finanziert vom

Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

KIRaPol.5G

Code of Practice

Mögliche Vorgehensweisen für die Entwicklung von ELSI-Bewertungen im Kontext von Beobachtungstechnologien

Arbeitspapier im Projekt KIRaPol.5G

Künstliche **I**ntelligenz für **Ra**darsysteme zur Unterstützung von **pol**izeilichen Überwachungen auf öffentlichen Plätzen und Bahnhöfen

Erstellt von Monika Eigenstetter und Fatma Dönmez im Dezember 2024

Hochschule Niederrhein
University of Applied Sciences

Inhaltsverzeichnis

1 Einleitung

1.1 Das Projekt KIRAPol.5G

Mit dem Projekt KIRAPol.5G wurde an einer KI-gestützten Radartechnologie geforscht, die am Ende eine Verminderung der Beobachtungslast im öffentlichen Raum zur Folge haben und gleichzeitig die Persönlichkeitsrechte der Bürgerinnen und Bürger besser gewährleisten soll. Ziel des Forschungsprojekts KIRaPol.5G ist daher Radartechnologie unter Nutzung von künstlicher Intelligenz (KI) zu nutzen, um unter Gewährleistung von Persönlichkeitsrechten öffentliche Räume beobachten zu können, und in potenziell gefährlichen Situationen die Polizei-Leitstelle für eine Einleitung geeigneter Maßnahmen zu alarmieren. KIRaPol.5G hat eine Laufzeit vom 01.01.2022 bis zum 31.12.2024 und ist gefördert vom Ministerium für Wirtschaft, Industrie und Klimaschutz in Nordrhein-Westfalen.

Die Entwicklung einer KI-gestützten Radartechnologie bietet gegenüber der herkömmlichen Videobeobachtung eine Reihe von Vorteilen[1]. Die Radartechnologie erzeugt Spektren anstelle von Bildern, und verbessert damit den Datenschutz. Radar ist weniger anfällig für Umwelteinflüsse wie Dunkelheit und Wetter. Die Technologie ermöglicht eine effizientere Erkennung und Erfassung von Objekten über größere Entfernungen und kann mehrere Objekte gleichzeitig verarbeiten. Die Kombination von KI und Radartechnologie kann daher die Beobachtungstätigkeiten unterstützen.

Für eine Bewertung der Datenschutzverbesserungen durch Radartechnologie ist ein grundlegendes Verständnis ihrer Funktionsweise erforderlich. Radarsensoren emittieren (wie Fledermäuse) hochfrequente Signale, deren Reflektion durch Objekte und Personen eine Frequenzänderung bewirkt. Bei in Bewegung befindlichen Objekten oder Personen wird zudem ein so genannter Doppler-Effekt erzeugt, eine Stauchung oder Dehnung dieses Signals. Diese physikalischen Effekte erlauben über die Auswertung der emittierten Mikro-Doppler-Spektren, Bewegungen systematisch zu differenzieren: z.B. normales Gehen, Schlägerei, Weglaufen, ...). Die Daten werden über ein 5G-Mobilfunknetz an eine zentrale Einheit übertragen, wo eine KI die Radardaten klassifiziert. Detektiert die KI eine potenziell gefährliche Situation, warnt sie. In Abbildung 1 sind drei beispielhafte Szenen dargestellt, die mit einem Radarsensor aufgenommen und als Mikro-Doppler-Spektren ausgegeben wurden.

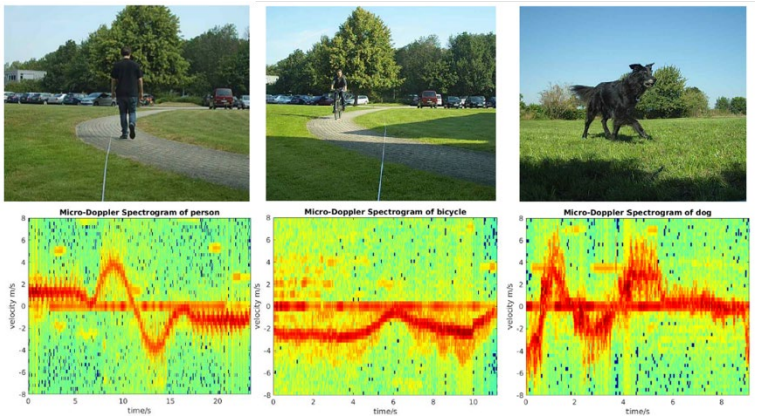

Abbildung 1. Mikro-Doppler-Spektren drei unterschiedlichen Szenen (Hirsch, Stahler, Hagelen & Kulke, 2020)

[1] Hirsch, H.-G., Stahler, J., Hagelen, M., Kulke, R. (2020). Analyzing the classification capabil-ity of Micro-Doppler spectra. In: 2020 IEEE Radar Conference (RadarConf20). 2020 IEEE Radar Conference (RadarConf20), Florence, Italy, 21.09.2020 - 25.09.2020, pp. 1–6. IEEE https://doi.org/10.1109/RadarConf2043947.2020.9266685

Die Ziele, die in diesem Projekt formuliert wurden und mit der entwickelten KI-gestützten Radartechnologie erreicht werden sollen, sind von großer Bedeutung und dürfen nicht vernachlässigt werden. Mit dem Fortschreiten der Digitalisierung nehmen auch die Bedenken hinsichtlich des Datenschutzes zu, was zu Widerständen gegen technologische Innovationen wie die gesichtserkennende Videobeobachtung führt[2]. Daher ist es entscheidend, für den öffentlichen Raum eine Technologie zu entwickeln, die sowohl die Sicherheit der Bevölkerung gewährleistet als auch die Datenschutzbedenken durch eine reduzierte Beobachtung adressiert. Auch wenn es naheliegend erscheint, dass eine solche Technologie sinnvoll und schnell eingeführt werden sollte, können im Kontext einer ELSI-Bewertung unvermutete Nebenwirkungen deutlich werden: ELSI steht für ethischen, legislativen, sozialen Implikationen. Insofern ist es sinnvoll, grundsätzlich jede neue Technologie einem Risikocheck zu unterwerfen.

Letztlich geht zentral um Menschenrechte im Kontext der Technikentwicklung sicherzustellen.

1.2 Ziele und Struktur des Leitfadens: ELSI-Bewertung

Dieser Leitfaden soll als Code of Practice eine exemplarische ELSI-Bewertung im Kontext der Beobachtungstechnologien nachvollziehbar machen. Datenschutz

Eine auf KI basierende Technikentwicklung sollte zwingend auf einen humanzentrierten Entwicklungsprozess fußen. Eine umfangreiche Stakeholder-Analyse ist die Basis, um mit weiteren Methoden (z.B. Befragungen und/oder Workshops) Akzeptanz und Kommunikationsstrategien für die Beteiligung verschiedener Stakeholder zu entwickeln (Kapitel 2 und 3).

Der Leitfaden integriert wissenschaftliche Perspektiven mit praktischen Vorgehensweisen, um ein der Komplexität der neuen Technologie angemessene Bewertung entlang ethischer, legaler und sozialer Implikationen (ELSI) zu ermöglichen.

- Ethische Implikationen: Eine ethisch reflektierte Technikentwicklung kann z.B. nach den Schritten entlang der nach ISO/IEC/IEEE 7000 erfolgen. Für eine umfassende Verantwortung der Unternehmen können weitere Facetten der gesellschaftlichen Verantwortung als Corporate Digital Responsibility einfließen (Kapitel 4).
- Legale Implikationen: Es werden die rechtlichen Grundlagen und rechtlich notwendigen Schritte vorgestellt, um nach den Vorgaben der Datenschutzgrundverordnung (DGSVO) eine Datenschutzfolgenabschätzung vorzunehmen und rechtlichen Vorgaben Folge zu leisten (Kapitel 5).
- Soziale Implikationen: Ob derartige Technologien in den Einsatz kommen können, ist abhängig von der Akzeptanz bei Nutzenden (z.B. Polizei, Überwachungsdienste) aber auch diesem Fall der möglichen Nutznießenden der Technik, nämlich Bürgerinnen und Bürger (Kapitel 6).

[2] Reclaim Your Face: The future must be ours to shape. https://reclaimyourface.eu/. Accessed 15 January 2025

2 Die soziotechnische Perspektive

Eine auf KI basierende Technikentwicklung braucht einen humanzentrierten Entwicklungsprozess. Im Folgenden werden die Vorteile einer auf den Menschen hin optimierten Technik dargestellt. Technische Systeme sind in der Regel in größere Zusammenhänge eingebettet. Gesetze und Regeln sowie gesellschaftliche Erwartungen spielen eine große Rolle für die Akzeptanz. Und gerade bei Beobachtungs- und Überwachungstechnologien im öffentlichen Raum sind dem Einsatz enge Grenzen gesetzt. Der Datenschutz muss gewährleistet werden, ethische Aspekte müssen beachtet werden, vor allem dann wenn ein Einsatz von Künstlicher Intelligenz geplant ist. Eine umfangreiche Stakeholder-Analyse ist die Basis, um später mit weiteren Methoden (z.B. Befragungen und/oder Workshops) Akzeptanz und Kommunikationsstrategien für die Beteiligung verschiedener Stakeholder zu entwickeln. Die soziotechnische Perspektive ist die Basis auch für die ethischen, legalen und sozialen Implikationen.

2.1 Technik für den Menschen

Ein soziotechnisches System besteht aus mehreren miteinander verbundenen Komponenten, die sowohl technische, organisatorische und personenbezogene Aspekte umfassen. Zudem ist das soziotechnische System in eine Regulatorik eingebunden.

Die technischen Komponenten beziehen sich auf die physischen und digitalen Technologien, die innerhalb des Systems genutzt werden. Dazu gehören Hardware, die Maschinen, Geräte, IT-Infrastruktur, die eingesetzte Software mit ihren Algorithmen und Benutzerschnittstellen, sowie die Daten und Informationen, die gesammelt und verarbeitet werden.

Die sozialen Komponenten umfassen Menschen, die mit den technischen Systemen interagieren, sowie die soziale Organisation, die dazu erforderlich ist, um mit Hilfe der Technik z.B. eine Aufgabe zu erfüllen. Zur Organisation gehören die Art und Weise, wie Arbeit organisiert und koordiniert wird, Zusammenarbeit, Feedback und Entscheidungswege, Hierarchien und Verantwortlichkeiten.

Eine soziotechnische Perspektive ist entscheidend für die Technologieentwicklung, weil sie sowohl technische als auch soziale Faktoren berücksichtigt. Zentrale Gründe sind:

- Mensch-Technik-Interaktion optimieren: Technische Lösungen sollten in schrittweisen Prozessen menschzentriert gestaltet werden, um damit an menschliche Bedürfnisse, Fähigkeiten und Verhaltensweisen angepasst zu werden. Dies ist zentral für Nutzendenfreundlichkeit und so genannte User Experience. Rein technikgetriebene Lösungen können scheitern, wenn sie nicht mit bestehenden sozialen Strukturen harmonieren.
- Technikakzeptanz sicherstellen: Technologien sind nur erfolgreich, wenn sie akzeptiert werden. Nur wenn der Nutzen erkannt wird, oder sich die Technologien gut Aktivitäten einpassen lassen ohne lange umlernen zu müssen oder sich beeinträchtigt zu fühlen, kann Akzeptanz gefördert werden.
- Nachhaltigkeit und ethische Verantwortung erhöhen: Technische Innovationen haben vielfältige gesellschaftliche Auswirkungen. Ethische Fragen betreffen z. B. Datenschutz, Diskriminierung oder Umweltauswirkungen. Technische Systeme sind immer in soziale, wirtschaftliche und politische Strukturen eingebettet. Eine isolierte technische Entwicklung erzeugt meist unbeabsichtigte Folgen.

2.2 Menschzentrierte Technikentwicklung als zentraler Aspekt der soziotechnischen Systemgestaltung

Digitalisierungsprozesse nutzen häufig den Ansatz des Human Centered Design nach der ISO 2410-210. Eine systematische Einbindung der zukünftigen Nutzerinnen und Nutzer spezifischer Technologien in eine sozitechnische Systementwicklung ermöglicht eine Anpassung der Technik an soziale Erwartungen und spezifisches Vorwissen der Nutzenden.

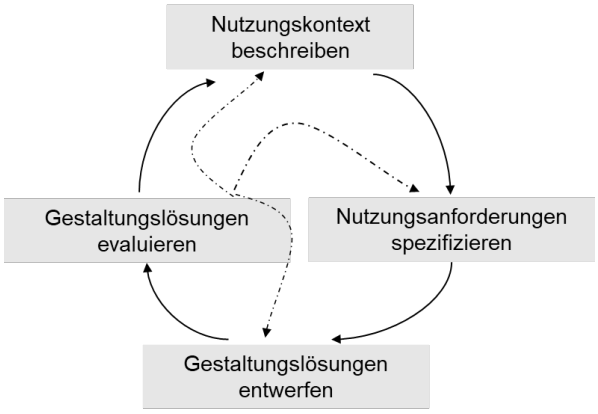

Abbildung 2. Human Centered Design

Das Vorgehen nennt vier Phasen, die den Technikentwicklungsprozess strukturieren (siehe Abbildung 2).

1. Verstehen und Beschreiben des Nutzungskontexts: „Was soll so ein System leisten?“ Ein Verstehen des Nutzungskontextes umfasst z.B. eine Kontextanalyse. Wer nutzt das System in welcher Umgebung? Welche Umgebungsbedingungen bestehen (Licht, Lärm, …). Sind die Nutzenden Expertinnen und Experten?
2. Definieren der Nutzungsanforderungen: „Wer soll was tun?“ Rollen im System werden definiert, die Anforderungen werden konkretisiert. Wer soll die Technik kontrollieren?
3. Entwerfen der Gestaltungslösungen: „Wie soll das System im Interface designt werden?“ Verschiedene Gestaltungslösungen werden mit Story Boards und Skizzen veranschaulicht und diskutiert.
4. Testen und Evaluieren der Lösungen: „Wie tauglich ist das System in der konkreten Anwendung?“ Mock-ups werden Nutzerinnen und Nutzern vorgestellt, um frühzeitig ein Feedback einzuholen und für die weitere Entwicklung nutzbar zu machen. Die Evaluation wird begleitend zum Entwicklungsprozess durchgeführt und erfährt möglichweise einige Iterationen von Entwurf bis zur Fertigstellung der Anwendung.

In diesem Projekt war die Polizei von vorneherein als mögliche zukünftige Nutzende dieser Technologie als Co-Creator und Partner integriert. Die Polizei definierte die Use Cases der Anwendung (Nutzungskontext) und half weitere Nutzungsanforderungen zu spezifizieren. Da das Projekt insgesamt die Möglichkeit der Entwicklung und Anwendung der oben genannten Technologie prüfte, wurden noch keine Gestaltungslösungen entworfen. Bürgerinnen und Bürger werden als Nutznießende nach ihren Befürchtungen qualitativ befragt (siehe soziale Implikationen).

3 Die Rolle der Stakeholder in der Technikentwicklung

Stakeholder sind die Personen und Interessengruppen, die im Zusammenhang mit dem Unternehmen stehen und von deren Handeln betroffen sind. Allen Stakeholdern ist gemein, dass diese Ansprüche an Projekte oder Unternehmen haben und eigene Interessen in diesem Kontext besitzen. Auch all jene Personen, die unmittelbar oder mittelbar vom Handeln des Unternehmens betroffen sind, sind Stakeholder: als Kundin oder Kunde, als Anwohnenden usw. Hinter dem Stakeholder-Ansatz steckt die Idee, dass die Berücksichtigung vielfältiger Interessen hilft, Produkte und Prozesse auf die Bedürfnisse der Betroffenen zu entwickeln, und damit z.B. Akzeptanz oder Nachfrage geschaffen werden kann.

3.1 Stakeholder für die Entwicklung von Beobachtungstechnologien

Stakeholder sind von der Technikentwicklung Betroffene: das sind z.B. die Personen, die die Technik benutzen, entwickeln, oder auch Aufsichtsbehörden. Eine Analyse und ein Verstehen der ist ein integraler Bestandteil von Projekten, Businessmodell-Entwicklung, von Designprozessen aller Art, oder auch von Evaluation.

Für die Entwicklung von Beobachtungstechnologien im öffentlichen Raum gibt es viele Stakeholder. Dazu zählen z.B. als große Stakeholder-Gruppen die öffentlichen Institutionen wie Aufsichtsbehörden, Gesellschaft und Öffentlichkeit, die von der Technologie erfasst werden, die Wissenschaft mit ihrem Forschungs- und Erkenntnis-Interesse sowie die Unternehmen, die die Technologie anbieten und vermarkten wollen. Alle diese Stakeholder haben eigene Interessen und Befürchtungen, die im Vorfeld der Technikentwicklung Berücksichtigung finden sollen (Tabelle 1).

Tabelle 1. Stakeholder-Analyse: Beispielhafte Betroffene mit Interessen und Befürchtungen (ohne Anspruch auf Vollständigkeit, eigene Übersicht)

Stakeholder	**Interessen: Beispiele**	**Befürchtungen: Beispiele**
Gesetzgeber: national, EU	Regulator, Einhaltung grenzüberschreitender Sicherheitsstandards	Missachtung der gesetzlichen Standards, fehlende Kontrolle
Technische Normierungsorganisationen (z. B. ISO, IEEE)	Freiwillige Selbstregulation, Verlässliche Sicherheits-standards für die Anwender von Beobachtungs-technologien	Langwierige, problembehaftete Prozesse, Angst vor Überregulierung
Kommunen & Stadtverwaltungen	Smart-City-Konzepte für ein erhöhtes Sicherheitsgefühl vor Ort	Widerstand anderer Stakeholder gegen die geplanten Maßnahmen
Polizei & Sicherheitsbehörden	Anwender, Kriminalitäts-prävention und -aufklärung	Verlust von Vertrauen in der Bevölkerung durch vermehrte Überwachungstechnologien
Datenschutzbehörde	Sicherstellen der Datenschutzmaßnahmen nach DSGVO, Schutz demokratischer Grundrechte	„Feindbild“ der Gesellschaft, Missbräuchliche Verwendung von Daten

Tabelle 1 Fortsetzung. Stakeholder-Analyse: Beispielhafte Betroffene mit Interessen und Befürchtungen (ohne Anspruch auf Vollständigkeit)

Bürgerinnen und Bürger	Nutznießende, Schutz der Privatsphäre und Grundrechte, Schutz vor Gewalttaten	Fehleranfällige Technologien, „falsches“ Sicherheitsgefühl
Medien	Aufklärung	Verheimlichen von Informationen, Fehlinformation
Bürgerrechtsorganisationen & NGOs	Schutz der Persönlichkeitsrechte, der Menschenrechte und der Transparenz, Schutz demokratischer Grundrechte	Staatlicher Missbrauch von Daten, Datendiebstahl, Cyber Crime
Personen aus der Wissenschaft	Entwicklung neuer Technologien für die Gesellschaft, Erkenntnisinteresse	Starre Regulierung, die den Erkenntnisfortschritt behindert
Unternehmen: Hardware-, Software- und KI-Anbietende	Marktliches Interesse	Misstrauen aus der Bevölkerung, Reputationsverlust
Betreiber öffentlicher Infrastrukturen	Bereitstellen der Technologien, geringer Wartungsaufwand,	Cyber Crime, Beschädigung, Vandalismus
Versicherungen & Sicherheitsfirmen	wirtschaftliche Interessen am Einsatz von Sicherheits- und Überwachungslösungen.	Fehlalarme, vermehrte Einsätze
Gesetzgeber: national, EU	Einhaltung grenzüberschreitender Sicherheitsstandards	Missachtung der gesetzlichen Standards, fehlende Kontrolle
Technische Normierungsorganisationen (z. B. ISO, IEEE)	Verlässliche, freiwillige Sicherheitsstandards für die Anwender von Beobachtungstechnologien	Langwierige, problembehaftete Prozesse

3.2 Personas aus Stakeholder-Analysen entwickeln

Personas können auf Basis von Stakeholder-Analysen entwickelt werden, um die Bedürfnisse, Erwartungen und Bedenken der verschiedenen Akteure greifbar und verständlich zu machen. Ein Stakeholder wird ~~ja~~ oft recht abstrakt beschrieben (z.B. Medien, Bürgerinnen und Bürger, siehe Tabelle 1). Als Persona, als ausgestaltete prototypische Person, werden sie anschaulich für Entwicklerinnen und Entwickler. Persona stehen als stellvertretende Charaktere mit Namen, Zielen und Sorgen für eine Gruppe. So kann man sich besser in ihre Perspektive hineinversetzen. Als Beispiel für eine Persona mag „die Bürgerin Anna“ gelten

Kasten 1. Persona „Bürgerin Anna“

Anna, 32, ist Mutter von zwei Kindern (acht und zwölf Jahre alt), die als Medienwissenschaftlerin gebildet, Wert auf Datenschutz legt. Gleichzeitig wünscht sie sich aber auch mehr Sicherheit im Stadtpark. Sie ist halbtags berufstätig und ist in der Freizeit gerne mit den Kindern draußen. Sie bedauert, dass viele Drogenabhängige die Grünflächen verunreinigen. Die herumliegenden Spritzen sieht sie als Gefahr für ihre Kinder.

Mit Personas lassen sich Technologien passender für die Zielgruppen entwickeln, da sie helfen, konkrete Anwendungsfälle und Probleme zu identifizieren. Zudem erleichtern sie die Kommunikation mit Teammitgliedern oder Entscheidungsträgern, da Erwartungen und Befürchtungen in die Personas modelliert werden können. Eine Stadtverwaltung hat andere Erwartungen an Beobachtungstechnologien als eine Bürgerrechtsorganisation. Eine Persona für den Datenschutzbeauftragten hilft, dessen Anforderungen klar zu verstehen. Es lassen sich mögliche Konflikte besser vorhersehen und mögliche Lösungen besser vorausdenken.

Es können auch weitere Fragen anhand von Stakeholder-Analysen beantwortet werden: Welche Aufgaben übernehmen sie im System? Sind mit den Aufgaben Verantwortlichkeiten verbunden? Werden diese Verantwortlichkeit vermutlich wahrgenommen, und wenn nein, warum nicht? Können durch die Technologien nicht intendierte Nebenwirkungen entstehen? (z.B. Zunahme von Misstrauen in der Bevölkerung).

Mit solchen Personas können auch die ethischen Implikationen und Werte herausdefiniert werden, die dann z.B. bei der Technikentwicklung explizit berücksichtig werden sollen.

4 Ethische Implikationen

Ein ethischer Designprozess ist besonders relevant für Beobachtungstechnologien, da diese erhebliche Auswirkungen auf Privatsphäre, Ethik, Sicherheit und gesellschaftliche Akzeptanz haben. Der Absatz des Value Based Engineering (VBE) folgt einem soziotechnischen Systemansatz des Engineering und basiert auf den Grundlagen verschiedener Ethiken. Der Ansatz Corporate Digital Responsibility (CDR) ist ein Konzept der unternehmerischen Verantwortung im Kontext ganzheitlicher Nachhaltigkeitsstrategien, das die spezifischen Herausforderungen und Verantwortlichkeiten der digitalen Transformation inkludiert.

4.1 Value Based Engineering nach Standard ISO/IEC/IEEE 7000

Der Value Based Engineering (VBE) will sowohl die Innovation fördern als auch ethische Belange schützen. Dies soll erreicht werden durch die Berücksichtigung der Werte und Tugenden, die für direkte und indirekte Interessengruppen wichtig sind sowie durch die Übersetzung der ethischen Wertanforderungen in die Spezifikation entsprechender Systemanforderungen.

Werte steuern Handeln. Als solche durchdringen sie z.B. Tätigkeiten oder im Fall der Technikentwicklung Design- und Entwicklungsprozesse. Werte bestimmen die Auswahl der verfügbaren Mittel und Ziele des Handelns. Werte können ranggeordnet werden[3].

VBE ist ein Ansatz, der sicherstellt, dass technische Systeme und Produkte nicht nur funktionale Anforderungen erfüllen, sondern auch ethische, soziale und wirtschaftliche Werte berücksichtigen. Der Standard ISO/IEC/IEEE 7000[4] definiert einen methodischen Rahmen zur Integration dieser Werte in den Entwicklungsprozess und unterstützt ethische Verantwortung in der Technikgestaltung. Diese Norm unterstützt bei einer transparenten Kommunikation mit ausgewählten Stakeholdern zur Ermittlung und Priorisierung von Werten.

Zehn wertebasierte Vorgehensweisen werden im Kontext des Standards definiert:

1. Verantwortung für das Ökosystem übernehmen.
2. Auf die Investitionen verzichten, wenn wichtige ethische Gründe dagegensprechen.
3. Die wesentlichen Interessengruppen (Stakeholder) einbeziehen.
4. Bekannte Ethiken anwenden, um wichtige ethische Werte zu ermitteln.
5. Den Kontext verstehen, in dem das System implementiert wird und mögliche Auswirkungen antizipieren.
6. Lokale Gesetze und internationale Vereinbarungen achten.
7. Führungsverantwortung übernehmen und ein öffentliches Commitment seitens der Leitung einer Organisation zu den gewählten Grundwerten geben.
8. Priorisierte Kernwerte und ihre Verknüpfung mit den Systemanforderungen des zu erstellenden Systems dokumentieren und transparent kommunizieren.
9. Die gewählten Werte für die Anwendung in der Tiefe verstehen und operationalisieren.
10. Eine Risikoanalyse für Entwicklung von Systemanforderungen durchführen.

[3] Eigenstetter, M. (2021). Werthaltungen in Unternehmen. In M. Aßländer (Hrsg.), Handbuch Wirt-schaftsethik (S. 218-228). Stuttgart: Metzler.

[4] 24748-7000-2022 ISO/IEC/IEEE IEEE/ISO/IEC International Standard--Systems and software engineering--Life cycle management--Part 7000: Standard model process for addressing ethical concerns during system design.

In zwei Phasen, Phase der Konzepterkundung und der Entwicklungsphase sind mehrere Subphasen definiert (Abbildung 3).

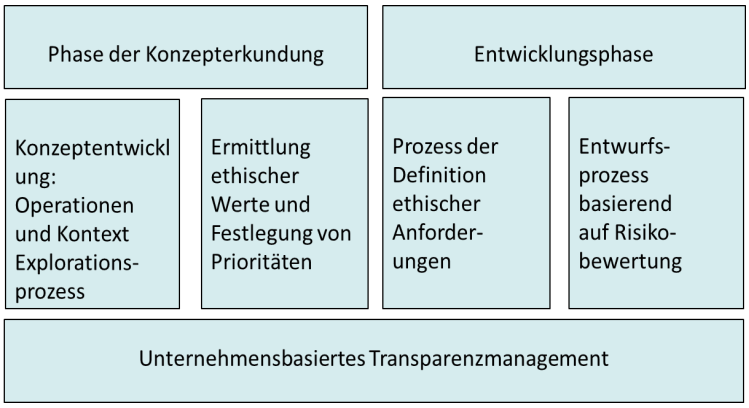

Abbildung 3. Überblick über die Phasen nach ISO/IEC/IEEE 7000, eigene Übersetzung

Phase der Betriebskonzept und Kontexterkundung

- Konzeptentwicklung - Operationen und Kontext Explorationsprozess: Dieser Prozess zielt darauf ab, ein erstes Verständnis des Kontexts, der relevanten Interessengruppen, der rechtlichen, sozialen, ökologischen und ethischen Machbarkeit zu gewinnen.
- Ermittlung ethischer Werte und Festlegung von Prioritäten: Die Auswirkungen eines vorgeschlagenen Systems auf Werte und Tugenden werden unter Verwendung verschiedener Ethiken analysiert: Utilitarismus, Werte- und Tugendethik sowie Pflichtethik nach Kant. Zudem werden kulturspezifische Besonderheiten aufgenommen (z.B. Unterscheiden sich asiatische und europäische Kulturen).

Entwicklungsphase

- Prozess der Definition ethischer Anforderungen: Während dieses Prozesses werden die Kernwerte und ihre Wertequalitäten definiert, die dann in Systemanforderungen übersetzt werden müssen.
- Entwurfsprozess auf Basis von Risikobewertungen: Für die Spezifikation der Systemanforderungen auf Basis der Werte werden schließlich Risikobewertungen integriert: Bedrohungsanalysen oder eine Folgenabschätzung werden nach Schadenspotenzial und Eintrittswahrscheinlichkeit bewertet.

Ein unternehmensbasiertes Transparenzmanagement gibt Klarheit über die priorisierten Grundwerte und deren logische Verknüpfung mit den Systemanforderungen. Die Werte sollen dokumentiert und kommuniziert werden.

ISO/IEC/IEEE 7000 bietet damit einen strukturierten Ansatz, um Werte in technische Systeme zu integrieren – insbesondere bei Beobachtungstechnologien, die hohe gesellschaftliche Auswirkungen haben. Durch die Anwendung von Value Based Engineering können Entwickler und Organisationen sicherstellen, dass ihre Überwachungstechnologien ethisch vertretbar, datenschutzfreundlich und nachhaltig sind. Der Standard ist damit eine Methodik auch zur Technikfolgenabschätzung, welche in den Phasen der Konzeptentwicklung mit Systeminitiierung, -analyse und -entwurf eingesetzt werden kann. Dieser Standard bietet der Ingenieurswissenschaft einen implementierbaren Prozess, der Innovationsmanagementprozesse, Systemdesignansätze und Software-Engineering-Methoden aufeinander abstimmt, um ethische Risiken während des Designprozesses angemessen zu berücksichtigen. Hier sollen nicht nur Menschenrechte, sondern auch Umweltrechte berücksichtigt werden. Digitalisierung braucht viel Energie während der Nutzung: Insbesondere Anwendungen der

künstlichen Intelligenz und /oder der Blockchain-Anwendungen sind große „Energiefresser“. Rohstoffe aus Edelmetallen, seltenen Erden, die für Interfaces und Technologien gebraucht werden sowie toxische Abfallstoffe sind weitere Probleme im Kontext der digitalen Technologien und erzeugen einen hohen ökologischen Impact[5].

4.2. Corporate Digital Responsibility

Corporate Digital Responsibility (CDR) erweitert das Konzept der unternehmerischen Verantwortung im Kontext ganzheitlicher Nachhaltigkeitsstrategien. Unternehmen sollen nicht nur soziale und ökologische Aspekte berücksichtigen, sondern auch die spezifischen Herausforderungen und Verantwortlichkeiten der digitalen Transformation adressieren[6]: Das sind untere anderem Datenschutz, ethische Fragen im Zusammenhang mit künstlicher Intelligenz, die ökologischen Auswirkungen digitaler Infrastrukturen sowie die Auswirkungen auf Mitarbeiter im Kontext digitaler Arbeit. Die Studie bietet ein wissenschaftlich fundiertes Konzept, wie Unternehmen ihre Digitalisierung im Einklang mit einer nachhaltigen Entwicklung gestalten können. Sie betont die Notwendigkeit eines Zusammenspiels von Unternehmen, Politik und Zivilgesellschaft, um digitale Verantwortung effektiv zu übernehmen. Sechs Handlungsfelder werden abschließend definiert.

1. Management der digitalen Unternehmensverantwortung: Dieser Bereich fokussiert sich auf die Integration von CDR in die Unternehmensstrategie und -kultur. Es betont die Bedeutung von Governance-Strukturen, die sicherstellen, dass digitale Verantwortung systematisch und nachhaltig im Unternehmen verankert ist.
2. Verantwortung für die Beschäftigten im Kontext digitaler Arbeit: Hierbei geht es um die Auswirkungen der Digitalisierung auf die Arbeitswelt. Themen wie Qualifizierung, Arbeitsbedingungen und der Schutz der Mitarbeitendenrechte im digitalen Umfeld stehen im Mittelpunkt.
3. Ökologische Verantwortung einer digitalisierten Leistungserstellung: Dieses Feld adressiert die ökologischen Konsequenzen der Digitalisierung, beispielsweise den Energieverbrauch von Rechenzentren oder die Umweltbelastung durch die Produktion digitaler Geräte.
4. Digitale Produktverantwortung: Unternehmen sind verantwortlich für die ethische Gestaltung ihrer digitalen Produkte und Dienstleistungen. Dies umfasst Aspekte wie Datenschutz, IT-Sicherheit und die Vermeidung von Diskriminierung durch Algorithmen.
5. Verantwortung in der digitalen Lieferkette: Dieser Bereich beleuchtet die Verantwortung von Unternehmen für die digitalen Aspekte ihrer Lieferketten, einschließlich der Transparenz von Datenflüssen und der Sicherstellung fairer Arbeitsbedingungen bei Zulieferern.
6. Gesellschaftliche Digitalverantwortung – Corporate Digital Citizenship: Unternehmen tragen Verantwortung gegenüber der Gesellschaft im digitalen Kontext. Dies beinhaltet Engagements wie die Förderung digitaler Bildung (digital Literacy), den Abbau digitaler Ungleichheiten z.B. zwischen den Geschlechtern und die Unterstützung bei der Bewältigung gesellschaftlicher Herausforderungen durch digitale Lösungen (z.B. bei Fehlinformation durch technische Systeme).

[5] IEA (2024) Recycling of Critical Minerals Strategies to scale up recycling and urban mining A World Energy Outlook Special Report: https://www.iea.org/reports/recycling-of-critical-minerals. IEA (2024). World Energy Outlook 2024: https://iea.blob.core.windows.net/assets/140a0470-5b90-4922-a0e9-838b3ac6918c/WorldEnergyOutlook2024.pdf.

[6] Lautermann und Frick (2023). Corporate Digital Responsibility: Wie Unternehmen im digitalen Wandel Verantwortung übernehmen. Verfügbar unter:

4.3 Ethikbewertung in KIRAPol.5G: Ethikworkshop mit KI Campus

Ein Workshop zur ethischen Bewertung der Bewertung der KI-gestützten Radartechnologie fand über den KI Campus statt. Die Ethikbewertung startete – aufgrund der umfassenden Vorarbeiten an der Datenschutzfolgenabschätzung – mit einer soziotechnischen Systemanalyse, welche als Ergebnis einen Sollprozess in einem Flussdiagram visualisierte. Da man sich im Projekt immer noch in der Konzeptionsphase befand, wurde mögliche Szenarien variiert. Die wahrscheinlichste Variante wurde ausgewählt und im weiteren Vorgehen vertieft. Die gewählte Variante ermöglicht eine kontinuierliche Beobachtung durch Radar, wobei die Videosequenzen von mitlaufenden Kameras durch permanentes Überschreiben gelöscht werden. Sollte es zu einer der vorab definierten Situationen (Use Cases) kommen, können über die Ringspeicher in den Kameras zurückwirkend einige Minuten Videosequenz abgerufen werden und von Polizeibeamten bewertet werden. Im Kontext dieser Technologien wurde z.B. die zeitliche Erhöhung der „Beobachtungslast" problematisiert, die akzeptiert werden muss, bevor das Projekt insgesamt zu einer Reduktion der Beobachtungslast durch optische Überwaschungsmittel führen kann.

Eine umfassende Stakeholderanalyse identifizierte 13 Stakeholdergruppen, die mit unterschiedlichen Verantwortlichkeiten belegt sind, und die mit weiteren Methoden, z.B. der sogenannten RACI-Methode[7], ausdifferenziert werden können. Aus der Stakeholderanalyse wurden Handlungsempfehlungen abgeleitet, die im Rahmen des Projektes teilweise auch schon umgesetzt wurden, so die umfassende Information und umfängliche Einbindung der betroffenen Bevölkerung. Andere Empfehlungen konnten im Rahmen des Projektes nicht weiterverfolgt werden, wie Schulung der Beamten in Leitstellen, oder Feedbacksysteme für die Product-Owner.

Es wurden aus dem Entwicklerteam Anforderungen an das System formuliert, die über die bisherigen im Projektantrag formulierten Anforderungen wie Nutzerfreundlichkeit, Zuverlässigkeit des Gesamtsystems und Diskriminierungsfreiheit deutlich hinausgehen, so z.B. geringer Energieverbrauch oder die Grenzen des Systems zu kennen und zu schulen. Das bedeutet im Umkehrschluss, dass eine große Menge an Daten aus dem öffentlichen Raum und im Einsatz vorhanden sein muss, um diese Anforderungen umzusetzen.

Im Kontext dieses Workshops kamen vielfältige ethische und soziale Fragen auf, die den Einsatz in der Praxis hinterfragen, z.B. ob das System in der Lage sein wird

- Kulturelle Unterschiede zu erkennen, z.B. freundliches Schlagen auf die Schulter als Begrüßungsritual
- Genderspezifische Unterschiede zu erkennen: Frauen schlagen anders zu als Männer
- Insgesamt wird es erforderlich sein, umfangreiche Kosten-Nutzenbewertungen für einen realen Einsatz in der Breite vorzunehmen.

Gesamtgesellschaftliche Auswirkungen wurden in diesem Workshop gemeinsam kritisch reflektiert, konnten aber aufgrund der Kürze des Projektes nicht weiter vertieft werden. Besonders relevant ist das Thema Sicherheit, subjektiv und objektiv: Wird die Technologie zu einer Erhöhung der Sicherheit subjektiv und objektiv beitragen: Steigt das Vertrauen in die Polizei? Oder werden durch Fehlalarme die Anzahl der Einsätze der Polizei steigen, das gesellschaftliche Misstrauen in die staatlichen Institutionen durch eine wahrgenommene Überwachung vertieft. Die Zusammenfassung wurde seitens des KI Campus nur zur internen Verfügung zur Verfügung gestellt.

[7] Responsibility Assignment Matrix. Wikipedia Freie Enzyklopädie: verfügbar unter: https://en.wikipedia.org/wiki/Responsibility_assignment_matrix

5 Legale Implikationen

Mit den legalen Implikationen werden wichtige rechtliche Grundlagen bei der Entwicklung (noch nicht für den regelgerechten Einsatz) der Technologien berücksichtigt. Hier sind insbesondere die vergleichsweise neuen Regeln für Künstliche Intelligenz, wie auch die Datenschutzgrundverordnung relevant. Weitere Regulierungen werden zum aktuellen Stand der Entwicklung noch nicht berücksichtigt.

5.1 Regeln für Künstliche Intelligenz in der EU

Die EU verfügt seit dem 21. Mai 2024 über das weltweit erste verbindliche Regelwerk zur Regulierung von Künstlicher Intelligenz, der so genannte AI Act[8].

Der AI Act (EU-KI-Verordnung) folgt einer risikobasierten Einschätzung, um den Einsatz von Künstlicher Intelligenz (KI) zu regulieren. Je höher das Risiko, desto mehr Auflagen gibt es für den Einsatz der KI. Unternehmen müssen sicherstellen, dass ihre KI-Systeme sicher, fair und nachvollziehbar sind. Es werden vier Risikostufen mit Beispielanwendungen definiert[9]:

1. Minimales Risiko: Harmlose KI, wie z. B. Spam-Filter oder KI-gestützte Produktempfehlungen, kann frei genutzt werden und erfordert keine besonderen Empfehlungen.
2. Begrenztes Risiko: KI, die mit Menschen interagiert oder Inhalte erzeugt über Chatbots und Deepfakes muss die Nutzenden informieren, dass sie mit einer KI kommunizieren. Es besteht eine Transparenzpflicht.
3. Hohes Risiko: KI, die wichtige Bereiche betrifft wie Medizin, Justiz, Kreditvergabe, kritische Infrastruktur muss hohe Sicherheits- und Transparenzanforderungen erfüllen und ist damit streng reguliert. Hier muss eine Risikobewertung mit klarer Dokumentation erfolgen. Die KI muss systematisch kontrolliert werden, ob sie richtig arbeitet und Maßnahmen zur Sicherstellung der Cyber Security erfolgen müssen.
4. Unzulässiges Risiko: KI-Systeme, die eine klare Gefahr für Menschenrechte oder Sicherheit darstellen, sind verboten. Beispiele hierfür sind: Social Scoring (wie in China), manipulierende KI, Emotionserkennung am Arbeitsplatz.

Beobachtungstechnologien gehören in Kategorie 4 (unzulässiges Risiko), wenn sie zur biometrischen Überwachung in Echtzeit im öffentlichen Raum genutzt werden, z. B. Gesichtserkennung. Sie gehören in Kategorie 3 (begrenztes Risiko), wenn die Beobachtungstechnologie zur nachträglichen biometrischen Identifikation genutzt wird, z. B. Gesichtserkennung in Polizei-Datenbanken[10].

[8] EU Artifical Intelligence Act (2024). Die Gesetzestexte. Verfügbar unter: https://artificialintelligenceact.eu/de/das-gesetz/

[9] EU Artifical Intelligence Act (2024). Zusammenfassung der AI-Gesetzes auf hoher Ebene. Verfügbar unter: https://artificialintelligenceact.eu/de/high-level-summary/

[10] Max-Planck-Gesellschaft (2025). AI Act: Was er regelt und wen er betrifft. Der AI Act regelt, wie Anbieter und Betreiber künstliche Intelligenz einsetzen können. Was sich zum 2. Februar 2025 ändert. Verfügbar unter: https://www.mpg.de/24096506/faq-was-regelt-der-ai-act

Kasten 2. EU AI ACT Compliance Checker

Mit einem EU AI ACT Compliance Checker können KI-Systeme in der Entwicklung geprüft werden, in welche Kategorie sie fallen werden[11].

5.2 Wichtige Grundlagen nach der Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz

Die Datenschutz-Grundverordnung (DSGVO) ist eine EU-Verordnung, die den Schutz personenbezogener Daten regelt. Sie trat am 25. Mai 2018 in Kraft und gilt für alle Unternehmen und Organisationen, die Daten von EU-Bürgern verarbeiten – unabhängig davon, ob sie in der EU ansässig sind. Verstöße gegen die DSGVO können mit hohen Geldstrafen von bis zu 20 Mio. € oder 4 % des weltweiten Jahresumsatzes geahndet werden. Die DSGVO soll sicherstellen, dass personenbezogene Daten in der EU sicher und transparent verarbeitet werden. Die DSGVO dient:

- Dem Schutz personenbezogener Daten,
- Der Stärkung der Rechte der betroffenen Personen,
- Der Vereinheitlichung des Datenschutzrechts in der EU,
- Und der Erhöhung der Transparenz und Rechenschaftspflicht von Unternehmen.

Personenbezogene Daten dürfen nur unter definierten Voraussetzungen verarbeitet werden, nämlich:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz – Art. 5 Abs. 1 lit. a DSGVO
- Mit Zweckbindung – Art. 5 Abs. 1 lit. b DSGVO
- Unter dem Grundsatz der Datenminimierung – Art. 5 Abs. 1 lit. c DSGVO
- Der Richtigkeit – Art. 5 Abs. 1 lit. d DSGVO
- Speicherbegrenzung (z.B. Löschungfristen nach zwei Jahren) – Art. 5 Abs. 1 lit. e DSGVO
- Integrität und Vertraulichkeit (Daten dürfen nicht durch Dritte veränderbar sein: Sicherheit der Verarbeitung) – Art. 5 Abs. 1 lit. f DSGVO
- Rechenschaftspflicht gegenüber den Betroffenen – Art. 5 Abs. 2 DSGVO

Betroffene haben wichtige Rechte gegen über der Instanz, die die Daten sammelt und verarbeitet:

- Auskunftsrecht – Art. 15 DSGVO
- Recht auf Berichtigung – Art. 16 DSGVO
- **Recht auf Löschung („Recht auf Vergessenwerden“) ** – Art. 17 DSGVO
- Recht auf Einschränkung der Verarbeitung – Art. 18 DSGVO
- Recht auf Datenübertragbarkeit – Art. 20 DSGVO
- Widerspruchsrecht gegen die Verarbeitung – Art. 21 DSGVO
- Recht auf keine automatisierte Entscheidung (inkl. Profiling) – Art. 22 DSGVO

[11] EU AI Act Compliance Checker. Verfügbar unter: https://artificialintelligenceact.eu/de/bewertung/eu-ai-act-compliance-checker/

Unternehmen müssen daher immer eine Einwilligung zur Datenverarbeitung einholen (Art. 6, Art. 7 DSGVO), die Betroffene auch über ihre Rechte aufklärt, ein Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO) führen. Sie haben eine Meldepflicht bei Datenpannen innerhalb von 72 Stunden an die Betroffenen und die Behörden (Art. 33 DSGVO).

Sie müssen einen Datenschutzbeauftragten nach Bundesdatenschutzgesetz (§ 38 BDSG) bestellen, wenn mindestens 20 Personen regelmäßig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, wenn personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, anonymisierten Übermittlung oder Marktforschung verarbeitet werden oder eine Datenschutzfolgenabschätzung (DSFA) durchgeführt werden muss. Eine Durchführung einer Datenschutzfolgenabschätzung ist bei hohem Risiko immer notwendig, d.h. bei Einsatz von neu entwickelten und/oder Beobachtungstechnologien zwingend.

5.3 Datenschutzfolgenabschätzung

Eine Datenschutzfolgenabschätzung (DSFA) sollte in jedem Fall bei Einsatz neuer Techniken durchgeführt werden: Sie hilft Unternehmen, datenschutzrechtliche Vorgaben frühzeitig zu erkennen und umzusetzen, um Bußgelder und Reputationsschäden zu vermeiden.

Eine DSFA ist ein Verfahren zur Bewertung der Risiken, die eine Datenverarbeitung für die Rechte und Freiheiten von betroffenen Personen mit sich bringen kann. Sie ist in der Datenschutz-Grundverordnung (DSGVO, Art. 35) vorgeschrieben, wenn eine Verarbeitung voraussichtlich ein hohes Risiko für personenbezogene Daten darstellt. Eine DSFA muss grundsätzlich durchgeführt werden, wenn neue Technologien eingesetzt werden, eine umfangreiche Verarbeitung sensibler Daten (z. B. Gesundheitsdaten) stattfindet, eine systematische Überwachung öffentlicher Bereiche erfolgt und/oder automatisierte Entscheidungsfindungen mit erheblichen Auswirkungen genutzt werden.

Im Rahmen der DFSA muss daher ein umfassendes Dokument erstellt werden, das eine risikobasierte Bewertung enthält. Diese umfasst die Identifikation und Bewertung potenzieller Risiken für die Privatsphäre sowie die Ableitung von Maßnahmen zur Risikominimierung, falls Risiken festgestellt werden, um die Einhaltung der DSGVO nachzuweisen. Der Ablauf umfasst eine Beschreibung der Verarbeitung: Art, Zweck, Umfang der Datenverarbeitung inclusive eine Beschreibung der dafür eingesetzten Technologien.

Es erfolgt damit

- Bewertung der Notwendigkeit und Verhältnismäßigkeit: Rechtliche Grundlage und Zweckmäßigkeit.
- Analyse der Risiken: Welche Gefahren bestehen für die betroffenen Personen?
- Maßnahmen zur Risikominimierung: Technische und organisatorische Schutzmaßnahmen.
- Dokumentation und ggf. Konsultation der Aufsichtsbehörde bei einem hohen Restrisiko.

Datenschutzfolgenabschätzung müssen vor Beginn der Datenverarbeitungstätigkeit erstellt werden. Idealerweise sollte DFSA vor und während der Planungsphase des Projekts durchgeführt werden: Dazu ist es erforderlich, sich mit Datenschutzbeauftragten und den am Projekt direkt beteiligten Partner zu beraten. Dies ist ein langwieriger Prozess.

5.4 Datenschutzfolgenabschätzung im Projekt KIRAPol.5G basierend auf §17 DSG NRW

Die Hochschule wollte Daten für das Forschungsvorhaben auf der Grundlage des §17 DSG NRW erheben. Die Verarbeitung personenbezogener Daten kann auch ohne explizite Einwilligung für wissenschaftliche Forschungszwecke erfolgen, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und schutzwürdige Belange der betroffenen Person nicht überwiegen. Für die Erstellung der Datenschutzfolgenabschätzung wurden Leitfäden verschiedener Organisationen gesichtet. Die Stiftung Datenschutz hat 2020 einige Leitfäden zusammengetragen[12]. Templates gibt es auch direkt auf den Seiten der EU[13].

Der wissenschaftliche Forschungszweck nach §17 DSG NRW im Bereich der angewandten Forschung gem. Erwägungsgrund 159 (Verarbeitung zu wissenschaftlichen Forschungszwecken) kann in einem durch ein Forschungsförderprogramm, gefördert durch das Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen angenommen werden. Eine Verarbeitung der Daten zu den definierten Forschungszwecken ist erforderlich, da ohne Daten ein Trainieren der KI nicht möglich ist („überwachten Lernen).

„Schutzwürdige Belange“ i.S.d. §17 DSG-NRW wurden definiert und es wurde dargelegt, wie sie eingehalten werden (gekürzt aus der Datenschutzfolgenabschätzung KIRAPol5.G S. 20 bis 21).

- Datenschutz: persönliche Informationen müssen angemessen und sicher behandelt werden. Der Schutz der Daten bis zur relativen Anonymisierung wird durch angemessene technische und organisatorische Maßnahmen (TOM) gewährleistet.
- Die Verarbeitung von personenbezogenen Daten darf nicht unverhältnismäßig in die Privatsphäre der Betroffenen eingreifen, z.B. Offenlegung sensibler Informationen. Eine Offenlegung sollte z.B. nicht erfolgen.
- Recht auf informationelle Selbstbestimmung: An den Messstellen werden Hinweisschilder mittels QR-Code auf eine spezielle Informationsseite verweisen, um über das Projekt, die Ziele und die Beteiligten usw. zu informieren. Die Art der Datenerhebung, das Anonymisierungsverfahren sowie die Verwendung der anonymisierten Daten wird dort erläutert. Weiterhin wird ein Ansprechpartner genannt, der auf spezielle Fragen und/oder Kritik reagieren kann.
- Einwilligung: Schutzwürdige Belange können auch die Notwendigkeit einer wirksamen Einwilligung der Betroffenen in die Datenverarbeitung betreffen. Dies bedeutet, dass die Betroffenen über die Zwecke der Verarbeitung und andere relevante In-formationen informiert werden sollten und die Möglichkeit haben sollten, ihre Zu-stimmung zu geben oder zu verweigern. Im Rahmen der öffentlichen Messkampagne wird rechtzeitig durch Hinweisschilder auf die Datenerhebung hingewiesen und welcher Bereich davon tangiert ist, so dass durch Umgehung des Bereichs einer Beteiligung am Verfahren widersprochen werden kann.
- Diskriminierung: Betroffene sollten vor diskriminierender Verwendung ihrer Daten geschützt werden, wie beispielsweise bei der automatisierten Entscheidungsfindung. Mit der Verwendung anonymisierter Daten zur Validierung, ist eine diskriminierende Verwendung der Daten nicht gegeben.

[12] Stiftung Datenschutz (2020). Datenschutzfolgenabschätzung. Verfügbar unter: https://stiftungdatenschutz.org/fileadmin/Redaktion/Dokumente/Dossiers_Infoplattform/2020-07-Update/DSGVO-Praxis__Datenschutzfolgenabschaetzung_Juni2020.pdf

[13] GDRPR.EU (2020). Data Protection Impact Assessment (DPIA) https://gdpr.eu/data-protection-impact-assessment-template/

Die verschiedenen eingesetzten Technologien wurden detailliert beschrieben und bewertet: Zudem wurden die Übertragungswege und die Informationsübermittlung entlang der verschiedenen Stationen inclusive Verschlüsselungstechnologien, Anonymisierung, Zugriffsrechte ec. beschrieben. Alle die mit den Technologien, Verfahrensweisen und beteiligten Personen einhergehenden Risiken wurden kollektiv erfasst. Um diese Risiken angemessen zu erfassen, ist es hilfreich, sich in die Rolle einer Person zu versetzen, die diese Technik und die Übermittlung der Daten korrumpieren möchte und die Daten stehlen möchte. Erst mit dieser Sichtweise ist es überhaupt möglich, angemessene Maßnahmen auf technischer, organisatorischer und personenbezogener Ebene zu definieren.

Eine beispielhafte Übersicht der Verarbeitung ist der folgenden Abbildung 4 dargestellt. In der weiteren DSFA wurden die an der Verarbeitung beteiligten Personen und Rollen, die jeweils erhobenen Daten, die durchgeführten Verarbeitungsvorgänge sowie deren rechtliche Grundlage und Verantwortung nochmals expliziert.

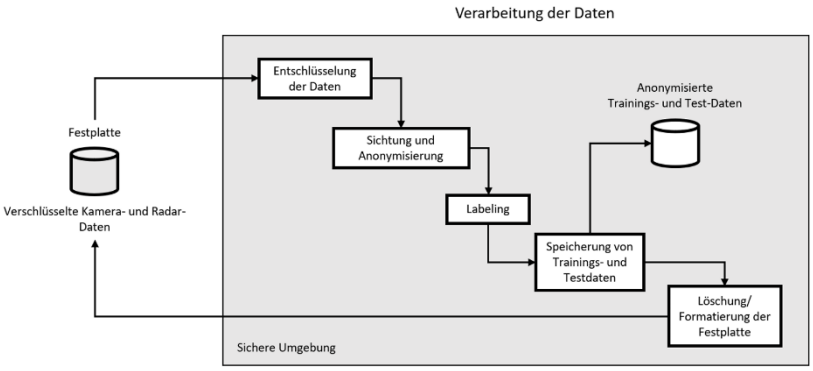

Abbildung 4. Verarbeitung der Radar- und Kameradaten
(entnommen dem Datenschutzkonzept KIRAPol.5G, S. 23)

Mit dieser sorgfältig durchgeführten DSFA wird in einer Arbeitsgruppe ein hohes Verständnis für die Chancen und Risiken im Einsatz gewonnen. Über 50 Risiken wurden definiert, z.B. Diebstahl der Hardware, Manipulation von Daten, Verbindungsabbrüche und mit Maßnahmen hinterlegt, so dass die Wahrscheinlichkeit, dass eine missbräuchliche Verwendung von Daten erfolgen kann, auf ein geringes Restrisiko minimiert wird.

Die vollständige Datenschutzfolgenabschätzung kann auf Wunsch bei der Erstautorin eingesehen werden.

6 Soziale Implikationen: Akzeptanz der KI-gestützten Technologie bei Bürgerinnen und Bürgern im öffentlichen Raum

Mit den Sozialen Implikationen ist es wichtig zu erfassen wie die Technologie von der Gesellschaft wahrgenommen wird und welche Bedenken gebildet werden. Die Erfassung der Akzeptanz, Einstellung sowie Bedenken der Bürgerinnen und Bürger gegenüber der Beobachtungstechnologie ist gleichzeitig essenziell für die zukünftige Implementierung. Da die KI-gestützte Radarbeobachtungstechnologie, wie sie in diesem Projekt vorgesehen ist, bisher noch nicht eingesetzt wird und somit eine neue Form des Beobachtungssystems darstellt, ist es wichtig, frühzeitig im Entwicklungsprozess die Meinung der Bürgerinnen und Bürger als zentrale Stakeholder-Gruppe einzubeziehen. Dies trägt nicht nur zu einer bedarfsgerechten Einführung der Technologie bei, sondern unterstützt auch eine transparente und zielgerichtete Kommunikation über die notwendigen Informationen zur Förderung der gesellschaftlichen Akzeptanz. Eine frühzeitige Einbindung der Bürgerinnen und Bürger stärkt das Vertrauen in die Technologie, während eine fehlende Beteiligung Befürchtungen und Widerstände hervorrufen könnte, die eine effektive Implementierung erschweren. Ethische Beurteilung der Privatsphäre spielen in diesem Kontext eine entscheidende Rolle – die Gesellschaft definiert, welche Technologien akzeptabel sind und wo Grenzen gezogen werden sollten. Die Berücksichtigung der Bürgerakzeptanz fördert nicht nur die Legitimität neuer Überwachungstechnologien, sondern auch deren langfristige Nachhaltigkeit. Für Akzeptanzforschungen werden meist Forschende aus den Sozialwissenschaften beauftragt, da hier soziale Fragestellungen zum Tragen kommen.

6.1 Theoretische Basis der Akzeptanzforschung

Bürgerinnen und Bürger akzeptieren grundsätzlich digitalisierte Anwendungen, die ihre Sicherheit verbessern[14]. Die Akzeptanz von Überwachungstechnologien durch die Polizei variiert jedoch je nach Kontext und Art der Technologie. Während Beobachtungssysteme wie Körperkameras, prädiktive Polizeisysteme oder Videoüberwachung im öffentlichen Raum auf Zustimmung stoßen, nimmt die Akzeptanz tendenziell ab, wenn diese Technologien in großem Umfang eingesetzt werden.[15; 16]. Dabei entsteht ein ethisches Dilemma: Sicherheit versus Privatsphäre.

Akzeptanzforschung zu Radartechnologie als Beobachtungstechnologie war noch nicht erforscht. Für die Einführung neuer Technologien ist es entscheidend, die Einstellungen und die Akzeptanz der Beteiligten frühzeitig und kontextbezogen zu erfassen. Insbesondere Bürgerinnen und Bürger sind als zentrale Stakeholder von Beobachtungstechnologien für die Polizei von großer Bedeutung, da die Ablehnung dieser Technologien aufgrund großer Bedenken hinsichtlich der Privatsphäre und Datenschutz zu öffentlichem Widerstand und massiven Protesten führen kann[17]. Ein prominentes

[14] Zink, W., Zimmermann, K. (2023). Öffentliche Akzeptanz der Digitalisierung bei der Polizei. In: Wehe, D., Siller, H. (Hrsg.) Handbuch Polizeimanagement. Polizeipolitik – Polizeiwissenschaft – Polizeipraxis, 2nd edn. Springer Gabler, Wiesbaden

[15] Öffentliche Akzeptanz digitaler Technologien für die deutsche Polizei. (2020). Verfügbar unter: https://www.pwc.de/de/branchen-und-markte/oeffentlicher-sektor/pwc-studie-polizei-technikakzeptanz-2020.pdf

[16] Bayerl, P.S., Butot, V., Jacobs, G. (2023). Produktion urbaner Sicherheit aus Bürgerperspektive. In: Wehe, D., Siller, H. (Hrsg.) Handbuch Polizeimanagement. Polizeipolitik – Polizeiwissenschaft – Polizeipraxis, 2nd edn. Springer Gabler, Wiesbaden

[17] Ebd.

Beispiel hierfür ist der Widerstand gegen die biometrische Überwachung: „Holt euch unseren öffentlichen Raum zurück. Verbietet die biometrische Massenüberwachung!“[18].

In der Technologieakzeptanzforschung ist das Technologieakzeptanzmodell (TAM) von Davis[19; 20] ein etabliertes Modell. Für die Akzeptanzforschung von Beobachtungstechnologien aus Sicht der Bürgerinnen und Bürger ist das TAM-Modell jedoch nicht direkt anwendbar, da diese keine klassischen „Nutzer“ sind. Um diese Lücke zu schließen, entwickelte Krempel[21] eine modifizierte Version, das TAM-VS-Modell, um die Akzeptanz von Videoüberwachung in der Bevölkerung zu untersuchen. Das TAM-VS-Modell berücksichtigt Faktoren wie das Risiko des Missbrauchs, den Nutzen und die Transparenz. Es konzentriert sich auf die technischen Aspekte von Überwachungssystemen. Eine weitere relevante Studie von Kudlacek[22] untersuchte die Einstellung zur Videoüberwachung unter Einbeziehung von Sicherheitsaspekten, der Angst vor Kriminalität sowie sozioökonomischen Faktoren wie Alter, Geschlecht und Bildungsniveau. Nach Krempel könnte eine Kombination beider Forschungsansätze umfassenderes Verständnis der Akzeptanz von Beobachtungstechnologien liefern. Für die Erfassung der Akzeptanz und dessen Einflussfaktoren wurde das TAM-VS Modell von Krempel für das Projekt KIRaPol.5G modifiziert (siehe Abbildung 5).

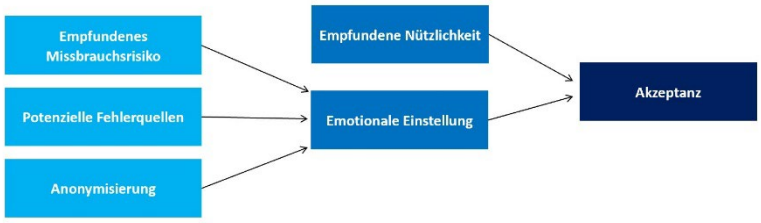

Abbildung 5. Modifiziertes Akzeptanzmodell TAM-VS von Krempel für die Stakeholder-Kommunikation

6.2 Stakeholderkommunikation mit den Bürgerinnen und Bürgern

Um sowohl Bedenken als auch die Akzeptanz der Bürgerinnen und Bürger gegenüber der Technologie zu erfassen und die Bevölkerung frühzeitig in den Entwicklungsprozess einzubinden, wurden Interviews und eine Onlinebefragung durchgeführt. Dadurch kamen sowohl qualitative als auch quantitative Methoden zum Einsatz, während die Interviews einen direkten Dialog ermöglichten und einen explorativen Ansatz verfolgten, lieferte die Onlinebefragung messbare Ergebnisse. Die gewonnenen Erkenntnisse bilden die Grundlage für eine gezielte und transparente Stakeholderkommunikation. Sie tragen dazu bei, künftige Bedenken gezielt abzubauen und das Vertrauen in die Technologie zu stärken. Dies geschieht durch eine angemessene Ansprache von Vorbehalten sowie eine offene und verständliche Vermittlung relevanter Informationen, um die Akzeptanz der Technologie nachhaltig zu fördern.

[18] Reclaim Your Face: The future must be ours to shape. https://reclaimyourface.eu/.
[19] Davis, F.D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of In-formation Technology. MIS Quarterly https://doi.org/10.2307/249008
[20] Davis, F.D., Bagozzi, R.P., Warshaw, P.R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. Management Science https://doi.org/10.1287/mnsc.35.8.982
[21] Krempel, E.L. (2016). Steigerung der Akzeptanz von intelligenter Videoüberwachung in öffentlichen Räumen. Dissertation, KIT; Karlsruher Institut für Technologie
[22] Kudlacek, D. (2015). Akzeptanz von Videoüberwachung. Springer Fachmedien Wiesbaden, Wiesbaden

6.2.1 Explorierende Interviews

Die Befragung der Interviews wurde im Bereich des Hauptbahnhofs Mönchengladbach durchgeführt, sowohl im Bahnhof selbst als auch in dessen unmittelbarem Umfeld. Es wurden explorierend vierzehn Personen im Alter zwischen 19 und 62 befragt, mit einem Altersdurchschnitt von 36,5 Jahren.

Der Interviewleitfaden umfasst folgende Fragen, die nach einer kurzen Vorstellung des Projekts, der Zielsetzung sowie der KI-gestützten Radartechnologie gestellt wurden:

- Was halten Sie von einer solchen Überwachungstechnologie auf öffentlichen Plätzen oder an Bahnhöfen?
- Sehen Sie irgendwelche Nachteile in Bezug auf diese Technologie?
- Was empfinden Sie, wenn Sie darüber nachdenken, dass eine KI für Überwachungszwecke eingesetzt wird?
- Welche Chancen sehen Sie bei der Anwendung von Künstliche Intelligenz?
- Welche Risiken sehen Sie bei der Anwendung von Künstliche Intelligenz?
- Sehen Sie Risiken für den Datenschutz, die infolge der vorgestellten Überwachungstechnologie entstehen könnten? Wenn ja, welche?
- Würden Sie sich mit einer solchen Überwachungstechnologie auf öffentlichen Plätzen oder an Bahnhöfen sicher fühlen?

In der folgenden Tabelle 2 sind die Äußerungen der Interviewten Personen zusammengefasst. Vereinzelt wurden verschiedene Bemerkungen und Anmerkungen geäußert, die in der folgenden Tabelle in einer komprimierten Form erfasst werden.

Tabelle 2. Zentrale Erkenntnisse aus den Interviews

	Bemerkungen:
Allgemeine Einstellung	Mehrheit bewertet die Technologie positiv und oder sieht Vorteile für die Sicherheit (9 Personen). Weitere Aussagen beinhalten, dass die Technologie als sinnvolle Zusatzmaßnahme angesehen wird aber nicht als Ersatz, als besonders hilfreich in dunklen Bereichen gilt, als fortschrittlich wahrgenommen wird und das Sicherheitsgefühl steigert. Zudem wird sie als förderlich für eine schnellere Reaktionszeit des Sicherheitspersonals betrachtet.
Nachteile der Technologie	Es wurden Bedenken hinsichtlich der Fehleranfälligkeit geäußert, wie Fehlalarme, falsche Alarme und unnötige Polizeieinsätze sowie nicht identifizierte Gefahrensituationen. Zudem bestehen Sorgen über mögliche Missbräuche, Defekte oder Vandalismus. Weitere Anmerkungen umfassen die fehlende Gesichtserkennung zur Täteridentifikation und die Präferenz für Sicherheitspersonal vor Ort.
Einsatz der Technologie	Es wurden Aussagen gemacht, dass die Technologie als geeignet angesehen wird, solange sie zuverlässig funktioniert. Gleichzeitig äußerten einige Skepsis gegenüber autonomen Systemen, befürchteten den Verlust menschlicher Kontrolle und fragten nach der Haftung bei Fehlern der Technologie.
Chancen Nutzung der KI	Vorteile werden in der objektiven Bewertung von Situationen (sofern korrekt programmiert), der Entlastung von Sicherheitskräften, der kontinuierlichen (24/7) Verfügbarkeit, präziseren Datenerfassung (frühzeitige Gefahrenidentifizierung)

	sowie einer erhöhten Sicherheit und Hilfestellung bei der Überwachung gesehen.
Risiken Nutzung der KI	Geäußerte Risiken beinhalten technische Ausfälle, Fehlalarme und falsche Einschätzungen. Zudem gibt es die Sorge, dass voreingenommene Algorithmen Diskriminierung verursachen könnten. Einige fordern weiterhin menschliche Kontrolle und sehen diese als notwendig an. Andere sehen keine Risiken, solange das System zuverlässig und korrekt implementiert wird.
Datenschutzbedenken	Die Mehrheit äußerte keine Datenschutzbedenken (8 Personen). Weitere Äußerungen beinhalten Sorgen über mögliche Datenmissbräuche und die Möglichkeit der Identifizierung durch wiederholte Aufnahmen. Es wird die Notwendigkeit der Transparenz gefordert, insbesondere hinsichtlich des Zugriffs, der Speicherung und der Nutzungsbedingungen. Flächendeckende Überwachung wird abgelehnt, jedoch wird die Nutzung im öffentlichen Bereich akzeptiert.
Sicherheitsgefühl durch die Technologie	7 Personen gaben an, sich sicherer zu fühlen, wobei einige diese Sicherheit an die Voraussetzung knüpften, dass die Technologie fehlerfrei und zuverlässig funktioniert. 2 Personen würden sich nicht sicherer fühlen, da sie davon ausgehen, dass Täter sich anpassen und andere Wege finden könnten. Einige Personen bleiben unentschlossen oder bevorzugen weiterhin Sicherheitspersonal.

Zusammenfassend lässt sich sagen, dass die Bürgerinnen und Bürger die Chancen und Risiken der Technologie reflektiert und kritisch bewertet haben. Sie sehen insbesondere die Fehleranfälligkeit, wie falsche oder ausbleibende Alarme, als Risiko. Gleichzeitig erkennen sie die Vorteile wie die Entlastung von Sicherheitspersonal und die objektive, rund-um-die-Uhr Beobachtung von Situationen. Die Akzeptanz und das Sicherheitsgefühl hängen maßgeblich von der Fehlerfreiheit und dem transparenten Einsatz der Technologie ab. Eine klare und verständliche Kommunikation über die geplanten Maßnahmen und Ergebnisse der Messkampagnen der entwickelten KI-gestützten Radartechnologie ist daher entscheidend.

6.2.2 Quantitative Befragung

> *„Es erscheint jedoch wenig zielführend, etwa die polizeiliche Präsenz permanent zu erhöhen oder viel mehr Überwachungskameras zu installieren, wenn ein Großteil der Bevölkerung an deren positiver Wirkung zweifelt.“ – Köhn und Bornewasser (2012, S. 48)*

Eine Akzeptanzbefragung ermöglicht die Erfassung der Akzeptanz und Einstellung gegenüber der Beobachtungstechnologie sowie der Einflussfaktoren, die diese prägen. Auf dieser Grundlage können Zusammenhänge identifiziert und gezielte Maßnahmen zur Steigerung der Akzeptanz entwickelt werden. Gleichzeitig stellt das Sicherheitsempfinden einen wichtigen Faktor dar, der berücksichtigt werden sollte, da die subjektive Wahrnehmung der Sicherheit durch den Einsatz der Beobachtungstechnologie beeinflusst werden könnte.

In diesem Zusammenhang wurde eine Online-Befragung unter Verwendung eines Fragebogens durchgeführt. Die Befragung wurde online über verschiedene Plattformen und Informationskanäle öffentlich zugänglich gemacht, und auch durch die Presse und über Print-Medien wurde auf die Befragung hingewiesen, um eine größere Reichweite zu erzielen. 173 Personen nahmen teil. Die

Stichprobe beinhaltete 64 Frauen (37 %) und 99 Männern (57 %). Die Mehrheit der Teilnehmenden besitzt einen Hochschulabschluss (65%) und ist berufstätig (68%). Mit 27,8% war die Altersgruppe der 55- bis 65-Jährigen am stärksten vertreten. Im Folgenden werden einige Auszüge aus der Online-Befragung der Bürger zu Beginn des Jahres 2024 vorgestellt.

Sicherheitsempfinden

Die subjektive Einschätzung der Umgebungssicherheit durch die Bürgerinnen und Bürger ist ein wichtiger Faktor für Akzeptanz. Die gefühlte Sicherheit kann durch Faktoren wie gut beleuchtete und übersichtliche Flächen, Fluchtwege und technische Maßnahmen wie Videoüberwachung erhöht werden und ist abhängig von der Tageszeit[23; 24; 25]. So fühlen sich die Menschen nachts im Allgemeinen weniger sicher als tagsüber, und im Allgemeinen geben Frauen ein geringeres Sicherheitsempfinden an als Männer. Dies bestätigt sich in der vorliegenden Befragung (siehe Abbildung 6). Die Auswertungen zeigen, dass der Einsatz von KI-gestützter Radarbeobachtungstechnologie potenziell das Sicherheitsempfinden im öffentlichen Raum steigern könnte, insbesondere nachts. Tagsüber bleibt das Sicherheitsempfinden bei möglichem Einsatz der Technologie nahezu unverändert. Zusätzlich bestätigen die Ergebnisse, dass Männer im Vergleich zu Frauen ein höheres Sicherheitsempfinden besitzen.

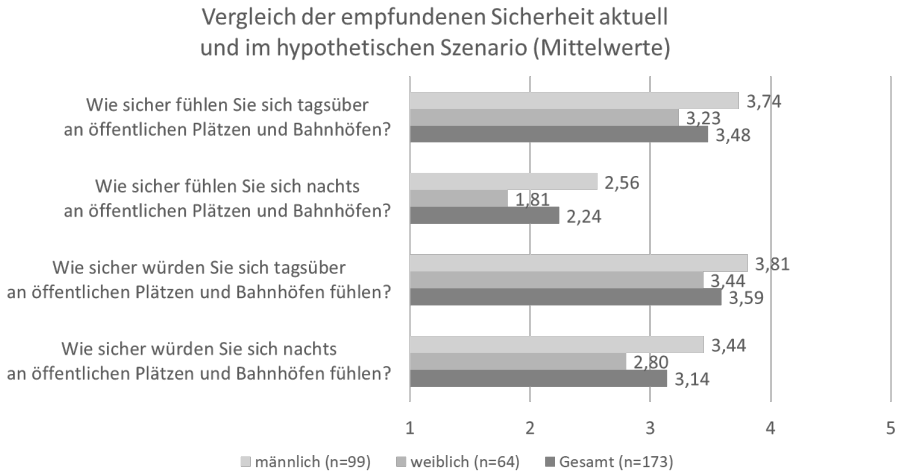

Abbildung 6. Aktuelles Sicherheitsempfinden und hypothetisches Sicherheitsempfinden bei Einsatz der KI-gestützte Radartechnologie (Fünfstufige-Skalen: von 1 sehr unsicher bis 5 sehr sicher)

[23] Gerhold, L. (Hrsg.) (2020). Sicherheitsempfinden, Sicherheitskommunikation und Sicherheitsmaßnahmen. Ergebnisse aus dem Forschungsverbund WiSima. Schriftenreihe Sicherheit des Forschungsforum Öffentliche Sicherheit, Nr. 27. Freie Universität Berlin, Berlin

[24] Birkel, C., Church, D., Erdmann, A., Hager, A., Leitgöb-Guzy, N. (2020). Sicherheit und Kriminalität in Deutschland - SKiD 2020. Bundesweite Kernbefunde des Viktimisierungssurvey des Bundeskriminalamts und der Polizei der Länder, 2020th edn. Bundeskriminalamt, Wiesbaden

[25] Köhn, A., Bornewasser, M. (2012). Subjektives Sicherheitsempfinden. Kooperative Sicherheitspolitik in der Stadt (KoSiPol). Working Paper Nr.9. Westfälische Wilhelms - Universität Münster, Münster. https://nbn-resolving.de/urn:nbn:de:hbz:6-01409437781

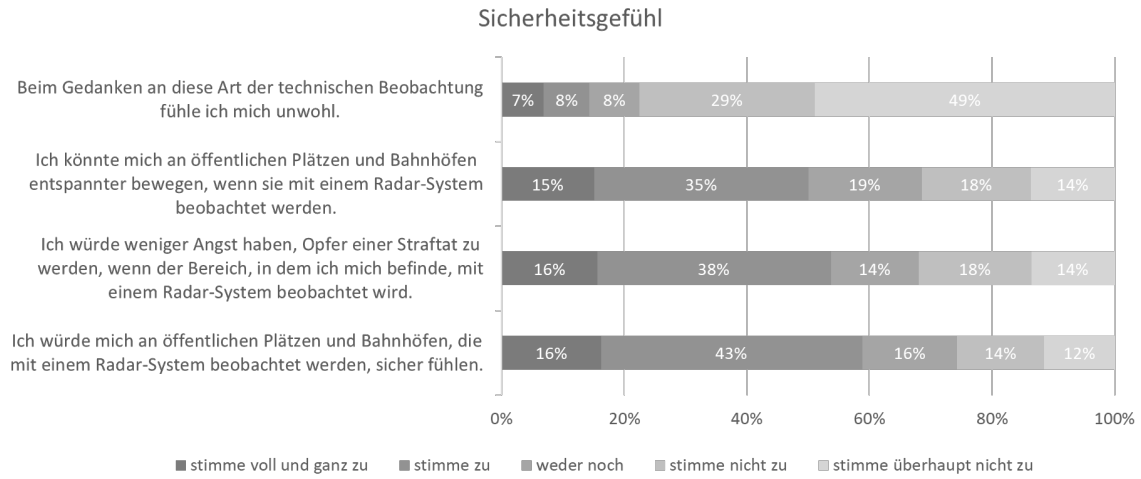

Abbildung 7. Überwachungs- und Sicherheitsgefühl

Technikakzeptanz

Die Befragung basierte auf den vorherigen Interviews sowie dem theoretischen Technikakzeptanz-Modell (TAM-VS). Auf Grundlage der Interviewdaten wurde jedoch das Konstrukt „potenzielle Fehlerquellen“ der KI neu aufgenommen, während das Konstrukt „Transparenz“ nicht abgefragt wurde. Eine erste deskriptive Auswertung der Akzeptanz zeigt insgesamt eine positive und akzeptierende Haltung gegenüber der Technologie. Die Mehrheit der Teilnehmenden bewertet die Technologie als einen wünschenswerten Fortschritt (ca. 70%) und spricht sich für die Installation weiterer Technologien dieser Art aus (ca. 65%). Etwa 83% der Befragten lehnen ein Verbot solcher Technologien ab. Die Ergebnisse deuten darauf hin, dass die Bürgerinnen und Bürger diese Technologie im Interesse ihrer Sicherheit akzeptieren und unterstützen (siehe Abbildung 8). Mehr als die Hälfte der Teilnehmenden ist bereit, die KI-gestützte Radartechnologie im öffentlichen Raum zu akzeptieren.

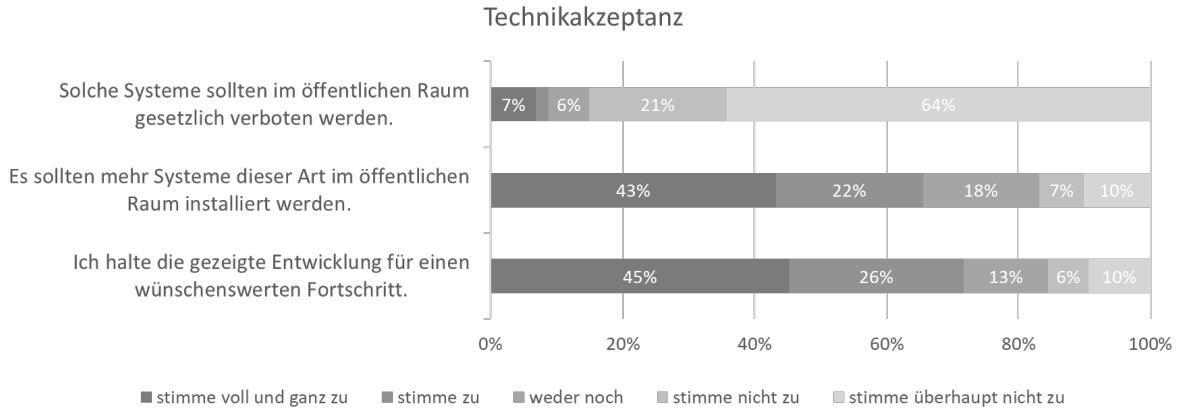

Abbildung 8. Technikakzeptanz

Mittels statistischer Regressionsanalysen (siehe Tabelle 3 und Tabelle 4) wurden die Einflussfaktoren ermittelt, die die Akzeptanz der Technologie bestimmen. Die Förderung dieser Prädiktoren könnte potenziell zu einer Steigerung der Akzeptanz führen. Die Ergebnisse zeigen, dass die Akzeptanz der KI-gestützten Radartechnologie maßgeblich von der emotionalen Einstellung und der empfundenen

Nützlichkeit abhängt. Eine positive Bewertung sowie die Wahrnehmung des Nutzens führen zu einer höheren Akzeptanz. Darüber hinaus wird die emotionale Einstellung zur Technologie sowohl durch die empfundene Nützlichkeit als auch durch das wahrgenommene Missbrauchsrisiko stark beeinflusst. Während eine hohe Nützlichkeit die Einstellung positiv beeinflusst, führt ein erhöhtes Missbrauchsrisiko zu einer negativeren Wahrnehmung. Auch Datenschutzbedenken und potenzielle Fehlerquellen spielen eine Rolle, wenn auch in geringerem Maße. Eine verstärkte Sensibilisierung für diese Aspekte könnte daher die Einstellung zur Technologie weiter verbessern.

Tabelle 3. Regression auf Technikakzeptanz

	Regressions-koeffizient	Std. Fehler	Beta	T-Wert	p-Wert
(Konstante)	,611	,136		4,484	<,001
Emot. Einstellung	,777	,053	,776	14,684	<,001
Empf. Nützlichkeit	,154	,055	,149	2,827	,005

Anmerkungen: N = 173; R^2 = ,80; korr. R^2 = ,80; F(2,170) = 98,67

Tabelle 4. Regression auf Emotionale Einstellung

	Regressions-koeffizient	Std. Fehler	Beta	T-Wert	p-Wert
(Konstante)	2,218	,375		5,921	<,001
Pot. Fehlerquellen	-,135	,067	-,095	-2,009	,046
Anonymisierung	,170	,072	,150	2,364	,019
Empf. Missbrauchsrisiko	-,273	,060	-,257	-4,524	<,001
Empf. Nützlichkeit	,582	,056	,564	10,412	<,001

Anmerkungen: N = 173; R^2 = ,71; korr. R^2 = ,71; F(4,168) = 104,22

Diese Erkenntnisse deuten darauf hin, dass die erfassten Einflussfaktoren einen starken bis mittleren Einfluss auf die Technikakzeptanz haben können. Eine differenzierte Betrachtung dieser Faktoren sowie ein besseres Verständnis der Wahrnehmung können dabei helfen, die Akzeptanz zu steigern. Im Folgenden wird ein kurzer Überblick über die wichtigsten Einflussfaktoren gegeben.

Mit dem „Empfundenes Missbrauchsrisiko“ wurde untersucht, inwieweit die Befragten befürchten, dass durch Fehler in der Datenerfassung oder -verarbeitung Nachteile entstehen oder dass die Daten missbräuchlich genutzt werden könnten. Die Mehrheit der Teilnehmenden äußert geringe bis keine Bedenken hinsichtlich des Missbrauchsrisikos der Daten (siehe Abbildung 9).

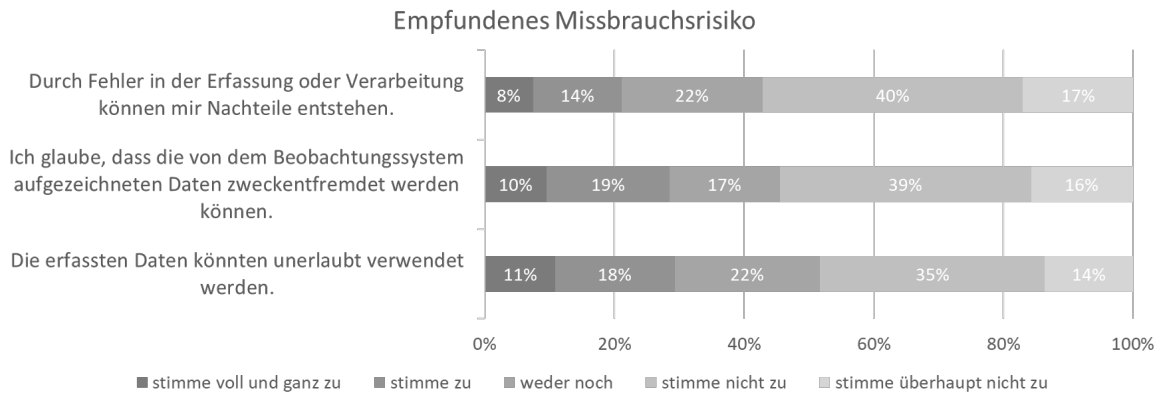

Abbildung 9. Empfundenes Missbrauchsrisiko

Die „Potenzielle Fehlerquellen“ erfassen mögliche Fehler im System, beispielsweise ob es in Notfällen versagen oder Fehlalarme auslösen könnte. Mehr als die Häfte der Befragte halten es für möglich, dass das System fehleranfällig ist (siehe Abbildung 10).

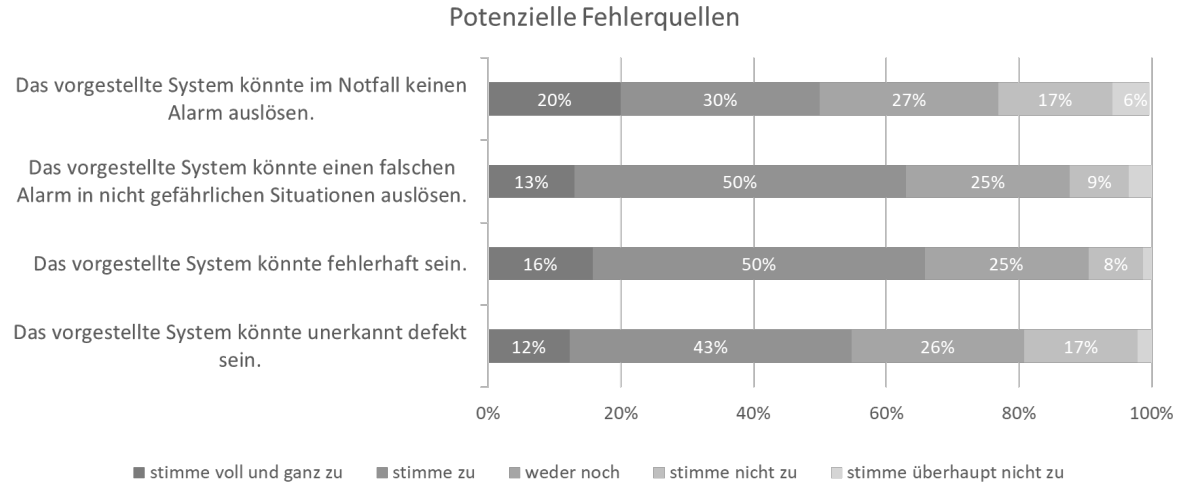

Abbildung 10. Potenzielle Fehlerquellen

Mit der „Anonymisierung“ wird die Wahrnehmung des Datenschutzes sowie der Wahrung der Anonymität erfasst. Die Mehrheit der Befragten gibt an, dass sie durch das Beobachtungssystem keine Verletzung des Datenschutzes befürchtet und den Schutz ihrer Privatsphäre sowie die Sicherheit und Vertraulichkeit ihrer Daten gewährleistet sieht (siehe Abbildung 11).

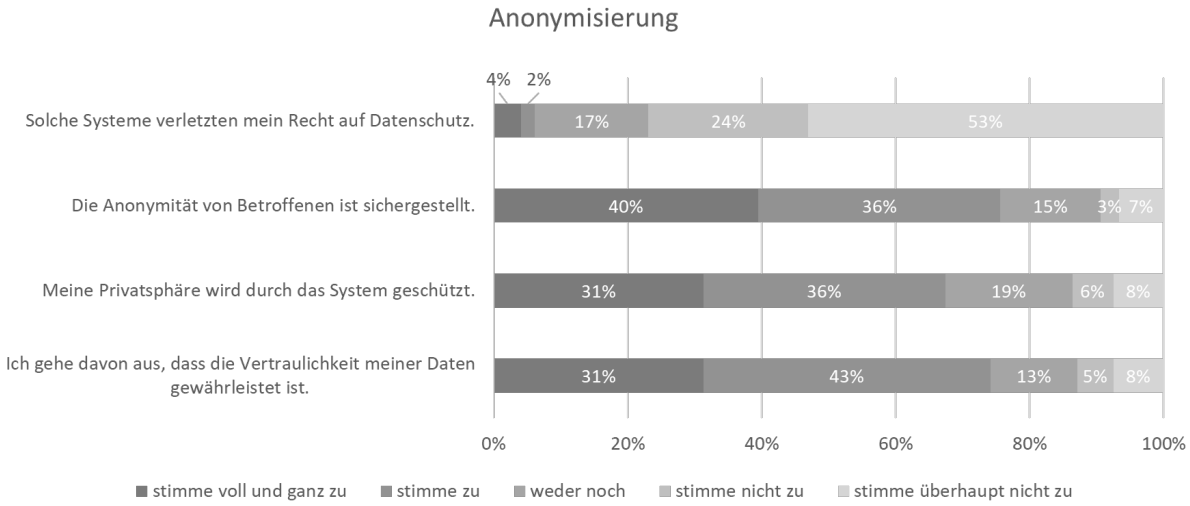

Abbildung 11. Anonymisierung

Mit der „Emotionale Einstellung“ wurde die Haltung gegenüber dem Beobachtungssystem erfasst. Die Mehrheit der Befragten hält den Einsatz für sinnvoll, macht sich keine Sorgen über das System und fühlt sich dadurch sicher (siehe Abbildung 12).

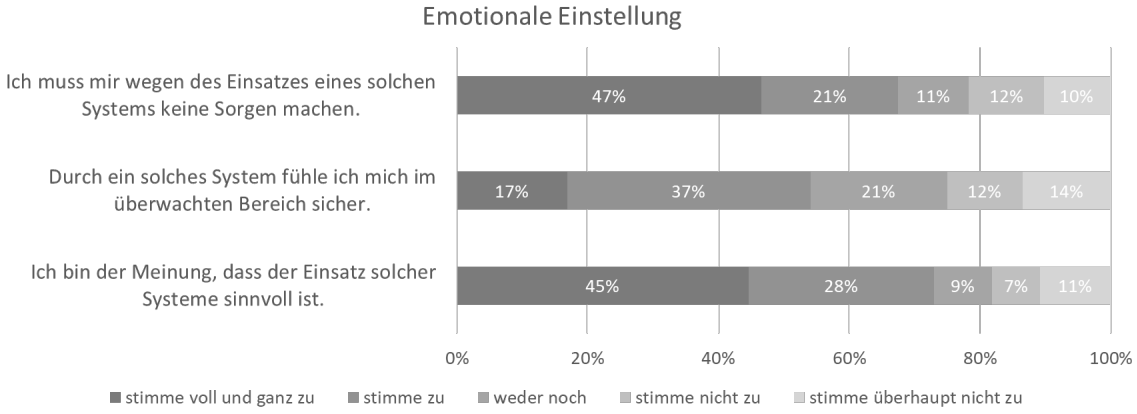

Abbildung 12. Emotionale Einstellung

Mit der „Empfundene Nützlichkeit“ wurde untersucht, wie nützlich das Beobachtungssystem für die Sicherheit wahrgenommen wird. Die Ergebnisse zeigen, dass es grundsätzlich als hilfreich empfunden wird, insbesondere bei akuten Sicherheitsproblemen oder der Erkennung von Straftaten und gefährlichen Situationen. Im Bereich der Verhinderung von Straftaten wird der Nutzen jedoch vergleichsweise geringer eingeschätzt (siehe Abbildung 13).

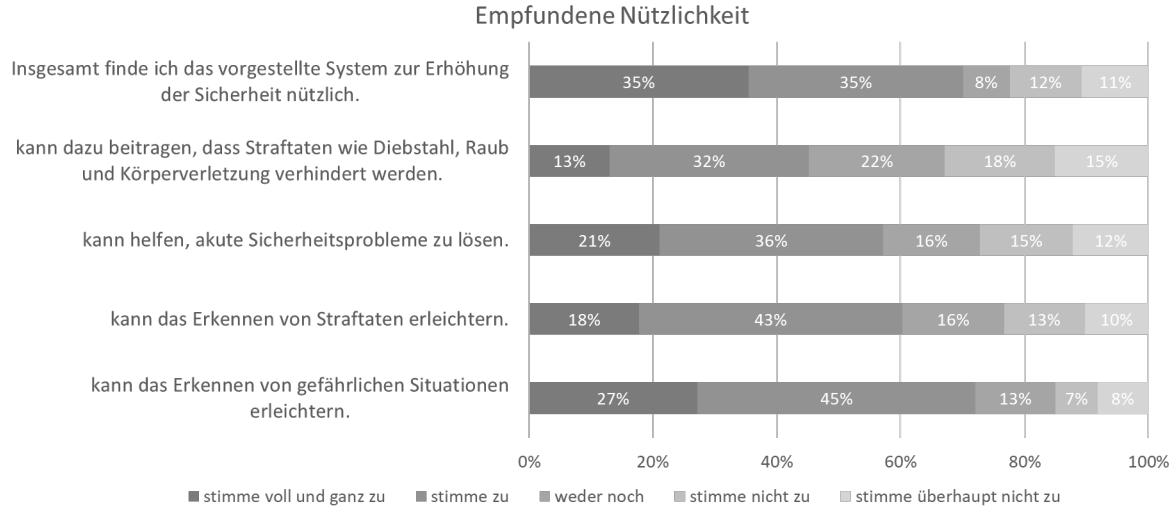

Abbildung 13. Empfundene Nützlichkeit

Zusammenfassend zeigt die Befragung eine überwiegend positive Bewertung der KI-gestützten Radarbeobachtungstechnologie. Die Mehrheit der Befragten hat keine großen Bedenken hinsichtlich des Missbrauchsrisikos der Daten sowie des Datenschutzes und der Privatsphäre. Allerdings bestehen stärkere Bedenken bezüglich möglicher technischer Fehler. Insgesamt zeigt sich eine grundsätzlich positive Einstellung gegenüber der Technologie, wobei der Nutzen von der Mehrheit anerkannt wird.

6.2.3 Workshops und weitere Öffentlichkeitsarbeit

Die Ergebnisse aus Interview-Erhebungen und Online-Befragung wurden auf dem Smart City Summit, 28. Fachtagung der Gesellschaft für angewandte Wirtschaftspsychologie (GWPs) und Gemeinschaften in Neuen Medien (GeNeMe) 2024 vorgestellt und mit betroffenen Bürgern diskutiert. Ähnlich wie in der Befragung konnte eine Akzeptanz der Technologien bei Betroffenen festgestellt werden, wenn auch hier – wie bei der Befragung wieder eine Selbstselektion von Interessierten – stattfindet. Die Personen, die den Nahverkehr eigentlich nutzen, sowie potenziell vulnerable Gruppen sind unterrepräsentiert.

Eine eigene Website mit umfangreichen Informationen wurde unter https://www.hs-niederrhein.de/auge/kirapol5g/ erarbeitet und von der regionalen Presse auch rege genutzt. Die Öffentlichkeit wurde über den Projektverlauf kontinuierlich informiert: Über Workshops in der Öffentlichkeit, z.B. am Smart City Summit in Mönchengladbach erfolgte ein regelmäßiger und intensiver Austausch mit der interessierten Öffentlichkeit. Fünf breit gestreute Berichte in den regionalen Medien erzeugten eine hohe Sensibilität für das Projekt.

Zur Information der Öffentlichkeitsarbeit wurden zu den Technologien eine Website mit FAQs (Frequently Asked Questions) erstellt sowie weitere Informationsmaterialien über die eingesetzten Methoden und Ergebnisse sind bereitgestellt.

7 Ein Fazit mit Danksagung

Die Arbeit an den ethischen, legalen und sozialen Implikationen im Projekt KIRAPol.5G war für alle beteiligten Entwicklerinnen und Entwickler ein Prozess, der von Lernschleifen und intensivem Austausch bestimmt war. Ein sehr großer Dank gebührt den Datenschutzbeauftragten der Unternehmen, der Bundespolizei und v.a. dem Datenschutzbeauftragten der Hochschule Niederrhein, die den teils mühsamen Prozess mit großer Geduld und Hingabe begleiteten. Großer Dank gebührt dem Ethikteam von KI Campus, das in einem zweitägigen Workshop das KIRAPol.5G-Team coachte und in einem intensiven Prozess auch mögliche Optimierungen der Technologie anstieß.

Im Projekt wurde insgesamt deutlich, dass vielfältige Disziplinen mit viel Respekt für die unterschiedlichen Blickwinkel der Disziplinen sinnvoll zusammenwirken können, und damit das Verständnis für die notwendigen Anpassungen in der Entwicklung und möglichen Wirkungen von Technik im sozialen Raum erweitern. Technikfremde Blickwinkel oder ein Hinterfragen wurden als wertvoller Beitrag seitens der Informatik und Ingenieurwissenschaft gewertet; die Sozialwissenschaften mussten lernen, die technologischen Komponenten zu verstehen und die Komplexität der technologischen Prozesse zu durchdringen.

Ein Learning für die Zukunft ist, dass Digital Literacy wird in Zukunft noch mehr umfassen müssen als ein reines Anwendungswissen. Gerade im Kontext der KI wird erforderlich sein, die System- und Anwendungsgrenzen mitzudenken. Da braucht es umfassendes Verständnis für Technologien als Grundwissen auch auf gesellschaftlicher Ebene. Da sind Unternehmen wichtige Partner in einem gesellschaftlichen Lernprozess, und es ist notwendig ethische Technikentwicklung sowie eine ethische Unternehmensführung im Kontext der Digitalisierung zu verankern.