ob die Daten mehrfach ausgewertet, dauerhaft gespeichert oder gar Nutzer:innenprofile gebildet werden sollen.

Die *Wiederholung der Einwilligung* (Re-consent) muss bei einem intensiven Eingriff in die Privatsphäre häufiger erfolgen als bei einem geringen Eingriff und stellt so sicher, dass Betroffene an schwerwiegende Eingriffe wiederholt erinnert werden und sie diese überdenken können, ohne selbst mittels Widerruf aktiv werden zu müssen (aA Martini 2014, der eine zeitliche Begrenzung der Einwilligung bei Big Data Verarbeitungen vorschlägt).

Das *Dialog-Verfahren* soll die Belastung der Betroffenen durch das Mehr an Informationen ausgleichen. Vorstellbar ist, dass der Roboter den Betroffenen mündlich

Tab. 1 Privacy-Interference-Matrix

	Zweckangabe	Wiederholung der Einwilligung	Dialogverfahren	Rahmenbedingungen	Informationsgehalt
K1	einfach	-			Zweck und Verantwortlicher
K2	einfach	1×/Jahr			+ Datenkategorie
K3	konkret	1×/Monat	×		+ Widerrufbarkeit
K4	konkret	1×/Woche	×	×	+ Risiken bei Datentransfer

(und ggf. zusätzlich schriftlich) strukturierte Informationen rund um die Einwilligung erteilt und sich im Rahmen eines Dialoges die Verständlichkeit der Informationen bestätigen lässt, ggf. Fragen der Betroffenen dazu beantwortet und abschließend die Einwilligung einholt.

Durch die *Berücksichtigung der Rahmenbedingungen*, die bei der Einholung der Einwilligung vorliegen, soll vermieden werden, dass die Betroffenen ihre Einwilligung erteilen, ohne dieser tatsächlich Aufmerksamkeit zu schenken, weil – wie unter 2.1 dargestellt – ihr "cognitive load" durch mehrere gleichzeitige Tasks so erhöht ist, dass sie den ihnen präsentierten Informationen kaum Aufmerksamkeit schenken können.

Werden Daten in großem Umfang miteinander verknüpft bzw. verarbeitet (Big Data), so könnte, unabhängig von der resultierenden Kategorie, die Verwendung eines Kaskadenmodelles bzw. ein zweistufiges Verfahren für die Einwilligung vorgesehen werden. Wie es bereits bei Einwilligungen im Forschungsbereich gehandhabt wird, könnten auch hier die Betroffenen in einem ersten Schritt der Verarbeitung der Daten zustimmen. In einem zweiten Schritt könnten sie dann der Verwendung der Ergebnisse der Datenanalyse für einen bestimmten Zweck zustimmen oder sie verweigern (Schulz 2018). Im letztgenannten Fall müssten anschließend die Analyseergebnisse gelöscht werden.

4 Ergebnisse für NIKA

Für die Interaktion mit NIKA ergeben sich hieraus mehrere Erkenntnisse, die für die Gestaltung der informierten Einwilligung wichtig sind. Zunächst einmal wird deutlich, dass die tägliche Interaktion schon einen erheblichen Eingriff in die Privatsphäre insbesondere von Nutzenden, aber auch Dritten, mit sich bringt. Die Aufzeichnung biometrischer Daten wie Gesicht oder Stimme zur Personenerkennung, deren dauerhafte Speicherung in einem Nutzer:innenprofil, sowie die sensorische Orientierung im häuslichen Umfeld – und damit im privaten Bereich der Nutzenden – erfordern für sich genommen, aber besonders in der Kombination (Datenquellen, Aggregierbarkeit der Daten) eine sehr spezifische Zweckangabe. Diese müsste, um den "cognitive load" der ohnehin vulnerablen Gruppe älterer Nutzenden nicht unnötig zu erhöhen, in einem ersten Schritt mindestens in ruhiger Umgebung und u.U. mittels eines "Kaskadenmodells" erfolgen, d.h. in inkrementellen Schritten im spezifischen Kontext der jeweiligen Zwecke.

Ganz besonderes Augenmerk ist darauf zu richten, wenn nicht nur NIKA selbst die gesammelten Daten zur Orientierung und Interaktion verarbeitet, sondern diese an weitere Datenempfänger:innen wie Pflegekräfte, Therapeut:innen oder Ärzt:innen weitergibt. Da NIKA nolens volens viele Lebensgewohnheiten der Nutzenden dauerhaft aufnimmt (Ess-, Trink-, und Schlafgewohnheiten, sportliche Aktivitäten etc.), lassen sich diese medizinisch relevanten Daten leicht zu sensiblen – d. h. vor allem medizinischen – Daten aggregieren und sogar in diachroner Perspektive im Längsschnitt Gesundheitsentwicklungen verfolgen. Hier müssen sehr klare Zweckangaben zur Datensammlung erfolgen, die auch regelmäßig erneuert werden müssen (Re-consent).

Darüber hinaus wird deutlich, dass auch innerhalb der eigenen Wohnung unterschiedlich sensible Bereiche bestehen. Die Sphärentheorie macht deutlich, dass Badezimmer oder Toilette als Intimsphäre besonders zu schützen und hier u.U. gesonderte Einwilligungen einzuholen sind. Während aus einer Usability-Design-Perspektive die "seamless interaction" (Hassenzahl 2008) ein zentrales Designziel darstellt, wird mittels der Privacy-Interference-Matrix sichergestellt, dass mit der Konkretisierung der Zweckangabe ein weiteres Designziel ebenbürtig hinzutritt: Design for Privacy (Fronemann et al. 2021). Durch die Minimierung potenzieller Ablenkungen und Störungen, aber auch durch eine disruptive Durchbrechung der "seamless interaction", um Aufmerksamkeit zu generieren, konkrete Zweckangaben zu machen und eine informierte Einwilligung einzuholen, schließt die Matrix nicht nur eine juristische Lücke, sondern erweitert gleichzeitig das traditionelle Designziel in der Mensch-Maschine-Interaktion.

Literatur

Ammicht Quinn, R (2019) Zwischen Fürsorge und Kontrolle. Ethische Überlegungen zu Techniken für ein gutes Alter. EthikJournal 5(1):1–20

Behrendt H, Loh W, Matzner T, Misselhorn C (Hrsg) (2019) Privatsphäre 4.0. Metzler, Stuttgart

Borchers JO (2000) A pattern approach to interaction design. In: Proceedings of the 3rd international conference on designing interactive systems: processes, practices, methods, and techniques, S 369–378

Cavoukian A (2011) Privacy by design. The 7 Foundational Principles. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwibiYqd7I3eAhXH_qQKHZOLAggQFjABegQIBxAC&url=https%3A%2F%2Fwww.ipc.on.ca%2Fwp-content%2Fuploads%2FResources%2FPbDReport.pdf&usg=AOvVaw3RcmBfwcjjE1k2ILAmHHx-. Zugegriffen: 17 Okt. 2018

Charland LC (2008) Decision-Making Capacity. https://plato.stanford.edu/entries/decision-capacity/, Zugegriffen: 15. Nov. 2018

Calo R (2012) Robots and privacy. In Lin P, Abney K, Bekey GA (Hrsg) Robot ethics. The ethical and social implications of robotics. MIT Press, Cambridge, S 187–202

Darling K (2017) Who's Johnny? Anthropomorphic framing in human-robot interaction, integration, and policy. In: Lin P, Abney K, Jenkins R (Hrsg) Robot Ethics 2.0. New challenges in philosophy, law, and society. Oxford Univ Press, S 173–188

Der Bayerische Landesbeauftragte für Datenschutz (2018) Die Einwilligung nach der DSGVO, S 5. https://www.datenschutz-bayern.de/datenschutzreform2018/einwilligung.pdf. Zugegriffen: 7. Okt. 2020

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (gmds) und Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD) (2017) Datenschutzrechtliche Anforderungen an die medizinische Forschung unter Berücksichtigung der EU-Datenschutz-Grundverordnung (DS-GVO), S 11. https://www.gesundheitsdatenschutz.org/download/forschung_ds-gvo.pdf. Zugegriffen: 7. Okt. 2020

DIN EN ISO 9241-11 (2018) Ergonomics of human-system interaction. Usability – Definitions and concepts. https://www.iso.org/standard/63500.html. Zugegriffen: 2. Okt. 2020

DIN EN ISO 9241-110 (2020). Ergonomics of human-system interaction — Part 110: Interaction principles. https://www.iso.org/standard/75258.html. Zugegriffen: 2. Okt. 2020

Drury JL, Hestand D, Yanco HA, Scholtz J (2004) Design guidelines for improved human-robot interaction. In CHI'04 extended abstracts on human factors in computing systems, S 1540

Dworkin G (1988) The theory and practice of autonomy. Cambridge University Press, Cambridge

Elgin C (2017) True enough. MIT Press, Cambridge

EDPB (2020) European Data Protection Board – Guidelines 05/2020 on consent under Regulation 2016/679. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Zugegriffen: 29. Sept. 2020

Europäische Kommission (2020) Weissbuch. Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, S 24. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_de.pdf. Zugegriffen: 7. Okt. 2020

Eyal N (2011) Informed consent. https://plato.stanford.edu/entries/informed-consent/. zuletzt aktualisiert am 16. Jan. 2019, zuletzt geprüft am 15. Nov. 2018

Frankfurt H (1987) Identification and wholeheartedness. In: Schoeman F (Hrsg) Responsibility, character, and the emotions: new essays in moral psychology. Cambridge University Press, Cambridge, S 27–45

Fronemann N, Loh W, Pollmann K (2021) Should my robot know what's best for me? In: AI & Society, Online First

Gorin M (2014) Towards a theory of interpersonal manipulation. In: Coons C, Weber M (Hrsg) Manipulation. Theory and practice. Oxford Univ. Press, Oxford, S 73–97

Hauser A, Haag I (2019) Einwilligungen. In: Hauser A, Haag I (Hrsg) Datenschutz im Krankenhaus- mit allen Neuerungen durch die DSGVO. Deutsche Krankenhausverlagsgesellschaft mbH, Düsseldorf, S 39

Habermas J (2009) Vorlesungen zu einer sprachtheoretischen Grundlegung der Soziologie. In Habermas J (Hrsg) Sprachtheoretische Grundlegung der Soziologie. Suhrkamp (Philosophische Texte, 1), Frankfurt a. M. S 29–156

Hassenzahl M (2008) User experience (UX). Towards an experiential perspective on product quality. In ACM International Conference Proceeding Series 339. https://doi.org/10.1145/1512714.1512717

Kahn PH, Freier NG, Kanda T et al (2008) Design patterns for sociality in human-robot interaction. In: Proceedings of the 3rd ACM/IEEE international conference on Human robot interaction, S 97–104

Kant I (AA V) Kritik der praktischen Vernunft. Akademie-Ausgabe Band V, Berlin 1903

Korsgaard CM (2009) Self-constitution. Agency, identity, and integrity. Oxford University Press, Oxford

Li H, Chen Q, Zhu H, Di M, Wen H, Shen XS (2020) Privacy leakage via de-anonymization and aggregation in heterogeneous social networks. IEEE Trans Dependable Secure Comput 17(2):350–362. https://doi.org/10.1109/TDSC.2017.2754249

Litman-Navarro K (2019) We Read 150 Privacy Policies. They Were an Incomprehensible Disaster. In: New York Times, 12.Mai 2019. https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html. Zugegriffen: 16. Sept. 2019

Loe J, Robertson CT, Winkelman DA (2015) Cascading consent for research on biobank specimens. Am J Bioethics 15(9):68–70

Loh W (i. Ersch.) Level Up? Zur Gamifizierung von Fitness- und Gesundheits-Apps. In: Ring-Dimitriou (Hrsg) Aktives Altern im digitalen Zeitalter, Springer

Maclean A (2009) Autonomy, informed consent and medical law. A relational challenge. Cambridge University Press, Cambridge

Martini M (2014) Big Data als Herausforderung für den Persönlichkeitsschutz und das Datenschutzrecht. In: DVBI 2014, S 1486

Matejek M, Mäusezahl S (2019) Gewöhnliche vs. sensible personenbezogene Daten. Zeitschrift für Datenschutz, S 551–556

Moos F, Schefzig J, Arning M (Hrsg) (2018) Die neue Datenschutz-Grundverordnung. Praxishandbuch, 1. Aufl, Deutscher Fachverlag GmbH, Berlin., C.5.Rn. 175

Narayanan A, Shmatikov V (2008) Robust de-anonymization of large sparse datasets. In: Proceedings of the 2008 IEEE symposium on security and privacy. Oakland CA, 18.05.2008. Institute of Electrical and Electronics Engineers; Computer Society; International Association for Cryptologic Research. IEEE, Piscataway, S. 111–125

O'Connor Y, Rowan W, Lynch L, Heavin C (2017) Privacy by design. Informed consent and internet of things for smart health. Procedia Comput Sci 113:653–658

Parfit D (1984) Reasons and persons. Clarendon, Oxford

Pollmann K (2019) Behavioral design patterns for social, assistive robots. In: Mensch und Computer Workshopband

Rost M, Nast R, Elger BS, Shaw D (2020) Trust trumps comprehension, visceral factors trump all: a psychological cascade constraining informed consent to clinical trials: a qualitative study with stable patients. Research Ethics. https://doi.org/10.1177/1747016120914335

Rudinow J (1978) Manipulation. Ethics 88(4):338–347

Scheutz M (2012) The inherent dangers of unidirectional emotional bonds between humans and social robots. In: Lin P, Abney K, Bekey GA (Hrsg) Robot ethics. The ethical and social implications of robotics. MIT Press, Cambridge, S 205–222

Schulz (2018) Bedingungen für die Einwilligung. In: Gola (Hrsg) Datenschutz-Grundverordnung – Kommentar, 2. Aufl, Art. 7 Rn. 35

Steinrötter B (2020) Datenschutzrechtliche Implikationen beim Einsatz von Pflegerobotern. Frühzeitig eingeholte Einwilligungen als Schlüssel für zulässige Geriatronik-Anwendungen. In: ZD 2020, S 336–340

Susser D, Rössler B, Nissenbaum H (2019) Technology, autonomy, and manipulation. Internet Policy Rev 8(2):1–22

Tidwell J (2010) Designing interfaces. Patterns for effective Interaction Design. O'Reilly Media Inc, Canada

Turkle S (2010) In good company? On the threshold of robotic companions. In Wilks Y (Hrsg) Close engagements with artificial companions. Key social, psychological, ethical and design issues. John Benjamins, Philadelphia, S 3–10

Wood A (2014) Coercion, manipulation, exploitation. In: Coons C, Weber M (Hrsg) Manipulation. Theory and practice. Oxford Univ. Press, Oxford S 17–50