# DiDaT
# Ein transdisziplinäres Forschungsprojekt

# Booklet der Feinpläne zur 2. Stakeholderkonferenz

## 22. Januar 2020

Editiert von Larissa Kätker, Dirk Marx, Marcel Mönch, Roland Scholz, Verena Zyl-Bulitta

Die Veranstaltung wird von dem «DiDaT Stakeholder Konferenz Konsortium» finanziert, welches aus BTU Cottbus, Deutsche Bahn AG, Donau Universität Krems, Fraunhofer Fokus Berlin, NABU, TMG Systemhaus Lauf, Uni Bremen (ABWL) besteht.

**Verantwortlich:**
Transdisziplinäre Ko-Leitung: M. Beckerdahl, S. Noller, O. Renn, R. W. Scholz
Wissenschaftliche Leitung: E. Albrecht, M. Mißler-Behr, O. Renn, R. W. Scholz
Die Grundfinanzierung erfolgt durch BMBF FONA (11-2019 bis10-2021)

Liebe Teilnehmerinnen und Teilnehmer der 2. Stakeholderkonferenz,

die sieben Arbeitsgruppen der Vulnerabilitätsräume haben sich seit Oktober 2018 sukzessive vervollständigt und Grundlagen für die Erarbeitung der Kapitel des Weißbuches erstellt. Mit den nachfolgenden Feinplänen wurde ein erster Umriss der „sozial robusten Orientierungen“ mit dem Ziel skizziert in dem Weißbuch fünf bis sieben Orientierungen für einschlägige/relevante Unseens zu konstruieren.

Unsere 1. Veranstaltung bei Fraunhofer Fokus Berlin soll uns weiter dabei unterstützen, das transdisziplinäre Forschungsprojekt DiDaT gemeinsam voranzubringen.

Viel Spaß auf der Konferenz und beste Grüße wünschen

Roland Scholz & Dirk Marx

# Inhaltsverzeichnis

DiDaT

Digitale Daten als
Gegenstand eines
transdisziplinären
Prozesses

# Vulnerabilitätsraum 01 (VR01)

# Digitale Mobilitätssysteme und vernetzte Räume

DiDaT Grobplanung für Vulnerabilitätsraum 01 (VR01)

# Digitale Mobilitätssysteme und vernetzte Räume

*Markus Hofmann (Universität Freiburg, NETWORK Institute), Karl Teille (AutoUni), Denise Baidinger (Deutsche Bahn AG), Walter Palmetshofer, Wolfgang Serbser (European College of Human Ecology), Johanna Tiffe (Form: F), Thomas Waschke (die denkbank)*

## 1. Gegenstand, Ziele und Leitfrage

Mobilität von Menschen und Gütern, als ein gesellschaftliches Grundbedürfnis, wird durch die Nutzung unterschiedlicher Infrastruktur- und Verkehrssysteme, Fahrzeuge und Dienstleistungen ermöglicht. Mobilität ist eine nicht speicherbare Dienstleistung in einem sozialen System, die das koordinierte Zusammenwirken von Personen, Infrastruktur- und Transportsystemen und Energieträgern voraussetzt, was im Sinne einer erweiterten Systembetrachtung auch aktive Mobilität wie Radfahren oder Laufen im physischen, meist öffentlichen Raum umfasst. Durch die zunehmende Digitalisierung und die globale Vernetzung unterliegen die Anforderungen an Infrastruktursysteme und Fahrzeuge einer grundlegenden Dynamik, die durch die Verfügbarkeit und den Zugang zu Daten, deren Austausch und wirtschaftliche Nutzung angetrieben wird. Dabei ist anzunehmen, dass das Internet sich als universale-Infrastruktur der Moderne für Kommunikation zwischen Personen sowie die Vernetzung von Maschinen dynamisch weiterentwickeln und auch eine zentrale Koordinationsfunktion im Mobilitätssektor übernehmen wird. Durch die digitale Abbildung und Simulation von Mobilitätsbedürfnissen können Angebot und Nachfrage im Mobilitätssektor digital sicher erfasst, Fahrzeugeinsatz und Passagierströme gelenkt und Verkehrsflüsse effizient koordiniert werden. Dazu wären zeitnah große Datenmengen von Verkehrsteilnehmern und Fahrzeugen zu erfassen. Je nach Verwendungszweck der Daten sind dazu Rechte, Pflichten und Erhebungsintervalle sowie Pull und Push Strategien von zukünftigen Infrastrukturbetreibern und Datendiensten abzuwägen.[1] In einer traditionell geprägten Branche und den Kommunen sind innovative Angebote, veränderte Wertschöpfungsstrukturen und neue Handlungsoptionen absehbare Entwicklungen, die sowohl positive wie auch negative Auswirkungen als Folge für Mensch, Natur und die Wirtschaft oder Gesellschaft haben können. Eine Vernetzung von Infrastruktur, Fahrzeugen, Gütern und Nutzern in Echtzeit birgt große wirtschaftliche Chancen und erhöht gleichzeitig die Komplexität, verbunden mit Interdependenzen und Systemabhängigkeiten sowie neuartigen Risiken.

**DiDaT** untersucht mögliche Auswirkungen auf Mobilitätsakteure, Räume und Umwelt und mit dem Anspruch zur nachhaltigen Gestaltung von digitalen Mobilitätssystemen

[1] Konzeptdiskussion: Mündiger Bürger vs. Staatliche Ordnung in asymmetrischen Märkten

Vulnerabilitäten aufzuzeigen und Vorschläge für gesellschaftliche Leitplanken vordenken und deren Entwicklung anregen zu können.

Angesichts dieser – in einigen Bereichen stärker, in anderen weniger – disruptiven Entwicklungen im Mobilitätssektor wurden von einem transdisziplinären Team die folgenden, lösungsorientierten **Leitfragen** für den VR „Digitale Mobilitätssysteme und vernetzte Räume“ entwickelt:

**Analyseraum**

**Wie wirkt die Digitalisierung der Mobilitätssysteme - insbesondere KI und Automatisierung der Fahrfunktion – aus auf die Beziehungen von „Mensch“ ↔ Maschine, Bevölkerung ↔ Umwelt und Nutzung ↔ Eigentum und somit auf das individuelle räumliche Mobilitätsverhalten?**

**Welche Risiken und Vulnerabilitäten sind durch die digitalen Entwicklungen im Mobilitätssektor denkbar und zu erwarten? Welche sekundären Auswirkungen sind möglich?**

**Wie können potenzielle Interessenskonflikte zwischen öffentlichen, privaten und kommerziellen Akteuren transparent gemacht werden und wie wird Zugang zu privaten und öffentlichen Daten, Infrastruktursystemen und Mobilitätsangeboten verbindlich und sozial gerecht gestaltet?**

**Innovationsraum**

**DiDaT will in VR01 die dichotome Betrachtung von privaten Gütern in Märkten und gesellschaftliche Anforderungen an modernen Commons aus der Perspektive einzelner Akteursgruppen aufzeigen. Welche Rahmenbedingungen wären förderlich, um bei der zunehmenden Digitalisierung des Mobilitätssektors soziale, ökonomische oder ökologische Anforderungen in Einklang zu bringen und – unter Wahrung einer noch zu definierenden «Privatheitssphäre» - sozial robuste Richtlinien und Regeln für den verantwortlichen Umgang mit digitalen Systemen und Daten sicherzustellen?**

## 2. Welche nicht intendierten, unbeabsichtigten Nebenfolgen sind von Interesse und warum?

Die Analyse fokussiert sich auf komplementäre Perspektiven von Mobilität, die in fünf Handlungsebenen beschrieben werden: Die technisch-funktionale Ebene, die soziale und personale Ebene, die rechtlich institutionelle, die ökonomische sowie die physisch-ökologische Ebene. Durch diese bewusste Differenzierung können Ursachen für Vulnerabilitäten z.B. zwischen einem physischen Datenzugang (Leitung, Kanal) und einem rechtlichen Datenzugang (Zugriffs- und Nutzungsrechte) besser zu unterscheiden:

**a. Technisch-Funktionale Ebene:**

Neben der Safety-Funktion für Fahrzeug und Nutzer ist auch die Security im digita-

len und physischen Raum auf höchstem Niveau zu gewährleisten, die hier im VR nicht weiter vertieft werden.

**A1) Datennutzungs-Allokationsmodell:**

Abhängigkeit von universeller Regelung von Datenzugang, Nutzung und Verwertung [2] Die Frage des Zugangs, der Nutzung, des Eigentums und des Wertes von Daten eines Fahrzeuges bzw. Verkehrsteilnehmers wird zum Schlüssel für eine nachhaltige Gestaltung von Verkehrssystemen und -räumen, Infrastrukturen und attraktiven und stärker automatisierten Mobilitätsangeboten sowie die intermodale Abrechnung von Mobilitätsleistungen (Mobility as a Service, MaaS). Dabei entsteht durch die unverstandene Wechselbeziehung von Zugang, Nutzung, Wert von Daten ein gesellschaftlicher Handlungsbedarf, der die Verwundbarkeit von persönlichen Schutzrechten, Eigentumsrechten und übergeordnete Anforderung des Gemeinwesens neu ordnet. Darauf hat der internationale Experten Round Table des BMBF 2016/17 hingewiesen. Wir sprechen dabei von personalisierten Daten und nicht-personenbezogenen oder anonymisierten Metadaten. Es besteht Regelungsbedarf, der über das wirtschaftliche Eigentum an Daten hinaus auch gesellschaftliche Nutzung und die soziale Robustheit berücksichtigt.

**A2) Abhängigkeit von wenigen Dateninfrastrukturbetreibern (DIP[3]) - Monopol der digitalen Ökosysteme:**

Unter der Bezeichnung „Mobility as a Service“ (MaaS) entstehen neue Dienstleistungen und Geschäftsmodelle, die eine zunehmende Trennung von physischen Assets und Wertschöpfung durch Dienstleistung ermöglichen (Asset light). Als Folge könnten internationale Plattformbetreiber im Mobilitätssektor technische und faktische Monopole bilden, die Netzwerk- und Skaleneffekte nutzen und gleichzeitig Datenschutz, soziale Standards und ggfls. Sicherheitsanforderungen (durch Datenverarbeitung außerhalb der EU) absenken. Für Nutzer/Reisenden, Firmen sowie die öffentliche Hand kann dadurch eine Abhängigkeit von wenigen Daten-Infrastruktur-Anbietern entstehen. (Beispiel sind Moia, HERE, Flixbus, AirBnB und UBER). Es stellt sich die Frage, welche Daten eines Fahrzeuges (Objekt) und eines Verkehrsteilnehmers (Subjekt z.B. Reiseroute) sollen mit wem (DIP; Nutzer, Dritte) geteilt werden oder im Interesse der Allgemeinheit als open Access generell bereitgestellt werden.

**A3) Machtmissbrauch durch Oligopole:** - Surveillance Abhängigkeit von intransparenten Algorithmen und autonom entscheidende KI Systeme

Durch KI und digitale Subjekte[4] entsteht eine nie gekannte „Konsequenz“ systemischer Digitalisierung, die Entscheidungen

[2] European Round-Table Bezug, BMBF (Quelle Verena)

[3] DIP Digital Infrastructure Provider – (Suprastaatliche Akteure) DEFINTION PRÜFEN

[4] Da Algorithmen individuelle Entscheidungsprozesse von Menschen zunehmend ersetzten, bliebe als zentraler Lösungsansatz, 'an die Algorithmen selbst heranzugehen'. Normative Standards müssten ebenso wie menschliche Entscheider integriert werden und kompetitive Systeme und Plattformen erhalten bleiben, um ausschließlich algorithmenbasierte Entscheidungsmonopole zu verhindern."
hhttps://akademie-der-polizei.hamburg.de/verschiedene-veranstaltungen/11592502/systemische-digitalisierung-a/

über Mobilität und Datennutzung auf leistungsstarke Maschinen überträgt. Dabei ist die Berücksichtigung von ethischen und sozialen Kriterien noch nicht definiert, bzw. kulturell unterschiedliche geprägt. (Vgl. MIT Moral Machine Experiment 2016ff). Gleichzeitig kann ein Verschlafen innovativer Trends und mangelnde europäische Aktivitäten bei der Standardisierung eine Verlagerung der Wortschöpfung und eine Monopolbildung zu Lasten Europas für Fahrzeugtechnologien und Mobilitätsdienste Beschleunigen.

**b. Soziale und personale Ebene:**

**A4.1) Umweltzerstörungs-Brandbeschleuniger:** Mehrverkehr und Emissionen durch Rebound Effekte

Die Digitalisierung im Mobilitätssektor könnte zu Rebound Effekten führen wie Mehrverkehr, zu negativen Umwelteffekten und einer Verschlechterung der öffentlichen Gesundheit (IT-Energieverbrauch, Schadstoffe, Lärm, Bewegungsmangel). Auch preisreduzierte Angebote (free oder flatrate Mobilität) können zu negativen Auswirkungen führen.

**A4.2)** Die Gestaltung von Städten als soziale Räume, Infrastruktursystemen und Siedlungsstrukturen – abhängig von Transportkosten und Raumwiderständen - und die Gestaltung des öffentlichen Raumes (auch Verkehrsräume und ruhender Verkehr) wirken dauerhaft auf das Mobilitätsverhalten und die Umwelt. Aus sozialen Überlegungen sind beispielsweise lokale oder nicht-kommerzielle Angebote für Mobilität (z.B. Sharing-, Senioren-, Behinderten- und weitere Mitfahrangebote) diskriminierungsfrei in digitale Mobilitätsassistenten anderer Anbieter (z.B. Plattformen) zu integrieren.

**A4.3) Verwundbarkeit durch Zunahme der internationalen Mobilität**

Globale Frachtströme, Fernpendler in Arbeitsverhältnissen, Mobilie Nomaden.

**A4.4) Abhängigkeiten durch erhöhte Intermodale Mobilität**

Vernetzung, Betreiberübergreifende Informations- und Buchungs-Systeme, Handover- und Roaming Modelle, Mikromobilität

**c. Rechtliche und Institutionelle Ebene:**

**Dysfunktionale Übertragung analog entstandener Rechtssysteme im Mobilitätssektor**

**A5) Verwundbarkeit durch Steuerungs- und Maintenance-Monopole durch Dritte**

Den technischen Einsatzmöglichkeiten der automatisierten Steuerung von Mobilitätsprozessen, beispielsweise einer integrierten Verkehrslenkung oder Messungen für präventiven Instandhaltung, stehen heute nur unzureichend geklärte Zugangs- und Nutzungsrechte zwischen Herstellern und Betreibern von Mobilitätssystemen gegenüber. Dieses Risiko trifft auch die Systemnutzer und die öffentliche Hand, die als Leistungsbesteller auftritt sowie als Aufsichtsfunktion. Insbesondere die neuen Anbieter nutzen diese Freiräume zur Entwicklung von neuen Produkten, umfangreichen Analysen und Prozessoptimierung. In Bezug auf wirtschaftliches Eigentum, Nutzung, öffentliche Räume und Interessen sind diese Rechtsgüter auch mit den Akteuren außerhalb der EU verbindlich auszuhandeln.

**A6) Abhängigkeit durch Verlust der Daten-Souveränität**

Schutz und Nutzungsallokation (A1) Dieses Risiko für eine unbeabsichtigte Datennutzung sowie Missbrauch in betrügerischer Absicht (Fraud) erhöht sich überproportional, wenn durch Dritte oder aufgrund mangelnder Compliance die Anonymität der Verkehrsteilnehmer nicht mehr ausreichend geschützt wird. Zur Vermeidung dieses Missbrauchs von Nutzer- und Systemdaten ist eine Anpassung des Verkehrs- und Infrastrukturrechts, die Schaffung eines fehlenden Rechtsrahmen für organisierten und vernetzten Individualverkehr (und Logistik) erforderlich. Für die systematische Analyse der Problematik und die Entwicklung differenzierte Regelwerke mit spezifischen Rechten und Pflichten für Infrastrukturbetreiber, Diensteanbieter und Nutzer könnte sich eine mobilitätsrelevante Taxonomie für «öffentliche» und «private» Daten (z.B. Objekte, Räume, Nutzer) als sinnvoll erweisen.

**A7) Verwundbarkeit durch - nicht rechtsstaatliche - Überwachung und intransparente, private Sicherheitsprävention (Surveillance).**

Die Digitalisierung der Mobilität kann durch Monitoring von Verkehrsbewegungen und einer automatisierten Überwachungen öffentlicher Räume zur Gefahrenprävention herangezogen werden, gleichzeitig kann diese Entwicklung jedoch zu einer Erosion des Datenschutzes und der Selbstbestimmung der Bürger (Datensouveränität, Mobilitäts-Souveränität) führen. Durch Terrorbedrohung und Anonymität in digitalen Netzen erfordern Sicherheitsabwägungen (Terror, Sabotage) möglicherweise neue hoheitliche Schutz- und Eingriffsmöglichkeiten der öffentlichen Hand. Privacy und Datenschutz sind in Europa individuell unveräußerliche Rechte, die im Zeitalter asymmetrischer, digitaler Risiken neu zu definieren sind.

**d. Ökonomische Ebene:**

**A8.1) Abhängigkeit von neuen Marktteilnehmern**

Die mit der Digitalisierung verbundene Vernetzung im Mobilitätssektor ermöglicht den Eintritt neuer Anbieter, mit servicebasierten Geschäftsmodellen, und verändert die traditionellen Angebotsstrukturen. Ein Rückgang der Anbietervielfalt insbesondere im ländlichen Raum kann somit zu einem Verlust der zivilgesellschaftlichen Gestaltungsmöglichkeiten führen. Hier gilt es eine sinnvolle Abgrenzung von legitimen Geschäftsinteressen, individuellen Nutzungsrechten und Belangen der öffentliche Daseinsvorsorge und einen verantwortlichen Umgang mit Gemeingütern (Städte, öffentlicher Raum, Mobilität sowie der Gesundheitsaspekte) zu finden.

Restrukturierung der Wertschöpfung vom Fahrzeug- zum Datenmarkt Veränderung Wettbewerbsregeln und Wettbewerbsteilnehmer – Wertschöpfung durch Datenmanagement – Asset light – Kapital, Arbeit, Resources inkl. Daten,

**A8.2) Abhängigkeiten vom globalen Markt für Mobilitätssysteme**

Aufgrund der hohen wirtschaftlichen Bedeutung des Maschinenbaus für den Standort Deutschland sowie die gestiegenen Abhängigkeiten im globalen Markt für Mobilitätssysteme, Fahrzeuge und Dienstleistungen sind hier auch wirtschaftliche Risiken in

die Betrachtung der Unseens einzubeziehen.

**e. Physische und ökologische Ebene:**

A9) Verwundbarkeit sensibler Ökosysteme Mobilität ist immer physisch und bedarf daher wirksamer Schutzmechanismen für Leib und Leben (safety). Mobilität und technische Systeme benötigen Energie, so dass Grundbedürfnisse nach Mobilität bei hoher Digitalisierung im Falle des Ausfalls von Energie- oder Kommunikationsnetzen, bei Naturkatastrophen, Blackout, Sabotage oder Terror- sowie im Verteidigungsfall stark eingeschränkt werden könnten. Sicherung der Ausfallsicherheit durch redundante Systemfunktionen und eingebaute System-Resilienz (Recovery time)

**A10) Raumstrukturelle Auswirkungen** → Dauerhafte Veränderungen in Siedlungs- und Wegestrukturen als Folge neuer, digital gesteuerter Mobilitätsangebote (automatisierte Güter, autonomes Fahren), Auswirkungen auf Nachhaltigkeit von Pendler- und Warenströme, Innenstädte (ruhender Verkehr), Agglomerationen und den ländlichen Raum.

**A11) Verwundbarkeit durch Stoffliche Umwelteinflüsse**

Mobilität benötigt Energie und verursacht Emissionen. Trotz technischer Fortschritte ist die CO2-Belastung durch Mobilität ist in den letzten 30 Jahren in Deutschland nahezu konstant geblieben. Auch Elektromobilität, Digitalisierung und der Einsatz autonomer Fahrzeuge sind nicht per se umweltverträglich. Durch nachhaltige Stoffbilanzen soll Transparenz sichergestellt und eine messbare Reduktion physischer Verbräuche je Leistungseinheit erreicht werden. Der Übergang zu Elektromobilität führt zu erheblichen Verschiebungen in der stofflichen Basis der technologischen Schlüsselkomponenten – vom Verbrennungsmotor zu E-Motor und Batterie. Ebenso verschiebt sich die Relevanz hinsichtlich ökologischer Auswirkungen von der Nutzen- zur Produktionsphase. Dazu kommt der Energiebedarf der digitalen Komponenten und Netzwerke selbst. Die Digitalisierung des Mobilitätssektors ermöglicht – wie Industrie 4.0 – eine sehr vollständige Rückverfolgung der Transporte und Wertschöpfung in intermodalen Mobilitätsnetzwerken. Daten können somit eine stoffliche Bewertung der echten „Kosten“ für Mobilitätssysteme unterstützen, die zur Gestaltung von transparenten Anreiz- und Lenkungssystemen im Sinne der Nachhaltigkeitsziele der Bundesregierung und der EU genutzt werden könnten.

## 3. Auswahl Stakeholder und WissenschaftlerInnen - Welche Kompetenzen aus Wissenschaft und Praxis sind für das Verständnis von „Unseens“ und den Umgang mit Folgen besonders relevant?

Die Beschreibung der Vulnerabilitäten anhand konkreter oder fiktiver Beispiele unterscheidet die Stakeholder nach ihren jeweiligen Rollen, Betroffene, Verursacher und Problemlöser (z.B. Regulator), die zwischen den Vulnerabilitäten situativ durchaus wechseln können.

**Tabelle 1: Vulnerabilitäts/Unseen x Stakeholder Tabelle**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | **Stakeholder/ Vulnerabilitäten** | Infrastruktur-/ Netzbetreiber (Telekommunikation, Energie und Verkehr) | Mobilitäts dienstleister/ new Mobility Anbieter | Fahrzg.-herst./ Zulieferer | System-Hersteller/ Betreiber/DIP | Behörden/ Kommunen/ Besteller | Nutzer/ Verkehrsteilnehmer |
| | **Rollen** | **Verursacher** | | **Betroffene** | | **Problemlöser** | |
| 1 | Datensnutzungsallokation (A6) | Plattformbetreiber, Fahrzeug-Hersteller, Mobilitäts-Dienstleister Behörden | | Unternehmen, Mobilitäts-Dienstleister, Verbünde, Verbraucher, Behörden | | Nationale und internationale Regulierer, Selbstverwaltung, Verbände, | |
| 2 | Allgemeingut vs. wirtschaftliche Privatgut Welche Daten aus dem Fahrzeug werden geteilt (Club Good) oder sind frei (open access, ...) | Plattformbetreiber, Fahrzeug-Hersteller, Mobilitäts-Dienstleister Behörden | | Unternehmen, Mobilitäts-Dienstleister Verbraucher, Hochschulen, Behörden | | Nationale und internationale Regulierer, Selbstverwaltung, Verbände, Berater | |
| 3 | DIP Oligopol-Macht (surveillance-Risiken) | Plattformbetreiber, Fahrzeug-Hersteller Mobilitäts-Dienstle Behörden | | | | Nationale und internati- le Regulierer, stverwaltung, bände, | |
| 4 | Brandbeschleuniger für Ressourcen-verbrauch (Effizienter und billiger und damit mehr km) | Unternehmen, Verbraucher | | Gesell Umwelt, kommende Generationen | | Nationale und internationale Regulierer, Selbstverwaltung, Verbände, Berater | |
| 5 | Dysfunktionale Übertragung analog entstandener Rechtssysteme | Legislative, Behörden, Standardisierungsgremien | | Unternehmen, Verbraucher, Hochschulen, Behörden | | Nationale und internationale Regulierer, Selbstverwaltung, Verbände, Berater | |
| 6 | Restrukturierung der Wertschöpfung vom Fahrzeug zum Datenmarkt (Gefahr für deutsche Auto-Industrie) | Plattformbetreiber, Fahrzeug-Hersteller, Mobilitäts-Dienstleister Verwaltung | | Unternehmen, Verbraucher, Öffentliche Hand, Arbeitnehmer | | Nationale und internationale Regulierer, Selbstverwaltung, Verbände, Berater Gewerkschaften | |
| 7 | Raumstrukturelle Auswirkungen (Siedlung, Warenströme, Wegestruktur) | Plattformbetreiber, Fahrzeug-Hersteller, Mobilitäts-Dienstleister Verwaltung | | Kommunen, Gesellschaft, Umwelt, Gesundheit, kommende Generationen | | Nationale und internationale Regulierer, Politik, Verwaltung | |
| 8 | tbd. | | | | | | |

*AUSWAHL WICHTIGER VULNERABILITÄTEN! Stakeholder sind zu ergänzen und eingängige Beispiele noch zu formulieren!* ***Auteilung auf VR01 Mitglieder!***

Für Mitarbeit und fachlich kritische Begleitung des VR Mobilität wurden Personen angesprochen ihre Expertise als Vertreter ihrer Stakeholdergruppen in das VR Mobilität einzubringen.

- Legislative: Bund/Länder und EU
- Städte/Kommunen, Stadt- und Regionalplaner, Architekten z.B. FHH Hamburg, Wolfsburg
- Regionen, Landkreise, ländliche Räume (smart regions), Akteure
- Verkehrs-Infrastruktur Betreiber, Telekommunikations- und Datennetze-Betreiber
- Mobilitätsanbieter, Fahrzeughersteller, Energieversorger
- Emerging Mobility Services (Car-, Ride, bike- Sharing, MDM, Plattformen)
- Nutzer Verkehrsmodi, Pendler, Berufskraftfahrer, Mobilitätseingeschränkte, Senioren, Kinder
- Konsumenten-Vertreter, NGOs /Umweltorganisationen (VCD, BUND, Open Data, NIMBY)
- New Player: Internet-Unternehmen, Versicherungen, TIMES-Industrie, (Digital Subjects?)

## 4. Unseens-Orientierungen Tabelle VR01

Tabelle 1: Unseens-Orientierungen Tabelle: Von Unseens, Ursachen und Maßnahmen zu sozial robusten Orientierungen.

| | **1. Unseens**<br><br>(behandelt werden hier die „negativen unerwünschten Folgen“) | **2. Ursachen/ Kausalitäten/ Entstehungs-prozesse der Unseens** | **3. Maßnahmen möglicher sozio-technologischer Innovationen zur Mitigation** | **4. Ziele** | **5. Sozial robuste Orientierungen zum Umgang mit Unseens** |
|---|---|---|---|---|---|
| 1 | **Systembarrieren und Datennutzungsallokation** | **Systemzugang und -Datennutzung (1)** Wer gewährt physischen Zugang zu digitalen Mobilitätsdiensten (Digital Divide) Wer generiert, liefert, speichert und nutzt Daten von Fahrzeugen, Personen und Gütern? | Sensibilisierung aller Akteure für Disruption im Mobilitäts-sektor, Kompetenzvermittlung über digitale Systeme und Geschäftsmodelle für Entwickler, Entscheider und Nutzer | Effizienz und Komfort sollen durch Digitale Mobilitätssysteme gesteigert werden, dennoch bleibt Mobilität bleibt ein Grundrecht Leib und Leben der Verkehrs-teilnehmer, sowie Persönlichkeitsrechte und Daten zu schützen ist mit Priorität zu berücksichtigen | *Differenzierte Szenarien für Anwendungsfälle erforderlich:* - Raum-, Stadt- u. Systemplanung -Mobilitätsnutzung Normalfall - Notfall Situationen (Saftey) - Hoheitliche Eingriffe - Systemresilienz - Fraud/Forensik |
| 2 | **Datengenerierung im öffentlichen Verkehrsraum (*Allgemeingut vs. Privatgut;* *Recht auf “Privatsheits-sphäre”*)** | **Datensouveränität (2)** Welche Daten von Verkehrsteilnehmern, Infrastrukturen und Fahrzeugen werden generiert. Was wird | Nachhaltige Qualitätssicherung für innovative Produkte (z.B. Reallabore für Mikromobilität, aut. Fahren). | - Verbindliche und transparente Regeln bei Datenweitergabe und Nutzung durch Dritte (Kommerziell, sonstige) auch | *Rechte/Pflichten für neue Rollen:* System-Hersteller, Supplier |

| | | | | | |
|---|---|---|---|---|---|
| | | geteilt (Club Good) oder ist frei (open access). Wer prüft Kriterien, wo Algorithmen entscheiden? | | für internationale Mobilitätsanbieter (Verbraucherschutz) | Mobilitätsanbieter (trad./new)<br>Infrastruktur-Betreiber (phys.)<br>Digitale Infrastruktur Provider<br>Kommunen als Raumwalter<br>Nutzer, Bürger, next Generation |
| 3 | **Daten-Missbrauch und Überwachungsrisiken durch Digitale Infrastruktur Provider (DIP)** | **Oligopol-Bildung (3)** Infrastrukturkosten fördern Monopolbildung. Netzwerkeffekte führen zu Anbieterkonzentration, oligopolistische Akteure entziehen sich nationaler Kontrolle | Schaffung von Datenstandards und offenen Plattformen für öffentlichen Verkehrsraum<br>Diskriminierungsfreier Systemzugang und reziproke Datennutzungsmodell etablieren.<br>Digitale Barrierefreiheit für Mobilitäts-eingeschränkte und für Non-Digital Nutzer. | -Anbieter verpflichten Standards des jeweiligen Landes zu berücksichtigen,<br>- Hoheitliches Daten-Privileg gewährleisten, int.<br>- Mindest-standards für staatl. Eingriffe, auch international | *Beste Sicherheits-standards:*<br>-System-zugang /Datenzugang<br>- Fahrzeuge u. Leitsysteme<br>- Datenintegrität und –aktualität<br>- Intermodale --Nutzer-Souveränität |
| 4 | **Erhöhter Ressourcenverbrauch durch Zunahme von Mobilität** | **Rebound-Effekte (4)** Effizienzgewinnen führen zu Kostensenkung, die zu mehr Nachfrage (Pkm) führt. Wirkung als Brandbeschleuniger für Ressourcenverbrauch und Klimabelastung. | Transparenzkriterien und Leitlinien für automatisierte Entscheidungen/KI-Einsatz im Verkehr (z.B. autonomes Fahren, Nachhaltigkeit, Saftey).<br><br>. | Digitalisierung als nachhaltigen Beitrag zur Mobilitätswende gestalten, d.h. ökonomische, Soziale und ökologische Ziele in Einklang zu bringen, Investitionen an Gemeinwohl und Klimazielen ausrichten | *Leitplanken für Umweltziele:*<br>„Gemeinwohl“ vor Einzelnutzen<br>Kompatible LCC-Analysen<br>Unterstützung von Klimazielen<br>Verknappung von Raum/Luft<br>Commons-Mechanismen (Allokation.) |
| 5 | **Dysfunktionale Übertragung «analog» entstandener Rechtsysteme auf digitalisierte Geschäftsprozesse** | **Rechtssysteme Upgrade (5)** Ohne Anpassung von Regularien und Sanktionen führen neue Technologien zu sozialen Erosionserscheinungen | Transparenz und praktikable Opt-Out-Mechanismen für Datengenerierung, -speicherung und Nutzung. Definition | Cyberspace kein rechtsfreier Raum,<br>Re-Etablierung von Persönlichkeitsrechten und common sense im vernetzten | Für digitale Mobilitätssysteme sind, wie für alle Verkehrsmittel, Sicherheitsstandards und Prozessqualität |

| | | | | | |
|---|---|---|---|---|---|
| | | | Public-Access Domain und gleichzeitig Begrenzung von Weitergabe an Dritte. | Raum (Briefgeheimnis, anonyme Transportpflicht u.a.) | nachzuweisen (z.B. Simulation als Zulassungsverfahren) |
| 6 | **Restrukturierung der Wertschöpfung vom Fahrzeug zum Datenmarkt (Beschäftigungsrisiko deutsche Autoindustrie)** | **Datengetriebene Geschäftsmodelle (6)** Wertschöpfung durch Daten statt Maschinenbau | Transparenzkriterien und Leitlinien für automatisierte Entscheidungen/KI-Einsatz im Verkehr (z.B. autonomes Fahren, Saftey). | Sicherung Arbeitsplätze und Wohlstand durch Innovation und Migration der Wertschöpfungsnetzwerke | *Globale Perspektive:*<br>- Wirtschaftsfaktor Mobilität<br>-Intern. Rechtssicherheit<br>-Kompatible Standards |
| 7 | **Veränderte Mobilitätsangebote beeinflussen Wegemuster, Siedlungsstrukturen und Pendler- und Warenströme** | **Raumstrukturelle Auswirkungen (7)** Mobilitätssysteme verändern Gestaltungs-rahmen für urbane und ländliche Räume. | Wohnsituationen und Arbeitsprozesse neu denken. | Langfristige Raumplanung für nachhaltige Regionen und lebenswerte Städte mit verringertem Mobilitätsbedarf | Digitale Systeme tragen zur Wegeoptimierung bei, Ströme vermeiden, bündeln, reduzieren und optimieren |

## 5. Methodische Überlegungen zur Unterstützung von Kernaussagen

Welches Systemmodell wird für den öffentlichen Verkehrsraum, Fahrzeuge und Nutzer und das entsprechenden Datenmanagement zu Grunde gelegt? ZU Beginn des Projektes wird erarbeitet, welche Bereiche des Mobilitätssektors mit welcher Intensität analysiert werden? Könnten durch eine Differenzierung von Objekt-, Raum- Nutzerspezifischen Daten Risiken im Vulnerabilitätsraum reduzieren werden und wie könnte die entsprechende Verwendung auch rechtlich, sowie Sektor- und Grenzübergreifend, sichergestellt werden. Welche Rolle spielen Vernetzung und KI-Systeme, die raumspezifische Entscheidungen beeinflussen/treffen und wie kann Datenqualität und -integrität einerseits und Datensouveränität für Nutzer und Betreiber andererseits gewährleistet werden? Welche kommerziellen, ethischen und technischen Auswirkungen (Unseens) damit verbunden sein können ist heute unklar und soll interdisziplinär erörtert werden.

Für die Gestaltung digitaler UND öffentlicher Mobilitätsräume sollten sowohl die öffentliche Hand (EU, Bund, Länder, Städtetag) als auch die die beteiligten Unternehmen im Sinne einer aktiven Rolle für Co-Finanzierung zu gewinnen sein. Es ist geplant, Szenarien zu erstellen, die Entwicklungsvarianten für Vulnerabilitätsrisiken anhand definierter Parameter (Umweltwirkung, Individualität, Automatisierung) gegenüberstellen. Für den Roll-Out der Level des automatisierten Fahrens sowie die Entwicklung von Rechten und Pflichten digitaler Subjekte erfolgen eigene szenarische Überlegungen. Spezifische Befragungen, transdisziplinäre Workshops zu priorisierten Themen und explorative (Delphi) oder vertiefende qualitative Untersuchung zum Umgang mit heiklen Tradeoffs könnten im Bedarfsfall definiert und ggfls. auch finanziert werden.

## 6. Ausblick: Erwartete Ergebnisse und Folgeinitiativen[5]

Wir erwarten, in dem Weissbuch für den Bereich Mobilität

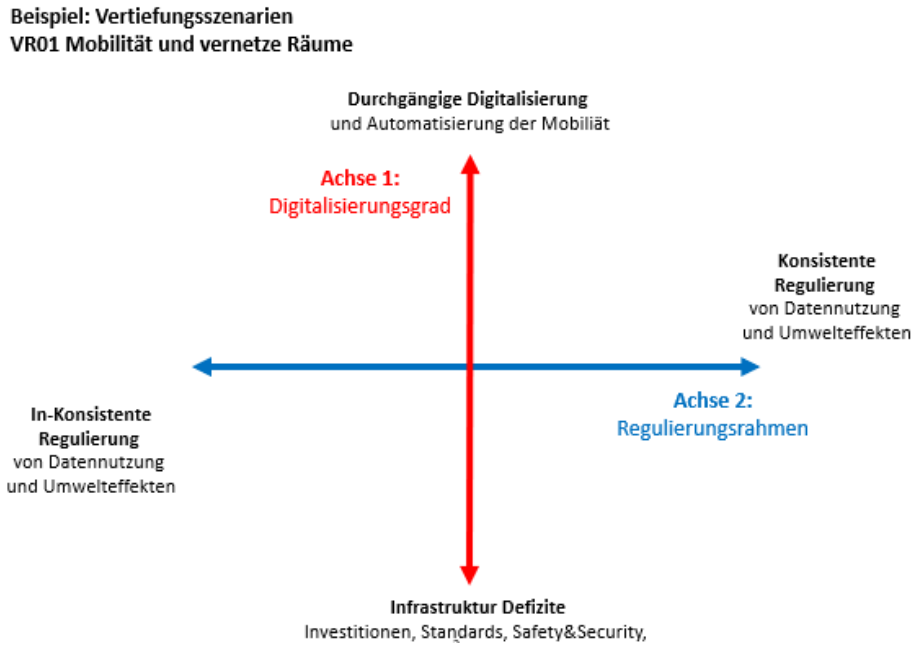
- Eine Beschreibung der Vulnerabilitäten für betroffene Stakeholdergruppen aus dem Mobilitätssektor sowie eine Darstellung der diesen Vulnerabilitäten unterliegenden (kausalen) Mechanismen
- Eine Beschreibung der wesentlichen Prozesse und wirtschaftlichen Veränderungen, auf die Mobilitätsanbieter, Infrastrukturbetreiber und Räume (exemplarisch, cases) sich einzustellen haben.
- Eine transparente Darstellung der stofflichen und ökologischen Wirkungen digitaler Mobilitätssysteme im Hinblick auf die Erreichung von Nachhaltigkeitszielen.
- Anregungen für einen verlässlichen Umgang mit privaten und öffentlichen Daten, Infrastrukturen und Räumen im Sinne der Nachhaltigkeit und einer transparenten Ausgewogenheit zwischen kommerziellen und sozialen Zielen und
- Interessen (Differenzierte Daten Taxonomie, Objekte, Subjekte, Räume u.a.)

[5] In den Feinplänen der anderen VRs vorhandenen Kapitel 6 „Von Unseens zu Orientierungen“ und „Vertiefungsforschung“ befinden sich im Appendix

– Branchenübergreifende Beispiele an denen gelernt werden kann, welche Anpassungsleistung (adaptive Kapazität) Mobilitätsunternehmen aufweisen müssen

Im Weißbuch werden von VR01 mögliche Szenarien zur Digitalisierung von Mobilität skizziert. Diese berücksichtigen, dass Mobilität immer im physischen Raum, urban oder ländlich stattfindet und Digitalisierung im „Brown-Field“ stattfinden wird. Auch wenn innovative Endgeräte (eScooter, Drohnen, Flugtaxis u.a.) neue Lösungsansätze anbieten, ist die Anpassung von Infrastruktursystemen (Ladesäulen, Heliports, Schienennetze) und die Integration in den sozialen Raum bei Mobilitätsinnovationen zu berücksichtigen.

Für die Entwicklung robuster Mobilitäts-Szenarien wurden zwei Achsen ermittelt an denen die relevanten Trends und Restriktionen eingeordnet und priorisiert werden können. Die erste Achse beschreibt den „Digitalisierungsgrad“ als Indikator für Durchsetzung von Digitalisierung und Automatisierung im Verkehrssektor, einschließlich der Akzeptanz und Diffusion von Innovationen. Die zweite Achse beschriebt den „Regulierungsrahmen“ im Sinne von Vorgaben für die Erreichung von Umweltpolitischen Zielen und die Einhaltung von Regeln zur Datennutzung Anhand von konkreten Beispielen, wie einem Quartier einer Smart City, einer digitalen Markplatz für Mobilitätsdaten und -dienste oder einem neuartigen Fahrzeug werden mit diesem Vorgehen mögliche Entwicklungen beschrieben und die Unseens als Folgen bewertet. Mit Hilfe der geplanten Vertiefungsforschung können über die Orientierung hinaus mögliche Lösungsansätze aufgezeigt und mit Stakeholdern diskutiert werden.



## Referenzen

E. Awad, S. Dsouza, R. Kim, J. Schulz, J. Henrich, A. Shariff, J.-F. Bonnefon, I. Rahwan (2018). The Moral Machine experiment. Nature.

Frischmann, Brett M., 2013, Infrastructure, The Social Value of Shared Resources, Oxford University

Hofmann, Klaus Markus, 2015, Connecting People, an Evolutionary Perspective on Infraculture – The Changing Role of the State, in The Economics of Infrastructure Provisioning, Picot, Arnold, Florio, Massimo Florio, Nico Grove and Johann Kranz, 2015 MIT Press Cambridge, U.S.A.

Krcmar, H. Wolf, T., 2017 Mobilität.Erfüllung.System. Zur Zukunft der Mobilität 2025+ Zukunftsstudie MUNCHNER KREIS Band VII, München 2017

Rohde, Phillip; Hoffmann, Christian, 2015, Towards New Urban Mobility, LSE Cities, London

https://www.itf-oecd.org/sites/default/files/docs/itf-transport-outlook-2017-launch.pdfa

https://www.itf-oecd.org/sites/default/files/docs/11outlook.pdf

https://nuernberg.digital/festival/programm/2019/the-day-after-digitization-dorf-edition-394) ein Workshop, an welchem Beispiele aus seiner Gemeinde gegeben wurden:

https://digitales-dorf.bayern/index.php/die-modelldoerfer/dd-projekt-nord/

https://www.steinwald-allianz.de/projekte/digitales-dorf-mobiler-dorfladen/

DiDaT

Digitale Daten als
Gegenstand eines
transdisziplinären
Prozesses

# Vulnerabilitätsraum 02 (VR02)

# Gesundheit, Digitalisierung und digitale Daten im deutschen Gesundheitswesen

DiDaT (Grob-)Feinplanung für Vulnerabilitätsraum 02 (VR02)

# Gesundheit, Digitalisierung und digitale Daten im deutschen Gesundheitswesen

*Heike Köckler, Lisa A. Rosenberger, Roland Scholz*

*Inputs durch Gerd Antes, Minou Friele, Gerd Glaeske, Felix Tretter, Marcel Weigand, Michael Weller*

## 1. Gegenstand (Was wird betrachtet?), Ziele und Leitfrage[6]

Der VR Gesundheit umfasst aus einer Systemperspektive Gesundheit und Krankheit, Prävention, Gesundheitsförderung und –versorgung. Gesundheit wird entsprechend dem Verständnis der Weltgesundheitsorganisation als ein Zustand des vollständigen körperlichen, geistigen und sozialen Wohlergehens und nicht nur als Fehlen von Krankheit oder Gebrechen gesehen (WHO, 1984). Gesundheit wird als ein Kontinuum verstanden (Franke & Antonovsky, 1997). Entsprechend diesem breiten Verständnis werden verschiedene Akteure betrachtet: Individuen, nicht nur als Patient*innen, in Gesundheitsberufen Tätige (insbesondere Ärzt*innen, Therapeut*innen, Pflegende, Apotheker*innen, Pharmazeut*innen, Public Healther*innen), Krankenkassen, Unternehmen (Pharma-, Medizintechnik, Abrechnungswesen, …) und NGO´s/ Vereine.

Diese Akteure generieren und nutzen digitale Daten unterstützend in Diagnostik, Therapie, Kommunikation und Information. Zu den zentralen positiven Effekten zählen die Möglichkeiten die Vielzahl unterschiedlicher Informationen aus verschiedenen Bereichen zusammenzuführen. Neue Analyseverfahren können Diagnostik und Therapie durch Algorithmen unterstützen oder zu neuen Forschungshypothesen führen. Über die Digitalisierung und die Dynamik mit der diese voranschreitet werden im Gesundheitsbereich jedoch verschiedene Anwendungen für Individuen bereitgestellt, deren Wirksamkeit im Sinne einer evidenzbasierten Gesundheitswissenschaft nicht als gesichert angesehen werden. Kommerzielle Einzelinteressen stehen bei manchen Anwendungen, die für Nutzer*innen als reine Gesundheitsprodukte (insbesondere Apps) erscheinen, im Fokus. Zudem stellen Individuen freiwillig digitale Daten zu ihren physischen und auch psychischen Faktoren bereit, ohne sicher zu gehen, dass diese in ihrem Sinne und unter Wahrung des Datenschutzes nach deutschem oder europäischen Recht verarbeitet und genutzt werden (Antes, 2018).

Ein aktuelles Thema der Digitalisierung gesundheitsbezogener Daten ist die Einführung der elektronischen Patientenakte

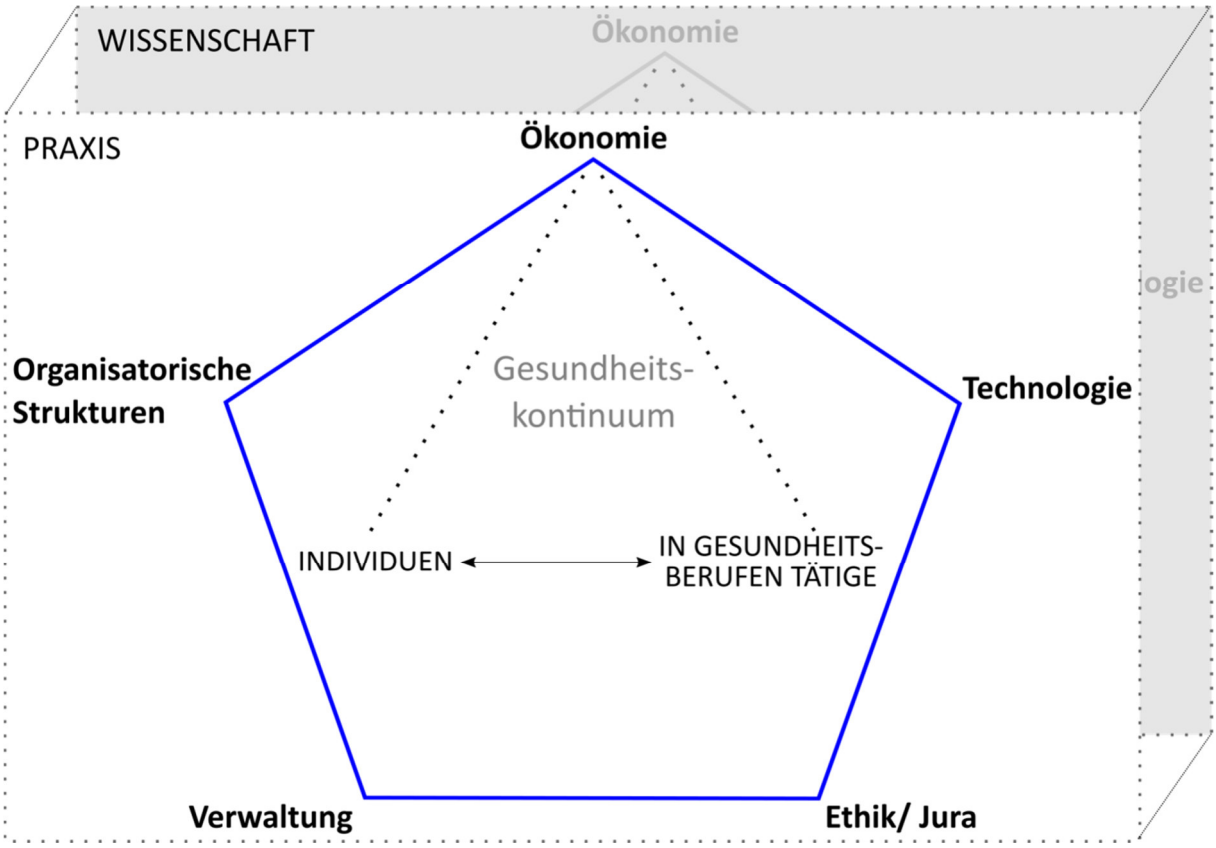
[6] Die positive und negative Wirkung der Digitalisierung im deutschen Gesundheitssystem wurde von den VR Gesundheit-Teilnehmern kritisch diskutiert und ist hier noch nicht ausgewogen beschrieben. Durch eine einseitige negative, oder einer einseitigen positiven Betrachtung besteht die Gefahr der Fehleinschätzung des Gesamtnutzens der Digitalisierung für das Gesundheitssystem. Im Feinplan wird dies nuancierter ausgearbeitet.

(ePA). Durch das kürzlich verabschiedete Terminservice- und Versorgungsgesetz (TSVG) ist die Einführung der ePA in Deutschland durch die Krankenkassen ab Januar 2021 vorgeschrieben. Die Nutzung ist den Individuen freigestellt. Hierdurch werden Versicherten Informationen wie Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte und Impfungen orts- und zeitunabhängig zugänglich sein. Diese Akten können auch für diejenigen, die in Gesundheitsberufen für die jeweilige Individuen tätig sind, bereitgestellt werden. Die derzeit in der Diskussion befindlichen Lösungen unterscheiden sich sowohl in ihrer organisatorischen als auch technischen Umsetzung. So reichen mögliche ePA Modelle von einem web-basierten Angebot in dem die Daten auf einem zentralen Server gesichert sind bis hin zu einer App Anwendung mit einer lokalen Speicherung von Daten auf dem Endgerät der Individuen. Die Techniker Krankenkasse und die AOK sind hier als Krankenkassen besonders aktiv. Auch im Ausland, beispielsweise in Estland und Australien, gibt es bereits langjährige Erfahrungen (Shaw, Hines, & Kielly-Carroll, 2017). Mit Hilfe der ePA können insbesondere doppelte Untersuchungen, unerwünschte Arzneimittelwirkungen und Fehldiagnosen aufgrund unzureichender Informationen vermieden werden. Zudem haben Individuen die Möglichkeiten ihre persönlichen Unterlagen einzusehen. Allerdings können mit der Einführung der Nutzung digitaler Daten im Rahmen der ePA auch unbeabsichtigte negative Effekte verbunden sein: Individuen können unter Umständen Arztbriefe ohne Erläuterung nur unzureichend einordnen, die Digitalisierung kann in den einzelnen Praxen und Kliniken noch nicht ausreichend etabliert sein, und auch die direkte Kommunikation zwischen Ärzt*innen/Therapeut*innen, Pfleger*innen, Apotheker*innen und Patient*innen kann durch die digitale Kommunikation verändert werden. So kann es im positiven Sinne mehr Zeit für tiefergehende Gespräche auf der Basis vorher bekannter Befunde und auch Messungen geben. So müssen aber zum Beispiel Lösungen entwickelt werden, wie mit sensiblen Informationen in der Psychotherapie umgegangen wird, bei der Protokollieren entweder durch die Patient*innen oder die Ärzt*innen nicht gewünscht ist. Es besteht je nach technischer Lösung die Gefahr, dass diese sensible Informationen an Dritte – wie (potentielle) Arbeitgeber – oder virtuelle soziale Netzwerke gelangen. (Vor- und Nachteile können anhand des Beispiels noch weiter exemplarisch herausgearbeitet werden).

Solche unbeabsichtigten Nebeneffekte sind aus gesellschaftlicher Sicht als negativ und unbeabsichtigt zu bewerten. Aus Partikularinteressen heraus, bspw. die Platzierung von Werbung im Internet, können diese Effekte jedoch von Einzelnen intendiert sein.

Vor diesem Hintergrund wird im Vulnerabilitätsraum Gesundheit der übergeordneten Frage nachgegangen: *Welche negativen Auswirkungen können aus einer Generierung und Nutzung digitaler Daten im deutschen Gesundheitssystem auf die oben genannten Akteure kurz-, mittel- und langfristig resultieren und wie kann diesen begegnet werden?*

Hierbei ist es das Ziel, unbeabsichtigte Nebeneffekte für das deutsche Gesundheitswesen zu systematisieren, in ihrer Funktionsweise zu antizipieren. Das Systemmodell in Figur 1 dient hier als Denk- und Analyserahmen. Spezifische Beziehungen zwischen den Systemelementen werden in der Vertiefungsforschung exemplarisch qualifiziert. Zwischen relevanten Akteuren sollen Vereinbarungen getroffen werden, die unbeabsichtigte Nebeneffekte verhindern oder eindämmen, um die Entfaltung der positiven Effekte von der Generierung und Nutzung digitaler Daten ergeben, zu befördern.




Figur 1. Systemmodell zur Rolle der Nutzung digitaler Daten im deutschen Gesundheitswesen. Die Systemgrenze ist das deutsche Gesundheitswesen mit den in Deutschland lebenden Nutzer*innen/ Beteiligten. Die blau gerahmten Elemente stehen im komplementären Spannungsfeld, welches den Umgang mit Daten im deutschen Gesundheitswesen prägen. Alle Systemelemente sind in den jeweiligen wissenschaftlichen Gebieten begründet. Basierend auf Tretter und Kollegen (Tretter, Batschkus, & Adam, 2019).

Tabelle 1. *Begriffserklärung der Elemente des Systemmodells.*

| | |
|---|---|
| Individuen | Daten der Bürger*innen, Menschen, Personen, Patient*innen & Gesunden, sowie „Objekte der Rohdatenerzeugung“.<br>Daten der Individuen beziehen sich zum einen auf digitale Informationen bzw. Messungen des Gesundheitszustands und zum Anderen auf die digitale Aufbewahrung von Gesundheitsdaten. |
| In Gesundheitsberufen Tätige | Daten der in Gesundheitsberufen Tätigen und Leistungserbringer*innen. Diese sind professionelle Datennutzer.<br>Daten der in Gesundheitsberufen Tätigen beziehen sich auf die digitale Prävention, die digitale Diagnostik und die digitale Behandlung. |
| Ökonomie | Auf Daten bezogene Leistungsträger, Leistungsanbieter, den (Gesundheits-) markt und die (Gesundheits-)wirtschaft, aber auch neue Spieler im Bereich Gesundheit, wie Anbieter von Gesundheits-Apps, oder große Internetkonzerne. |
| Technologie | Technologien zur Aufbewahrung, Nutzung (z.B. für Prävention und Diagnose) und dem Transfer digitaler Daten |
| Ethik/ Jura | Auf Daten und Gesundheit ausgerichtete Rechte, Pflichten und Normen der Individuen und Gesundheitsberufen Tätigen |
| Verwaltung | Auf Daten und Gesundheit bezogene administrative Tätigkeiten |
| Organisatorische Strukturen | Auf Daten und Gesundheit bezogene Strukturen des Gesundheitbetriebs |

## 2. Welche nicht intendierten, unbeabsichtigten Nebenfolgen sind von Interesse und warum?

### Individuen:

Eine sensitive Stakeholder-Gruppe im Bereich Gesundheit sind Individuen der allgemeinen Bevölkerung, wobei deren Vulnerabilität durch verschiedene Faktoren beschrieben werden kann. Eine Gefahr, der das Individuum ausgesetzt sein könnte, ist eine Einschränkung in ihrem Recht auf individuelle Entwicklung und Selbstbestimmung. So können Apps und Suchalgorithmen im Internet auf Informationen lenken, die ein kommerzielles oder staatliches Interesse verfolgen und mögliche Alternativen, die für das Individuum relevant wären, nicht bereitstellen.

Hier könnte der ohnehin bestehende Mechanismus, der das Recht auf Selbstbestimmung durch normierte Vorgaben und Vorgehensweisen im Gesundheitsbereich einschränkt, durch die Nutzung digitaler Medien verstärkt werden. Zusätzlich impliziert die Nutzung digitaler Medien auch eine Sammlung von Daten ohne opt-out Möglichkeit, die in der Gesundheitsanwendung extra sensitive Informationen befassen. Mit diesem Druck zur Datenpreisgabe entstehen Fragen zur Ökonomisierung und der Hoheit über die Daten.

*UNSEEN 01: Funktionsweisen der Bereitstellung und Nutzung digitaler Daten können die Berücksichtigung der individuellen Entwicklung und Selbstbestimmung vermindern.*

### In Gesundheitsberufen Tätige:

Eine weitere sensitive Stakeholder-Gruppe sind in Gesundheitsbereichen Tätige, die Methoden und Aussagen, die durch digitale Daten möglich werden, kompetent für ihren Wirkungsbereich einsetzen. Ein unbeabsichtigter negativer Nebeneffekt kann in einem begrenzten Einblick in Algorithmen durch Gesundheitsexpert*innen sein. Ein Health-Technology Assessment, das einer Fachkraft im Gesundheitsbereich bei der Einordnung digitaler Dienstleistungen und Produkte hilft, gibt es derzeit in Deutschland nicht.

Hier könnte der Mechanismus zum Tragen kommen, dass Evidenz vor allem in einem quantitativen und im Hinblick auf die Fallzahl großen Sample gesucht wird.

Die Einordnung von Information und Evidenz ist mit beiden Mechanismen verbunden.

*UNSEEN 02: Veränderung und teilweise Verschlechterung der Qualität von Diagnostik und Therapie durch Nutzung automatisch mit Hilfe von machine learning Algorithmen generierter Daten ohne ausreichendes Health-Technology Assessment*.

**Forschungsmethodik**:

Somit wären auch Forschende als eine sensitive Gruppe zu betrachten. Eine Datenmonopolisierung von Tech-Unternehmen ist aus Forschungssicht ein unbeabsichtigter Nebeneffekt: mit den kontinuierlichen Datenströmen der Health-Apps und Wearables verändert sich der messbare Zeitpunkt von Gesundheit und Krankheit. Traditionell gesehen wurde anhand von einem Datenpunkt (= während des Arztbesuches) festgelegt ob jemand gesund oder krank ist. Mit der Nutzung kontinuierlich erhobener Daten über den Gesundheitszustand von Individuen verändert sich unser Verständnis von Gesundheit und Krankheit und können tägliche/ wöchentliche/ monatliche Fluktuationen erforscht werden um evidenzbasierte und wahrscheinlich umfassendere Diagnosen stellen zu können. Die Daten die durch Health-Apps und Wearables erhoben werden, sind aber in der Regel nicht der akademischen Forschung zugänglich und Erkenntnisse aus den Daten werden unter Umständen durch Tech-Unternehmen als Marktvorteil zur Konkurrenzfähigkeit genutzt (aber siehe auch www.patientslikeme.com als Beispiel einer öffentlich zugänglichen Datenbank mit von Patienten erhobenen Gesundheitsdaten). Diese Daten werden von den Tech-Unternehmen (teilweiße) auch nicht aus Forschungsinteresse generiert und sind in der Auswertung nicht den 4P Kriterien - predictive, personalised, preventive, participatory verschrieben.

Zudem bieten Algorithmen neue Analyseverfahren, die jedoch in ihrer Qualität bestehende Standards einer evidenzbasierten Medizin (randomisierte Kontrollstudien) nicht ersetzen dürfen.

*UNSEEN 03: Änderungen, die sich aus der digitalen Erhebung und Nutzung gesundheitsbezogener Daten ergeben, sind nicht immer an den 4P-Kriterien orientiert.*

**Ökonomie:**

Die Generierung digitaler Daten kann durch die Nutzung digitaler Technologien bei in Gesundheitsberufen Tätigen (z.B. durch automatisches Protokollieren mit Hilfe von Spracherkennungssoftware) und in der Verwaltung zu Zeitersparnissen führen. Allerdings ist es ungeklärt wie sich eine Generierung und Nutzung digitaler Daten zur Leistungssteigerung und Kosteneinsparung aus Effizienzüberlegungen auf die Qualität der gesundheitlichen Versorgung und der Verwaltung auswirkt. Hierbei spielen die ökonomischen Interessen der App-Entwickler und –betreiber auch eine Rolle.

*UNSEEN 04: Auf ökonomische Effizienz ausgerichtete Nutzung digitaler Daten führt in bestimmten Bereichen zur Verschlechterung der gesundheitlichen Versorgung.*

**Apps:**

Momentan fehlen Strukturen zur Bewertung, Evaluation und Zertifizierung von Apps in Deutschland (internationales Beispiel sind die WHO Richtlinien: (WHO, 2019)). Zugleich gibt es zwar Statistiken über den Verkauf von Gesundheits-Apps, es

ist aber nicht klar inwiefern diese auch tatsächlich bei der Prävention, Diagnose und Behandlung von in Gesundheitsberufen Tätigen genutzt werden. Es besteht die Möglichkeit, dass die Integration der Gesundheits-Apps in die berufliche Praxis derjenigen, die in Gesundheitsberufen tätig sind, durch fehlende Zugriffsmöglichkeiten auf die gesammelten Daten erschwert beziehungsweise unmöglich gemacht wird. Des Weiteren ist unklar ob die Nutzung der Gesundheits-Apps von Individuen gar den analogen Besuch bei Ärzten, Therapeuten oder Apothekern oder anderen in Gesundheitsberufen Tätigen ersetzen, und diese mit den Apps in Konkurrenz stehen. Die Daten die von den Gesundheits-Apps gesammelt werden, befassen äußerst sensitive Gesundheitsinformationen von Individuen bei denen Fragen (wie in den anderen Abschnitten beschrieben) zum Eigentum, Zugang, zur Nutzung und zur Ökonomisierung offen sind.

*UNSEEN 05: Die gesundheitliche Versorgung kann durch die Nutzung von Apps in vielen Bereichen verbessert werden, unverändert bleiben, aber auch verschlechtern, da eine umfassende Validierung der Apps fehlt.*

**Kommunikation und Austausch:**

Durch die Sensitivität der Gesundheitsinformationen der Individuen ist die Sicherheit der Datenübertragung und die Datensouveränität von äußerster Wichtigkeit. Hierbei muss geklärt werden welche Akteure die Verantwortung für die Gewährleistung der Datensicherheit tragen und ob die betroffenen Parteien (Individuen, in Gesundheitsberufen Tätige, Verwaltung) für diese Aufgabe hinreichend unterstützt werden. Für eine sachkundige Wahl der Kommunikationstechnologien ist die teilweiße fehlende Qualitätszertifizierung der für Kommunikation und Austausch verwendeten Technologien äußerst wichtig.

Individuen sind durch ihr «Dr. Google Verhalten« Pseudoaufgeklärte über ihren Gesundheitszustand. Es besteht daher die Gefahr eines informatorischen Overflows der in Gesundheitsberufen Tätigen im Kontakt mit den Individuum, welcher die Beziehung zwischen dem Individuum und dem im Gesundheitsberuf Tätigen unter Druck setzen kann. Es ist unklar ob Individuen die unterschiedliche Qualität der Informationsquellen erkennen und ob sie durch diese zusätzlichen Informationen besser oder schlechter in der Lage sind mit den in Gesundheitsberufen Tätigen zu kommunizieren.

*UNSEEN 06: Die Nutzung von Informationen mittels digitaler Daten, deren Qualität nicht gesichert ist, kann Austausch und Kommunikation Beteiligter Akteure überformen, wenn Daten missbräuchlich verwendet werden.*

**Digitale Behandlungsmethoden:**

Digitale Behandlungsmethoden sammeln explizit von den Anwender*innen preisgegebene Gesundheitsdaten, sowie implizite, durch die Nutzung der Technologie, generierte Daten. Beide sind anfällig für kriminelle Aktivitäten (z.B. durch Datendiebstahl). Das Eigentum beider Gesundheitsdaten ist außerdem ungeklärt: gehören sie den Patient*innen, die die Daten produzieren, oder den Entwickler*innen/ Vertreiber*innen der digitalen Technologie die

diese für ihren wirtschaftlichen Fortschritt nutzen? Bekommen In Gesundheitsberufen Tätige von den Unternehmen Zugang zu beiden Arten von Daten um diese für Diagnose oder Forschungszwecke nutzen zu können?

*UNSEEN 07: Daten im Kontext digitaler Behandlungsmethoden können missbräuchlich verwendet werden und das Recht auf informationelle Selbstbestimmung einschränken.*

**Gesundheit:**

Die Nutzung digitaler und sozialer Medien hat ein hohes Suchtpotential (Andreassen, 2015). Dies ist ein Schwerpunkt des Vulnerabilitätsraumes V05 „Soziale Medien, digitale Daten und ihre Auswirkungen auf den einzelnen Menschen“. Es ist nicht klar, inwiefern dies innerhalb von Gesundheitseinrichtungen und –behörden in Deutschland erkannt und anerkannt wird und was für Gegenmaßnahmen erforscht beziehungsweiße angewandt werden.

Kontinuierlich erhobene Daten, die auch dem Individuum über Wearables unmittelbar und kontinuierlich verfügbar sind (d.h. kontinuierliche Datenströme) verändert unser Verständnis von Gesundheit (siehe Beschreibung Forschung).

*UNSEEN 08: Eine Übernutzung von digitalen Medien und kontinuierliche Datenflüsse über physiologische Prozesse können negative Auswirkungen auf die Gesundheit haben.*

**Gesundheitssystem:**

Technologieunternehmen sind mit ihrem Datenmonopol neue Spieler im Gesundheitssystem, welche die traditionellen Rollen und Aufgaben verschiedener Systemelemente (vor allem in Gesundheitsberufen Tätige, Verwaltung, Organisation) verändern und unter Umständen ersetzen. Diese veränderten Beziehungen werden aus einer Systemperspektive erforscht.

*UNSEEN 09: Technologieunternehmen verändern Rollenverteilung und kreieren neue Märkte im Gesundheitssystem.*

**3. Welche Stakeholder sind für ein Verständnis und ein Management der „Unseens“ von besonderer Bedeutung? Welche wissenschaftlichen Wissensbereiche sind relevant?**

Die hier abgebildete Stakeholdertabelle ist eine vereinfachte Schematisierung der schwerpunktmäßigen Zuordnung der Stakeholdergruppenrepresentanten zu den oben beschriebenen Unseens. In der Vertiefungsforschung wird die Tabelle exemplarisch konkretisiert. Zusätzlich werden weitere Akteure (wie zum Beispiel Ärzte spezialisiert in digitalen Behandlungsmethoden) durch Vertiefungsforschung im VR Gesundheit mit einbezogen.

| | **Unseens** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Individuen: Einschränkung der Möglichkeiten auf individuelle Entwicklung und Selbstbestimmung | Gesundheitsberufler*innen: Verlust der Qualität von Diagnostik und Therapie durch Einsatz von KI | Verschlechterung der gesundheitlichen Versorgung | | Forschungsmethodik: Epistemische Schwächen in Forschungsprozessen sowie Vernachlässigung der 4P Kriterien | Datenmissbrauch und Einschränkung des Rechts auf informationelle Selbstverwaltung | | Gesundheit: unbalancierte Nutzung digitaler Medien macht krank | Gesundheitssystem: Technologieunternehmen verändern Rollenverteilung im Gesundheitssystem |
| | | | Ökonomie: durch eine auf ökonomische Effizienz gerichtete Digitalisierung | Apps: durch Nutzung von Apps ohne nachgewiesene Wirkung | | Bei Kommunikation und Austausch von Informationen | Bei digitalen Behandlungsmethoden | | |
| **Stakeholdergruppen** | | | | | | | | | |
| Gesundheitsberufler | Ärzte | Ärzte | Ärzte | Ärzte | Ärzte | Ärzte | Ärzte | | Ärzte |
| | Therapeuten & Pflegepersonal | Therapeuten & Pflegepersonal | Therapeuten & Pflegepersonal | Therapeuten & Pflegepersonal | Therapeuten & Pflegepersonal | Therapeuten & Pflegepersonal | Therapeuten & Pflegepersonal | | Therapeuten & Pflegepersonal |
| | | | | | Pharmazeuten & Apotheker | | | | Pharmazeuten & Apotheker |
| | Public & Community Healther | | Public & Community Healther | Public & Community Healther | Public & Community Healther | | | | Public & Community Healther |
| | | Medizinethiker | | Medizinethiker | Medizinethiker | Medizinethiker | | | Medizinethiker |
| | | | | | | | | | |
| Individuen & Verbände | Verbraucherzentrale | | | Verbraucherzentrale | | Verbraucherzentrale | Verbraucherzentrale | Verbraucherzentrale | Verbraucherzentrale |
| | | Aktionsbündnis Patientensicherheit | Aktionsbündnis Patientensicherheit | | | Aktionsbündnis Patientensicherheit | Aktionsbündnis Patientensicherheit | Aktionsbündnis Patientensicherheit | Aktionsbündnis Patientensicherheit |
| | | Selbsthilfegruppen (Senioren, Pflege, Krankheitsbilder (zB Psoriarisverband)) | Selbsthilfegruppen (Senioren, Pflege, Krankheitsbilder (zB Psoriarisverband)) | | | | | Selbsthilfegruppen (Senioren, Pflege, Krankheitsbilder (zB Psoriarisverband)) | Selbsthilfegruppen (Senioren, Pflege, Krankheitsbilder (zB Psoriarisverband)) |
| | | | | | | | | | |
| Sozialversicherungsträger | GKV Spitzenverband | GKV Spitzenverband | GKV Spitzenverband | GKV Spitzenverband | | GKV Spitzenverband | | | GKV Spitzenverband |
| | Krankenkassen (zB DAK) | Krankenkassen (zB DAK) | Krankenkassen (zB DAK) | Krankenkassen (zB DAK) | | Krankenkassen (zB DAK) | | | Krankenkassen (zB DAK) |
| | | | | | | | | | |
| Unternehmen | | | Pharmaunternehmen (zB Bayer, Rosch) | | Pharmaunternehmen (zB Bayer, Rosch) | | Pharmaunternehmen (zB Bayer, Rosch) | | Pharmaunternehmen (zB Bayer, Rosch) |
| | Entwickler von Gesundheitstechnologien * | Entwickler von Gesundheitstechnologien * | Entwickler von Gesundheitstechnologien * | Entwickler von Gesundheitstechnologien * | Entwickler von Gesundheitstechnologien * | Entwickler von Gesundheitstechnologien * | Entwickler von Gesundheitstechnologien * | Entwickler von Gesundheitstechnologien * | Entwickler von Gesundheitstechnologien * |
| | | | Genanalysenlabor (Humatrix) | | Genanalysenlabor (Humatrix) | | Genanalysenlabor (Humatrix) | | Genanalysenlabor (Humatrix) |

Notizen:*(Apps, Wearables, medizinische Datenverarbeitungsunternehmen, Medizinbedarfsunternehmen (zB Braun), Fraunhofer ISST Dortmund). VR- Teilnehmer repräsentieren folgende Stakeholdergruppen: Felix Tretter - Ärzte, Gerd Glaeske - Pharmazeuten & Apothere, Heike Köckler - Public & Community Healther, Minou Friele - Medizinethiker, Gerd Antes - Medizinethiker, Susanne Mauersberg - Verbraucherzentrale, Marcel Weigand - Aktionsbündnis Patientensicherheit, Michael Weller - GKV Spitzenverband.

## 4. Unseen x Orientierungen im VR02

Tabelle 4. Unseens x Orientierungen Tabelle VR 02

| | 1. Unseen | 2. Ursachen/ Kausalitäten/ Ent-stehungs-prozesse der Unseens | 3. Maßnahmen möglicher sozio-technologischer Innovationen zur Mitigation | 4. Ziele | 5. Sozial robuste Orientierungen zum Umgang mit Unseens |
|---|---|---|---|---|---|
| 1 | Individuen: Funktionsweisen der Bereitstellung und Nutzung digitaler Daten können die Berücksichtigung der individuellen Entwicklung und Selbstbestimmung vermindern.<br>Zudem können bei Individuen Erwartungen geweckt werden, deren Erfüllung noch offen ist. | • Apps und Suchalgorithmen im Internet können auf Informationen lenken, die ein kommerzielles oder staatliches Interesse verfolgen und mögliche Alternativen, die für das Individuum relevant wären, nicht bereitstellen<br>• Recht auf Selbstbestimmung wird durch normierte Vorgaben und Vorgehensweisen durch die Nutzung digitaler Medien eingeschränkt<br>• Druck zur Datenpreisgabe durch fehlende opt-out Möglichkeit bei Nutzung digitaler Medien | In Diskussion | | |
| 2 | In Gesundheitsberufen Tätige: Veränderung und teilweise Verschlechterung der Qualität von Diagnostik und Therapie durch Nutzung automatisch mit Hilfe von machine learning Algorithmen generierter Daten ohne ausreichendes Health-Technology Assessment. | • Begrenzter Einblick in Algorithmen<br>• Fehlendes Health-Technology Assessment zur Unterstützung der Einordnung digitaler Gesundheitsanwendungen von in Gesundheitsberufen Tätigen<br>• Evidenz wird vor allem in einem quantitativen und im Hinblick auf die Fallzahl großen Sample gesucht | • Entwicklung dimensionaler Kriterien zur Beurteilung des Nutzens, der Risiken und Kosten digitaler Gesundheitsanwendungen im transdisziplinären Diskurs | • Bundesweit einheitliche Struktur zur HTA und Zertifizierung digitaler Gesundheitsanwendungen durch unabhängiges Organ | |

| | | | | | |
|---|---|---|---|---|---|
| | | • Geringfügige Einbindung von in Gesundheitsberufen Tätigen bei Entwicklung digitaler Gesundheitsanwendungen | | | |
| 3 | Forschungsmethodik: Änderungen, die sich aus der digitalen Erhebung und Nutzung gesundheitsbezogener Daten ergeben, sind nicht immer an den 4P-Kriterien orientiert. | • Veränderung Verständnis von Gesundheit und Krankheit durch Veränderung messbarer Zeitpunkte durch kontinuierliche Datenströme der Health-Apps & Wearables<br>• Datenmonopolisierung von Tech-Unternehmen, dadurch kein Zugang für akademische Forschung<br>• Datengenerierung von Tech-Unternehmen nicht aus Forschungsinteresse, dadurch Auswertung nicht 4P Kriterien verschrieben<br>• Machine-Learning Analyseverfahren dürfen bestehende Forschungsstandards (randomisierte Kontrollstudien) nicht ersetzen | | | |
| 4 | Ökonomie: Auf ökonomische Effizienz ausgerichtete Nutzung digitaler Daten führt in bestimmten Bereichen zur Verschlechterung der gesundheitlichen Versorgung. | • Ökonomische Interessen der Entwickler & Betreiber digitaler Anwendungen liegen nicht bei der Förderung gesundheitlicher Versorgung<br>• Vermarktung digitaler Gesundheitsprofile durch Techunternehmen | | | |
| 5 | Apps: Die gesundheitliche Versorgung kann durch die Nutzung von Apps in vielen Bereichen verbessert werden, unverändert blei- | • Strukturen zur Bewertung, Evaluation und Zertifizierung von Apps fehlen<br>• fehlende Zugriffsmöglichkeiten auf die ge- | Siehe unseen 2 für HTA | Siehe unseen 2 für HTA | |

| | | | | | |
|---|---|---|---|---|---|
| | ben, aber auch verschlechtern, da eine umfassende Validierung der Apps fehlt. | sammelten Daten erschwert Integration in berufliche Praxis<br>• Konkurrenz der Nutzung von Gesundheits-Apps mit analogen Besuch bei Gesundheitsberufler*innen<br>• Ökonomisierung sensitiver, persönlicher Gesundheitsdaten (Vermarktung digitaler Gesundheitsprofile) | | | |
| 6 | Kommunikation & Austausch: Die Nutzung von Informationen mittels digitaler Daten, deren Qualität nicht gesichert ist, kann Austausch und Kommunikation Beteiligter Akteure überformen, wenn Daten missbräuchlich verwendet werden. | • Unklarheit bei wem Verantwortung für die Gewährleistung der Datensicherheit liegen<br>• fehlende Qualitätszertifizierung der für Kommunikation und Austausch verwendeten Technologien<br>• informatorischen Overflows der in Gesundheitsberufen Tätigen im Kontakt mit den Individuum, wodurch deren Beziehung unter Druck gesetzt wird<br>• Vermarktung digitaler Gesundheitsprofile durch Techunternehmen | Siehe unseen 2 für Qualitätszertifizierung | Siehe unseen 2 für Qualitätszertifizierung | |
| 7 | Digitale Behandlungsmethoden: Daten im Kontext digitaler Behandlungsmethoden können missbräuchlich verwendet werden und das Recht auf informationelle Selbstbestimmung einschränken. | • Eigentum Gesundheitsdaten ungeklärt<br>• Zugang zu Gesundheitsdaten durch in Gesundheitsberufen Tätige ungeklärt<br>• Vermarktung digitaler Gesundheitsprofile durch Techunternehmen | | | |
| 8 | Gesundheit: Eine Übernutzung von digitalen Medien und kontinuierliche Daten- | • Nicht geklärt inwiefern Gesundheitseinrichtungen und –behörden Suchtpotential von Nutzung digitaler | | | |

| | | | | | |
|---|---|---|---|---|---|
| | flüsse über physiologische Prozesse können negative Auswirkungen auf die Gesundheit haben. | & sozialer Medien anerkannt & bearbeitet wird<br>• Kontinuierliche für Individuum verfügbare Datenströme von Wearables verändert Verständnis von Gesundheit | | | |
| 9 | Gesundheitssysteme: Technologieunternehmen verändern Rollenverteilung und kreieren neue Märkte im Gesundheitssystem. | • Technologieunternehmen durch Datenmonopol neue Spieler im Gesundheitssystem, die traditionelle Rollenverteilung verändern und ersetzen<br>• Konkretes Ziel der Disruption des dt. Gesundheitssystems von Unternehmen mit erheblichen Finanz-, Entwicklungs- und Marketingressourcen | | | |

## 5. Methodische Überlegungen zur Unterstützung von Kernaussagen

Zu unterschiedlichen Teilthemen, die sich an den Fragen der Konzeptskizze orientieren können, findet Vertiefungsforschung statt. Hierbei werden systematisch verschiedene Stakeholderperspektiven (Individuum, in Gesundheitsberufen Tätige, Krankenkassen, Unternehmen, ggf. Weitere) erfasst im Hinblick auf jeweils beabsichtigte und unbeabsichtigte Effekte (UNSEENS). So könnte die Einführung der elektronischen Patientenakte aus der Perspektive Langzeitarbeitsloser, als einer Gruppe der Individuen, untersucht werden. Hierbei erfolgt eine Orientierung an den im European Roundtable entwickelten Elementen: “ownership, economic value, use and access of data”.

Folgende Themen wurden bis jetzt für die Vertiefungsforschung besprochen:

- Einführung der elektronischen Patientenakte
- Qualitätsassessment digitaler Gesundheitstechnologien
- Übersicht zu bestehenden Regulierungen des Dateneigentums
- Übersicht zur heutigen Implementierung digitaler Gesundheitstechnologien in die ärztliche Praxis (Ist-Stand, Konkurrenz in Gesundheitsberufen Tätige – Gesundheitstechnologien)
- Besteht ein informatorischer Overflow bei in Gesundheitsberufen Tätige durch „Dr.Google“ Verhalten der Individuen (Qualitätserkennung der Informationsquellen, Kommunikationsveränderung mit in Gesundheitsberufen Tätige)

- Systemveränderungen und Aufgabenverschiebung durch Techunternehmen im Gesundheitssystem

Technikfolgenabschätzung für ausgewählte Digitalisierungsprodukte – und prozesse

Systematisierung von Einzelelementen.

Case-based Learning

## 6. Erwartete Ergebnisse und Folgeinitiativen

Für das Weißbuch werden konkrete Empfehlungen aus der Perspektive verschiedener vulnerabler Stakeholder (Individuen, in Gesundheitsberufen Tätige, Wissenschaftler*innen) verfasst. Diese basieren auf Vertiefungsforschung in unterschiedlichen lebensweltlichen Bezügen und Einrichtungen der gesundheitlichen Versorgung.

- Die Vertiefungsforschung sollte in Orten der gesundheitlichen Versorgung (Klinik und Praxis, Therapie-, Pflegeeinrichtung) durchgeführt werden, da die dort tätigen Individuen ansonsten kaum in das DiDaT Projekt einbezogen werden können.
- Als konkretes Projekt könnte darüber hinaus die Einführung der Patientenakte vergleichend in zwei Krankenkassen aus Sicht von Individuen, denjenigen, die Informationen in diese Akte einpflegen sowie Krankenkassen und IT Unternehmen bearbeitet werden. Aufgrund des oben angesprochen Terminservice- und Versorgungsgesetz (TSVG) ist dies ein aktuelles Thema in dem zentral Weichen gestellt werden.
- Eine Forschung mit unterschiedlichen Bevölkerungsgruppen (Nutzer*innen von Gesundheits-Apps, chronisch Kranke, Akuterkrankte, Menschen in Betreuung, Pflegebedürftige, Ältere, …) zu Akzeptanz und Erfahrungen mit digitalen Produkten und Anwendungen wäre ebenfalls hilfreich.
- Eine Forschung zu Bedarfen von Unternehmen zu Digitalisierung und Ethik im Gesundheitsbereich. DiDaT hätte hier eine große legitimatorische Wirkung für die Unternehmen, da es sich nicht um Auftragsforschung handelt.

[1] World Health Organization 2016 Monitoring and Evaluating Digital Health Interventions. A practical guide to conducting research and assessment. Genf, WHO
[1] EUnetHTA 2019. https://eunethta.eu
[1] l.nhs.uk/services/nhs-apps-library/guidance-for-health-app-developers-commissioners-and-assessors/how-we-assess-health-apps-and-digital-tools, accessed 20 Nov 2019
[1] Mobile App Rating Scale (MARS): Stoyanov et al 2015) https://mhealth.jmir.org/2015/1/e27/
[1] MAST: *Kidholm* K(1), Ekeland AG, Jensen LK, Rasmussen J, Pedersen CD, Bowes *A*, Flottorp SA, Bech M. Int J Technol Assess Health Care. 2012 Jan;28(1):44-51. doi: 10.1017/S02664623110006
[1] Bertelsmann-Stiftung AppQ https://www.bertelsmann-stiftung.de/de/publikationen/publikation/did/appq/
[1] BCSSS: Human Digitalization. https://wwwa.bcsss.org/de/research/fields-and-groups/human-digitalization/

## Literaturverzeichnis

Andreassen, C. S. (2015). Online social network site addiction: A comprehensive review. *Current Addiction Reports, 2*(2), 175-184.

Antes, G. (2018). Die Medizin im Datenrausch. *Frankfurter Allgemeine Zeitung*. Retrieved from https://edition.faz.net/faz-edition/feuilleton/2018-01-02/9b583344667f696c3b3aabbc13b7424f/

Deloitte, & GKV-Spitzenverband. (2018). Digitalisierung des Gesundheitsmarktes.

Fitte, C., & Teuteberg, F. (2018). Ein Rezept für die Apotheke 2.0. *HMD Praxis der Wirtschaftsinformatik, 56*(1), 223-240. doi:10.1365/s40702-018-00485-3

Franke, A., & Antonovsky, A. (1997). Salutogenese. Zur Entmystifizierung der Gesundheit. *Aufl. Tübingen: dgvt-Verlag*.

OZG-Umsetzungskatalog (2018). Bundesministeriums des Innern, für Bau und Heimat. Berlin ISBN 978-3-947660-01-8, Online verfügbar https://www.it- planungsrat.de/DE/Service/Downloads/downloads_node.html, Zugriff vom 19.01.2020)

Kunst, A. (2019). Umfrage in Deutschland zu beliebten Smartwatch-Marken 2019 Retrieved from https://de.statista.com/prognosen/999765/umfrage-in-deutschland-zu-beliebten-smartwatch-marken

Lindner, R. (2019). Google übernimmt Fitbit für zwei Milliarden Dollar. Retrieved from https://www.faz.net/aktuell/wirtschaft/google-uebernimmt-fitbit-fuer-zwei-milliarden-dollar-16463653.html

Mansholt, M. (2019). Bewegung als Vorsorge: Diese Krankenkassen zahlen Ihnen Fitness-Tracker. Retrieved from https://www.stern.de/digital/online/apple-watch---co---diese-krankenkassen-zahlen-fuer-fitness-tracker-8546308.html

Shaw, T., Hines, M., & Kielly-Carroll, C. (2017). *Impact of Digital Health on the Safety and Quality of Health Care*. Sydney: ACSQHC.

Tretter, F., Batschkus, M., & Adam, D. (2019). Die Medizin in der Zange zwischen Wirtschaftsinteressen und technologischer Entwicklung. *Bayerisches Ärzteblatt*(6).

Vezyridis, P., & Timmons, S. (2019). Resisting big data exploitations in public healthcare: free riding or distributive justice? *Sociol Health Illn, 41*(8), 1585-1599. doi:10.1111/1467-9566.12969

WHO. (1984). *Health promotion : a discussion document on the concept and principles : summary report of the Working Group on Concept and Principles of Health Promotion*. Copenhagen: WHO Regional Office for Europe.

WHO. (2019). *WHO guideline: recommendations on digital interventions for health system strengthening.* Geneva: World Health Organization.

Wiegard, R.-B., & Breitner, M. H. (2017). Smart services in healthcare: A risk-benefit-analysis of pay-as-you-live services from customer perspective in Germany. *Electronic Markets, 29*(1), 107-123. doi:10.1007/s12525-017-0274-1

Zuboff, S. (2015). Big other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology, 30*(1), 75-89. doi:10.1057/jit.2015.5

DiDaT

Digitale Daten als Gegenstand eines transdisziplinären Prozesses

# Vulnerabilitätsraum 03 (VR03)

# KMU, Digitalisierung und Digitale Daten

DiDaT Grobplanung für Vulnerabilitätsraum 03 (VR03)

# KMU, Digitalisierung und Digitale Daten

*Reiner Czichos (CTN München, Donau Uni Krems), Daniel Baier (Uni Bayreuth), Wolfgang Hofmann (TSG), Georg Müller-Christ (Uni Bremen), Wolfgang Probst (IHK Cottbus), André Reichel (Zukunftsinstitut ISM, Stuttgart), Roland W. Scholz (Donau Uni Krems)*

mit Input von

*Rahild Neuburger (MÜNCHNER KREIS), Magdalena Mißler-Behr (BTU Cottbus)*

15.10.19 (Überarbeitung)

## 1. Gegenstand, Ziele und Systemanalyse

### 1.1 Digitale Daten zwingen KMU zur Transformation: Von der Analyse bis zu soziotechnischen Innovationen

Der Vulnerabilitätsraum KMU und digitale Daten untersucht die unbeabsichtigten Nebenwirku-ngen (unintended side effects; unseens) der Digitalisierung für KMU. Dabei wird den negativen Auswirkungen, welche sich aus den Interaktionen von Eigentum, ökonomischem Wert, Zugang und Nutzung von digitalen Daten ergeben, besondere Beachtung geschenkt.

Dies betrifft insbesondere auch den Bereich der kleinen und mittleren Unternehmen (KMU)[7], dem traditionellen Rückgrat der deutschen Wirtschaft. Art und Umfang ebenso wie Beschaffungs-, Erstellungs- und Vertriebsprozesse haben sich dort in unterschiedlicher Intensität bereits verändert. So kann man mit Hinblick auf Unterschiede in den Auswirkungen und dem Ausmaß der Digitalisierung etwa unterscheiden zwischen

1. KMU, die (primär) Daten nutzen (1a), und KMU, die Daten generieren, die an andere Unternehmen zu deren Prozess-, Produkt- oder Dienstleistungsoptimierung weitergereicht werden können (1b),
2. KMU ohne (2a) und KMU mit direkter Interaktion zu Endkunden (2b), wie z.B. Printmedien und Unternehmen in der Werbebranche.
3. KMU der (primären) Sachgüterproduktion (3a) und KMU im Dienstleistungsbereich (3b) sowie
4. KMU in verschiedenen Wirtschaftszweigen oder Branchen mit ähnlichem Produkt- und/oder Dienstleistungsschwerpunkt, z.B. nach der bekannten NACE Klassifikation der EU: Land- und Forstwirtschaft (A), Bergbau (B), Verarbeitendes Gewerbe (C), Energieversorgung (D), Wasserversorgung (E), Baugewerbe (F) usw. bzw. feiner aufgegliedert (siehe https://ec.europa.eu/eurostat/ramon/nomenclatures).

Viele KMU (z.B. IT-Systemhäuser und andere digitale Dienstleister) besitzen hin-

[7] Gemäß EU-Definition (EU, 2003) werden Unternehmen mit 249 und weniger Mitarbeitern und einem Umsatz von bis zu 50 Mio. € als KMU angesehen. In der Praxis – und im Rahmen von DiDaT – verstehen sich Unternehmen bis zur Größenordnung von 1.000 oder gar mehr Mitarbeitern als mittelständische Firmen oder auch als KMU.

sichtlich der Auswirkungen und des Ausmaßes der Digitalisierung sogar eine interessante Doppelrolle, da sie einerseits Treiber der Digitalisierung bei anderen KMU sind, indem sie dort Digitalisierungsprozesse befördern, andererseits aber auch intern wieder stark von Veränderungen der Digitalisierung betroffen sind (etwa hinsichtlich der Organisation der internen Prozesse oder des Qualifikationsbedarfs bei Mitarbeitern).

Wir verstehen unter KMU Kleinst- und Kleinunternehmen und Unternehmen bis zur Größenordnung von ca. 1000 Mitarbeitern. Die Arbeitsgruppe startet unter der Prämisse, dass die KMU in Deutschland eine Art Schutzgut darstellen. Da diese in traditionell in besonderer Weise das Rückgrat der Wirtschaft darstellen.

Die Digitalisierung, das heißt die Repräsentation von Gegenständen und Prozessen in Form von durch Algorithmen verknüpfbaren digitalen Informationen, stellt eine bisweilen disruptive Transformation und Umgestaltung der Gesellschaft, der Wirtschaft und aller Bereiche des Lebens dar. Digitale Daten werden heute als eine Ressource und ein geldwertes, handelbares Gut (Commodity) begriffen, welches insbesondere eine Grundlage von automatisierten Prozessen der Produktion und verschiedener Dienstleistungen darstellt. Verschiedene Berufe und Wirtschaftsbereiche von KMUs werden durch künstliche Intelligenz, Big Data Analytics, GPS-basiertes autonomes Fahren, Big Data Analytics basierte Analysen und die IOT-Technologien, 3D/4D Printing weitgehend umgestaltet und/oder gar aufgelöst. In diesem Zuge entstehen neue Wirtschaftsbereiche, Produkte und Dienstleistungen, die von KMUs übernommen werden können. So setzt zum Beispiel “Digital Manufacturing” die produzierenden Unternehmen durch “End-to-End-Prozesse” (von Design und Engineering, über Produktion und Versand bis hin zur Anwendung und Sanierung) in die Lage, Qualität und Effizienz wesentlich zu verbessern.

Während in vielen Veröffentlichungen, Studien und Leitfäden KMU bisher vor allem auf die Notwendigkeit, die Möglichkeiten und die zügige Umsetzung einer digitalen Transformation hingewiesen wurden, soll im Rahmen von DiDaT untersucht werden, mit welchen unerwünschten und unerwarteten Nebenfolgen (Rebound Effekten) dieser Transformation zu rechnen ist. Darüber hinaus sollen geeignete Maßnahmen entwickelt werden, die es KMU einerseits ermöglichen von der Digitalisierung zu profitieren, andererseits aber auch auf Bedrohungen und Risiken der Digitalisierung vorbereitet zu sein.

Dass die Digitalisierung neben der erwünschten Stärkung der Wettbewerbsfähigkeit von KMU auch Bedrohungen und Risiken bedingt, wird etwa im Gutachten des WBGU im Auftrag der Bundesregierung (2019) anhand eines Beispiels deutlich. Dort wird darauf hingewiesen, dass die Digitalisierung der Beschaffungs-, Erstellungs- und Vertriebsprozesse es heute vielen KMU ermöglicht, Waren über Datentausch kostengünstiger von weit entfernten Wertschöpfungspartnern zu beziehen, dass diese Verlagerung neben einer erheblichen Steigerung der Umweltbelastung mittelfristig aber auch eine Substitution der Wertschöpfung durch diese weit entfernten Partner bedeutet. Bundesministerin Svenja Schulze etwa befürchtet anhand dieses Beispiels, dass die Digitalisierung so zum „Brandbeschleuniger

für die ökologischen und sozialen Krisen unseres Planeten“ werden kann. Es ist daher ein wesentliches Ziel dieses Projekts, neben den zahlreichen Chancen der Digitalisierung auch diese – oft nicht rechtzeitig erkannten – Bedrohungen und Risiken für KMU zu identifizieren und zu überlegen, die Einleitung welcher Maßnahmen diese Vulnerabilität reduzieren kann.

der negativen Auswirkungen der Digitalisierung an. Wir unterscheiden zwischen dem Unternehmen und seiner Umwelt.

Ziel der Arbeit ist es, soziotechnische Innovationen zu beschreiben, die KMUs helfen, mit den Veränderungen und negativen Auswirkungen der Digitalisierung geeignet umzugehen. Dazu setzen wir an einer Identifikation und Analyse der Entstehung und der Art der Unseens und

| | |
|---|---|
| Human species | |
| Supranational systems | Digital Infrastructure Providers |
| Human society | |
| Institutions | |
| Organisation | |
| Commercial | Non-commercial |
| Group | |
| Small group | Internet group |
| Individual | |

**Tabelle1: Levels of a human systems and new layers in the turn to the digital age, (yellow) shaded new levels with the rise of globalization and digital technology**

In Abbildung 1 repräsentieren die beiden rechten Spalten die Organisationale Ebene und die Human Resources von Unternehmen. Bei der Umwelt differenzieren wir zwischen dem Markt und deren Akteuren und Prozessen sowie den Rahmenakteuren. Damit betrachten wir fünf Ebenen von Akteuren (oder Humansystemen) der industriellen Gesellschaft (siehe Tabelle 1). Neben den Individuen (die teilweise in Ihrer Arbeitszeit als Teil der Organisation aufgefasst werden können), den kommerziellen Organisationen, betrachten wir Behörden (Institutionen und andere Einrichtungen, die den Markt regeln) und die Gesellschaft (d.h., hier die verfassungs-mässigen, rechtlichen, kulturellen etc. Regelungssysteme und die Politiker und deren Entscheidungen). So stellen zum anderen Handlungen (zum Beispiel Förderprogramme) von Politikern oder Änderung des legislativen Systems im Parlament wichtige Grundlagen für das Handeln von KMU dar.

Als zusätzliche vierte Ebene, die betrachtet wird, ist die Europäische Union (Supranational System) zu begreifen. Aus soziologischer und anthropologischer Perspektive werden aber auch die Digitale Infrastruktur Provider (DIPs) als ein supranationales System gesehen, die sich der nationalen Kontrolle weitgehend entziehen und als zentraler überstaatlicher Akteur fungieren. Die Big Five (Google, Amazon, Facebook, Apple, und Mircrosoft) liefern große Teiler der Infrastruktur, d.h. für die Speicherung, den Transfer (etwa dem Mailversand), den

Zugang (etwas Suche von Informationen) und die Verarbeitung (etwa im Rahmen von Cloud Nutzungen) von digitalen Daten. Diese digitale Infrastruktur stellt nur unter bedingter Steuerung und Kontrolle durch das deutsche politische System (i.e., der „German Society“). Aus diesem Grund findet sich in Abbildung 1 neben supranationalen Institutionen (EU, welche gleichermaßen wichtige Regularien für Tätigkeiten von KMUs vorgibt) die Digital Infrastructure Provider. Die Daten und die digitale Infrastruktur stellen somit ein (auf allen Ebenen) teilweise von den gleichen Akteuren bestimmtes Fundament der Tätigkeiten von KMU in der post-industriellen Gesellschaft dar

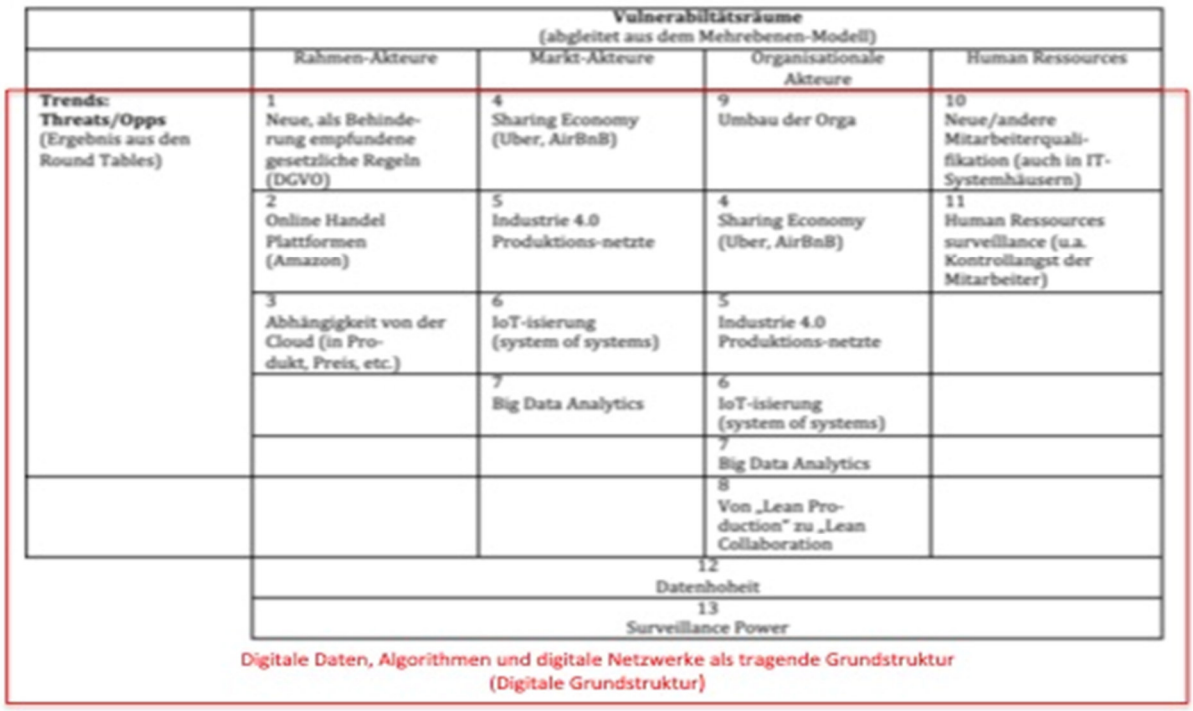



Abbildung 1: Wichtige Veränderungen oder Bedrohungen durch Digitalisierung für Akteure verschiedener Ebenen von Akteuren (die Veränderungen/Bedrohungen finden teilweise in mehreren Feldern statt.

## 1.2 Vulnerabilitätsanalyse an Stelle von Risiko

Für die Arbeit im Projekt DiDaT und in der Arbeitsgruppe KMU und digitale Daten besitzt das Vulnerabilitätskonzept eine besondere Bedeutung. Die Vulnerabilität einer KMU wird als eine Funktion der (1) Sensitivität, der (2) Exposition und der (3) adaptiven Kapazität gegenüber digitalen Veränderungen und Bedrohungen definiert.

Die Sensitivität wird durch Unseens (hier Ereignisse oder Gegebenheiten, die ohne angemessene Anpassungen und Veränderungen auf der Seite der KMU negative Auswirkungen haben) bestimmt. Dazu gehört die Konkurrenzfähigkeit (durch Marktverluste, schlechtem Cash Flow oder Mangel an geeignet qualifizierten MitarbeiterInnen) und die Überlebensfähigkeit („viability“) des Unternehmens, etwa, wenn keine geeigneten Maßnahmen zur Anpassung gefunden werden.

Unter Exposition verstehen wir die Wahrscheinlichkeit, mit der eine solche Auswirkung ein Unternehmen oder eine Teilbranche treffen.

Und unter der adaptiven Kapazität wird die Anpassungsfähigkeit der KMU begriffen, mit der negative Auswirkungen (zum Beispiel reduzierte Auftragsvolumen in Druckereien) kompensiert werden können.

Um Strategien für die Entwicklung der Anpassungsfähigkeit zu definieren, werden im Auswirkungsraum VR03 KMU und digitale Daten zunächst die Unseens identifiziert und strukturiert.

Dazu werden wir im ersten Schritt in Anlehnung an Porter (Porter, 2001) und die Aktionsfeldanalyse von Gimpel et al. (2018, siehe Abschnitt 2) die Bereiche Organisation und Markt in den Komponenten Produktion, Organisation und Transformationsmanagement sowie Wertversprechen und Kunden analysieren.

Wir werden anschließend danach auf Veränderungen im Human Resources Management und potenzielle Veränderungen im Bereich Rahmung (Rahmenakteure) eingehen.

In einem abschließenden Schritt werden wir dann eine Reihe von Prozessen und Beispiele für Unseens beschreiben, die es erlauben, die spezifischen Prozesse, Ursachen, Betroffene etc. eines Unseens zu verstehen.

Diese Beispiele finden sich nummeriert bereits in Abbildung 1. Die Beispiele wurden in einer Studie zur Vulnerabilität und Anpassungsstrategien von Organisationen entwickelt bzw. stammen aus der Praxiserfahrung der Mitglieder der Arbeitsgruppe des VR03.

Die Beispiele werden dazu dienen zu illustrieren, welche Anpassungsmaßnahme KMU ergreifen müssen und welche sozio-technologischen Maßnahmen notwendig sind, um die Viability von KMU zu sichern.

Alle Arbeiten in der Arbeitsgruppe VR03 beziehen sich auf die folgende Leitfrage, die in einem diskursiven Prozess zwischen Wissenschaft und Praxis bis zum Ende des Jahres (Beginn der Hauptphase, zweite Stakeholder-Konferenz) abschließend formuliert werden soll:

**Guiding Question:**

What changes and threats (unseens) of digitalization cause vulnerabilities for what type of German SME (e.g., domains of craft, commerce and industry)?

What unseens result for SME from interaction between unfavorite relations between ownership, economic value, use, and access to digital data.

What adaptive capacity (e.g., in integrative data analytics) and new competences (including security management) are needed to keep short-, medium, and long-term competitive power with large-scale firms.

## 2. Welche unbeabsichtigten Nebenfolgen sind von Interesse und warum?

Es wurden folgende Vulnerabilitäten identifiziert.

***1 KMU haben beträchtlichen Aufwand, die gesetzlichen Regeln intern umzusetzen und einzuhalten.***

Die deutsche Wirtschaft kämpft immer noch mit der Datenschutz-Grundverordnung. Fast eineinhalb Jahre nach Geltungsbeginn haben zwar zwei Drittel der Unternehmen (67 Prozent) die neuen Datenschutzregeln mindestens zu großen Teilen umgesetzt. Dabei hat allerdings erst ein Viertel (25 Prozent) die Umsetzung der DSGVO vollständig abgeschlossen." 20.09.2019 https://www.it-daily.net/analysen/22381-zwei-drittel-der-unternehmen-haben-dsgvo-umgesetzt Zum Teil werden in CRM-Datenbänke Mengen an Kunden-Daten gelöscht, genauso wie persönliche Daten von Mitarbeitern.

***2 Online Handel Plattformen***

halten in verschiedenen Bereichen eine Monopolstellung[8]. Die globalen Plattformen verfügen über einmalige Marktkenntnisse und treten in lukrativen Geschäftsfeldern mit KMU Aufgaben in Konkurrenz.

***3 Abhängigkeit von Cloud-Anbietern (in Produkt, Preis, etc.)***

Cloud-Anbieter binden KMU vertraglich eng an ihre Leistungen. Cloud-Infrastrukturen werden zu proprietären System ausgebaut. Je mehr Infrastruktur die IT von KMU in die Cloud verlagert und sich also umstrukturiert, desto abhängiger werden sie von diesen Anbietern, weil es einen hohen Aufwand bedarf, auf andere Anbieter umzustellen oder gar wieder eine eigene Infrastruktur aufzubauen. Diese können Produkte und Dienste sowie deren Preise und Einsatzbedingungen je nach eigener Strategie verändern.

***4 Sharing Economy***

Prozesse (Uber, AirBnb, etc.; mit teilweise hohen digitalen Transaktionsgebühren) stellen akute Bedrohungen für die Existenz und den Ertrag einiger KMU Branchen (Taxigesellschaften, Übernachtungsgewerbe) dar. Mit welchen Mitteln kann eine Positionierung bei Erhalt der Qualität der (Dienst-) Leistungen gesichert werden?

***5 Industrie 4.0 Produktionsnetze***

Industrie 4.0 stellt eine vollständige digitale Repräsentation und ein Management-Tool für gesamte Produktionsketten dar. KMUs sind Bestandteil, aber in der Regel nicht die steuernden Größen dieses Prozesses. Dies wird durch die Metapher der „Verlängerten Werkbank" ausgedrückt.

***6 IoTisierung***

Viele handwerkliche Betriebe werden digitalisiert und Produkte (im Rahmen von IoT Netzwerken) modularisiert. Dies führt dazu, dass Innovationen im Bereich des Schnittstellenmanagements zu einem wesentlichen Gegenstand der Viability von Unternehmen werden. Im Handwerksbereich kann die energetische Optimierung durch integrale Lösungen von Heizung, Fensterbau (inkl. Lüftungs- und Lichtsteuerung) und Elektrik als Beispiel genommen werden.

***7 (Big) Data Analytics***

Wirtschaftliche Prozesse werden durch die Nutzung digitaler Daten der Produktion (z.B. beim Einsatz der Maschinen), firmeninterner organisatorischer Prozesse, der Marktprozesse etc. wettbewerbsfähiger. Um konkurrenzfähig zu bleiben, müssen KMU vielfältige Daten-Analyse-Fähigkeiten (inkl. Big Data) erwerben.

***8 Von „Lean Production" zu „Lean Collaboration" (agility based short time collaboration)***

Der Einsatz von Collaboration Tools (z.B. Microsoft 365) ermöglicht neue Formen der Zusammenarbeit über Hierarchien und Abteilungsgrenzen hinweg. Folge: Abbau von Hierarchien? Mittelmanager obsolet?

***9 Umbau der Organisation***

KMU müssen sich auf die Konzepte (siehe z.B. Agilisierung) Prozesse und IT-Systeme ihrer großen Unternehmenskunden einstellen. Daher mögliche Überforderung durch Umfang und Vielfältigkeit der Änderungen, Tiefe und Geschwindigkeit notwendiger organisatorischer Restrukturierung und Mangel von notwendigem Wissen (human ressources bottleneck).

***10 Neue/andere Mitarbeiterqualifikationen (auch in IT-Systemhäusern)***

Durch den Einsatz von IT-Systemen sowie Algorithmen und Data Analytics verändern sich die Rollen von Mitarbeitern in fast allen Bereichen und folglich auch deren Anforderungsprofile. Viele Tätigkeiten können von Computern übernommen werden. Beispiele: Der klassische Buchhalter hat ausgedient; Market Research wird erledigt durch Algorithmen; Maschinenbediener werden zu Maschinenüberwachern. IT-Systemhäuser zum Beispiel haben erkannt, dass sie viel mehr Beratungsleistungen in puncto Prozesse - ja sogar allgemein in puncto Innovationsmöglichkeiten - bieten müssen statt nur IT-Systeme technisch zu installieren.

***11 Human Resources Überwachung (u.-a-) Kontorollangst der Mitarbeiter***

Chefs können in Echtzeit die Bildschirm-Arbeit ihrer Mitarbeiter „tracken" und sie genauestens kontrollieren. Jüngere Mitarbeiter sind es gewohnt, via Sozialer Medien tagtäglich tausende Daten unüberlegt an Daten-Sammler zu liefern. Was für diese im Privatleben Normalität ist, kann aber durchaus im Unternehmen für dieselben Personen zum Problem werden. Ältere Mitarbeiter werden wohl eher Kontroll-Angst haben und, wie schon immer gewohnt, kreative Wege finden, diese digitalen Kontrollen auszutricksen.

***12 Allokation der Datennutzungsrechte***

Konzepte wie Industrie 4.0 ermöglichen den Zugang zu allen Daten der Produktions- und Wertschöpfungskette. Welche Daten bleiben in der Hoheit der Endproduzenten, aller Beteiligten, der KMU etc.

***13 Surveillance Power (Überwachungskapitalismus)***

Surveillance capitalism ist ein (nach Shoshana Zuboff , 2014) System, „das die mit technischen Mitteln von Menschen abgeschöpften persönlichen Daten dazu benutzt, Informationen über Verhaltensweisen zu sammeln, diese zu analysieren und für marktökonomische Entscheidungsfindungen aufzubereiten, um daraus Verhaltensvorhersagen generieren zu können und über deren Nutzung Gewinne zu erwirtschaften." https://de.wikipedia.org/wiki/Überwachungskapitalismus

**Tabelle 2: Liste der unbeabsichtigten Nebenfolgen**

Ein wesentliches Zwischenziel besteht darin, eine Gruppierung (Klassifikation) der Vulnerabilitäten (Risiken), die sich für KMU aus der Digitalisierung ergeben und der Mechanismen, die diesen unterliegen, zu erarbeiten. Darauf aufbauend sollen Anpassungsstrategien (adaptive Strategien) und Handlungsprogramme (soziale und technologische Innovationen) umrissen werden, die für eine erfolgreiche Positionierung von KMU sinnvoll oder gar notwendig sind.

Dazu haben wir die Vulnerabilitäten in die in Abbildung 1 (Seite 3) eingefügt. Die detaillierte Beschreibung der 4 Räume findet sich im Appendix

**3. Welche Stakeholder sind für ein Verständnis und ein Management der „Unseens“ von besonderer Bedeutung? Welche wissenschaftlichen Wissensbereiche sind relevant?**

Aus einem vereinfachten Systemmodell für KMU als Teil einer zunehmenden Digitalisierung ergeben sich folgende Bereiche, zu denen Wissen vorhanden sein sollte:

- Neue digitale Produkte/Produktbereiche: Welche Transformationen werden notwendig (Bsp. Autoschlosser-Automechaniker-Automechatroniker)?
- Neue digitale internen Prozesse: Welche Folgen hat Industrie 4.0 auf die firmeninternen Prozesse (etwa in Buchführung, Verwaltung, Monatsabrechnungen, digitalisierte Spesenabrechnungen/Belegerfassung https://www.lexoffice.de/funktionen/belegerfassung/, online Erfassung der Produktion, etc.)?
- Für Unternehmen die keine Endprodukte für den Konsumenten produzieren: Wie verändert sich die Schnittstelle zu den Zulieferern/Abnehmern? Welche persönlichen Schnittstellen per face to face/Telefon bleiben erhalten? Wo kann ich auf digitale Prozesse besser/effizienter zurückgreifen? Wie sehen die Modelle von Industrie 4.0 aus?
- Welche Besonderheiten zeigen IT Betriebe?
- Daten
- Welche Rolle spielen branchenspezifische Plattform-Economics?
- Für Unternehmen für den Konsumenten zusätzlich: Welche Bedeutung hat für die Branche der Vertrieb über Plattformen wie Amazon etc.?

| | Stakeholder-Gruppen | | | | | |
|---|---|---|---|---|---|---|
| | Rahmen-Akteure | | Wirtschaft | | Society at large | |
| | Behörden | Infrastructure Provider | Wirtschafts-verbände BVDW, IHK | Berater, Kompetenzzentren (Wirtschaft und IT) | Gewerk-schaften | Konsumenten und Bürger |
| **Vertreter** | | | L. Probst (IHK) | W. Hofmann (Systemhaus) | | |
| **Vulnerabilitäten** | | | | | | |
| 1. *Neue, als Bedrohung empfundene gesetzliche Regeln* | | | BVDW | Kompetenz-zentrum Mittelstand | | |
| 2. *Online Handel Plattformen* | | | | Komp-Zentrum Mittelstand Strategie-Berater | | |
| 3. *Abhängigkeit von Cloud-Anbietern (in Produkt, Preis, etc.)* | | | BVDW | IT-Berater | | |
| 4. *Sharing Economy* | | | | Komp-Zentrum Mittelstand | | |
| 5. *Industrie 4.0 Produktionsnetze* | | | BVDW | Untern-Berater IT-Berater | | |
| 6. *IoTisierung* | | | | IT-Berater Strategie-Berater | | |
| 7. *(Big) Data Analytics* | | | | IT-Berater Strategie-Berater | | |
| 8. *Von „Lean Production" zu „Lean Collaboration" (agility based short time collaboration)* | | | | Untern-Berater IT-Berater Strategie-Berater | | |
| 9. *Umbau der Organisation* | | | IHK | Untern-Berater | | |
| 10. *Neue/andere Mitarbeiterqualifikationen* | | | IHK | Untern-Berater Coach | | |
| 11. *Human Ressources, Überwachung (u.a. Kontorollangst)* | | | IHK | Untern-Berater Coach | | |
| 12. *Allokation der Datennutzungsrechte* | | | BVDW | | | |
| 13. *Surveillance Power (Überwachungskapitalismus)* | | | | | | |

**Tabelle 3: Stakeholder-Gruppen Die 3 wichtigsten Stakeholder pro Vulnerabilitätsraum sind gelb markiert**

## Stakeholder in den Vulnerabilitätsräumen bzw. Aktionsfeldern

| **Stakeholder im Aktionsfeld „Rahmen-Akteure** | | | |
|---|---|---|---|
| | **Verursacher** | **Betroffene** | **Problemlöser** |
| | • Nationale und internationale Gesetzgeber | • Alle KMU | • Wirtschaftsverbände |
| | • Plattformen | • Besonders B2C-KMU | • KMU-Netzwerke<br>• IT-Systemhäuser und Unternehmensberater |
| | • IT-Infrastruktur-Provider | • Alle KMU, je kleiner desto eher abhängig | • Nationale und kleine Cloud-Anbieter<br>• IT-Systemhäuser und Unternehmensberater |
| **Repräsentanten** | • NN | • Lothar Probst (IHK) | • Dr. Wolfgang Hofmann (Systemhaus)<br>• NN |

| **Stakeholder im Aktionsfeld „Markt-Akteure"** | | | |
|---|---|---|---|
| | **Verursacher** | **Betroffene** | **Problemlöser** |
| | • Plattformen<br>• Automatisierer, KI-Provider<br>• IT-Systemhäuser<br>• IT-Provider<br>• Unternehmenskunden | • Alle KMU<br>Insbesondere produzierende KMU im B2B | • Strategie-Berater/-Coaches<br>• IT-Systemhäuser und Unternehmensberater<br>• Wirtschaftsverbände<br>• IHKs<br>• Innovationsberater |
| **Repräsentanten** | • Dr. Wolfgang Hofmann (Systemhaus)<br>• NN | • Lothar Probst (IHK) | • Dr. Wolfgang Hofmann (Systemhaus)<br>• Lothar Probst (IHK)<br>• NN |

| **Stakeholder im Aktionsfeld „Organisationale Akteure"** | | | |
|---|---|---|---|
| | **Verursacher** | **Betroffene** | **Problemlöser** |
| | • Plattformen | • Alle KMU | • Strategische Organisations-entwickler |

| | | | |
|---|---|---|---|
| | • Automatisierer, KI-Provider<br>• IT-Systemhäuser<br>• IT-Provider<br>• Unternehmenskunden | insbesondere produzierende KMU im B2B | • Coaches und Trainer<br>• IT-Systemhäuser und Unternehmensberater<br>• Wirtschaftsverbände<br>• Gewerkschaften |
| **Repräsentanten** | • Dr. Wolfgang Hofmann (Systemhaus)<br>• NN | • Lothar Probst (IHK) | • Dr. Wolfgang Hofmann (Systemhaus)<br>• NN |

| **Stakeholder im Aktionsfeld „Human Ressources“** | | | |
|---|---|---|---|
| | **Verursacher** | **Betroffene** | **Problemlöser** |
| | • IT-Systemhäuser<br>• IT-Provider<br>• Topmanager | • In allen KMU insbesondere Mittel-manager und Mitarbei-ter, aber auch Top-manager selbst | • Coaches und Trainer<br>• IHKs<br>• Wirtschaftsverbände<br>• Gewerkschaften<br>• Gesetzgeber |
| **Repräsentanten** | • Dr. Wolfgang Hofmann (Systemhaus)<br>• NN | • Lothar Probst (IHK) | • Lothar Probst (IHK)<br>• NN |

| | | | |
|---|---|---|---|
| **Noch fehlende Repräsentanten** | • **Plattformen**<br>• **IT-Infrastruktur-Provider**<br>• **Automatisierer**<br>• **KI-Provider**<br>• **Topmanager** | | • **Wirtschaftsverbände**<br>• **Gewerkschaften** |

**Tabelle 4: Verursacher, Betroffene und Problemlöser in den Vulnerabilitätsräumen bzw. Aktionsfeldern**

## 4. Unseens x Orientierungen Tabelle VR03

| Nr. | 1. Unseens | 2. Ursachen/Kausalitäten/ Entstehungsprozesse der Unseens | 3. Mögliche soziotechnologische Innovationen zur Mitigation | 4. Ziele | 4. Sozial robuste Orientierungen zum Umgang mit Unseens |
|---|---|---|---|---|---|
| 1 | Umsetzung gesetzl. Regeln | Geringe Umsetzungsquote<br>Gelöschte Daten-banken<br>Bürokratischer Aufwand<br>Unwissen<br>Mitarb. haben eigene Datenbanken | Dienstleister einsetzen<br>IHKs informieren<br>Einfache Heuristiken<br>Datenschutz als Chance (siehe Portfoliomgt) | Stärkung er KMU als Inno- und Tech-Motor<br>Verantwortlicher Datenschutz<br>Entwicklung neuer Geschäftsmodelle | Einfachere Anwendung<br>Information und Trg |
| 2 | Online Handel Plattformen | Abhängigkeit von Plattformen<br>Verlust an Kunden | | | |
| 3 | Abhängig von Cloud-Anbietern | Vertragliche Bindungen<br>Verringerte Flexibilität | | | |
| 4 | Sharing Economy | Existenz von Branchen bedroht | | | |
| 5 | Industrie 4.0 ProdNetze | Degeneration zu verlängerten Werkbänken | | | |
| 6 | IoTisierung | Innovationen werden zwingend notwendig | | | |
| 7 | (Big) Data Analytics | Mangelnde Daten-Analysefägkeiten | | | |

| | | | | | |
|---|---|---|---|---|---|
| 8 | „Lean Prod“ zu „Lean Collab“ | Abbau von Hierarchien? Mittelmana-ger obso-let? | | | |
| 9 | Umbau der Orga-nisation | Mangel an Change-Wis-sen und –Ressour-cen | | | |
| 10 | Mitarbeiterquali-fikationen | IT-Systeme verändern Rollen, schaffen neue Rollen | Neue Visionen<br>Redesign (Struktur, Pro-zesse)<br>Nachhaltige Transfor-mation<br>Interne Business Con-sultants<br>Agilitäts-Training | Entw. Digital Rea-diness<br>Digital-Wissen er-höhen<br>Unterstützung durch öffentl. Hand, Verbände | Beratungsoffensive<br>Regionale KMU-Netz-werke<br>Systemhaus-Netz-werke |
| 11 | Kontrolle der Mitarbeiter | Chefs tracken Mit-ar-beiter<br>Misstrauenskultur ent-steht | | | |
| 12 | Allok. Datennut-zungsrechte | KMU verlieren Hoheit über ihre eigenen Da-ten | | | |
| 13 | Überwachungs-kapitalismus | Manipulation von Ver-halten und Entschei-dungen | | | |

## 5. Methodische Überlegungen zur Unterstützung von Kernaussagen (Vertiefungsforschung)

Es bestehen große Unsicherheiten, grundsätzliche Unvorhersehbarkeiten über die anstehenden Veränderungen von Bereichen der deutschen KMU durch Digitalisierung, die Tiefe der Veränderung, der Geschwindigkeit der Veränderung, der negativen (und positiven) Auswirkungen und der Maßnahmen, die von Seiten der KMUs zu beschreiten sind.

Vor diesem Hintergrund macht es Sinn, eine Experten basierte, formative Szenario-Analyse für die Veränderung von zwei oder drei unterschiedlichen KMU-Branchen durchzuführen, in der für jede Branche 3-4 Digitalisierungs-Szenarien erstellt werden.

Darauf aufbauend können dann Innovations-/Interventionsszenarien konstruiert werden, deren Wirkung auf KPIs sogar (semi-)quantitativ abgeschätzt werden.

Dies würde für die Arbeitsgruppen eine formende Wirkung haben, da dann gemeinsam an Beispielen Zukunftsszenarien gebildet werden, die gegebenen und nichtgegebenen Anpassungsmöglichkeiten der KMU (Branchen) beschrieben werden und somit eine Grundlage für weitergehende Rahmungen und Unterstützung der KMUs gegeben werden kann.

## 6. Erwartete Ergebnisse und Folgeinitiativen

Wir erwarten, dass in dem Weissbuch für den Bereich KMU

- die wesentlichen Prozesse und wirtschaftlichen Veränderungen, auf die KMUs zu reagieren haben, dargelegt wird,
- aus den Beispielen ausgewählter Branchen gelernt wird, welche Anpassungsleistung (adaptive Kapazität) KMUs aufweisen müssen,
- aufgezeigt wird, in welchen Bereichen durch welche Unternehmensstrategien und gesellschaftspolitische Entscheidungen sich KMUs anpassen können und wo es zu disruptiven Veränderungen kommt, denen es gilt geeignet zu begegnen.

## Referenzen

Capgemini. (2017). Studie IT-Trends 2017. Überfordet Digitalisierung etablierte Unternehmensstrukturen. Berlin: Capgemini Deutschland.

EU. (2003). Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, Aktenzeichen K(2003) 1422. Eur-Lex, Document 32003H0361.

Gimpel, H., Hosseini, S., Huber, R., Probst, L., Röglinger, M., & Faisst, U. (2018). Structuring digital transformation: a framework of action fields and its application at ZEISS. Journal of Information Technology Theory and Application, 19(1), 31-54.

Porter, M. E. (2001). Strategy and the Internet Harvard Business Review, 79, 62-79.

Scholz, R. W., Bartelsman, E. J., Diefenbach, S., Franke, L., Grunwald, A., Helbing, D., . . . Viale Pereira, G. (2018). Unintended side effects of the digital transition: European scientists' messages from a proposition-based expert round table. Sustainability, 10(6), 2001; https://doi.org/10.3390/su10062001.

# Vulnerabilitätsraum 04 (VR04)

# Landwirtschaft, Digitalisierung und digitale Daten

DiDaT Grobplanung für Vulnerabilitätsraum 04 (VR04)

# Landwirtschaft, Digitalisierung und digitale Daten

*Jana Zscheischler (ZALF), Gert Berger (ZALF), Reiner Brunsch (Leibniz-ATB), Hermann Buitkamp (VDMA), Walter Haefeker (DBIB), Hans-Werner Griepentrog (DLG und Uni Hohenheim), Steffi Ober (NABU), Christian Reichel (Leibniz IRS), Roland W. Scholz (DUK)*

25. September 2019 (Entwurf)

## 1. Gegenstand, Ziele und Leitfrage

Die landwirtschaftliche Produktion stellt eine kritische Infrastruktur dar und hat damit eine wesentliche Bedeutung für wichtige gesellschaftliche Funktionen. Darüber hinaus nimmt sie starken Einfluss auf die natürliche Umwelt und die entsprechenden Ökosystemleistungen (einschließlich Biodiversität). Die Digitalisierung und die Nutzung digitaler Daten bringen wesentliche Veränderungen entlang der landwirtschaftlichen Produktionskette. Dies beginnt bei der agronomischen Optimierung der genutzten Pflanzen und Tiere (über Optimierung von Züchtung oder – global – genetischer Veränderung[9]), dem effizienteren Gebrauch von Nährstoffen und Hilfsmitteln (wie etwa dem Einsatz von Pestiziden), einer zunehmend digitalisierten, weniger menschliche Arbeit benötigenden, mit dem Potenzial einer, umweltfreundlicheren tierischen und pflanzlichen Produktion und einer darauf aufbauenden Nahrungsmittelproduktion. Die Landwirtschaft gilt heute (in einigen Ländern) als eine der am stärksten digitalisierten Branchen. Durch die Digitalisierung der Landwirtschaft werden von verschiedenen Seiten eine Steigerung der wirtschaftlichen und ökologischen[10] Effizienz, des Tierwohles, des Umweltschutzes und ein Beitrag zur Welternährungssicherheit erwartet.

Begriffe wie «precision agriculture» werden seit der Mechanisierungsdiskussion der Landwirtschaft (Meek, 1947) verwendet. Andere Begriffe wie „smart farming“ und „Landwirtschaft 4.0“ stehen in der Tradition dieser Konzepte. Digitale Daten der Landwirtschaft zu einer umfassenden internen und externen Vernetzung auszubauen und

[9] An dieser Stelle sei angemerkt, dass die *DNA als ein genuin digitales Konstrukt* zu begreifen ist. Eine spezifische DNA eine Folge der Zahlen 1-4 (d.h., der verschiedenen Ausrichtung von zwei Säurepaaren). In den Life Sciences, der Biologie und anderen Wissenschaften werden nicht nur die «unbeabsichtigte Nebenfolgen (Unseens)» des Konstruktes DNA und die positiven und potentiell negativen Folgen der Digitalisierung von Konstrukten und Technologien. Zu nennen sind hier, die potentiellen Folgen von «directed evolution» auf die Resilienz von Ökosysteme. Ein landwirtschaftliches Beispiel sind die Auswirkungen der Folgen der Patentrechte, welches den landwirtschaftlichen Betrieben in den USA nicht erlaubt, Glyphosat-resistenten, selbstproduzierten Mais als Saatgut zu verwenden. Damit wird der ökonomische Handlungsraum des Landwirtes in der Wertschöpfungskette eingeschränkt. Diese Aspekte (und andere fundamentale Fragen, wie sich der Übergang von analogen zu digitalen Modellen auf die Wissenschaft auswirkt) werden im Rahmen des Gesamtprojekts diskutiert und stellen keinen Schwerpunkt von DiDaT dar.

[10] Im einfachsten Sinne zu verstehen als eine Senkung der negativen Umweltauswirkung pro produzierte Nahrungsmitteleinheit.

zu vertiefen, ist ein wesentliches Ziel von „Landwirtschaft 4.0“ (Griepentrog, 2018).

Für «digital farming» stellt die die Verknüpfung von (grossen) Daten(mengen) aus dem landwirtschaftlichen Betrieb, dem Umweltsystem (z.B., Wetter, Insekten, Pilzen, etc.) und den Märkten etc. einen zentralen Erfolgsfaktor dar. Damit ist eine fundamentale Umstrukturierung der landwirtschaftlichen Produktionskette und ihrer Akteure zu erwarten. Dennoch bewerten Agrarexperten die Digitalisierung sehr unterschiedlich (Deutscher Bundestag, 2019). Mit dieser Umstrukturierung sind eine Reihe möglicher unerwünschter Veränderungen, Risiken und Vulnerabilitäten verbunden. Die Landwirtschaft stellt eine der kritischen Infrastrukturen dar und nationale Ernährungssicherheit sieht sich neuen Gefahren durch «Hacking» und «Cyberattacks» ausgesetzt.

Im Rahmen von Landwirtschaft 4.0 werden hier digitale Daten und ihre Nutzung entlang der landwirtschaftlichen Produktionskette bis zur Stufe der Erstverwertung berücksichtigt. Es wird in besonderer Weise die Wertschöpfung durch die Nutzung der digitalen Daten und (aus der Sicht verschiedener Stakeholdergruppen) unerwünschte Auswirkungen (nicht-intendierte Nebeneffekte, auch so genannte „Unseens“) betrachtet, die sich durch neue Formen der Datennutzung ergeben. Die Rolle der Akteure (und der landwirtschaftlichen Betriebe) in der Wertschöpfungskette wird durch die Digitalisierung neu definiert. Die Kategorisierung und Nutzungsrechte der entstehenden Daten sind unklar, sowie das Wissen, welche Daten überhaupt erzeugt werden (z.B. Daten, die von dem Traktor eines Landwirts generiert werden, auf welche der Betrieb selber keinen Zugang hat). Es besteht daher dringlicher Klärungsbedarf darüber, wer welche Daten wann für welche Zwecke verwenden darf und wer hier welchen wirtschaftlichen Nutzen daraus ziehen soll.[11] Dazu bedarf es geeigneter gesellschaftlicher und gesetzlicher Rahmungen.[12]

An dieser Stelle wird es auch aus Nachhaltigkeitsperspektive schwierig, zu geeigneten Abwägungen zwischen gemeinwohlorientierten Interessen (z.B. Naturschutz, sozialer Gerechtigkeit), wirtschaftlichen Interessen (der landwirtschaftlichen Einzelbetriebe, der landwirtschaftlichen Maschinenhersteller, der Agrar- und Lebensmittelkonzerne, etc.) bezogen auf Zugangsrechte zu digitalen Daten zu kommen. Landwirtschaftliche Betriebe sehen sich hier schwierigen Fragen und Investitionen gegenüber. Die Fragen besitzen eine technische Dimension (Welche Stufe der Digitalisierung ist kurz- und mittelfristig sinnvoll und notwendig?) und eine auf Qualifikation der Beteiligten der Wertschöpfungskette bezogene Dimesnio (Welche Fähigkeiten zur Auswertung von Daten brauche ich? Wem vertraue ich meine betrieblichen Daten an?). Es entstehen für den Landwirtschaftsbetrieb auch

[11] Dieser Punkt bezieht sich unmittelbar auf die vom Europäischen Experten-Roundtable gegebene Hauptaussage, dass die weitgehend unverstandene Wechselbeziehung zwischen Eigentum, ökonomischen Wert, Zugang und Nutzung von Daten zu schwerwiegenden, gesellschaftlich unerwünschten Folgen der Digitalisierung führen kann (Scholz et al., 2018).

[12] Hier sei angemerkt, dass es auf Europäischer Ebene für den personengebundenen Datenschutz umfassende Regelungen gibt, diese aber auf der Ebene der wirtschaftlichen Daten nicht in vergleichbarem Masse vorhanden sind.

neue Abhängigkeiten bezogen auf Funknetze, Datenauswertung etc. Unsicher ist, ob und in welchem Rahmen wird eine «Agrarmasterplattform» aufgebaut wird und wer welchen Zugang und Nutzen von dieser Plattform erhält. An dieser Stelle sollte der Verlust von individuellem Wissen und die veränderte Positionierung des Landwirtes **durch Digitalisierung und Datennutzung** problematisiert werden. Eine marktgerechte, konkurrenzfähige Bewirtschaftung basiert in vielen Bereichen auf einer guten Nutzung der digitalen Daten und geeigneter, gekaufter Software. Dieses Wissen wurde früher (häufig weitgehend in analoger Form) von den Landwirten verfügt. Hinzu kommen weitere Fragen zum Datenmanagement wie: Wer verwaltet die Daten, programmiert und verfügt die Software? Welche systemischen Vulnerabilitäten liegen hier in einer bestimmten Auswahl von Wissen, Daten, Fakten, und Interpretationen?

Im Rahmen des Vulnerabilitätsraumes sollen für die Zukunft der Landwirtschaft Digitalisierungs-Szenarien erstellt, analysiert und diskutiert werden, die in ihren Grundannahmen und jeweiligen Auswirkungen weit auseinander gehen. Ein mögliches Szenario wäre, dass der aktuell zu beobachtende Trend immer größerer, stärkerer und breiterer (auch teurerer) Agrartechnik sich fortsetzt und zu weniger und größeren Betriebe führt. Ein anderes, konträres Szenario setzt auf die Möglichkeiten durch kleinere, intelligentere und effizientere Feldroboter. Dies ermöglicht eine an den Standort angepasste, kleinteiligere sowie auf Multifunktionalität ausgelegte Bewirtschaftung und ermöglicht auch kleineren Betrieben zu partizipieren. Für diese Szenarien, die sich beider möglichweise in verschiedenen Gebieten (i.e. im Norden und Süden Deutschlands) für die landwirtschaftliche Nutuzung angemessen sind, ist aus Umweltschutzgesichtspunkten zu bewerten welche Feldroboter etwa in derl Lage sind sowohl Beikräuter als auch Schädlinge zu identifizieren. Wie müssen die die räumlichen und biologischen Gegebenheiten durch welche digitalen Daten abgebildet werden, damit für eine ökologische Bewirtschaftung die richtigen Schlüsse gezogen werden. Es ist zu erwarten, dass neues und anderes der lokalen Akteure neues und anderes Wissen über die Stärken und Schwächen der digitalen landwirtschaftlichen Geräte und Maschinen und das lokale Ökosystem verfügen müssen.

Ziel der Arbeitsgruppe ist es, durch einen wechselseitigen Lernprozess zwischen Repräsentanten wichtiger Stakeholdergruppen zukünftige (und aus ihrer Sicht wahrscheinliche) Entwicklungen zu diskutieren, Chancen und Risiken zu identifizieren und in ihren Wirkmechanismen zu beschreiben. Darauf aufbauend soll in einem Kapitel des Weissbuches “Verantwortungsvolle Umgang mit Digitalen Daten” Orientierungen soziale und technische Innovationen im Umgang mit unerwünschte Wirkungen der Digitalisierung entworfen und beschrieben werden.

.

**Leitfragen**:

Die Leitfragen für Vulnerabilitätsraum "VR04 – Landwirtschaft, Digitalisierung und digitale Daten"[13] lauten:

- Von welchem (negativen und positiven[14] Auswikunten) der Digitalisierung und der Nutzung digitaler Daten sind Landwirtschaft, Umwelt, sozioökonomische Systeme betroffen?
- Wie verändert sich die Beteiligung aller beteiligten Unternehmen entlang der Lebensmittelkette (beginnend bei den bäuerlichen Klein- und Mittelbetrieben, über den Transport, die Verarbeitungsstufen bis hin zum Handel und schließlich den Konsumenten) an der Wertschöpfungskette?
- Welche Folgen haben unterschiedliche Realitäten der Datenhoheit auf betriebliche Souveränität und Wertschöpfung?
- Wie muss der Rahmen gesetzt werden, um die Vorteile für Gesellschaft und Umwelt zu steigern und die Risiken zu minimieren?

## 2. Welche nicht intendierten, unbeabsichtigten Nebenfolgen der Digitalisierung und von digitalen Daten sind von Interesse und warum?

Trotz unterschiedlicher Ansichten über zukünftige Entwicklungen wird in den gängigen Zukunftsszenarien jeweils die Bedeutung der *Datenrechte* hervorgehoben. Risiken ergeben sich hier auch aus neuen Geschäftsmodellen, die die verschiedenen Akteure durch die Nutzung digitaler Daten erwerben können. In diesem Zusammenhang stehen Fragen der Erhebung, Nutzung, des Zugangs zu, dem Besitz und der Sicherheit von Daten. Hier wird von den Akteuren ein wichtiger aktueller Gestaltungsraum beschrieben, der „spielentscheidend" die weitere Entwicklung prägen wird. Noch ist offen, ob und in welchen Bereichen sich „offene Systeme" (in Form von Daten-Allmenden) gegenüber den Interessen großer (möglicherweise agrarfremder und ganz neuer) Datenkonzerne (mit „geschlossenen" Service-Angeboten) durchsetzen werden. Im Zusammenhang mit Letzterem wird auch das Risiko einer Vollautomatisierung landwirtschaftlicher Prozesse für den Landwirt thematisiert, der sich durch digitale Daten und Werkzeuge in starke Abhängigkeit und Kontrolle durch Agrarkonzerne begibt. Es ist anzunehmen, dass sich damit auch das Selbstverständnis der Landwirte verändern wird.

Im Zuge der Ausarbeitung einer Feinplanung für die Erstellung eines Kapitels eines Weissbuchs, zum Thema Soziale und technologische Innovationen für eine resiliente und gesellschaftlich verantwortungsvolle

[13] Hier geht es um die Qualität und Rückverfolgbarkeit der Argarprodukte (dies schliesst die Voraussetzungen für eine individualisierte Ernährung)
[14] Das Projekt DiDaT zielt auf den verantwortungsvollen Umgang mit Daten. Vor diesem Hintergrund stehen die Risiken und Vulnerabilitäten in DiDaT im Vordergrund.

Nutzung digitaler Daten in der landwirtschaftlichen Produktonskette gilt es, folgende Thesen zu diskutieren, zu überprüfen und Orientierungen für einen nachhaltigen Umgang mit den negative Auswirkungen zu erarbeiten, die mit den Thesen verknüpft sind. Die Leser mögen berücksichtigen, dass die nachfolgenden Thesen aus der Diskussion der Teilnehmenden der ersten Stakeholder-Konferenz abgeleitet wurden und sich im Prozess der Erstellung des Feinplanes unter Beiziehung einer grösseren Anzahl von Wissenschaftlern und Repräsentanten von Experten auf der Seite der Praxis verändern können/werden.

Im Anschluss an These 7 finden sich Ausführungen, welche stärker die Position landwirtschaftlicher Verbände (DLG, 2018) und des VDMA darstellen (die aus Termingründen nicht an der 1. Stakeholderkonferenz teilnehmen konnten). Es wird Aufgabe während der Erstellung des Feinplanes sein, die Thesen so zu fassen, dass sie für die Hauptphase von DiDaT und die Formulierung sozio-technologischer Innovationen umfassende Orientierung und eine gute Ausgangsposition darstellen

- **These 1 (Unseen[15] 1): Weitere ökonomische Optimierung der Betriebe zu Ungunsten ökologischer Funktionen.**

Die Auseinandersetzung mit Fragen zur Digitalisierung in der Landwirtschaft und dem Zugang zu digitalen Daten konzentriert sich auf die betriebswirtschaftlich ökonomische (und vornehmlich an der produzierten Biomasse orientierten) Optimierung einer industriellen Landwirtschaft von Gross-/Megabetrieben in Pflanzenbau und Tierproduktion. [16] Dies birgt die Gefahr (an vielen Stellen) eine mangelhafte Betrachtung ökosystemarer, kleinräumiger ökologischer Funktionen vorzunehmen und zu dem Verlust nachhaltiger kleinräumiger, die Artenvielfalt erhaltender landwirtschaftlicher Kleinbewirtschaftung beizutragen.[17] [18] Die Umsetzbarkeit von Vorschlägen des Maschinenrings kleinen und mittleren Betrieben Grundlagen für eine wirtschaftliche Nutzung digitaler Technologien zu ermöglichen (Griepentrog, Weis, Weber, & Schneider, 2019) sind hier kritisch konstruktiv zu diskutieren und zu bewerten.

[15] Die Thesen beziehen sich auf unintendierte Folgen/Wirkungen der Nutzung digitaler Daten. Das Akronym Unseens steht für «Unintended Side Effects» welches im Rahmen von DiDaT auch synonym für Vulnerabilität verwendet wird.

[16] Es gibt Hinweise darauf, dass Groß-und Megabetriebe mehr von der Digitalisierung profitieren als Kleinbetriebe (Kernecker et a. 2019, Paustian and Theuvsen, 2017). Allerdings ist dies bislang nicht empirisch untersucht.

[17] Einzelne Akteure gehen von einem Szenario aus, in dem vor allem eine zunehmende ökologische Optimierung durch den Einsatz kleiner, leichter und smarter Feldroboter für eine ökologische Landnutzung in Kleinbetrieben denkbar ist (siehe oben). Dieses Szenario stößt jedoch bei einem großen Teil der Akteure auf Skepsis. Da sich die Diskussion im Grobplan zudem vor allem um „Unseens“ und Risiken drehen soll, ist diese konträre These hier nur im Rahmen dieser Fußnote aufgeführt.

[18] Es ist im Sinne des Projekts DiDaT hier ökonomisch tragfähige, technologische, auch digitale Innovationen zu beschreiben, die zu einer verbesserten ökologischen Leistung der landwirtschaftlichen Nutzung führen.

- **These 2: Die Digitalisierung führt zu einem Verlust von Beschäftigungsmöglichkeiten in der Landwirtschaft und der Akteursvielfalt in agrarisch geprägten Räumen.**

Die mit der Digitalisierung verbundene zunehmende Rationalisierung der Landwirtschaft führt zu einer weiteren Abnahme landwirtschaftlicher Betriebe. Diese Entwicklung resultiert in einen weiteren Abbau von Beschäftigungsmöglichkeiten und einem Rückgang der Akteursvielfalt im ländlichen Raum sowie letztlich zu einem weiteren Verlust der zivilgesellschaftlichen Gestaltungskraft.[19]

- **These 3: Zunehmende Abhängigkeit der Landwirte von Agrar- bzw. „Datenkonzernen".**

Die Digitalisierung führt zur weiteren Marktkonzentration mit dem Trend zur Monopolbildung und damit stärkeren Abhängigkeit des Landwirts von Agrar- und Datenkonzernen. Der «Besitz» (d.h. die Erlaubnis mit den Daten umzugehen), der Zugang, die Nutzung und der Wert von Daten eines landwirtschaftlichen Betriebes für eine ökonomisch sozial verträgliche und ökologische Bewirtschaftung (einschliesslich der Erhebung von «Feebates» für Düngung, Pestizide, und Herbizide) kann die Souveränität des Landwirtes einschränken.

- **These 4: Wissen und Urteilsfähigkeiten des Landwirts gehen verloren. Damit steht er zunehmend in Abhängigkeit zu den großen Agrar- und Datenkonzernen.**

Durch die Digitalisierung verändert sich das Qualifikationsprofil des Landwirts. Wissen über praktische Handhabungen (beispielsweise zur Bedienung eines Pflugs) aber auch Urteilsfähigkeiten gehen verloren, wenn alle Entscheidungen abgenommen werden. Digitale Instrumente arbeiten nach bestimmten Algorithmen (vordefinierte Strukturen: basieren auf Wertemodellen durch Indikatoren, Regeln). Dies nimmt dem Landwirt und anderen Akteuren Entscheidungen aber letztlich auch Entscheidungskompetenz ab (siehe These oben). Der Landwirt wird so zum technologieabhängigen Datenmanager, der in grosser Abhängigkeit von digitalen, agrotechnischen und Lebensmittel produzierenden wirtschaftlichen Schlüsselakteuren steht. Das ursprüngliche, aber weiterhin wichtige, erfahrungsbasierte, direkt durch Interaktionen mit dem organismischen Boden-Pflanze-Tiersystem erworbene (Anwendungs-)Wissen eines (traditionellen mittel-Europäischen) Landwirts geht verloren. Der Landwirt wird zum Datenlieferant und reinen Handlungsausführenden degradiert. Die Individualität und Kreativität in der Kultur der Gedanken und Konzepte geht (aus auch unter dem Einfluss der KI) Abhängigkeit verloren.

[19] Es wurde die Frage aufgeworfen, in welcher Beziehung und Reihenfolge die einzelnen Ereignisse sich in eine Wirkungskette reihen. Insgesamt aber war die These im Stakeholder-Treffen auf breite Zustimmung gestoßen, wird jedoch durch andere Akteure auch kritisch/konträr gesehen (siehe Kommentare seitens der DLG). Es bleibt hier anzumerken, dass große sozio-technische Transformationsprozesse häufig zu unvorhersehbaren Beschäftigungseffekten in neuen Berufsfeldern geführt haben. Allerdings ist abzuwarten, ob sich diese in ländlichen oder urbanen Räumen ergeben werden bwz. in welchem Teil der Wertschöpfungskette.

- **These 5: Entscheidungsprozesse des Landwirts werden von außen manipulierbar.**

Darüber hinaus sind mit der Digitalisierung Automatisierungsprozesse verbunden, die die Entscheidungsebene des Landwirts zunehmend schwächen. Damit werden Entscheidungen in landwirtschaftlichen Betrieben manipulierbar/beeinflussbar von außen.

- **These 6: Die Wertschöpfung für den Landwirt verringert sich.**

Die Digitalisierung ermöglicht –eine sehr vollständige Rückverfolgung/Transparenz der Erträge und Mehrwertschöpfung der landwirtschaftlichen Lebensmittelkette. Dies verringert den Anteil der Wertschöpfung durch den landwirtschaftlichen Unternehmer (siehe auch Seite 1, Fussnote 1).

- **These 7: Die Digitalisierung erhöht Risiken für die „Ernährungssicherheit“.**

Digitale Systeme sind hoch komplexe Systeme, die eine hohe Fehleranfälligkeit und Instabilitäten aufweisen. Dies kann zu großen Schäden und Skaleneffekten (Gruppenentscheidung) führen. Zugleich steigt aber auch die Vulnerabilität durch Hackerangriffe, wenn wir einen Großteil der Landwirtschaft digital vernetzt haben. Dies gefährdet die „Ernährungssicherheit“ (Food Security) und damit den gesellschaftlichen Frieden und die Demokratie in hoch entwickelten Ländern. Die Digitalisierung führt zu einem steigenden Energiebedarf und zur Beschleunigung durch autokatalytische Prozesse.

Über diese sieben Thesen hinaus wurden weitere Aspekte angesprochen, jedoch nicht mehr ausreichend bezüglich ihrer Auswirkungen erörtert. Dazu gehörte die Annahme, dass die Digitalisierung einen Einfluss auf die Qualität agrarischer Produkte haben wird und möglicherweise zu einem weiteren Fokus auf Quantität statt auf Qualität führt. Zudem könnten digitale Währungen einen Einfluss auf Wertschöpfungsketten haben.

Einige Punkte, wie “Transparenz der Big Data Analyse”, “Öffentliche und behördliche Daten kostenfrei zur Verfügung stellen” (DLG, 2018), die aus der Sicht der Landwirtschaft gestellt werden, sind ggf. noch nicht hinreichend integriert. Bei der weiteren Bearbeitung dieser Thesen sollen die gegenwärtigen Diskussionen in den Landwirtschaftsverbänden mit den deutlich kritischeren Positionen der Naturschutzverbände in eine gute Beziehung gebracht werden. Dazu soll noch ein Treffen mit Vertreter*innen beider Richtungen vor der 2. DiDaT Stakeholderkonferenz stattfinden und Eingang in die Erstellung des Feinplanes geben. DiDaT konzentriert sich auf die Nutzung digitaler Daten. Es ist abzuwägen, inwieweit Aussagen “Die Digitalisierung bietet zugleich enorme Chancen für die ländlichen Räume. Es entstehen neue Möglichkeiten der Stadt-Land-Verflechtungen” in der weiteren Arbeit sinnvoll behandelt werden können

.

## 3. Auswahl Stakeholder und Wissenschaftlerinnen

Die Stakeholder-Auswahl erfolgt(e) zum einen entlang der Fragestellung, wer die zukünftige Entwicklung maßgeblich beeinflusst oder von dieser beeinflusst wird. Zum anderen richten sich die Überlegungen zur Stakeholder-Auswahl entlang der landwirtschaftlichen Produktion und Wertschöpfungskette aus. Dabei wurde vorwiegend auf die Methode des Snowball-Samplings zurückgegriffen sowie auf die Befragung von Experten(Reed et al., 2009).

Nach wie vor bleibt jedoch kritisch zu hinterfragen, inwiefern hier relevante Akteursgruppen noch nicht berücksichtigt sind.

Bislang wurden folgende Akteursgruppen als besonders relevant identifiziert:

- Landwirtschaftliche Produktionsbetriebe und entsprechende Verbände (z.B. Deutscher Bauernverband, Maschinenringe)
- Digitale Agrarberater und -dienstleiter
- Agrochemische Grossbetriebe
- Landwirtschaftsmaschinen-Hersteller
- Staatliche regulierende Akteure, Verwaltung und Kontrollorgane (z.B. BSI-Bundesamt für Sicherheit in der Informationstechnologie)
- Experten für die Strategien von Agro- (Syngenta, Monsanto) und Nahrungsmittelkonzernen (Unilever, Oetker) bezogen auf Digitalisierung
- Umweltorganisationen, Tierschutz und alternative Sichtweisen (z.B. NABU, WWF, Oxfam, CCC)
- Konsumenten-Verbände/alternative Sichtweisen (z.B. VZBV)

Die folgende Tabelle soll als Grundlage für die Diskussion zur Feinplanung in der Arbeitsgruppe genutzt werden:

**Tabelle 1. Zuordnung der identifizierten Vertreter*innen von Stakeholdergruppen zu den beschriebenen "Unseens"**

| | Stakeholder/ Unseens (gemeinsam definierte Probleme | | | |
|---|---|---|---|---|
| | Rollen | "Verursacher" | "Betroffene" | "Problemlöser"/ Regulatoren |
| | *Repräsentanten von Stakeholder-gruppen in DiDaT* | Landmaschinen-technik (VDMA)[1], Agrar/Datenkon-zerne (N.N.)[2] Hacker, | Landwirtschaftl. Betriebe (DLG/Bauernverband)[3], Umweltverbände (NABU, DBIB)[4], [5] | Maschinenring[6], Ministerien(z.B. BSI)[7], FMS[8] |
| 1 | Ökonomische Optimierung zu Ungunsten ökologischer Funktio-nen | 1,2,3 | 3,4,5 ökonomisch schwächere Beriebe (z.b. über So-LaWi), Naturschützer | |
| 2 | Beschäftigung und Akteursvielfalt im ländlichen Raum | 1,2,3 | 3 Kommunen (z.B. Ge-meinde- und Städtetag) | |
| 3 | Marktkonzentration/ Daten-rechte | 1,2 | 3 Offizialberater, Um-weltverbände | 6 |
| 4 | Verlust von Wissen und Urteilsfä-higkeit | 1,2 | 3 Bildungsträger | |
| 5 | Vollautomatisierung (Abhäng-igkeit und Manipulierbarkeit) | 1,2, | 3 Finanzdienstleister | |
| 6 | Verlust an Wertschöpfung durch hohe Transparenz | 1,2 | 3 | |
| 7 | Ernährungssicherheit | | Bundesregierung (z.B. Verbraucherschutz), Ver-band Lebensmittelindust-rie | |

## 4. Unseens x Orientierungstabelle VR04 als methodische Überlegungen zur Unterstützung von Kernaussagen

Die Reflektion zu «Unseens» bezogen auf die Digitalisierung der Landwirtschaft ist relevant aber kaum entwickelt. Es ist anzunehmen, dass sich die Situation in landschaftlich vergleichsweise homogenen, grossflächigen Nutzungsstrukturen in der norddeutschen Tiefebene anders darstellt als in landschaftlich kleingliedrigen Systemen. Auch sind die verschiedenen Zweige der Landwirtschaft zu differenzieren.

Deshalb braucht es für alle Bereiche angemessene Systemmodelle, auf deren Grundlage sich potentielle Rebounds und «Unseens» identifizieren lassen.

Die Veränderung der Produktionskette zwischen «farm and table» sind bislang wenig erforscht. Ob und – wenn ja – in welcher Weise sie einbezogen werden wird im Verlauf der Erstellung des Grobkonzeptes in einem transdisziplinären Dialog zwischen Wissenschaft und Stakeholdern bestimmt werden.

- Welche Vertiefungsforschung in der Hauptphase zu machen wäre, ist gegenwärtig ebenfalls noch offen. Es gibt hier verschiedene Möglichkeiten: Diskursive Konsultationen mit Experten/Stakeholdern zu den identifizierten Vulnerabilitäten (siehe oben aufgeführte Thesen).
- Experten-Delphi zur Wirkung von «Unseens» auf die Ertragsfunktion des Landwirtes, die Veränderung der landwirtschaftlichen Wertschöpfungskette und die Umweltqualität (ökologischen Funktionen).
- Formative Szenarienkonstruktion (mit den Experten und weiteren Beteiligten) über verschiedene Wege der Digitalisierung der Landwirtschaft und deren Wirkungen auf wirtschaftliche, ökologische und soziale Systeme; Bewertung der Szenarien mittels multi-kriterieller Bewertung durch verschiedene Stakeholder-Gruppen, um Hypothesen über Wahrnehmung und Expertenurteile zu messen
- Fallbezogenes Lernen: Betrachtung bestimmter Agrarprodukte oder Produktionsketten.

| | 1. Unseens | 2. Ursachen/ Kausalitäten/ Entstehungs-prozesse der Unseens | 3. Maßnahmen möglicher sozio-technologischer Innovationen zur Mitigation | 4. Ziele | 5. Sozial robuste Orientierungen zum Umgang mit Unseens |
|---|---|---|---|---|---|
| 1 | Ökonomische Optimierung zu Ungunsten ökologischer Funktionen | Mechanismen eines wettbewerbsorientierten Marktes<br>➔ Externalisierung von Umweltkosten<br>➔ Verhärtete Fronten/Konfliktlinien<br>➔ tbd | Informationen über die Abhängigkeit solcher Mechanismen | Entkopplungsmechanismus verstehen<br>Transparenz zu Handlungsalternativen | Community making/ building (neue Ideen) |
| 2 | Beschäftigung und Akteursvielfalt im ländlichen Raum | Rationalisierung und „fraglose“ Automatisierung<br>➔ Entkopplung Entscheidungen vom Raum<br>➔ „Ist die Kuh lila?“<br>➔ tbd | Verbindung Stadt und Land | „Lebendige“ und vielfältige Gesellschaften im ländlichen Raum | Unterstützung und Verstärkung |
| 3 | Marktkonzentration/ Datenrechte | Trend zur Monopolbildung<br>➔ Übernahme innovativer Unternehmen<br>Abhängigkeit des Landwirts von Agrar- und Datenkonzernen<br>Souveränität des Landwirtes eingeschränkt<br>➔ „Paketursache“ und Kompatibilitätsdefizite<br>➔ fehlende Auswahl (und Entscheidungsfreiheit) am Markt<br>➔ fehlendes Bewusstsein | Alternative Anbieter unterstützen<br>Sensibilität für Datenrechte erhöhen<br>Patentrecht (öffentlich finanzierte Forschung) | Offene Systeme (Daten-Allmende) | „Beipackzettel“ |
| 4 | Verlust von Wissen und Urteilsfähigkeit | Verändertes Qualifikationsprofil des Landwirts<br>➔ Entscheidungen mit Hilfe von Algorithmen (normative Prägung)<br>➔ Vollautomatisierung<br>➔ Abnahme direkte Interaktion zw. Landwirt und Umwelt<br>➔ Einfluss auf „Denkkultur“ | Bewusstsein zur Funktionsweise von Algorithmen stärken | tbd | Aus- und Weiterbildung<br>Netzwerke und Foren<br>Kommunikation und kritischer Austausch |
| 5 | Vollautomatisierung (Abhängigkeit und Manipulierbarkeit) | Vollautomatisierung<br>➔ Entscheidungsebene des Landwirts wird geschwächt<br>➔ Zunehmende Manipulierbarkeit von außen | „Entscheidungsschutz- und kontrolle“<br>Dokumentations- Bestätigungspflichten (z.B. Kontrollkästchen)<br>Bewusstsein schaffen | Transparenz, Dokumentation (Nachvollziehbarkeit) und Auswahlmöglichkeiten;<br>Kompetenzerhalt | Aus- und Weiterbildung von Landwirten<br>Beratung und Reflektion |
| 6 | Verlust an Wertschöpfung durch hohe Transparenz | Rückverfolgung und Transparenz<br>➔ Verhandlungsspielraum eingeengt | Datenschutz<br>tbd | Marktposition der Landwirte<br>tbd | Datenpolitik |
| 7 | Ernährungssicherheit | Komplexität digitaler Systeme<br>➔ Fehleranfälligkeit und Instabilität<br>➔ Skaleneffekte (Gruppenentscheidungen)<br>Hackerangriffe<br>Abnehmende Redundanzen | tbd | tbd | tbd |

## 5. Erwartete Ergebnisse und Folgeinitiativen

Für das Kapitel des Weissbuches erwarten wir eine

- Beschreibung der Vulnerabilitäten von (negativen Auswirkungen auf) sensitive(r) Stakeholdergruppen durch Digitalisierung und insbesondere digitale Daten aus der landwitschaftlichen Produktionskette,
- Eine Erklärung dieser Vulnerabilitäten durch eine Beschreibung unterliegenden (kausalen) Mechanismen
- Illustration der Vulnerabilitäten und von Strategien des Umgangs mit diesen an Beispielen
- Darlegung von Strategien (ein bis zwei Beispiele) sozialer und technologische Innovationen, mit denen diesen Vulnerabilitäten entgegnet werden kann und/oder positive Wirkungen auf die Agro-Food Chain gewonnen werden kann

**Literatur**

Deutscher Bundestag. (2019). Agrarexperten bewerten Digitalisie-rung sehr unterschiedlich. Dokumente.

DLG. (2018). Chancen. Risiken. Akzeptanz. Digitale Landwirtschafft. Eon Positionspapier der DLG. Frankfurt: DLG.

Griepentrog, H. W. (2018). In Medienwandel in Garten und Landwirtschaft (pp. 20-21). Stuttgart: Ulmer.

Griepentrog, H. W., Weis, M., Weber, H., & Schneider, W. X. (2019). Maschinenring Digital (MR digital). In M. D. M. digital) (Ed.), 39. GIL-Jahrestagung, Digitalisierung für landwirtschaftliche Betriebe in kleinstrukturierten Regionen-ein Widerspruch in sich? Bonn.

Meek, W. E. (1947). Mechanization of cotton. Proc Cotton Res Congr, 8, 20-27.

Reed, M. S., Graves, A., Dandy, N., Posthumus, H., Hubacek, K., Morris, J., . . . Stringer, L. C. (2009). Who's in and why? A typology of stakeholder analysis methods for natural resource management. Journal of Environmental Management, 90(5), 1933-1949. doi:10.1016/j.jenvman.2009.01.001

Scholz, R. W., Bartelsman, E. J., Diefenbach, S., Franke, L., Grunwald, A., Helbing, D., . . . Viale Pereira, G. (2018). Unintended side effects of the digital transition: European scientists' messages from a proposition-based expert round table. Sustainability, 10(6), 2001; https://doi.org/10.3390/su10062001.

Wallace, A. (1994). High-precision agriculture is an excellent tool for conservation of natural-resources. Communications in Soil Science and Plant Analysis, 25(1-2), 45-49. doi:10.1080/00103629409369002

DiDaT Grobplanung zum Vulnerabilitätsraum 04 (VR04)

# Appendix: Antrag zur Vertiefungsforschung

Projektskizze: Vertiefungsforschung DiDaT20 „Digitalisierung Landwirtschaft“ zur Vorlage beim BMEL

## Konsens und Dissens zur Datenhoheit von Schlüsselakteuren der landwirtschaftlichen Wertschöpfungskette („Datenhoheit“)

*Roland W. Scholz (IASS/Donau Uni Krems), Jana Zscheischler (ZALF), Reiner Brunsch (Leibniz ATB)*

### 1. Hintergrund und Zielstellung

Das Projekt DiDaT beschäftigt sich mit den ungeklärten Fragen einer verantwortungsvollen Nutzung digitaler Daten. Es zielt darauf ab, die intendierten sowie unerwünschten Nebenfolgen („Unseens“) besser zu verstehen und sichtbar zu machen, um einen nachhaltigen und „gesellschaftlich“ erwünschten Umgang mit digitalen Daten und Technologien zu ermöglichen. Der Bereich Landwirtschaft (Agrar-Ernährungskette bis zur ersten Verarbeitungsstufe) ist einer von vier Auswirkungsräumen in DiDaT (neben Mobilität, Gesundheit und KMUs), in denen Orientierungen für einen verantwortungsvollen Umgang mit digitalen Daten geschaffen werden sollen. Ziel ist es, sensible Subsysteme und Stakeholdergruppen (wie etwa bestimmte Gruppen von Landwirten) vor vermeidbaren negativen Auswirkungen zu schützen, indem ihre Anpassungsfähigkeit (wir sprechen hier technisch von „adaptiver Kapazität“) verbessert wird.

Die Frage der **Datenhoheit** stellt ein besonders kontrovers diskutiertes Thema dar. Hierzu gehören Fragen der Erhebung, der Speicherung, des Zugangs zu, der Nutzung, dem Besitz und der Sicherheit von Daten. Digitale Daten stellen ein wesentliches Wertschöpfungspotenzial dar und erlauben neue Geschäftsmodelle. Dabei werden die Rollen der Akteure entlang etablierter Wertschöpfungsketten neu definiert. Es ergibt sich die Frage: Wer darf unter welchen Bedingungen Zugriff auf welche Daten nehmen, sie wie verarbeiten und zu welchem Zweck nutzen?

Ziel der Untersuchung ist es, mittels einer **multikriteriellen Bewertung von Szenarien** zur Datenhoheit in der landwirtschaftlichen Produktionskette, die unterschiedlichen Präferenzen und Sichtweisen sowie **Konsens und Dissens zwischen verschiedenen Stakeholdergruppen** zu bestimmen. Wir greifen dazu auf eine ADN[21] genannte, bewährte Methode zurück, welche in der

[20] Informationen über DiDaT finden sich unter https://www.iass-potsdam.de/de/forschung/didat.
[21] Die Methode heißt “Area Development Negotiations”. Sie wurde im Rahmen der Transformation von Industriearealen entwickelt. Hier wurden verschiedene Entwicklungsvarianten bzw. -szenarien entwickelt und Vertreter*innen von Stakeholdergruppen vorgelegt, um darauf aufbauend den Aushandlungsprozess strukturierter und begründeter zu gestalten. Die Methode wurde rund ein Dutzend Mal in ganz verschiedenen Bereichen erfolgreich angewendet.

Erkenntnisgewinnung schriftlichen Befragungen oder (qualitativen) Interviews überlegen ist. Die Methode erlaubt es, Konsens und Dissens unter (Schlüsselakteuren von) Stakeholdergruppen zuverlässig „zu messen“. Aufbauend auf den Ergebnissen kann das Ministerium (oder das Projekt DiDaT) dann in einer Diskussionsveranstaltung (der durch die Methode eindeutig identifizierten) Hauptunterschiede (der Bewertung) diskutieren und Wege für möglichst allseitig akzeptierbare Lösungen erarbeiten.

## 2. Ein erster Aufriss zu Stakeholder, Merkmalen von Szenarien und Bewertungskriterien

An dieser Stelle erlauben wir uns einen ersten Aufriss von Stakeholdergruppen, Nutzungsvarianten, Bewertungskriterien und der Methode, die wir als sinnvoll erachten, zu skizzieren. Es ist klar, dass diese in der Arbeitsgruppe zu den Vulnerabilitätsräumen (siehe Organigramm DiDaT) weiter ausgearbeitet und modifiziert werden müssen.

**Stakeholdergruppen**: Die auf dem landwirtschaftlichen Betrieb erhobenen Daten sind nicht nur für den *Landwirt* (1) von Interesse. Die Daten dienen *Behörden* (2) für viele Zwecke des Monitorings, *Landtechnikherstellern* (3) zur Verbesserung der Produkte sowie als Verkaufsgrundlagen, aber auch für *Betriebsmittelhersteller* (4) zur Optimierung ihrer agrarchemischen Produkte. Daten sind auch als Produktinformation für den *Handel* (6) und die *Verbraucher* (6) zentral. Schließlich sind auch *Umwelt-* und *Naturschützer* (7) an vielen landwirtschaftlichen Daten interessiert.

**Nutzungsvarianten von Daten**: Unter den genannte Stakeholdergruppen gibt es unterschiedliche Vorstellungen darüber, was als (i) betriebliche landwirtschaftliche Daten zu betrachten ist, (ii) welche öffentlich sein sollen (open access), da diese teilweise (indirekt) über Steuergelder finanziert werden oder wann das Informationsrecht des Bürgers gegenüber Gefahrenquellen („the right to know Prinzip“) zur Anwendung kommt, (iii) welche Daten wie gesammelt und wie gespeichert werden müssen, damit der Landwirt im Bedarfsfall seinen Auskunftspflichten nachkommen kann, (iv) welche Sicherheitskriterien (und Speichermodi) bei welchen Daten anzuwenden sind, (v) wie landwirtschaftliche Maschinenhersteller oder Digitalunternehmen (zu Schlagdateien, Precision Farming, Flottenmanagement, etc.) Daten speichern und nutzen dürfen.

**Bewertungskriterien**: Bei der Bewertung unterschiedlicher **Szenarien der Digitalisierung** stehen naturgemäß [auch wenn wir uns auf die unerwünschten (Neben-)Folgen beziehen] folgende Aspekte im Vordergrund: (a) der Beitrag zur Wirtschaftlichkeit (und Funktionalität: Lohnen sich die Digitalisierungsinvestitionen? Wie hoch sind die Kosten für die Datengenerierung, Speicherung, etc.?), (b) die Datensicherheit (im Sinne von Verfügbarkeit; „Security“ im engeren Sinne) und (c) die Datensicherheit im Sinne von unerwünschter Nutzung (Missbrauch) durch Dritte („Safety“). Aus Nachhaltigkeitsgesichtspunkten unterscheiden

sich verschiedene Szenarien (der Datenverfügbarkeit) durch (d) unterschiedliche Transparenz hinsichtlich wirtschaftlicher und ökologischer Informationen (letzteres schließt auch das Tierwohl ein). Schließlich wäre (e) auch die Kostenverteilung der Dokumentation von Daten ein Gesichtspunkt.

**Besonderheiten von DiDaT:** Der Vulnerabilitätsraum DiDaT ist ein transdisziplinäres Projekt, bei dem auf allen Ebenen Wissenschaftler und Praktiker in gleicher Anzahl vertreten sind und sich auf gleicher Augenhöhe in einem geschützten Diskursraum begegnen[22]. Die Auswahl der Praktiker und Wissenschaftler wird so gestaltet, dass die verschiedenen Interessensperspektiven (bezogen auf den verantwortungsvollen Umgang mit Daten) und die relevanten wissenschaftlichen Gebiete vertreten sind, die es braucht, um Strategien für einen gesellschaftlich akzeptierten Modus zu entwickeln. Dies ist eine wichtige Voraussetzung, um die relevanten Stakeholdergruppen auszuwählen, eine transdisziplinäre Konstruktion von Daten sowie eine geeignete Auswahl von Bewertungskriterien vorzunehmen. Anhand der empirischen Ergebnisse wird so erkennbar, welche Stakeholdergruppen (oder Subsysteme) aus welchen Szenarien signifikante Nachteile zu erwarten haben, die zum Gegenstand von Mitigations- und anderer agrarpolitischer Maßnahmen gemacht werden sollen. Durch die gewählte Methode (Multikriterielle Bewertung verschiedener Digitalisierungsszenarien von Hauptstakeholdergruppen) werden die im Kapitel des Weißbuches von DiDaT (Erstellung Ende Juni 2020) dargelegten Orientierungen entscheidend gestützt.

## 3. Allgemeine Bemerkungen zu „Landwirtschaft und Digitalisierung“

Die landwirtschaftliche Produktion stellt eine kritische Infrastruktur dar und ist von besonderem gesellschaftlichen Interesse. Sie ist für verschiedene Akteursgruppen der Gesellschaft von Bedeutung. Es bestehen je nach Akteursgruppe unterschiedliche Interessen, wie mit der Erhebung, Nutzung und dem Zugang zu Daten in der landwirtschaftlichen Wertschöpfungskette umgegangen werden soll:

- die öffentliche Verwaltung benötigt Daten (open access), um ihren administrativen Aufgaben gerecht zu werden;
- Zivilgesellschaft und Umweltverbände fordern Open Access und „offene Datenplattformen“;
- Unternehmen des vorgelagerten Wirtschaftsbereiches benötigen Daten, um Maschinen und Produkte weiter zu optimieren und die Landwirte „bedarfsgerechter“ zu beliefern;
- die verarbeitende Industrie will möglichst viele Informationen über die Produktgenese, um spezielle Wertschöpfung betreiben zu können (z.B. gentechnikfrei, „Bio“, regional);

[22] Die Grundsätze transdisziplinärer Diskurse sind in der Broschüre zu DiDaT auf Seite 4 beschrieben.

- Landwirte selbst wollen die Datenhoheit über betriebsinterne Informationen wahren.

Aus den unterschiedlichen Interessen und Motivationen ergibt sich die Herausforderung, weiterhin eine wettbewerbsorientierte Entwicklung digitaler Systeme zu ermöglichen, aber gleichzeitig eine „gerechte“, am Allgemeinwohl orientierte Gestaltung zu gewährleisten.

Die Ergebnisse aus der vorgeschlagenen Bewertungsanalyse, um Konsens und Dissens zwischen den Akteuren zuverlässig zu untersuchen, sind daher in dreifacher Weise von Interesse:

1) Zum einen unterstützen sie das BMEL und Entscheidungsträger bei der weiteren Planung und Ausgestaltung von Instrumenten zur gezielten und planvollen Förderung der Digitalisierung in der Landwirtschaft bei Optimierung der positiven und Reduzierung gesellschaftlich unerwünschter Effekte.
2) Weiterhin sind die Ergebnisse (z.B. über Kenntnisse der verschiedenen Präferenzen) von zentraler Bedeutung für die strukturierte und fundierte Fortführung und Gestaltung des transdisziplinären Prozesses in DiDaT unter Beteiligung der relevanten Stakeholder-Gruppen im Landwirtschaftsbereich bzw. der Nahrungserzeugungskette.
3) Zudem sollen aus den Ergebnissen der Untersuchung allgemeine Thesen abgeleitet werden, die für die Diskussion zum Thema Datenhoheit, Datensicherheit und Datensouveränität, Design digitaler Systeme sowie Datenzugang auch in anderen Bereichen (wie z.B. Umgang mit medizinischen Daten, persönlichen Daten) relevant sind. Somit besitzt das vorgeschlagene Projekt auch für die Grundlagenforschung zur Digitalisierung eine Bedeutung.

## 4. Methode und Vorgehensweise

Aufbauend auf dem transdisziplinären Dialogprozess in DiDaT verfolgt die Vertiefungsstudie den Ansatz der formativen Szenarien-Analyse (FSA) und multikriteriellen Bewertung (MCA, multi-criteria assessment). Folgende Schritte sind methodisch zu unterscheiden:

1) Identifikation relevanter Schlüsselakteure durch die Mitglieder der Arbeitsgruppe und durch eine begleitende Expertenbefragung, einschließlich der interessierten BMEL-Mitarbeiter;
2) Konstruktion und Formulierung von Szenarien mit den Mitgliedern der Arbeitsgruppe des Vulnerabilitätsraumes und ausgewählten Akteuren;
3) Bestimmung geeigneter Kriterien zur Bewertung der Szenarien hinsichtlich bestehender Konflikträume (Konsens und Dissens) zwischen verschiedenen Stakeholder-Gruppen; Auswahl von mindestens sechs Vertretern für maximal sechs Stakeholder Gruppen;
4) Qualitativ-quantitative Befragung und Auswertung.

Es sollen Sichtweisen unterschiedlicher Stakeholdergruppen (z.B. öffentliche Verwaltung, Landwirte, Landtechnik, NGOs) entlang der Wertschöpfungskette zur Digitalisierung in der Landwirtschaft und Lebensmittelverarbeitung berücksichtigt werden. Dabei werden sechs bis zehn Interviews/Befragungen je identifizierter Stakeholdergruppe bei einer Auswahl von maximal sechs Gruppen angestrebt.

## 5. Zeitplan und Budget

Falls von Seiten des BMELs Interesse an dem Vorhaben besteht und es erwünscht sein sollte, erstellen wir gerne eine detailliertere Zeit- und Budgetplanung. Nachstehend eine chronologische Übersicht mit Darstellung der Arbeitspakete und zeitlichen Planung:

| | Personenmonate (VZÄ) / Arbeitsschritte | 1 | 2 | 3 | 4 | 5 | 6 | Stunden |
|---|---|---|---|---|---|---|---|---|
| 1 | Einarbeitung d. Mitarbeiters in Methodik | | | | | | | 120 |
| 2 | Td Szenarienkonstruktion, Auswahl Bewertungskriterien, Erstellung des Befragungsdesigns | | | | | | | 200 |
| 3 | Auswahl Schlüsselakteure und Durchführung der Expertenbefragung (ca. 40 Befragungen) | | | | | | | 200 |
| 4 | Statistische Analyse und ggf. Nacherhebung | | | | | | | 140 |
| 5 | Ergebnisdarstellung (Abschlussbericht und Skizze Veröffentlichung) | | | | | | | 150 |
| | | | | | | | | 810 |

Basierend auf den dargestellten Inhalten ergibt sich folgende Kostenkalkulation (ohne Overheads und Mehrwertsteuer; letztere sollte nicht erhoben werden, da das Projekt zu einem wesentlichen Teil der Forschung und Methodenentwicklung dient):

| | | |
|---|---|---|
| 36.000 | Euro | Personalausgaben |
| 3.000 | Euro | Dienstreisen (Reisen zur Datenhebung) |
| 3.000 | Euro | Verbrauchsmaterial (incl. Bücher und Software) |
| 3.000 | Euro | Beratung und Mitarbeit von Prof. Scholz |
| 45.000 | Euro | Gesamtausgaben (ohne Overheads und Mehrwertsteuer) |

**Erläuterung**:
Für die Durchführung des Vorhabens werden vom Antragsteller eine 80 % wissenschaftliche Mitarbeiterstelle (TVL 13) über einen Zeitraum von 8 Monaten beantragt. Der Mitarbeiter führt die im Arbeitsplan aufgeführten Tätigkeiten federführend durch und soll am ZALF im Zeitraum von 1/2020-8/2020 eingestellt sein.

Weiterhin sind 2.000 Euro für Dienstreisen vorgesehen zur Durchführung der Befragung. Die Erhebung wird optional online oder per Desktop mit Instruktion angeboten.

Prof. Dr. em. Roland W. Scholz ist Leiter von DiDaT. Für seine fortlaufende Betreuung bei der Szenarioerstellung, Datenanalyse und Berichterstattung wird ein Honorar gezahlt. Prof. Scholz fungiert als Ko-Antragsteller (IASS/DUK) ohne finanzielle Zuwendungsberechtigung außer der Honorarnote.

Die Auswertung und Analyse wird durch das TD-Method Lab (Softwareprogramm) unterstützt.

# Vulnerabilitätsraum 05 (VR05)

# Soziale Medien, digitale Daten und ihre Auswirkungen auf den einzelnen Menschen

# Soziale Medien, digitale Daten und ihre Auswirkungen auf den einzelnen Menschen

19.Jan.2020 RH

Felix Ebner (mecodia), Hanna Gleiss (Das NETTZ/BETTERPLACE LAB), Christian Montag (Universität Ulm), Lisa-Maria Neudert (Oxford University/GB), Roland W. Scholz (Donau Universität Krems/OE), Leena Simon (Frieda FrauenZ. – Anti-Stalking-Projekt), Cornelia Sindermann (Universität Ulm), Benjamin Thull (LfK Stuttgart)

Inputs durch Dirk Helbing (ETH Zürich), Michael Latzer (Universität Zürich), Hanns-Jörg Sippel (Stiftung Mitarbeit)

## 1. Gegenstand, Ziele und Leitfragen

### 1.1 Gegenstand: Was verstehen wir unter sozialen Medien?

Soziale Medien (aus dem Englischen: Social Media) werden allgemein wie folgt definiert: Soziale Medien sind Internet-basierte Kanäle und Plattformen, die Nutzer*innen erlauben bedarfsbezogen zu interagieren, sich selektiv selbst zu präsentieren und user-generierte Inhalte zu erstellen. Dies kann entweder in Echtzeit oder asynchron sowohl mit großen (Internet-)Gruppen, als auch kleinen (Internet-)Gruppen oder Individuen geschehen. Sie erhalten einen Wert durch die von Nutzer*innen vermittelten Inhalte und die Wahrnehmung der Interaktion mit anderen (Erweiterte Definition in Anlehnung an Carr & Hayes (2015, p. 50) und Howard & Parks (2012)).

Soziale Medien bestehen

a) aus der (digitalen) Informations-infrastruktur und den Werkzeugen, die für die Erzeugung und Verteilung von Inhalten genutzt werden,
b) aus den vermittelten Inhalten, die in digitaler Form persönliche Nachrichten, Botschaften, Ideen und kulturelle Produkte darstellen,
c) aus den Personen, Organisationen und wirtschaftlichen sowie politischen Akteuren, die digitale Inhalte produzieren oder aufnehmen / verarbeiten (abgeändert und erweitert durch politische Akteure von Howard & Parks (2012, p. 362)).

**Tabelle 1: Abgrenzung sozialer Medien an Beispielen (aus Carr & Hayes, 2015, S. 53)**

| *Social Medium* | *Not a Social Medium* |
|---|---|
| • Social network sites (e.g., Facebook, QQ, Google+, YouTube, Yelp, Pheed) | • Online news services (e.g., *NYT* online, PerezHilton.com) |
| • Professional network sites (e.g., LinkedIn, IBM's Beehive) | • Wikipedia |
| • Chatboards & discussion fora | • Skype |
| • Social/Casual games (e.g., Farmville) | • Netflix |
| • Wiki "Talk" pages | • E-mail |
| • Tinder | • Online news |
| • Instagram | • SMS/Texts |
| • Wanelo | • Oovoo |
| • Yik Yak | • Tumblr |
| | • Whisper |

## 1.2 Ziele und Leitfragen

Soziale Medien und Messenger-Applikationen sind für viele Menschen unmittelbar mit ihrem Alltag verknüpft und haben in kurzer Zeit großen Einfluss auf Wirtschaft, Staat, Gesellschaft und das Leben des einzelnen Menschen genommen. Am Beispiel des Konzerns Facebook lässt sich die enorme Entwicklungsgeschwindigkeit gut illustrieren: Facebook wurde erst im Jahr 2004 gegründet und zählt im März 2019 in etwa 2,3 Milliarden Nutzer*innen. Zum Unternehmen gehören auch andere wichtige App-Services wie der Facebook-Messenger, die Plattform Instagram oder der Messenger-Dienst WhatsApp. Zusammen haben die drei Hauptprodukte 2,7 Milliarden angemeldete Nutzer*innen, wovon 2,1 Milliarden jeden Tag in einem der Dienste aktiv sind.[23] Dadurch zeigt sich die relative Monopolstellung von Facebook, jedoch auch die große Beliebtheit und Relevanz von sozialen Medien in der täglichen, aktiven Mediennutzung, insbesondere im Bereich der Kommunikation.

Soziale Medien stellen entwicklungsgeschichtlich eine neue Form menschlicher Interaktion und Informationsvermittlung dar. Nutzer*innen können als passive und aktive Größe und Gestalter*innen wirken. Es werden verschiedene Formate durch die digitale Infrastruktur vorgegeben, welche zudem die gesamten Aktionen und Operationen steuern, überwachen und beeinflussen können.

Wie bereits erwähnt, beweist die hohe Nutzungsrate die große Beliebtheit von sozialen Medien. Die sozialen Medien haben in verschiedenen Bereichen aber auch „unerwünschte" Auswirkungen (unerwünschte (Neben-) Folgen bzw. *Unintended Side Effects* (= *Unseens)*.

Dazu gehören die Förderung der (Über-)Nutzung bis hin zur Sucht, die Enthemmung sozialen Verhaltens sowie die Erzeugung von verzerrten Realitäten. Daraus folgen unter anderem Prozesse der politischen Beeinflussung und Manipulation der Meinungsbildung.

Ein Grund für eine Vielzahl an *Unintended Side Effects* ist sicherlich das Monetarisierungs-Modell sozialer Medien: Nutzer bezahlen für die Teilnahme an sozialen Medien nicht mit tatsächlichem Geld, sondern mit ihrer Aufmerksamkeit und Daten, die monetarisiert werden. Die Daten können verwendet werden, um beispielsweise auf das Individuum angepasste Werbung zu gestalten (sowohl kommerziell, als auch politisch) (Gosh & Scott, 2018).

Ausgehend von den folgenden Leitfragen soll der Vulnerabilitätsraum „*Soziale Medien, digitale Daten und ihre Auswirkungen auf den einzelnen Menschen*" die Auswirkungen auf das (psychische) *Wohlbefinden* und die *Gesundheit* sowie die *Demokratiefähigkeit* der einzelnen Person betrachten und analysieren. Dazu werden verschiedene wissenschaftliche Ausrichtungen und Ansichten vertreten sein: Psychologie, Politikwissenschaft, Wirtschaftsinformatik und Philosophie. Darauf aufbauend sollen (sozial robuste) Orientierungen zur Entwicklung von Bewusstsein geschaffen werden, die dem Individuum helfen. Zudem sollen die Orientierungen helfen, soziotechnische Innovationen zu entwerfen. Die Orientierungen sollen auch bezüglich gesetzlicher und gesellschaftlicher Regelungen

[23] https://allfacebook.de/toll/state-of-facebook

gegeben werden und es sollen Vorschläge zur Kooperation von Nutzer*innen und gesellschaftlichen Akteuren mit den Betreibern von sozialen Medien zur Findung von neuen Regelungen einer *private-public partnership* umrissen werden.

Vor diesem Hintergrund formulieren wir die folgende

## Fragestellung und Leitfragen:

1. Welche „unerwünschten" Auswirkungen entstehen durch die neuartige Nutzung digitaler Daten in den Bereichen:
   Wohlbefinden /Gesundheit, Sozialverhalten und Demokratiefähigkeit auf Ebene des Individuums?
2. Welche Lernprozesse, Verhaltensänderungen, Regularien und (soziotechnischen) Innovationen für die Nutzung sozialer Medien und die dadurch entstehenden Daten können helfen, diese „unerwünschten" Auswirkungen durch das Handeln der Stakeholder zu mindern bzw. zu beseitigen?

## 2. Welche nicht intendierten, unbeabsichtigten und „unerwünschten" Auswirkungen sind bezüglich (psychischem) Wohlbefinden und Gesundheit sowie Demokratiefähigkeit von Interesse und warum?

Das Individuum steht im Fokus der Arbeit des Vulnerabilitätsraums. Somit werden die Auswirkungen von sozialen Medien auf das Individuum betrachtet.
Bezogen auf die Demokratiefähigkeit wird folgende Systemeingrenzung vorgenommen: Den Schwerpunkt der Arbeiten stellen Eigenschaften und Voraussetzungen dar, die eine einzelne Person für ein Funktionieren einer demokratischen Gesellschaft (Befähigung zu einer kompetenten, kundigen Wahl, Fähigkeit und Bereitschaft der Mitwirkung) besitzen sollte.[24]
Der Abschnitt „(Psychisches) Wohlbefinden und Gesundheit" stellt in kompakter Form die Mechanismen dar, die die *Übernutzung von sozialen Medien* bedingen, die *sozialen Beziehungen* beeinflussen und *Enthemmungen* fördern und somit Auswirkungen auf das *(psychische) Wohlbefinden* und die *Gesundheit* haben können. Dabei spielen auch die Auswirkungen von gefälschten / manipulierten Informationen auf die Kommunikation und Interaktion eine Rolle. Zudem ist wichtig zu beachten, dass digitale soziale Medien neue Rahmenbedingungen für soziale Interaktionen darstellen. Dies ist sowohl mit erwünschten als auch „unerwünschten" Effekten (auch mit Hinblick auf sensible und schützenswerte Gruppen) assoziiert. Gemäß des Ziels des Projekts werden vor allem „unerwünschte" Effekte betrachtet.
Der Abschnitt „Soziale Medien und Demokratiefähigkeit" betrachtet die Demokratiefähigkeit des/der Einzelnen. Der Einstieg in dieses Thema erfolgt über eine Diskussion philosophischer und politischer Grundannahmen und Konzepte zu Fähigkeiten eines demokratiefähigen (mündigen) Bürgers. Die zentralen kritischen Größen sind hier im Zusammenhang mit sozialen Medien Prozesse des „*Reality-Shifts*", Manipulation von Daten und un-/bewusste Meinungsbeeinflussung (Irreführung)

[24] Somit stellen die Wirkungen Einzelner *auf* soziale Medien auch im Rahmen der Demokratiefähigkeit keinen Schwerpunkt des Vulnerabilitätsraums dar. Hier beziehen sich die Analysen *nicht* auf evtl. induzierte Varianten von Demokratiemodellen, welche sich aus den Verhaltensmustern der Einzelnen und ihrer Interaktion ergeben. Gleichermaßen nicht im Mittelpunkt stehen die spezifischen gesellschaftlichen Prozesse, Institutionen, demokratischen Abläufe sowie die verschiedenen Formen der Demokratie (z.B. direkte / Basis- Demokratie vs. repräsentative Demokratie). Bezogen auf die Demokratiefähigkeit werden Anforderungen, welche durch die neue Form der E-Democracy erwachsen, nur betrachtet, wenn sie sich von den traditionellen Formen der Demokratie (etwa durch neue „Sprachformen oder Sprachformate" in sozialen Medien wesentlich unterscheiden.

im politischen und kommerziellen (Konsumenten-verhaltens-) Bereich.[25]

## Werteperspektiven

### WERTE-PERSPEKTIVE (I): (Psychisches) Wohlbefinden und Gesundheit

*„Facebook deactivation [...] increased subjective well-being; and [...] caused a large persistent reduction in Facebook use after the experiment.“*
(Allcott, Luca Braghieri, Sarah Eichmeyer, and Matthew Gentzkow, 2019)[26]

#### Übernutzung / Overuse

Die problematische Nutzung von sozialen Medien kann im ungünstigsten Fall zu einer Übernutzung (breiter auch: „***Internet communication disorder***“) führen. Diese wird auch als eine Form der *Internetsucht* („***Internet-use disorder***“) begriffen. Auch wenn noch keine offizielle Diagnose einer Übernutzung von sozialen Medien in den Diagnosehandbüchern vorhanden ist, gibt es bereits einige Literatur zu entsprechenden Symptomen. Dazu zählt unter anderem der Kontrollverlust der Nutzung trotz negativer Konsequenzen auf das soziale Umfeld sowie die schulische oder berufliche Leistung. Es ist zudem davon auszugehen, dass die Übernutzung von sozialen Medien mit niedrigerer Lebenszufriedenheit, höherer (Wahrscheinlichkeit der Entwicklung einer) Depressionssymptomatik sowie höherer Isolierung zur Offlinewelt einhergeht.

In Bezug auf die Übernutzung von sozialen Medien stellt sich unter anderem die Frage, ob es bestimmte persönliche Voraussetzungen gibt, welche das Entstehen dieser begünstigen oder reduzieren, eventuell sogar verhindern, können. Hierzu gibt es bereits einige Forschung, die zeigt, dass sowohl Persönlichkeitsvariablen (was bedeuten könnte, dass es hier sensible Gruppen gibt), als auch affektive Reaktionen, kognitive Prozesse und exekutive Funktionen eine wichtige Rolle für das Verständnis einer Übernutzung von sozialen Medien spielen (Brand, Young, Laier, Wölfling, & Potenza, 2016). Wie erwähnt, sind für diesen Vulnerabilitätsraum aber vor allem die Auswirkungen von sozialen Medien auf das Individuum von Bedeutung. Dementsprechend müssen neben personenbezogenen Variablen vor allem auch ***Umweltvariablen*** zur Erklärung der Entstehung einer Übernutzung von sozialen Medien betrachtet werden.
Bei der Nutzung von sozialen Medien werden die Nutzer*innen einer Reihe von Mechanismen ausgesetzt, welche eine verstärkte Nutzung auslösen können. Diese Mechanismen können zudem mittels künstlicher Intelligenz (d.h., Algorithmen, welche persönlichkeitseigene Geneigtheiten analysieren) verstärkt werden. Wichtige Mechanismen werden in Box 1 beschrieben:

**Box 1: Mechanismen zur Verstärkung der (Über-)Nutzung sozialer Medien**
Hierzu können nicht nur Erfahrungen des Individuums und das soziale Umfeld, sondern auch die Beschaffenheit von sozialen Medien gezählt werden. So gibt es diverse Mechanismen, die Nutzer*innen zur immer weiteren Nutzung treiben oder sie an die Plattform binden sollen. Einige Expert*innen warnen davor, dass auf sozialen Medien dabei dieselben Mechanismen verwendet werden, wie von der Glücksspielindustrie. Solche Mechanismen beinhalten den „***Like-Button***“ auf Facebook oder das „***Herz***“ auf Instagram, die Nutzer*innen bei Erhalt durch Andere kurzfristig ein positives Gefühl der Wertschätzung geben sollen. Zudem gibt es Mechanismen wie „***Pull-to-Refresh***“. Dabei erscheinen durch „Herunterziehen“ bzw. Aktualisieren des Startbildschirms von sozialen Medien häufig (aber nicht immer) neue Inhalte wie Nachrichten und Informationen (bspw. auch über Freunde und Bekannte). Dadurch soll die ***Gier nach Neuigkeiten*** befriedigt werden. Gleiches gilt für den „***Infinite Scrolling***“ -Mechanismus, bei dem permanent neuer Inhalt beim Scrollen durch soziale Medien geladen und aufgezeigt wird. Darüber hinaus gibt es die so genannten „***Push-Nachrichten***“, die Nutzer*innen Nachrichten auf das Smartphone senden, die sie zum Öffnen der sozialen Medien Plattform aktivieren sollen, auch wenn die Plattform gerade nicht geöffnet ist. Die „***Pull-to-Refresh***“ -Funktion wurde dabei bereits mit der Funktionsweise eines Glücksspielautomaten verglichen: Der/die Nutzer*in bedient einen Hebel bzw. aktualisiert die Startseite von sozialen Medien und erhält entweder eine direkte Belohnung (Geld bzw. neue Inhalte) oder nicht. Da die Nutzer*innen nicht wissen, ob und wann sie belohnt werden, entsteht eine Erwartungshaltung einhergehend mit Ungewissheit, genau wie bei Glücksspielautomaten. Und diese Erwartung gepaart mit potenziellen ungewissen Belohnungen („***Uncertain Rewards***“) halten Nutzer*innen auf den sozialen Medien.

[25] Gefälschte Daten und Reality Shift sind auch Gegenstand des VR06 „Vertrauenswürdige und zuverlässige digitale Daten und Informationen“. Hier wird jedoch das gesamte Internet und nicht nur soziale Medien betrachtet.

[26] https://web.stanford.edu/~gentzkow/research/facebook.pdf

Insgesamt zielen die meisten dieser Mechanismen darauf ab, Nutzer*innen durch die Nutzung kurzfristig ein positives Gefühl – eine Art ***Belohnung*** – empfinden zu lassen und die Nutzung so zu verstärken. Zur Entwicklung einer Übernutzung kommt es dann beispielsweise, wenn ein Trigger eingesetzt wird (bspw. ***„Push-Nachricht“***, die einen darüber informiert, dass auf der Plattform etwas Neues passiert ist), auf den eine Reaktion folgt (Öffnen der Plattform, um zu sehen was es Neues gibt), die dann (häufig) belohnt wird (es werden tatsächlich neue Inhalte präsentiert). Wird dies wiederholt, entstehen Zyklen, wodurch Gewohnheiten geformt werden. Nach einer gewissen Zeit werden die externen Trigger (bspw. ***„Push-Nachrichten“***) nicht mehr benötigt, um die sozialen Medien zu besuchen. Das ist dadurch bedingt, dass sich mit der Wiederholung der oben genannten Zyklen Assoziationen zwischen der Nutzung von sozialen Medien und der Befriedigung von Bedürfnissen bilden (z.B. Bedürfnisse nach Neuigkeiten / emotionale Bedürfnisse). Die IT Industrie hat die Designs von sozialen Medien also wohl gezielt an der Spieleindustrie (z.B. Las Vegas) orientiert, um den maximalen Kick, die maximale Suchtwirkung zu erzielen, damit Nutzer*innen möglichst viel Zeit auf den Plattformen verbringen. Dadurch sollen die gesammelten Daten über die Nutzer*innen und somit die Einnahmen der Betreiber maximiert werden. Daher scheint ein direkter Zusammenhang zwischen der Übernutzung von sozialen Medien und der Sammlung von digitalen Daten durch Betreiber von sozialen Medien zu bestehen. Mit künstlicher Intelligenz kann die Funktionsweise an die Individuen angepasst werden, um die Wirksamkeit weiter zu erhöhen.

Selbstverständlich ergibt sich erst in der Kombination persönlicher Eigenschaften und Umweltfaktoren eine hinreichend vollständige Sicht auf die problematische Nutzung von sozialen Medien. Wichtig ist zudem, dass die Übernutzung nicht nur direkte Effekte auf das Wohlbefinden und die Gesundheit eines Individuums hat, sondern auch auf dessen Leistungsfähigkeit bspw. am Arbeitsplatz. Insgesamt stellt es sich also als wichtig dar, die verschiedenen Faktoren zu erarbeiten. Darauf aufbauend können dann Maßnahmen auf verschiedenen Ebenen – wie der Wirtschaft, der Politik, der Gesellschaft, aber auch des Individuums – getroffen werden.

**Wirkungen von sozialen Medien auf Sozialverhalten und Wohlbefinden / Gesundheit Einzelner**

Soziale Kommunikation und Interaktion findet zunehmend digital, ohne direkten Kontakt statt. Das wird auch ***„Disembodied Communication“*** genannt. Dies führt zu veränderten Rahmenbedingungen und somit einer veränderten physischen Umwelterfahrung (Büchi, Festic, & Latzer, 2018) sowie zu positiven (Boulianne, 2015) und negativen Effekten (Brooks, 2015) auf das Wohlbefinden einzelner Individuen.
Eine wichtige Neuerung im Umfeld der sozialen Medien im Vergleich zur analogen („offline“) Kommunikation stellt die eingeschränkte Bereitstellung privater, personenbezogener Daten für andere Nutzer*innen dar. Aus der so entstehenden Anonymität von Nutzer*innen entsteht ein Konflikt zwischen Anonymität versus Verantwortung im sozialen Umgang. Durch die gesteigerte Anonymität, aber auch durch die räumliche Distanz zu anderen Nutzer*innen können antisoziale Verhaltensweisen verstärkt werden, die schon aus der Offlinewelt bekannt sind. Diese sollen zusammen mit ihren Auswirkungen auf einzelne Personen im Folgenden erörtert werden. Wie bei der Übernutzung gibt es hier eine größere Anzahl von psychologischen Mechanismen, die es erlauben Nutzer*innen in ihrem Selbstbild zu beeinflussen, sie zu beleidigen, deprivieren, verletzen, mobben, in verschiedener Art unter Druck zu setzen oder zu entwürdigen. Wichtige Mechanismen werden in Box 2 beschrieben.

**Box 2: Mechanismen zur sozialen Deprivation und Verletzung**
Sozialer Druck („***Social Pressure***“) bezieht sich auf zahlreiche Phänomene, die im Internet, im Speziellen in sozialen Medien, von Bedeutung sind. Es muss unter anderem im Kontext von sozialen ***Vergleichsprozessen*** betrachtet werden, die zu negativem Affekt führen können (sozialer Druck kann aber auch für die Übernutzung von Bedeutung sein: Wenn das soziale Umfeld ausschließlich über soziale Medien kommuniziert, wird auch der/die Einzelne dazu gezwungen). Beispielsweise werden junge Menschen über sozialen Medien ständig mit dem Schönheitsbild von sehr schlanken und sportlichen Models konfrontiert. In Bezug darauf stellen sich gerade die häufig bearbeiteten Fotografien von solchen Models auf beispielsweise Instagram als problematisch dar. Dies kann als manipulierte Darstellung von Daten angesehen werden. Diese fehlerhafte Darstellung des Körpers und die fehlgeleitete Einschätzung der Nutzer*innen, diese Fotografien wären echt (unbearbeitet) und ein Abbild von normalen Personen können weitreichende unerwünschte Auswirkungen für Individuen haben. Dies ist vor allem bei dem Vorliegen einer wahrgenommenen Diskrepanz der Fall; wenn also der Ist-Zustand (Körper des/der Nutzer*in) nicht dem Soll-Zustand (bearbeitete Fotografie des Models) entspricht. Diese wahrgenommene Diskrepanz kann einen negativen Einfluss auf das Selbstbild, das Selbstbewusstsein und Emotionen sowie Affekt (bis hin zur Depression) haben und Neid hervorrufen (Appel, Gerlach, & Crusius, 2016). Es ist zu erwarten, dass diese Diskrepanz letztendlich auch zu Essstörungen oder einer Art Fitness- / Sportsucht führen kann, um dem Ideal aus dem Internet näher zu kommen. Auch sonst

wird auf sozialen Medien auf Perfektion gesetzt: Nutzer*innen werden täglich mit perfekten Wohnungen, perfekten und häufigen Reisen, oder einem idealisierten Lebensstil von Online-Persönlichkeiten (oder auch „Influencern") konfrontiert. Die perfekten Darstellungen sind auch in Verbindung mit dem Begriff „Highlight-Reels" bekannt. Wie bereits erwähnt, kann auch hier die fehlerhafte Darstellung und Einschätzung zu negativen Konsequenzen für den/die Nutzer*in führen. Moderatoren, die diese Wenn-Dann-Beziehung erklären (auf individueller, sowie systembezogener Ebene) sind bisher nur wenig erforscht. Abschließend soll hier noch einmal erwähnt sein, dass es soziale Vergleichsprozesse auch in der Offlinewelt gibt. Soziale Medien bieten jedoch Zugriff auf weit mehr Inhalte und konfrontieren die Nutzer*innen so vermehrt mit irrealen Darstellungen. Dies ist nicht zuletzt auch dadurch zu begründen, dass es durch die heutige Technik einfach gemacht wird, manipulierte Bilder, Darstellungen, etc. auf sozialen Medien zu präsentieren. Zudem erleichtern die Anonymität und Distanz zwischen Nutzer*innen die Manipulation von Darstellungen und erhöhen die Glaubwürdigkeit, da entgegengesetzte Informationen nicht präsentiert werden. Daher muss ein Bewusstsein für diese Mechanismen geschaffen werden, um wirksame Gegenmaßnahmen und Umgangsweisen zu erarbeiten.
Neben solchen Vergleichsprozessen und deren Folgen, ergeben sich auf sozialen Medien weitere unerwünschte Konsequenzen hinsichtlich sozialen Drucks durch beispielsweise „***Online-Trolling***", „***Hate-Speech***" und „***Cyber-Mobbing***"[27]. Jede dieser Verhaltensweisen soll zu einer Herabsetzung mindestens einer Person führen. Finden sich in sozialen Medien vermehrt ***menschenverachtende Äußerungen***, kann dies in einer Spirale aus sich verstärkenden Hassbotschaften münden und dadurch ein Klima entstehen, in dem Diskriminierung und Gewalt legitim erscheinen. Wichtig ist, dass diese Verhaltensweisen im Internet und sozialen Medien, unter anderem aufgrund der Anonymität und der räumlichen Distanz (dem Opfer nicht in die Augen sehen zu müssen), noch wesentlich schlimmer ausfallen, als in der Offlinewelt. Ein Effekt, der auch „***Online-Enthemmungseffekt***" genannt wird. Einige Opfer von beispielsweise Cyber-Mobbing berichten unter anderem über höhere soziale Angst, Traurigkeit, Wut, Minderwertigkeitsgefühle, Depressivität bis hin zu suizidalen Gedanken (Diefenbach & Ullrich, 2016). Auch das so genannte „***Doxxing***" (engl.: dox, Abkürzung für documents), bei dem persönliche Daten in bösartiger Absicht ins Netz gestellt werden, stellt nicht nur einen Eingriff in die Privatsphäre dar, sondern wird häufig genutzt, um eine Person bloßzustellen und häufig weiteren Angriffen auch in der Offlinewelt auszusetzen. Auch Phänomene wie „***Cyberstalking***", ***ungewünschte Kontaktaufnahmen***, „***Revenge-Porn***", „***Upskirting***" (engl. unter den Rock blicken, z.B. Fotos aus Intimbereichen) und viele weitere können Grundlage negativer Emotionen und im Allgemeinen unerwünschter Konsequenzen für Nutzer*innen sein. Insgesamt lassen sich diese Phänomene unter dem Überbegriff „***Digitale Gewalt***" zusammenfassen.
Wie bereits erwähnt, vereinfachen soziale Medien aufgrund ihrer Beschaffenheit diese Formen der Gewalt gegenüber der Offlinewelt, unter anderem aufgrund der Anonymität. Allerdings handelt es sich bei den grundlegenden Phänomenen nicht um ausschließlich online zu erfahrende Phänomene. Da die so entstehenden Daten (bsp. Hass-Texte) im Internet zudem nur schwer gelöscht werden können („Das Internet vergisst nicht"), ergeben sich häufig, auch noch lange nach den eigentlichen Angriffen andauernde, Probleme für die Opfer solcher Attacken. Deshalb ist es von höchster Bedeutung, die Mechanismen, die zu „Digitaler Gewalt" führen zu untersuchen, zu verstehen und darauf aufbauend Umgangs- und Lösungswege zu erarbeiten.
Zuletzt beschreibt das Phänomen „***Normalisation of the Weirdo***" die Möglichkeit, über soziale Medien sehr einfach Bekanntschaften zu zahlreichen (auch räumlich entfernten) Personen zu schließen, die die gleichen Interessen haben (zusätzlich besteht ein Zusammenhang mit den weiter unten eingeführten ***„Echokammern" / „Filterblasen")***. So finden sich auch Personen mit seltenen, seltsamen oder sogar schädlichen Interessen in einer Interessensgemeinschaft. Das Vorhandensein einer solchen Gemeinschaft führt zu der Wahrnehmung, das eigentlich schädliche Interesse sei normal. Dies kann wiederum zu einer Verstärkung schädlicher Interessen führen (siehe soziale Gruppen wie „Pro Ana", die sich positiv über Anorexie äußern).

Zusammenfassend lässt sich sagen, dass die sozialen Gruppen, die sich auf sozialen Medien formieren, immense Macht haben. Sie können Nutzer*innen positiv beeinflussen (zum Beispiel durch soziale Unterstützung), aber auch negativ. So zeigt sich, dass gerade das Gefühl der Zugehörigkeit wichtig ist, um positive Konsequenzen der Nutzung sozialer Medien hervorzurufen.
Neben den bisher eher negativen Aspekten und Folgen auf das Wohlbefinden einzelner Personen, bieten sich zudem auch mehrere Perspektiven an, aus welchen Maßnahmen zur Verbesserung des Wohlbefindens angestoßen werden können. Unter

[27] Online-Trolling: „Trolling beschreibt ein destruktives, unsachliches und aggressives Kommunikationsverhalten. Trolls – das sind die Akteure – möchten provozieren, Konflikte innerhalb einer Community schüren oder durch falsche Informationen Diskussionen im Web manipulieren."
(https://www.klicksafe.de/themen/medienethik/verletzendes-online-verhalten/online-gewalt-ist-reale-gewalt/#s|Trolling).
Hate-Speech: Wenn Menschen abgewertet oder angegriffen werden, oder wenn gegen sie zu Hass oder Gewalt aufgerufen wird (https://www.bpb.de/252396/was-ist-hate-speech).
Cyber-Mobbing: „Unter Cyber-Mobbing (Synonym zu Cyber-Bullying) versteht man das absichtliche Beleidigen, Bedrohen, Bloßstellen oder Belästigen anderer mithilfe von Internet- und Mobiltelefondiensten über einen längeren Zeitraum hinweg." (https://www.klicksafe.de/themen/kommunizieren/cyber-mobbing/cyber-mobbing-was-ist-das/).

anderem die gesellschaftliche Perspektive, wobei die Frage gestellt werden muss, was Entscheidungsträger aus Politik und Wirtschaft diesbezüglich unternehmen können, wie zum Beispiel um Cyber-Mobbing zu verhindern. Des Weiteren bietet sich in der individuellen Perspektive an, darüber nachzudenken, was ein jede einzelne Person tun kann, um im digitalen Zeitalter sein eigenes Wohlbefinden und Gesundheit zu erhalten. Mögliches Themengebiet kann hier zum Beispiel sein, wie eine Struktur im digitalen Alltag geschaffen werden kann, um Zeiten auf sozialen Medien zu regulieren, um beispielsweise ausreichend Schlaf zu finden und ungestörte Arbeitszeiten (siehe auch Punkt „Übernutzung / Overuse“) zu generieren.

## WERTE-PERSPEKTIVE (II): Soziale Medien und Demokratiefähigkeit

### Demokratierelevante Aspekte aus der Sicht einzelner Bürger*innen

Unter Demokratie verstehen wir ein Regelungssystem der Gesellschaft, in dem die gesetzlichen, verfassungsmäßigen Grundsätze und Vorschriften, politische Ordnungen oder politische Systeme, die Macht und Verfügungsbefugnisse (gewählter) politischer Akteure durch die (Wahl-)Stimmen der Bürger*innen und die Beteiligung der Bürger*innen an politischen Prozessen (wie der Teilhabe an Parlamenten) bestimmt werden. Es gibt verschiedene Formen von Demokratie (z.B. direkte oder Basisdemokratien, repräsentative Demokratie, etc.). Im Rahmen des Projekts DiDaT wird das (sich in seinen gesetzlichen und konstitutionellen Grundlagen fortlaufend modifizierende) demokratische System Deutschlands als ein sensitives Subsystem Deutschlands und als ein Schutzgut begriffen (Renn & Scholz, 2019). Diese Aussage ist auch vor dem Hintergrund von Interesse, dass nach gängigen Demokratieindizes nur etwa knapp 5% der Weltbevölkerung in als voll demokratisch klassifizierten Staaten leben. Weitere knapp 45% leben in einer unvollständigen Demokratie (The Economist Intelligence Unit, 2016).
Betrachtet man den einzelnen Menschen, so gibt es eine Reihe von (normativen) Merkmalen, welche die Demokratiefähigkeit des/der Einzelnen (May, 2007) beschreiben. Dazu gehören, dass es etwa über die „Gleichheit der Stimmen aller Bürger*innen“ eine Gleichberechtigung für jeden Beteiligte*n an politischen Prozessen gibt. Darüber hinaus besteht die Freiheit auf Meinungsäußerung (auch im Politischen) und damit ist die Meinung Anderer (sofern diese sich im Gesetzesrahmen bewegt) erlaubt. Zwischen Meinungsfreiheit und gesetzlichen Regeln (etwa dem Grundgesetz oder den Menschenrechten) ist es etwa bei Tötungsaufrufen in den sozialen Medien zu schwierigen und kontrovers diskutierten Urteilen in Deutschland gekommen (siehe etwa Mascolo & Steinke (2019)).
Das angemessene, unverfälschte „Informiert-Sein“ (***„the right to know“***) kann als ein Grundrecht der Demokratie begriffen werden. Aus der Sicht des/der Einzelnen wird die Vertrauenswürdigkeit der Information, und somit der Daten, durch den Erfahrungsraum soziale Medien in grundsätzlicher (also sowohl ontogenetisch wie phylogenetisch) Weise in Frage gestellt.
Eine Demokratie ist zudem gekennzeichnet durch deliberative, diskursive Prozesse (Renn, Deuschle, Jäger, & Weimer-Jehle, 2007) (siehe auch Habermas (1998)), die Anerkennung der Andersartigkeit (der Meinungen und Forderungen) Anderer, das Akzeptieren von Mehrheits-entscheidungen sowie Kompromisse und Abwägungs- und Verhandlungsprozesse (um Mehrheiten zu erlangen).
Der Übergang von den ***klassischen Massenmedien*** zur Informationsbeschaffung und deren zentraler Aufgabe der nachrichtlichen Informations-bereitstellung stellt eine Verschiebung des Agenda-Settings (also der Auswahl von Informationen) dar. Diese wurde bei den Massenmedien durch die Redaktionen/Journalist*innen („Gate-Keeper-Funktion”) ausgeführt. In den sozialen Medien hingegen gibt es eine Vielzahl von professionellen Anbietern sowie mehr oder weniger aktive nichtprofessionelle Nutzer*innen, die Informationen erzeugen („mass-self communication“). Hinzu kommen die Personalisierungsfunktionen (bezogen auf Priorisierung, Streichung, etc.) der Anbieter von sozialen Medien oder Netzwerken.
Die Wirkung sozialer Medien ist umstritten. Positive Stimmen betrachten soziale Medien als einen Katalysator für demokratische Prozesse, indem sie das „***Bürger-Sein***“[28] (Vortkamp, 2013) ermöglichen. In der Rolle des „Bürger-Sein“ werden individualistische und egoistische Partikularinteressen mit sozialen Motivationen und einer Orientierung

[28] Vortkamp, Wolfgang, Forschungsjournal Soziale Bewegungen (2016), 26(1), pp. 117-120

am Gemeinwohl verbunden. Um dies zu ermöglichen, braucht es institutionalisierte Räume politischer Beteiligungsmöglichkeiten, und sozialer Mitwirkung und Einflussnahmen, die über den vierjährlichen Urnengang hinausgehen. Darüber hinaus ermöglichen soziale Medien neue Formen von Partizipation und kollektivem politischem Handeln: Online Bürgerbewegungen, Petitionen, Crowdfunding, oder Proteste. Eine Frage ist, inwiefern soziale Medien diesen institutionalisierten Raum bieten oder selbst bereits eine aktive Rolle in demokratischen und sozialen Prozessen spielen. Es stellt sich die Frage, welche Auswirkungen auf die Demokratiefähigkeit das Systemdesign von sozialen Medien (welche daten- und algorithmenbasierten Informationen werden verwendet?) und Prozesse wie ***Microtargeting*** oder der Einsatz von ***Social Bots*** haben. Diese werden in Box 3 beschrieben. **Zusammenfassend** können wir folgern, dass in sozialen Medien Informationen mit „unkontrollierter" Breite und Güte vermittelt werden. Diese Informationen unterliegen teilweise nicht nachvollziehbaren Verzerrungen, Verdrehungen und Fälschungen. Dies kann zu Werbezwecken, politischer, religiöser und anderweitiger Propaganda, Mobilisierung und Demobilisierung bezogen auf Wahlen und auf politische Prozesse dienen. Solche Informationen kommen zum großen Teil aus Quellen, deren Ursprünge nicht nachvollziehbar sind. Hinzu kommen Verstärkungsprozesse, welche unter anderem bedingt sind durch sogenannte ***„Filterblasen"*** (durch Algorithmen geschaffene personalisierte Darbietung von Informationen im Internet), ***„Echokammern"*** (man bekommt nur bestimmte, potenziell zu seinen Einstellungen passende, Informationen wiederholt dargeboten) oder ***„Political Social Bots"***, welche in subtiler (unbemerkter) und sublimer (unbewusster) Form die Herausbildung bestimmter Meinungen gezielt beeinflussen. Dies ist eine der Komponenten der ***„Political Surveillance Society"***.

**Box 3: Mechanismen auf sozialen Medien mit Einfluss auf Demokratiefähigkeit**

Viele Mechanismen bestehen auf dem Prinzip der ***„Individualisierung" / „Personalisierung"*** der gelieferten Informationen. Mittels Algorithmen erzeugen soziale Medien, aber auch andere Internetakteure, ***„Filterblasen"*** (dies sind durch solche Algorithmen gefilterte Informationspräsentationen). Auch eine digitale ***„Echokammer"*** (Umgebung, in der bestimmte Informationen, die potenziell zu der eigenen Einstellung passen, wie ein Echo immer wiedergegeben werden) kann durch Personalisierung entstehen. Mittels des Verhaltens und des Wahrnehmens von Informationen durch das Individuum lernt der Algorithmus den/die Einzelne*n kennen und schlussfolgert, welche Informationen dieses Individuum am meisten ansprechen, also in seiner/ihrer Meinung bestätigen. Algorithmen innerhalb sozialer Medien filtern daraufhin alle vorhandenen Informationen (Daten) und zeigen jedem Individuum vor allem das, was für das entsprechende Individuum als passend eingeschätzt wird. Dadurch wird das Medium selbst zum Gate-Keeper und der Algorithmus zum Analysewerkzeug. Durch die selektive Informationspräsentation kann es zu einer Verstärkung des „***Confirmation Bias***" (Interpretation von Informationen, sodass diese in das bestehende Weltbild passen) kommen. Durch das digitale Echo einer Meinung, ohne alternative Informationen zur Verfügung zu stellen, entsteht somit eine Verzerrung der wahrgenommenen Realität („***Reality Shift***"). Aus diesem Wandlungsprozess könnte somit eine Reduktion von Vielfalt in der Meinungsbildung und -äußerung („***silencing personal opinion***") resultieren, mit allen sich daraus ergebenden demokratiepolitischen Konsequenzen. Auch interpersonelle Kommunikation (siehe (ii)) wird durch diese Prozesse erschwert. Die voranschreitende „***Datafizierung"*** kann dabei nicht nur zu einer verstärkten Kommerzialisierung von Lebensbereichen führen. Regelmäßig wird über Datenschutzverletzungen in den sozialen Medien berichtet. Skandale wie der um Cambridge Analytica führen großen Bevölkerungsteilen regelmäßig vor Augen, dass das Individuum nicht mehr nur real, sondern auch digital existiert. Zudem wird deutlich, dass diese digitale Existenz zu analysierten Schlussfolgerungen von sozialen Medien und sonstigen Interessensträgern führen kann. Auf diesen Schlussfolgerungen folgen dann wieder weitere Handlungen, die das Individuum betreffen (personalisierte Werbung, Meinungsbeeinflussung, etc). Das Wissen um diese Mechanismen kann ein permanentes Gefühl von Überwachung hervorrufen, welches zu einer Abschreckung („***Chilling Effekt"***) führen kann, bei welcher auf eine Meinungsäußerung zunehmend verzichtet wird. Dadurch soll vermieden werden, Verantwortung für negative Folgen übernehmen zu müssen. Somit führt dies zu einer Selbstzensur der Meinungs- bzw. Kommunikationsfreiheit, was eine demokratiepolitisch sensible Wirkung darstellt. Interessant sind ebenfalls **„Chilling effects on speech"** durch algorithmische Entscheidungen.Zusätzlich und wie oben bereits kurz erwähnt, sind mögliche politische und kommerzielle Manipulationen zu beachten, die – personalisiert und durch ***„Microtargeting"*** und ***„Social Bots"*** unterstützt – von Interessengruppen außerhalb der Plattformanbieter und deren Algorithmen verwendet werden. Eine Vielzahl von Anbietern in den sozialen Medien ermöglicht das zielgerichtete Ausspielen von Botschaften an genau (über Algorithmen) definierte Zielgruppen gegen Bezahlung. So kann bereits länger praktiziertes „Microtargeting" effizient in sozialen Medien fortgesetzt werden. Unter Zuhilfenahme von „Social Bots" kann darüber hinaus viel häufiger und intensiver mit der gewünschten Zielgruppe in Kontakt getreten werden. In diesem Zusammenhang sind auch die Überwachung politischer und wirtschaftlicher Prozesse zu diskutieren (siehe (Zuboff, 2019); etwa, wenn Daten an Geheimdienste weitergeleitet werden).Zusätzlich ist auch die Problematik zunehmender gezielter Desinformation, auch als „***Fake News"*** diskutiert, zu beachten. Hier werden zwei Faktoren kombiniert: Das angenommene Einordnen von Individuen in ***„Filterblasen" / „Echokammern"***, in welche dann zielgruppengenau externer, bezahlter (manipulierter) Inhalt gespielt werden kann. Dies unterwandert tendenziell die Entscheidungsfähigkeit des/der Einzelnen. Für die jeweiligen Nutzer*innen verstärkt sich durch die Vielzahl von gleichen Inhalten der ***Confirmation Bias***.

## 3. Auswahl Stakeholder und Wissenschaftler*innen - Welche Kompetenzen aus Wissenschaft und Praxis sind für das Verständnis von „Unseens“ und den Umgang mit Folgen besonders relevant?

Um zu einer Auswahl von Repräsentant*innen von Stakeholdergruppen zu kommen, welche Verursacher*innen sind, oder auch das Wissen, die Betroffenheit sowie die Regulationsfähigkeiten von und durch Stakeholdergruppen hinreichend repräsentieren, und in das Projekt DiDaT einzubringen, gehen wir wie folgt vor:

Wir bestimmen in einem ersten Schritt wesentliche Auswirkungen von den oben aufgeführten Mechanismen. Der bisherigen Unterteilung folgend unterscheiden wir in einem zweiten Schritt zwischen Stakeholdern aus den Bereichen (i) (psychisches) Wohlbefinden und Gesundheit und (ii) Aspekte, die die Demokratiefähigkeit betreffen:

**Tabelle 2: Unseen x Stakeholder Tabelle**

| | Unseens | Stakeholder | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | A. Betroffene | | | B. Verursacher / Treibende Institutionen | | | C. Regulatoren | | |
| | **Übernutzung** | **„Un-reguliert“** social media Nutzende | **Soziales Umfeld** Betroffener | **Berufliches Umfeld** Betroffener | **Internet / Social Media Kultur** | Social Media **Provider Value-Network** | **Wert-Nutzer** der Target-Daten | Psycho-/**Thera-peuten** | „LFK“/ Landes **Medien-Anstalt** | **Rahmen-Geber** |
| | **Digitale Gewalt**<br>Hate-Speech<br>Cyber-Trolling<br>Cyber-Mobbing<br>Cyber-Stalking | **Opfer** | **Soziales Umfeld** der Opfer | **Berufliches Umfeld** der Opfer | Surfer/ Nutzer = **Täter** | **Verdeckte Daten-Operation** / -Verwertung /-Mechanik | Nicht-Wissende = **„Dumme“** | Social Media **Provider** | **Gesetz-geber** | Psycho-/**Thera-peuten** |
| | **digital-sozialer Kompetenz-Mangel**<br>Siehe : digitale Gewalt | Gruppen kommuni-zieren **„interna“** per Social Media | **Hilfe-Suchende** zB. in Foren | **Umfeld** der Betroffenen | digital sozial **In-Kompe-tente** | **sich Versteckende** sind anonym o.Verantwortung | Nicht-Wissende = **„Dumme“** | **Ge-schulte** | Bildungs-**Veran-stalter** | **Politik + Gesetz-geber** |
| | **Reality-Shift** | **Jeder Nutzer** sozialer Medien | **Lösch-Resistente / „Dumme“** | Nachrichten-/ Informations-**Nutzer** | **Verdeckte Daten-**Verwertung/ Mechanik | Social Media **Provider Network Robots** | **Politische + wirtschaftl. Akteure, Influencer** | **Politik + Gesetz-geber** | **Ge-schulte** (Bildungs-ämter) | Nachrich-ten-**Agen-turen** |

## 4. Methodische Überlegungen zur Konstruktion sozial robuster Orientierungen (SOR)

Aufgrund der Komplexität und der Vielzahl der Untersuchungen sehen wir verschiedene begleitende Forschungsvorhaben als sinnvoll an.

- Survey: Literatur- und Dokumenten-recherche zu Strukturierungen von („unerwünschten“) Wirkungen und Vulnerabilitäten und Ihrer Prozesse aus Nutzung sozialer Medien und Erstellung eines graphischen Gesamtbildes
- Bewertung: Erhebung der als kritisch betrachteten Auswirkungen und Vulnerabilitäten (unter den Stakeholder-gruppen) zu besseren Gestaltung des öffentlichen Diskurses und Priorisierung der Wirkungen und beschriebenen Maßnahmen.
- Vertiefende Forschung: Untersuchung der Mechanismen von Anbietern sozialer Medien zur Steigerung der Nutzung → Welche Mechanismen wirken unter welchen Bedingungen (v.a. persönliche Voraussetzungen, bspw. (epi-)genetische Variablen) in welcher Art und Weise?
- Vertiefende Forschung: Was sind die Marktmechanismen des Datenverkaufs?

Wie üblich werden wir bei den Beziehungen verschiedene Dimensionen unterscheiden, wie Wissen, Betroffenheit, Verantwortbarkeit, Interessen, etc. Dies dient sicherzustellen, dass die wesentlichen Stakeholdergruppen einbezogen werden und wesentlichen Aspekte betrachtet werden.

**Tab. 3 Von *Unseens* zu sozial robusten Orientierungen (= SOR)**

| I. Unseens | II. Ursachen<br>Kausalitäten/ Entstehung | III. Maßnahmen<br>Sozio-technische Innovation | IV. Ziele | V. Sozial robuste Orientierungen |
|---|---|---|---|---|
| **Über-nutzung**<br>- Symptome des Mangel an Wohlbefinden / Gesundheit infolge von SM-Interaktionen | **Social-Media Mechanismen / Soziale Belohnungen der Neuigkeits-Gier**<br>**Maßgeschneiderte/ personalisierte Inhalte der VermarktungsIndustrie**<br>**Übernutzungs-sensitive Nutzer*innen** | **Nachweis/Transparenz** der Mechanismen & Vermarktung: Aus-Wirkungen auf Nutzer*innen<br>**Präventionsprogramme** für vulnerable Nutzer*innen<br>**Medien-medizinisch-sozial-psychologischer Service** | **Nachweis/Transparenz** der Daten-Vermarktungen<br>**Steuer-& Medienkompetenz Schutz und Hilfen** vulnerabler Nutzer*innen<br>**Bewussteres Absenden** per IP-Adressen-Ausweis<br>**Pilot-Erfahrungen** | **Aufklärung & Debatten** zu „Spielweisen"/ Mechanismen/Nutzungen<br>**Effektive Hilfe-Services:** Vertrauenswürdige Stellen<br>Soziales Umfeld<br>Provider-Services<br>**Vulnerabilitäts-Reporting** |
| **Digitale Gewalt** | **«offline-Welten»** Einflüsse + Unzufriedenheiten<br>**Anonymität enthemmt** * mangels Korrekturen/Strafen | **Gefühlte sozial-mediale Distanz** zum Opfer minimieren:<br>* Auto-Nummernschild-Analogie<br>**online-Verbrechen ahnden** | **Bürger*innen Adressen der** digital-soziale Verantwortung<br>**Rechtliche Konsequenzen** digitaler Texte/Taten | |
| **Reality-Shift** | **Individual-/Personalisierung**<br>**Eingeschränkte/verzerrte Infos**<br>**Social-Media-Marketing**<br>**Political-Kampagnen—Bots**<br>**Medien-Daten-Kompetenz** fehlt Regierender/Ämtern etc. | **Transparenz & Daten-Verwertung**<br>**Soziale Medien-Kompetenz** zertifizieren<br>**Nutzer steuern Personalisierung**<br>**Zusammenarbeits-Formate** von Bürgern, Staat und Providern<br>**Parteien-Medienpräsenz regeln** | **UN-Resolution des IGF2020**<br>**Transparenz & Kompetenz** der Personalisierung steuern<br>**Betriebs-Genehmigung:**<br>* Nutzer-Nummernschild<br>* „Diversity by Design"<br>* Data-Qualität-Audits<br>**Parteien Medienpräsenz** | **Daten-Verwertungs -Zertifikat**<br>**Demokratie = mündige Bürger**<br>**Regulierung: Vielfältigkeit Verantwortung** |

## 5. Erste Gedanken zur Vertiefungs-forschung

Der deliberative, forschungsbasierte, transdisziplinäre Prozess in DiDaT sieht vor, dass wesentliche Fragen, welche auch in einer gut zusammengesetzten Expertenrunde aus Wissenschaftler*innen und Praktiker*innen nicht beantwortet werden können, zum Gegenstand einer Vertiefungsforschung werden.
Im Folgenden beschreiben wir zwei Forschungsthemen (1a und 1b), welche die Arbeitsgruppe „**Vulnerabilitätsraum 05** – Soziale Medien, digitale Daten und ihre Auswirkungen auf den einzelnen Menschen" untersuchen wird. Dies wird parallel und unterstützend zum Prozess der Erstellung eines Kapitels des Weißbuchs zum Thema „Zum Umgang mit unbeabsichtigten und unerwünschten Nebenfolgen der digitalen Transformation – hier: durch die Nutzung von Sozialen Medien" geschehen.
In den Vorbereitungsarbeiten und in der 14-monatigen Vorbereitungsphase in der Initiierungsphase des Projekts sind die Mitglieder der Arbeitsgruppe zu dem Schluss gekommen, dass ein besseres Verständnis für den Umgang, das Wissen und die Wertestruktur von Kindern und Jugendlichen ein wichtiger Schlüssel ist, um ein Konzept zur Sicherstellung der nachhaltigen Nutzung der Daten sozialer Medien zu erarbeiten. Vor diesem Hintergrund stehen in allen Forschungsfragen die Gruppen der Kinder und Jugendlichen im Mittelpunkt. Wir denken aber auch an Erwachsenenbildung als ein Bereich, der von den Ergebnissen der Projekte sowie von dem Kapitel des Weißbuchs, welches im Juli 2020 im ersten Entwurf vorliegen wird, profitieren kann

**Phase II der Vertiefungsforschung (22. Januar – 23. Juni 2020)**

- **Was wissen Nutzer*innen aus verschiedenen Altersstufen über den Datenschutz und die ökonomische Verwertung von Nutzerdaten von sozialen Medien?**

Zur Methodik

I. **Konstruktion von Szenarien**:
Mindestens 6 Expert*innen der digitalen Vermarktung von Daten sozialer Medien werden strukturiert interviewed, um
i) die gängige Praxis der Datenverwertung inklusive Vermarktungswege,
ii) die schwarzen Schafe bei dieser Nutzung,
iii) die zentralen rechtliche Regularien sowie
iv) die firmeninterne Anwendung von Regulationsmechanismen zur Erhaltung rechtlicher und sozialer Standards herauszuarbeiten
(Bereiterklärt haben sich hierfür bereits:
Margarethe Dopf (Admeira), Peter Wiegelmann (Interrogare + Bundesverband Marktforschung), Christopher Reher (Plattform 161), Anna Schenk (Semasio), N.N., N.N.)

II. **Befragung von Jugendlichen über deren Wissen** zu den zuvor konstruierten Szenarien

**III.** **Befragung von Jugendlichen über deren Bewertung** der zuvor in der transdisziplinären Arbeitsgruppe **Vulnerabilitästsraum 05** konstruierten Szenarien

- **Wie können wir und der Staat Einfluss darauf nehmen, dass soziale Medien das liefern, was „wir“ (als Nutzer*innen und als Gesellschaft) wünschen?**

Zur Methodik

I: Eine ausführliche Auflistung der wünschenswerten Ergebnisse (r.s. Orientierungen)
wird in Zusammenarbeit der Praktiker*innen und Wissenschaftler*innen im DiDaT-Projekt erarbeitet

II. Mindestens 6 Expert*innen aus den Bereichen Politik und Medienwissenschaften werden strukturiert interviewed, um robuste soziale Strategien zu erarbeiten,
mit denen diese Orientierungen erreicht werden können

**Phase II der Vertiefungsforschung ab August 2020 bis 2021**

**Entwicklung von Folgeprojekten und Durchführung von Transdisziplinaritäts-Laboratorien (Td-Lab)**

(in diesem Papier nicht weiter beschrieben)

- Welche Folgen hat die Personalisierung (Filterblasen und Echokammern) im Internet, speziell in sozialen Medien, bei Kauf- und politischen Entscheidungen der Nutzer?

- Digitale Kulturen bei Jugendlichen:
Begleitende Prozessanalyse der Internetnutzung in einer Schulklasse

## 6. Erwartete Ergebnisse und Folgeinitiativen

Wie erwarten, dass im Weißbuch für den Bereich soziale Medien die wesentlichen Prozesse und Auswirkungen von sozialen Medien, welche Einflüsse auf die Gesundheit und das (psychische) Wohlbefinden sowie die Demokratiefähigkeit haben, dargelegt werden, die prototypischen Prozesse und Auswirkungen, die diesen negativen Wirkungen unterliegen, anhand von Beispielen beschrieben werden und soziale Orientierungen sowie soziotechnische Innovationen beschrieben werden, um resiliente individuelle und gesellschaftliche Systeme zu schaffen, um psychische und psychosomatische Gesundheit zu sichern und die Demokratiefähigkeit zu sichern.

## Referenzen


Appel, H., Gerlach, A. L., & Crusius, J. (2016). The interplay between Facebook use, social comparison, envy, and depression. *Current Opinion in Psychology*, *9*, 44–49. https://doi.org/10.1016/j.copsyc.2015.10.006

Boulianne, S. (2015). Social media use and participation: A meta-analysis of current research. *Information, Communication & Society*, *18*(5), 524–538. https://doi.org/10.1080/1369118X.2015.1008542

Brand, M., Young, K. S., Laier, C., Wölfling, K., & Potenza, M. N. (2016). Integrating psychological and neurobiological considerations regarding the development and maintenance of specific Internet-use disorders: An Interaction of Person-Affect-Cognition-Execution (I-PACE) model. *Neuroscience & Biobehavioral Reviews*, *71*, 252–266. https://doi.org/10.1016/j.neubiorev.2016.08.033

Brooks, S. (2015). Does personal social media usage affect efficiency and well-being? *Computers in Human Behavior*, *46*, 26–37. https://doi.org/10.1016/j.chb.2014.12.053

Büchi, M., Festic, N., & Latzer, M. (2018). How social well-being Is affected by digital inequalities. *International Journal of Communication*, *12*(0), 21.

Carr, C. T., & Hayes, R. A. (2015). Social media: Defining, developing, and divining. *Atlantic Journal of Communication*, *23*(1), 46–65. https://doi.org/10.1080/15456870.2015.972282

Diefenbach, S., & Ullrich, D. (2016). *Digitale Depression. Wie neue Medien unser Glücksempfinden verändern.* Retrieved from https://www.m-vg.de/mvg/shop/article/6472-digitale-depression/

Gosh, D., & Scott, B. (2018). *Digital deceit: The technologies behind precision propaganda on the Internet*. Retrieved from https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit/

Habermas, J. (1998). *Faktizität und Geltung: Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats* (1.). Frankfurt am Main: Suhrkamp Verlag.

Howard, P. N., & Parks, M. R. (2012). Social media and political change: Capacity, constraint, and consequence. *Journal of Communication*, *62*(2), 359–362. https://doi.org/10.1111/j.1460-2466.2012.01626.x

Mascolo, G., & Steinke, R. (2019, September 27). Gefährliche Rede. Was man noch sagen darf. Und was man noch nie sagen durfte: Wo verläuft die Grenze zwischen Hass und Meinungsfreiheit? Und wer soll entscheiden, was bestraft wird? *Süddeutsche Zeitung*, p. 12.

May, M. (2007). *Demokratiefähigkeit und Bürgerkompetenzen: Kompetenztheoretische und normative Grundlagen der politischen Bildung* (Vol. 26). Berling: Springer.

Renn, O., Deuschle, J., Jäger, A., & Weimer-Jehle, W. (Eds.). (2007). Diskursive Verfahren zur Lösung von Ziel-und Transformationskonflikten. In *Leitbild Nachhaltigkeit: Eine normativ-funktionale Konzeption und ihre Umsetzung* (pp. 169–187). https://doi.org/10.1007/978-3-531-90495-5_7

Renn, O., & Scholz, R. W. (2019). *Gegenstand, Ziele, und Methodik des Projekts DiDaT*. 16.

The Economist Intelligence Unit. (2016). *Democracy Index 2016. Revenge of the "deplorables".* Retrieved from The Economist website: http://www.eiu.com/home.aspx

Vortkamp, W. (2013). Wozu braucht die repräsentative Demokratie die Bürger? *Forschungsjournal Soziale Bewegungen*, *26*(1). https://doi.org/10.1515/fjsb-2013-0104

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for the future at the new frontier of power*. New York: Profile Books.


-

# Vulnerabilitätsraum 06 (VR06)

# Vertrauenswürdigkeit undZuverlässigkeit digitaler Daten und Informationen

DiDaT Grobplanung zum Vulnerabilitätsraum (VR) 06

# Vertrauenswürdigkeit und Zuverlässigkeit digitaler Daten und Informationen

Sebastian Hallensleben (VDE), Roland. W. Scholz (Donau Uni Krems), Andreas Kaminski (HLRS Universität Stuttgart), Julio Lambing (VEZL)

Inputs durch Dirk Helbing (ETH Zürich), Karl-Heinz Simon (CESR Universität Kassel), Malte Reissig (IASS), Dirk Marx (BTU Cottbus-Senftenberg), Sabine Thürmel (TU München)

## 1 Gegenstand, Ziele und Leitfrage

Fälschungen von Texten und Fotos sind nicht neu – sei es in der Werbung, für politische Manipulationen, bei Betrügereien oder für andere Zwecke. Wir haben uns darauf eingestellt, Texten und Fotos mit gesunder Skepsis zu begegnen. Das gilt insbesondere im digitalen Raum.

Für Videos konnte man dagegen bisher annehmen, dass sie tatsächlich ein reales Geschehen zeigen. „Fälschungen" waren dort nur in engem Rahmen möglich, beispielsweise durch geschicktes Schneiden, eine falsche Zuordnung oder den Einsatz eines professionellen Filmstudios. Videos galten bisher als das weitgehend unbestechliche digitale Äquivalent des Augenscheins. Seit 2018 sind jedoch mit künstlicher Intelligenz ausgestattete Werkzeuge (v.a. Deep Fake[29]) verfügbar, mit denen praktisch jedermann beliebige Video- und Audioaufnahmen fälschen kann. Mit entsprechender Rechenleistung sind diese Fälschungen sogar in Echtzeit möglich, d.h. ein angeblicher Live-Fernsehauftritt einer prominenten Persönlichkeit kann während des Programms gesteuert werden. Die öffentliche Aufmerksamkeit ruht derzeit vor allem auf im WWW veröffentlichten Videos, in denen demonstriert wird, wie man US-Politiker Worte in den Mund legen kann. Entsprechend haben erste Staaten und Unternehmen Maßnahmen gegen die Verbreitung solcher irreführender Videos ergriffen.[30] Der politische Fokus über-

29 Melanie Ehrenkranz (2018): Researchers Come Out With Yet Another Unnerving, New Deepfake Method; Gizmodo; 09.11. 2018; unter: https://gizmodo.com/researchers-come-out-with-yet-another-unnerving-new-de-1828977488 *(abgerufen am 20.11.2019). Katyanna Quach (2018): The eyes don't have it! AI's 'deep-fake' vids surge ahead in realism; The Register; 11.09.2018; unter: www.theregister.co.uk/2018/09/11/ai_fake_videos/ (abgerufen am 20.11.2019). Bloomberg LP (2016): It's Getting Harder to Spot a Deep Fake Video; Youtube; 27.09.2018; unter: www.youtube.com/watch?v=gLoI9hAX9dw; (abgerufen am 20.11.2019)*

30 Der US-Bundesstaat Kalifornien verbietet seit Oktober 2019 60 Tage vor einer Wahl die Verbreitung von manipulierten Videos, Tonspuren und Bildern eines Wahlkandidaten, die in böswilliger Absicht den Rufschädigung oder Wählerbeeinflussung betreiben, es sei denn, sie wurden als manipuliert gekennzeichnet. Siehe https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB730 (abgerufen am 20.11.2019). Facebook hat angekündigt, solche Videos in seinen Streams zu entfernen, die Ergebnis einer KI-Manipulation sind (so dass sie authentisch erscheinen) und zugleich in einer Weise bearbeitet wurden, die für einen Durchschnittsrezipienten nicht erkennbar ist und die wahrscheinlich zu der Überzeugung führt, dass eine dargestellte Person etwas sagte, was sie in Wirklichkeit nicht sagte. Siehe https://about.fb.com/news/2020/01/enforcing-against-manipulated-media (abgerufen am 06.01.2020)

deckt jedoch, dass die überragende Mehrzahl solcher Videos derzeit eine neue Form nicht einvernehmlicher Pornografie zeigen, bei denen computer-generierte Gesichter von Prominenten auf die Köpfe der Sexdarsteller geschnitten werden, mit Abermillionen von Zuschauern.[31] Die allermeisten der von solchen „morph porn" betroffenen Personen sind öffentlich agierende Frauen. Zunehmend sind aber auch vollkommen unprominente Frauen betroffen. Die Fälschungen bergen also nicht nur das Potential für privaten Rufmord, Cyberstalking oder auch Identitätsdiebstahl eingesetzt werden zu können, mit verheerenden Folgen für die Betroffenen.[32] Sie demonstrieren auch ihre Zugänglichkeit und Eignung für den Einsatz in Alltagsauseinandersetzungen, etwa bei der Fälschung von rechtlichen Beweisen.

Gefälschte Videos sind also nur ein augenfälliges Symptom für die generellen neuen Möglichkeiten zur Fälschung von einflussreichen Informationen. Poltisch einflussreicher waren bisher sogenannte „Shallowfakes", also mit einfachen Mittel gefälschte Videos.[33] Auch überzeugende „Fotos" nichtexistenter Menschen sowie glaubwürdige Texte lassen sich mittlerweile mit minimalem Auf-wand in großer Menge und mit zahlreichen Stellschrauben generieren[34]. Im Ein-

**Leitfrage von VR6**
Wie können die Zuverlässigkeit digitaler Informationen sowie IT-gestützte Vertrauens-infra-strukturen in naher Zukunft in Deutschland so gestaltet werden, dass ein fakten- und werte-basierter öffentlicher, wissenschaftlicher und politischer Diskurs möglich bleibt, um eine Disruption der Grundlagen von Demokratie und Rechtsstaat zu verhindern? Wie sieht eine Kombination aus sozialen und technischen Ansätzen aus, die eine Verifi-zierung von Fakten unterstützt? Wie kann auch künftig mündige politische Meinungs-bildung ablaufen? Welche Anreizsysteme können vorgeschlagen werden, mit denen Wahr-heits---findung und -verbreitung präferiert werden? Wie lassen sich kluge Netze des Vertrauens knüpfen? Wie kann dies auf angemessene Weise technisch unterstützt werden?

31 Von 14,698 Deepfake Videos, die im Sommer 2019 online gefunden wurden, waren 96% pornographischer Natur. Siehe für diese und folgende Aussagen: Henry Ajder, Giorgio Patrini, Francesco Cavalli, and Laurence Cullen (2019): The State of Deepfakes: Landscape, Threats, and Impact; Amsterdam: Deeptrace; September 2019

32 Drew Harwell (2018): Fake-porn videos are being weaponized to harass and humiliate women: 'Everybody is a potential target'; The Washington Post; 30.12.2018; www.washingtonpost.com/technology/2018/12/30/fake-porn-videos-are-being-weaponized-harass-humiliate-women-everybody-is-potential-target/ (abgerufen am 20.11.209)

33 Siehe die bewusste Streuung von Videos, die die angeblich betrunkene Sprecherin des US-Repräsentantenhauses Nancy Pelosi und die angebliche körperliche Aggressivität des US-Reportes Jim Acosta belegen sollten. Dazu Henry Ajder, Giorgio Patrini, Francesco Cavalli, and Laurence Cullen (2019): The State of Deepfakes: Landscape, Threats, and Impact; Amsterdam: Deeptrace; September 2019; S. 11 f.

34 Katyanna Quach (2018): An AI system has just created the most realistic looking photos ever; The Register; 14.12. 2018; unter: https://www.theregister.co.uk/2018/12/14/ai_created_photos/ (abgerufen am 20.11.2019) Man beachte auch das eingebettete Video im Artikel.

zelhandel sind Fake Reviews ein weitverbreitetes und ernsthaftes Phänomen der Konsumententäuschung.[35]

Parallel zu dieser technologischen Entwicklung sinkt der Einfluss der traditionellen Massenmedien und ihrer Filter- und Verifizierungsfunktion für Informationen. Sie können nur schwer mithalten mit der Dynamik der Online-Medien, in denen Inhalte, egal, ob echt oder gefälscht, können sich rasend schnell verbreiten, teilweise gezielt vorangetrieben durch kommerzielle Dienstleister[36]. Die Werbewirtschaft und manche politischen Akteure haben sich bereits auf diese neuen Verbreitungsmöglichkeiten eingerichtet. Über gezielte Einflussnahmen beispielsweise der russischen *Internet Research Agency (IRA)*[37] sowie Wahlmanipulation durch *Cambridge Analytica*[38] ist ausführlich berichtet worden. In Gabun und Malaysia spielten Vorwürfe zum Einsatz von Deep Fakes eine relevante Rolle in schweren politischen Krisen.[39]

Eine Flut falscher Informationen hat das Potenzial, Fakten in der Wahrnehmung zu verdrängen. Dies geschieht nicht nur durch eine bewusste Entscheidung von Rezipienten, dieser oder jener Information eher zu vertrauen, sondern auch durch eine unbewusste Überlagerung bereits abgespeicherten Wissens.[40]

Der hier verwendete Begriff „Vertrauen" zeigt den Kern der umrissenen Problematik an: Vertrauen in und Vertrauenswürdigkeit von Informationen sind seit jeher für Menschen eine notwendige und zugleich heikle Angelegenheit. Die Entwicklung der Informationstechnik im Zeitalter der neuen sozialen Medien und der künstlichen Intelligenz hat die generelle Zeugenschafts- und Vertrauensproblematik verschärft. (Siehe: *Begriffliche und epistemologische Einordnung von*

35 Siehe die Recherchen der britischen Consumers' Association im Verbrauchermagazin *Which?* : Hannah Walsh (2019): Thousands of 'fake' customer reviews found on popular tech categories on Amazon; Which?; 16.04.2019; www.which.co.uk/news/2019/04/thousands-of-fake-customer-reviews-found-on-popular-tech-categories-on-amazon *(abgerufen am 20.11.2019). Shefalee Loth (2018): The facts about fake reviews Which? investigators reveal tricks that sellers use to mislead online shoppers: Which?; 25.10.2018; www.which.co.uk/news/2018/10/the-facts-about-fake-reviews (abgerufen am 20.11.2019)*

36 Lion Gu, Vladimir Kropotov, and Fyodor Yarochkin: The Fake News Machine. How Propagandists Abuse the Internet and Manipulate the Public (2017); TrendLabs Research Paper; Hrsg: Trend Micro, Incorporated; unter: https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf *(abgerufen am 20.11.2019).*

37 Adrian Chen (2015): The Agency. From a nondescript office building in St. Petersburg, Russia, an army of well-paid "trolls" has tried to wreak havoc all around the Internet — and in real-life American communities; New York Times; 02.06.2015; unter www.nytimes.com/2015/06/07/magazine/the-agency.html *(abgerufen am 20.11.2019). The Economist (2018): Inside the Internet Research Agency's lie machine (Briefing); The Economist; 22.02.2018; www.economist.com/briefing/2018/02/22/inside-the-internet-research-agencys-lie-machine (abgerufen am 20.11.2019)*

38 British Broadcasting Corporation (2018): Cambridge Analytica planted fake news; BBC; 20.03.2018; unter www.bbc.com/news/av/world-43472347/cambridge-analytica-planted-fake-news *(abgerufen am 20.11.2019)*

39 Henry Ajder, Giorgio Patrini, Francesco Cavalli, and Laurence Cullen (2019): The State of Deepfakes: Landscape, Threats, and Impact; Amsterdam: Deeptrace; September 2019; S. 9

40 Elizabeth F Loftus (2005): Searching for the neurobiology of the misinformation effect: Planting misinformation in the human mind: A 30-year investigation of the malleability of memory; in: Learning & Memory; July 1, 2005 Vol: 12; S. 361-366; DOI: 10.1101/lm.94705; unter: https://www.researchgate.net/publication/8045738_Searching_for_the_neurobiology_of_the_misinformation_effect *(abgerufen am 20.11.2019)*

*Vertrauen*). Es stellt sich die Frage: Wie können die Zuverlässigkeit digitaler Informationen sowie IT-gestützte Vertrauensinfrastrukturen in naher Zukunft in Deutschland so gestaltet werden, dass ein fakten- und wertebasierter öffentlicher, wissenschaftlicher und politischer Diskurs möglich bleibt, um eine Disruption der Grundlagen von Demokratie und Rechtsstaat zu verhindern?

## Begriffliche und epistemologische Einordnung von Vertrauen

Die Philosophin Annette Baier hat als Arbeitsdefinition vorschlagen, Vertrauen als akzeptierte Verletzbarkeit zu begreifen (1). Folgt man diesem theoretisch einflussreichem Vorschlag, muss eine Analyse des hier untersuchten Vulnerabilitätsraums berücksichtigen, dass Menschen einerseits auf elementare Weise, die Möglichkeit verletzt zu werden, nicht vermeiden können, dass sie anderseits jedoch lernen können und müssen, auf angemessene Weise Vertrauen zu gewähren oder zu entziehen.

**Die allgemeine Problematik von Vertrauen und Zeugenschaft**

Auf den ersten Blick mag die Annahme naheliegen, dass in modernen Gesellschaften die Bedeutung von Vertrauen abnimmt: Es könnte so scheinen, als ob Verwissenschaftlichung und Technisierung Vertrauen ablösten. Man muss und braucht anderen nicht zu vertrauen, weil man durch Technik und Wissenschaft Transparenz- und Kontrollmöglichkeiten gewonnen hat, die an die Stelle von Vertrauen treten. Doch bereits Gründerfiguren der Soziologie wie Max Weber und Georg Simmel waren anderer Meinung: Technik und Wissenschaft selbst vergrössern die *Abhängigkeit* des Einzelnen von den Leistungen a*nderer,* was den Vertrauensbedarf erhöht.

Diese Abhängigkeit von anderen wird besonders deutlich und relevant im Bereich von **Information und Wissen**. Das meiste, von dem wir annehmen, dass wir es wissen, haben wir *durch Andere* erfahren: dass es Bakterien gibt und einige davon unserer Gesundheit abträglich sein können; dass die Erde keine Scheibe ist und um die Sonne zirkuliert; wie weit Stuttgart und Frankfurt entfernt sind und wann der nächste Zug abfahren soll; welche Partei bei der letzten Wahl gewonnen hat, wer sie gewählt hat und wer jetzt die Regierung stellt. Selbst wann und wo wir geboren wurden wissen wir nicht qua eigener Erkenntnis.

Die Vertrauenswürdigkeit von Informationen ist eng verwoben mit dem erkenntnisbezogenen **(epistemischen) Abhängigkeit von Anderen**. Der klassische Wissensbegriff der Philosophie geht davon aus, dass Wissen eine (a) Überzeugung ist, die (b) wahr, zusätzlich aber (c) gerechtfertigt sein muss – man muss gute Gründe für die Überzeugung haben, damit man einen Wissensanspruch erheben darf, eine Überzeugung darf nicht bloß zufällig wahr sein. Dass Andere eine mögliche Quelle und Begründung eigener Wissensansprüche sind, ruft folgende Frage auf: Wie begründen und rechtfertigen wir es (c), dass wir etwas zu wissen glauben, weil Andere es uns gesagt haben – oder anders ausgedrückt: weil Andere es bezeugt haben.

Es ist nun eine offene Frage, wie wir (c) auffassen können. Eine mögliche Begründung, die aber vieles offen lässt, ist die folgende Antwort: Wir können einem Sprecher glauben, wem wir ihm *vertrauen.* Das damit aufgeworfene Problem können wir als Zeugenschafts- und Vertrauensproblem bezeichnen. Das allgemeine Problem lässt sich durch die Frage ausdrücken: Wann sind wir darin gerechtfertigt, den Anderen zu glauben? Wann sind wir darin gerechtfertigt, den Anderen zu vertrauen, wenn sie etwas behaupten?

**Problemverschärfung durch die Digitalisierung der Gesellschaft**

Die ohnehin bestehende, alltäglich aufscheinende Problematik von Zeugenschaft und Vertrauen verschärft sich durch die Digitalisierung der Gesellschaft, insbesondere durch die Entwicklung und alltägliche Verbreitung des Internets. Wir erhalten erstens viel mehr Informationsangebote aus zweitens mehr möglichen Quellen, die wir nicht persönlich kennen, zu drittens Themen, bei denen wir häufig weniger Möglichkeiten haben, sie durch eigene Erfahrung kritisch zu prüfen. Zudem scheint die Digitalisierung der Kommunikation neue Möglichkeiten ihrer Manipulation zu eröffnen. Ein Beispiel hierfür ist die auf Daten und Algorithmen basierte Selektion von Nachrichten, ein anderes Beispiel die erwähnten Deep Fake Videos. Sie verschärfen die allgemeine Frage, wann wir darin gerechtfertigt sind, Anderen zu glauben. Denn wir sind in mehr Themen, die für uns relevant sind, abhängig von dem, was (relativ anonyme) Andere uns mitteilen. Und die technischen Möglichkeiten der Manipulation scheinen gewachsen zu sein.

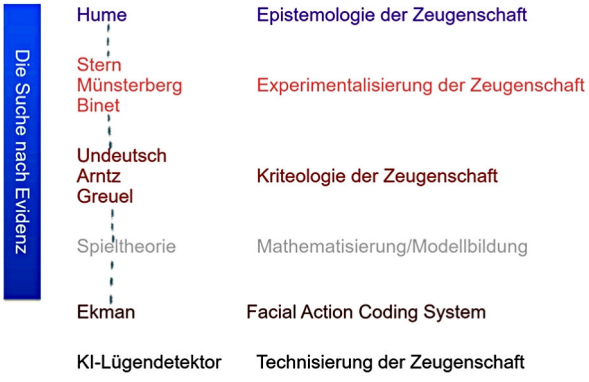
(1) Annette Baier (1986): Trust and Antitrust; in: Ethics; Vol. 96, No. 2 (Jan., 1986); S. 231-260; S. 235

Anders gefragt: Wie lassen sich kluge Netze des Vertrauens knüpfen? Wie kann dies auf angemessene Weise technisch unterstützt werden?

**Die Fragestellung des Vulnerabilitätsraums wird also in mehrfacher Hinsicht thematisch eingrenzt:** Selbstverständlich besteht die Möglichkeit, dass durch die Digitalisierung veranlasste Schwächung der Vertrauenswürdigkeit von Informationen auch ökonomische Effekte als Unseens hat, die relevante Auswirkungen auf einzelne Geschäftsbranchen oder auf Konsumgewohnheiten haben. (Siehe die Frage der Vertrauenswürdigkeit von Produktreviews.) Zur pragmatischen Beschränkung des Untersuchungsfelds sollte jedoch die Gefährdung von Demokratie und Rechtsstaat im Vordergrund stehen.

Auch eine geografische Eingrenzung ist aus pragmatischen Gründen geboten. Die bisher aufgezeigte Problemlage als auch die im Abschnitt 2 dargelegten Vulnerabilitäten sowie die darauf antwortenden, möglichen Lösungsansätze bestehen zwar global bzw. international, zumindest insoweit als Onlineinformationen und Onlinediskurs zugänglich sind und bereits eine signifikante Rolle in Politik und Gesellschaft spielen (dies schließt lediglich einige wenige geografisch abgelegene Räume aus).

**Technische Lösungen zu Vertrauen im Spiegel der Theoriegeschichte**




Technische Lösungen, die Vertrauenswürdigkeit messen und zwischenmenschliche Vertrauensprozesse nachbauen und ersetzen sollen, lassen sich vor dem Hintergrund der allgemeinen Theoriegeschichte von Vertrauen deuten. Es gibt aktuell zwei große Theorielinien, die einander widersprechende Antworten geben auf die Frage, wie begründet werden kann, dass man einer Person glaubt. Die eine Antwort lautet: Vertrauen *hat* epistemische Gründe. Die andere geht dagegen davon aus, dass Vertrauen nicht auf Gründe zurückgeführt werden kann, sondern selbst eine Orientierung gebender Grund *ist,* etwas für wahr zu halten. Die erste Linie versucht die Zeugenschaft also ganz auf ein *erkenntnistheoretisches* Problem zurückzuführen. Damit geht die Hoffnung einher, das vermeintliche Wissen, das wir durch *Andere* gewinnen, auf unser *eigenes* Wissen zurückzuführen. Wir beurteilen und bewerten

Angesichts der sich in der Stakeholder-Analyse (Abschnitt 3) abzeichnenden Akteurskonstellation, der Sprachabhängigkeit von Onlineinformationen sowie der Jurisdiktionsbezogenheit von Lösungsansätzen sollte zunächst Deutschland, fallweise auch die DACH-Region betrachtet werden. Im Verlauf des Projekts kann und soll jedoch herausgearbeitet werden, inwieweit sich Lösungen auch als Impulse bzw. Piloten für Europa (im Sinne der Europäischen Union) eignen.

Drittens soll hier nicht jede Form von Fälschung bei der Übermittlung von Informationen betrachtet werden. Kriminelle Angriffe auf die Datenübertragung bei Geldüberweisungen, der Übermittlung von Steuerungsbefehlen in der öffentlichen Stromversorgung oder der Koordination von öffentlichen und privaten Transport können sicherlich eine gewichtige Gefahr für eine Gesellschaft darstellen. Sie unterscheiden sich jedoch insofern von der hier geschilderten Thematik, als dass sie eine illegitime Manipulation der Übermittlungskanäle beinhalten und bestehende Informationen in der Übertragung durch falsche ersetzen. Solche Angriffe auf Datenübermittlungswege sind jedoch etwas anderes als Angriffe durch gefälschte Informationen, die erst **durch ihre Wahrnehmung und ihre diskursive Verhandlung in sozialen Räumen ihre schädliche Wirkung erhalten.**

Andererseits liegt der Fokus von VR6 auf der Information, unabhängig davon, wo sie im digitalen Raum vorliegt. In Abgrenzung zu VR05 betrachtet dieser Vulneabilitästraum also nicht (oder nur am Rande) die Funktion und Struktur spezifischer Bereiche des digitalen öffentlichen Raums (z.B. Social Media, klassische Nachrichtenmedien, Plattformen für nutzergenerierte Inhalte oder Fachpublikationen), sondern abstrahiert zur Information an sich sowie deren ursprünglicher Quelle.

## 2 Welche nicht intendierten, unbeabsichtigten Nebenfolgen sind von Interesse und warum?

### Gefährdung des demokratischen Gemeinwesens als Konsequenz

Wenn selbst Videos überzeugend gefälscht werden können und damit die letzte Bastion der Tatsachenprüfung durch Augenschein fällt, dann sind sämtliche Onlineinhalte fragwürdig. **Wahrheit und Lüge werden ununterscheidbar**. Nicht nur gefälschte Informationen können für echt gehalten werden, sondern auch echte Informationen können in Zweifel gezogen werden. Der Politiker, der bei der Annahme von Bestechungsgeldern gefilmt wurde, kann solche Videobelege künftig problemlos als Fälschung abtun. Aviv Ovadya hat für diese Entwicklung den Begriff „Infokalypse“ geprägt,[41] der inzwischen auch in Form einzelner Zwischenrufe an die breitere Öffentlichkeit gelangt ist.[42].Traditionelle

41 Charlie Warzel (2018): He predicted the 2016 fake news crisis. Now he's worried about an information apocalypse; Buzz Feed News; 11.02.2018; unter: www.buzzfeed.com/charliewarzel/the-terrifying-future-of-fake-news *(abgerufen am 20.11.2019)*

42 Miriam Meckel (2018): Eine neue Schicht Endfrustrierter treibt uns in die Infocalypse. Was dagegen

Massenmedien können zwar weiterhin versuchen, als Filter und Prüfer zu agieren, sind aber der emotionalen Wirkung und der rasend schnellen Verbreitung einer gefälschten „Nachricht“ gegenüber machtlos. Sie können ihre Filterfunktion im extrem beschleunigten Online-Nachrichtenfluss nur noch schwer oder verzögert ausüben. Gleichzeitig muss der Mensch weiterhin die Einschätzung der Glaubwürdigkeit von Informationen teilweise delegieren, da die Masse an Information ansonsten nicht zu bewältigen wäre und der einzelne Mensch nicht so viele sorgfältige Einzelbeurteilungen und -entscheidungen treffen kann. **Wenn sich Wahrheit und Lüge für den Einzelnen aber nicht mehr mit realistischem Aufwand trennen lassen, dann ist das Konstrukt des „mündigen Bürgers“ bzw. einer „mündigen Gesellschaft“ als Ausgangspunkt aller staatlichen Gewalt** (nach Art. 20, Abs. 2 des deutschen Grundgesetzes) **faktisch unmöglich geworden**. Das demokratische Gemeinwesen verliert seine Grundlage. Die Auseinandersetzung mit der Vertrauenswürdigkeit von Informationen im digitalen Raum wird so zur dringlichen Notwendigkeit.

Neben der Gefährdung demokratischer Systeme durch die informationelle Entmündigung des Bürgers sind weitere schwerwiegende Folgen realistisch: Die Zuverlässigkeit polizeilicher Untersuchungen oder die rechtsstaatliche Gültigkeit von Gerichtsprozessen kann möglicherweise durch die ausgeweitete Fälschbarkeit von Informationen nur noch eingeschränkt gewährleistet werden. Die Öffentlichkeit vertraut dem staatliche Rechtssystem nicht mehr. Finanzmärkte können aufgrund Fehlinformationen, deren Falschheit sich nur schwer und zeitlich deutlich verspätet nachweisen lässt, bisweilen so manipuliert werden, dass die Auswirkungen auf die Weltwirtschaft massiv sind etc. Verschärft wird die Situation durch **kommerzielle Anreize**, denn für Onlineinhalte dominiert als Geschäftsmodell die Werbefinanzierung. Dies führt dazu, dass die Auswahl und Darstellung von Inhalten allein auf eine hohe Aufmerksamkeit der Nutzer (z.B. gemessen durch Klicken oder Teilen) gerichtet ist.[43] Da extreme und/oder emotional erschütternde Nachrichten eine besonders hohe Aufmerksamkeit erregen, besteht ein hoher Anreiz für Plattformen, diese besonders prominent anzuzeigen. Gefälschte Informationen können genau dieses Muster besonders einfach bedienen und verbreiten sich daher besonders leicht.

helfen könnte; Wirtschaftswoche; 23.02.2018; unter; www.wiwo.de/politik/deutschland/schlusswort-laesst-sich-die-infocalypse-noch-abwenden/20989742.html *(abgerufen am 20.11.2019). Oscar Schwartz (2018): You thought fake news was bad? Deep fakes are where truth goes to die; The Guardian; 12.11. 2018; www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth (abgerufen am 20.11.2019). Elmar Theveßen (2019): Manipulierte Videos - Wie Deep Fakes die Welt gefährden ; in zdf – heute Nachrichten; 29.05.2019; www.zdf.de/nachrichten/heute/infokalypse-wie-deep-fakes-die-welt-gefaehrden-100.html (abgerufen am 20.11.2019)*

43 vgl. z.B. diese Tipps einer Werbeagentur: https://blog.hootsuite.com/de/facebook-algorithmus-organische-reichweite/ *(abgerufen am 20.11.2019)*

**Die Aporien der epistemisch-technischen Lösung**

Der den technischen Lösungen des Vertrauensproblems zugrundeliegende Vertrauensbegriff geht von folgenden Annahmen aus. Vertrauen (wie Vertrauenswürdigkeit) wird demnach begriffen als:

(1) **quantifizierbar**: Es handelt sich um eine durch einen Wahrscheinlichkeitsbegriff artikulierbare Größe.

(2) **begründet**: Vertrauen beruht auf Gründen, die für die Vertrauenden als evident gelten. Diese Evidenz geht auf Informationen zurück.

(3) **kognitive Erwartung**: Vertrauen geht daher mit einer kognitiven Erwartung einher. Kognitive Erwartungen unterscheiden sich von normativen u.a. dadurch, dass sie im Enttäuschungsfall aufgegeben werden, mit anderen Worten: Es wird gelernt.

(4) **epistemische Beziehung**: Die andere Person kommt darin nicht als Person vor. Denn eigentlich vertraue ich nicht ihr, sondern meinem Erkenntnisvermögen.

Diese Annahmen sind zwar grundsätzlich nicht falsch, führen jedoch in der vorliegenden Form zu Aporien. Wenn Evidenz, wie Annahme (2) besagt, unabhängig von Vertrauen ist, kann man auf der Grundlage der richtigen Evidenz (Information) eine vernünftige Entscheidung treffen zu vertrauen oder zu misstrauen. Genau diese Unabhängigkeit ist in den meisten Fällen jedoch nicht gegeben. Wir betrachten nämlich umgekehrt eine uns präsentierte Evidenz (Information) im Licht von Vertrauen und Misstrauen. Es stellt sich daher ein zirkuläres Verhältnis zwischen Evidenz/Informationen und Vertrauen ein. Diesen Zirkel kann man nicht vermeiden, man kann nur mit ihm besser oder schlechter umgehen.

Die Annahme, das Vertrauensproblem sei technisch lösbar, ignoriert diesen Zirkel. Gehen wir dazu zu der Annahme zurück, die Vertrauenswürdigkeit einer Information lasse sich evidentiell durch eine Technik messen. Selbst wenn dies der Fall wäre, bestünde das Problem, dass man dazu dieser Technik bzw. ihren Entwicklern vertrauen müsste. Man kann also nicht aus der Abhängigkeit von anderen und damit aus dem Zirkel aus Evidenz und Vertrauen heraus springen. **Daher ist auch die Vorstellung, Fake News ließen sich einfach als solche technisch identifizieren und aus der Welt schaffen, fraglich.** Keine Person, die glaubt, dass eine Regierung Informationen unterdrückt und ihre Bürgerinnen und Bürger gezielt desinformiert, wird sich durch eine von diesem Staat (oder von staatlich abhängigen Institutionen) entwickelten Technologie darüber 'aufklären' lassen, dass dies nicht der Fall ist.

**Ein soziotechnisches Problem – eine soziotechnische Lösung**

Das Problem muss also differenzierter begriffen und angegangen werden. Es trifft zwar zu, dass es sich *auch* um ein technisches Problem handelt; jedoch lässt es sich darauf nicht reduzieren. Daher ist auch die Lösung nicht rein technisch zu erzielen. Für die Erarbeitung von Lösungsansätzen muss davon ausgegangen werden, dass es sich um eine ebenso gesellschaftliche wie technische Aufgabe handelt. Techniken müssen demgemäß zwar eingesetzt oder gar neu entwickelt werden; diese können (in der Regel) das Vertrauensproblem jedoch nicht lösen, sondern uns lediglich dabei unterstützen, eine **Urteilskraft** auszubilden, um angemessen zwischen vertrauenswürdigen und nichtvertrauenswürdigen Personen und Aussagen zu unterscheiden. Dazu muss Vertrauen jedoch in einem Praxiszusammenhang begriffen werden, der sich daran zeigt

Die skizzierten unerwünschten Entwicklungen lassen sich unter folgenden Überschriften diskutieren:

- Desorientierung
- Gefährdung des sozialen Zusammenhalts und demokratischen Systems
- Machtverschiebungen im öffentlichen Diskurs
- Gefährdung von Beweisverfahren (polizeiliche Ermittlungen, Gerichtsentscheidungen)

Es wäre im VR6 außerdem zu klären, **welche positiven Entwicklungen** den nicht-intendierten und unbeabsichtigten Nebenfolgen möglicherweise gegenüberstehen, differenziert nach verschiedenen Nutzergruppen (Entwickler, Medien, Rezipienten). Eine explizite Beschreibung der intendierten Folgen (*benefits*) sollte den *unseens* gegenüber gestellt werden. *Benefits* könnten etwa sein: eine neue Form von Öffentlichkeit und Kommunikationsintensivierungen mit Folgen für sozialen Zusammenhalt, usw; auf technischer Seite die möglicherweise günstigere Film-, Bild und Audioproduktion; in künstlerischer Hinsicht die Entwicklung von neuen Ausdrucksformen, Stilmitteln oder gar ganzen Kunstgattungen in den darstellenden wie bildenden Künsten.[44]

Bei der Frage wie wir den hier skizzierten Vulnerabilitäten begegnen, muss das besondere Verhältnis zwischen Vertrauen, Verletzlichkeit und Technik beachtet werden. Wenn wir Vertrauen als akzeptierte Vulnerabilität verstehen (siehe *Begriffliche und epistemologische Einordnung),* stellt sich die Frage, ob ein auf den ersten Blick eventuell naheliegendes Ziel, Vulnerabilität komplett zu eliminieren, tatsächlich sinnvoll und/oder wünschenswert wäre.

Für viele Akteure in der digitalen Welt scheinen Vertrauensprobleme durch technische Anwendungen lösbar. Aktuell werden diverse Technologien entwickelt oder angeboten, die von dieser Annahme auszugehen scheinen:

Facebook will die Vertrauenswürdigkeit seiner Nutzer messen. Journalistische Recherchenetzwerke wollen algorithmenbasiert die Glaubwürdigkeit von Nachrichten prüfen. Im Rahmen eines von der EU geförderten Forschungsprojekts *(iBorderctrl)* wird unter anderem ein KI-basierter Lügendetektor entwickelt, der in drei Staaten (Griechenland, Lettland, Ungarn) getestet wird. Er soll die Vertrauenswürdigkeit von Personen, die in die EU einreisen wollen, messen und prüfen. Lange schon werden im Rahmen von Computersimulationen so genannte *trust games* durchgeführt, die die Erfolgsträchtigkeit unterschiedlicher Vertrauensstrategien messen. Entsprechendes zeichnet sich bereits auch für das hier beschriebene Phänomen ab.[45]

44 Siehe zumindest für den Einsatz von KI bei Multimedia-Produktionen in den Bildenden Künste die Werke von Gillian Wearing, etwa in ihrer Ausstellung im Cincinnati Art Museum: www.cincinnatiartmuseum.org/wearing . Ein Videoausschnitt demonstriert den Einsatz besonders anschaulich: https://player.vimeo.com/video/295991070 (abgerufen 20.11.2019)

45 Für die Enttarnung von DeepFakes siehe z.B.: TU München (2019): Software FaceForensics erkennt Fake-Videos am zuverlässigsten. Künstliche Intelligenz enttarnt Fake-Videos; Pressemitteilung der Technischen Universität München; 09.06.2019; www.tum.de/nc/die-

Allerdings muss genau geprüft werden, in welcher Hinsicht solche technischen Werkzeuge beim Aufbau von klugen Netzen des Vertrauens hilfreich sind.

## 3 Welche Stakeholder sind für ein Verständnis und ein Management der *Unseens* von besonderer Bedeutung? Welche wissenschaftlichen Wissensbereiche sind relevant?

Die Auswahl der Akteure kann sich am Raster der unter Punkt 4) skizzierten Perspektiven orientieren und entspricht der im Gesamtprojekt DiDaT angelegten und transdisziplinären Paarung von Wissenschaft und Praxis. Experten zur Bearbeitung der Fragestellungen könnten aus folgenden Bereichen kommen (wobei angesichts der Gruppengröße von 12 Personen Akteure mit übergreifendem Fachwissen bzw. mehrfachen Rollen bevorzugt sind):

- Schwerpunkt technische Perspektive: Experten für Künstliche Intelligenz, Deep Fakes, IT-Sicherheit, Zertifikatswesen, auch Datenwissenschaftler/ Bibliothekare
- Schwerpunkt gesellschaftliche Perspektive: Publizisten wie Journalisten, Verlagsinhaber, Blogger, Medienwissenschaftler; Juristen für Internetrecht, Datenschützer, Normungsspezialisten; auch Politiker
- Schwerpunkt philosophische Perspektive: Wissenschafts- und Technikphilosophen; Sozialtheoretiker
- Schwerpunkt ökonomische Perspektive: Wirtschaftswissenschafter; Akteure im Online Marketing, Product Information Management, Content-Plattformen, Anbieter von IT-Hardware und Software, die Verifizierungsprobleme lösen

Darüber hinaus ist die Einbindung von Stakeholdern denkbar, die Auskunft zu teilweise analogen Problem- und/oder Lösungsfeldern geben können. Die Parallelen zwischen einem „verschmutzten Informationsökosystem“ und der Verschmutzung unserer natürlichen Umwelt liegen nahe. Interessante Impulse könnten aber auch aus den Wirtschaftswissenschaften oder aus Buchhaltungsregularien (Basel III etc.) kommen, wo Systeme von jeher auf Resilienz gegenüber nicht gutwilligen Akteuren ausgerichtet werden.

Auch eine historische Betrachtung insbesondere von politischer Propaganda und Gegenmaßnahmen in unterschiedlichen Ländern und Gesellschaftssystemen wäre hilfreich und sollte idealerweise als Kompetenz im Kreis der Akteure vertreten sein.

Es ergibt sich folgende Matrix von Vulnerabilitäten und Stakeholdern. Dabei wird unterschieden zwischen Stakeholdern, die von einer Vulnerabilität besonders betroffen sind (B), und Stakeholdern, die diese Vulnerabilität lösen können (L), wobei diese Einordnung nur eine grobe Orientierung sein kann:

tum/aktuelles/pressemitteilungen/details/35501 (abgerufen am 20.11.2019);

| **Vulnerabilität →**<br>**Stakeholder ↓** | Technische Möglichkeit zur überzeugenden Fälschung von digitaler Realität | Herkunft und Vertrauens-würdigkeit von Information nicht mehr klar → Vertrauensverlust, Reality Apathy, Zynismus | Verlust der informatio-nellen Grundlage für funktionierende öko-nomische, soziale und politische Systeme | Gefährdung der Be-weisführung in Polizei und Justiz, Vertrauens-verlust in den Rechtsstaat |
|---|---|---|---|---|
| **Politik und Gesellschaft** | | | | |
| Politikentwickler und -entscheider, Verwaltungsentscheider | B | B,L | B,L | L |
| Einzelne Wähler / Bürger | B | B | B | B |
| Netzaktivisten, NGOs | L | L | B,L | |
| **Medien** | | | | |
| Journalisten, Blogger, Influencer etc. | B | B,L | B,L | |
| Medieninhaber, Chefredakteure | B | L | L | |
| Contentkuratoren und -aggregatoren Suchmaschinenbetreiber | L | B | L | |
| Betreiber sozialer Netzwerke | L | B,L | L | L |
| **Wissenschaft** | | | | |
| IT-Spezialisten, Kryptografen, Lösungsarchitekten | L | L | L | L |
| Medien- und Kommunikations-wissenschaftler, Psychologen | L | L | L | |
| Technikphilosophen, System-analytiker, Sozialtheoretiker | L | L | L | L |

| Vulnerabilität → / Stakeholder ↓ | Technische Möglichkeit zur überzeugenden Fälschung von digitaler Realität | Herkunft und Vertrauenswürdigkeit von Information nicht mehr klar → Vertrauensverlust, Reality Apathy, Zynismus | Verlust der informationellen Grundlage für funktionierende ökonomische, soziale und politische Systeme | Gefährdung der Beweisführung in Polizei und Justiz, Vertrauensverlust in den Rechtsstaat |
|---|---|---|---|---|
| Sicherheits- und Prüfinstitutionen Technikanbieter | | | | |
| Polizei, Verfassungsschutz, Rechtsprechung | B | B | B,L | B,L |
| Datenschutzaufsicht | L | L | | B,L |
| Vertrauenswürdige neutrale Instanzen (z.B. Prüfer, Zertifizierer) | L | B | L | L |
| Anbieter IT-Industrie Technik & Dienstleistungen | L | L | | |

## 4 Methodische Überlegungen zur Unterstützung von Kernaussagen

Zur Erarbeitung möglicher Antworten durchdringen wir gleichzeitig vier Perspektiven und führen sie zusammen:

1. Technische Perspektive:
   Was ist technisch machbar (jetzt oder in naher Zukunft)?
2. Gesellschaftliche, politische und rechtliche Perspektive:
   Was findet Akzeptanz? Was ist national/international wünschenswert, regulierbar und durchsetzbar? An welche Institutionen kann dies geknüpft werden?
3. Philosophische Perspektive:
   Welche Antworten sind hinsichtlich des von ihnen vorausgesetzten Verständnisses von Vertrauen/Vertrauenswürdigkeit, Wahrheit/Unwahrheit, Realität/Fiktion, Gewissheit, Bezeugung/Zeugenschaft, Wahrnehmung, Geltung, Legitimation und Beweis sowohl kohärent als auch anschlußfähig an die etablierte Sprachverwendung der medialen und politischen Öffentlichkeit?
4. Ökonomische Perspektive:
   Was ist finanzierbar, disseminierbar oder langfristig lohnend?

Es gilt die Hypothese, dass die grundsätzlichen IT-Voraussetzungen zur Beantwortung der Leitfragen im Wesentlichen bereits vorhanden sind und nicht im Rahmen des Projekts entwickelt oder gefordert werden müssen (siehe dazu Abschnitt 1).

Die Kombination eines ungewöhnlich breiten Spektrums von Akteuren aus Gesellschaft, Medien, Wissenschaft und Wirtschaft (vgl.

vorherigen Abschnitt) soll von Anfang an einen lebendigen Austausch von Wissen und die Generierung möglicher Lösungselemente ermöglichen. Gleichzeitig wird es dadurch möglich, die Folgen der aktuellen technischen und gesellschaftlichen Entwicklungen breitgefächert und konsequent zu Ende zu denken, ggf. mithilfe von Szenariotechniken. Dadurch wird zusätzlicher Handlungsdruck aufgebaut und ein späterer Ergebnistransfer vorbereitet.

Die Wirksamkeit und Sinnhaftigkeit von Lösungsansätzen soll anhand einer Reihe frühzeitig definierter **Test Cases** geprüft werden. Jeder Test Case beschreibt eine – bereits beobachtete oder auch konstruierte – problematische Situation, für die der Effekt eines Lösungsansatzes durchgespielt werden kann. – Beispiele: „Der gewählte Präsident eines einflussreichen Landes bestreitet offensichtliche Fakten und ermutigt Gewalt gegen kritische Journalisten“ oder „Ein Massenmedium stellt reißerische ‚Nachrichten‘ ohne Rücksicht auf deren Wahrheitsgehalt in den Vordergrund, um Aufmerksamkeit und Werbeeinnahmen zu generieren“ oder „Ein bestechlicher Politiker bestreitet die Echtheit von Videodokumenten und lässt gleichzeitig ein falsches Video seines politischen Gegners herstellen und streuen, in dem diesem abstoßende Aussagen in den Mund gelegt werden“ oder „Ein repressives Regime unterdrückt eine unabhängige Presse mit der Behauptung, sie würde ‚fake news‘ verbreiten“.

Mit der Formulierung von Test Cases wird frühzeitig ein Rahmen für die gemeinsame Arbeit und Diskussion gesetzt und ein Konsens zum Zielkorridor hergestellt.

**Bedarf für Vertiefungsforschung**

Es ist unklar, wie eine Infrastruktur für eine breit anerkannte, nicht staatlich beeinflusste Zertifizierung von Informationsquellen technisch aussehen könnte, insbesondere durch Reputationsträger und Autoritäten, die nicht bereits als „Marken“ aus dem Offline-Bereich bekannt sind. Die Vergabe von SSL-Zertifikaten für elektronische Signaturen kann ein Ausgangspunkt der Überlegungen sein, ist aber nur begrenzt übertragbar und hat zahlreiche Schwächen. Wichtig ist auch, dass eine anonyme (bzw. irreversibel pseudonyme) Kommunikation möglich bleibt. Zur Erarbeitung und prototypischen Demonstration technisch realisierbarer Vorschläge sollte Vertiefungsforschung im Umfang von **1 Personenjahr** eingeplant werden.

Dies kann auf insg. **1,5 Personenjahre** aufgestockt werden, um mehrere Informationsökosysteme parallel zu betrachten und Infrastrukturlösungen zuerarbeiten. Infrage kommen Informationsökosysteme wie die klassischen Nachrichtenmedien, Plattformen für nutzergenerierte Inhalte (Twitter, Facebook, YK, Wordpress, Medium etc.) sowie Fachpublikationen (auch in der Wissenschaft). Es können überdies weitere Ökosysteme herangezogen werden, um technologische Eigenschaften und Regulierungsmechanismen zu verstehen und ggf. durch Analogieschlüsse Handlungsmöglichkeiten für die Informationsökosysteme zu identifizieren.

Beispiele für dieses Umfeld sind App-Ökosysteme (Google, Apple), Datenökosysteme im Industrie-4.0-Bereich (z.B. Bosch IOTA), Zertifikatökosysteme (SSL klassisch bzw. mit CaCERT), Digitale Währungen oder Peer-to-Peer-Dateiaustausch-Ökosysteme (z.B. BitTorrent). Sinnvolle Unterstützung können auch Forschungen zur gesellschaftlichen Wirkung von Deep Fake-Videos sowie zur Evolution von Nachrichten im Internet liefern.

## 5 Erwartete Ergebnisse und Folgeinitiativen

**Im Rahmen des Vulnerabilitätsraums „Vertrauenswürdigkeit von Informationen im digitalen Raum“ erarbeiten wir im inter- und transdisziplinären Dialog konsensfähige und praktikable Antworten auf die oben beschriebenen Herausforderungen.**

**Mögliche Fragestellungen**: Wie können wir Informationsökosysteme so gestalten, dass ein faktenbasierter gesellschaftlicher, wissenschaftlicher und politischer Diskurs möglich bleibt? Wie sorgen wir dafür, dass ein Dialog und eine ggf. auch mühsame Konsensfindung attraktiver bleiben als das Verharren auf extremen Positionen? Welche Anreize für die Wahrheitsfindung und -verbreitung können wir schaffen? Wie kann auch künftig mündige politische Meinungsbildung ablaufen?

**Erste Arbeitshypothesen**: Als Gerüst für erwartete Ergebnisse, zur Planung der Akteursauswahl sowie für die ersten Dialogschritte im Vulnerabilitätsraum dienen die folgenden Arbeitshypothesen zur Gestaltung des künftigen digitalen Raums:

1. Bisherige primär technologische Gegenmaßnahmen gegen Fake News wie die KI-gestützte Untersuchung von Videos oder die internen Netzwerkaktivitätsanalysen großer Internetplattformen sind letztlich nur ein Wettrüsten mit immer besseren Fälschungswerkzeugen und –methoden und daher bestenfalls eine partielle Lösung.
2. Das Vertrauen in Informationen fußt fast immer auf dem Vertrauen in die Person/Institution, die sie verbreitet. Die Mechanismen zur Genese dieses Vertrauens (z.B. Andocken an den Augenschein in der realen Welt, Transfer, Crowdansätze etc.) sollten daher einen Schwerpunkt bilden. Die Frage ist, wie eine institutionelle Infrastruktur des Vertrauens aussehen könnte.
3. Es ist nicht ausgeschlosssen, dass es in einzelnen sozialen Handlungsbereichen zukünftig mehr Sinn macht, etablierte Beweisarten (z.B. Videobeweise) komplett zu ersetzen, d.h. alternative Strategien zu entwickeln, die helfen, Fakten von Fiktionen zu unterscheiden.
4. Auf technischer und regulatorischer Seite erscheinen Maßnahmen wie bspw. Mechanismen und Standards für die Rückverfolgbarkeit von Informationen (u.U. mit Offenlegungspflichten für große Internetplattformen), eine Zertifizierung von Quellen und Kuratoren in Anlehnung an die etablierte Vergabe von SSL-Zertifikaten etc. überlegenswert. Blockchain und andere Technologien mit Notariatsfunktion können eine unterstützende Rolle spielen (z.B. für fälschungssichere Fingerabdrücke und Zeitstempel). Grundlegende Werkzeuge zur elektronischen Verschlüsselung und Signierung sind seit vielen Jahren verfügbar und mathematisch abgesichert.

5. Die Auseinandersetzung „Anonymität vs. Pseudonymität vs. Klarnamen“ im Netz ist ein künstlich konstruierter Konflikt. Jeder der drei Ansätze ist in bestimmten Kontexten sinnvoll und muss für Menschen zugänglich sein. Die Verantwortlichkeit für eigene Inhalte ebenso wie für das Teilen von Fremdinhalten muss neu gedacht werden.
6. Der Nachweis einer Lüge genügt nicht. Gesellschaftliche Konventionen und andere Faktoren bestimmen den Umgang mit ertappten Lügnern (vgl. Trump vs. Relotius). Vgl. auch das Phänomen „Reality Apathy“. Wir benötigen eine pragmatische Auseinandersetzung zur Existenz „objektiver“ Fakten oder einer objektiven Wahrheit[46] sowie der Frage, inwieweit Wahrheit tatsächlich gewollt ist, auch mit Blick auf psychologische Mechanismen.
7. Gängige Geschäftsmodelle für Onlineinhalte – vor allem die Werbefinanzierung – stehen im Zielkonflikt mit Vertrauenswürdigkeit und müssen vermutlich weiterentwickelt bzw. ersetzt werden; gleichzeitig ist zu erwarten, dass nicht alle Lösungsvorschläge kommerziell tragfähig und stattdessen bspw. staatlich zu finanzieren sind. Letzteres wirft wiederum die Frage auf, inwieweit diese im Kontext repressiver Regime funktionieren würden.

**Diese Liste ist naturgemäß unvollständig und wird laufend verfeinert und ergänzt.**

46 unter Berücksichtigung der bereits vorhandenen philosophischen Erkenntnisse und Traditionen

DiDaT Grobplanung zum Vulnerabilitätsraum (VR) 06

# Annex:

# Vorschlag für Bewältigungsstrategien, vertiefte Ursachen-analyse und eine Konkretisierung der Vertiefungsforschung

Sebastian Hallensleben (VDE), Julio Lambing (VEZL), Andreas Kaminski (HLRS Universität Stuttgart)

## 1 Erster Entwurf von Orientierungen und Maßnahmen zur Innovation

In liberalen, rechtsstaatlich organisierten und demokratischen Gesellschaften versteht es sich von selbst, dass zu ihrem Funktionieren die Vertrauenswürdigkeit der für das Gemeinwohl relevanten Informationen gewährleistet sein muss. Die Bewertung der Vertrauenswürdigkeit von Informationen steht in einem engen Zusammenhang mit Frage ihrer Urheberschaft, selbst wenn diese Autorenschaft nicht soweit zurückgeführt werden kann, dass der Name, Aufenthaltsort oder andere private Charakteristika identifizierbar sind, denn auch das Recht auf Pseudonyme und Anonymität ist für ein liberales Gemeinwohl zentral. Die Polarisierung in den politischen und kulturellen Diskursarenen betrifft zunehmend nicht nur die Bewertung, sondern auch die Feststellung von Fakten;[47] neue soziotechnische Möglichkeiten der Täuschung scheinen diese Polarisierung daher zu verschärfen. Für das Kommunikationsklima sowohl in politischen Interessenauseinandersetzungen als auch bei erkenntnisorientierten Diskursen in Wissenschaft, Verwaltung und Kulturleben ist es jedoch bedeutsam, dass sie fair und verständigungsorientiert und nicht rein strategisch-instrumentell erfolgen. Zudem muss jede demokratische Gesellschaft naturgemäß darum ringen, die Urteilsfähigkeit der mündigen Bürger zu sichern und zu stärken. Wenn Vertrauen als akzeptierte Verletzbarkeit eine vernünftige Praxis sein soll,[48] dann muss individuell erlernt werden, wann es angemessen ist, zu vertrauen oder zu misstrauen. Etwas knapp und daher vielleicht zu apodiktisch formuliert: Vertrauen darf dann weder blind sein noch als bloß hilfreiche Fiktion (als eine nützliche Selbsttäuschung im Modus des „als ob“) betrachtet werden. Vor diesem sozialen

47 Jennifer Kavanagh, Michael D. Rich (2018): Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life; Rand Corporation: Santa Monica.

48 Vgl. zu evidentiellen und normativen Theorien von Vertrauen u.a. Richard Moran (2006): Getting Told and Being Believed; in: Jennifer Lackey und Ernest Sosa (Hg.): The Epistemology of Testimony; Oxford University Press,; S. 272–306. Paul Faulkner (1998): David Hume's Reductionist Epistemology of Testimony; in: Pacific Philosophical Quarterly Vol. 79, Nr. 4; S. 302–313. Paul Faulkner (2007): On Telling and Trusting; in: Mind ; Vol. 116, Issue 464; S. 875–902. Bernd Lahno (2002): Der Begriff des Vertrauens; Paderborn: Mentis Verlag. Olli Lagerspetz (1998): Trust: The Tacit Demand; Dordrecht: Springer Netherlands. Vgl. zur erforderlichen Vermittlung beider Perspektiven Andreas Kaminski (2017): Hat Vertrauen Gründe oder ist Vertrauen ein Grund? Eine (dialektische) Tugendtheorie von Vertrauen und Vertrauenswürdigkeit; in: Jens Kertscher und Jan Müller (Hrsg.): Praxis und 'zweite Natur' - Begründungsfiguren normativer Wirklichkeit in der Diskussion; Münster: Mentis Verlag: S. 121–139.

und normativen Hintergrund seien hier erste Ideen genannt, die zur Orientierung für die gesellschaftliche Entscheidungsfindung dienen können, um die aufgezeigten Vulnerabilitäten zu bewältigen und die gesellschaftliche Resilienz angesichts der neuen soziotechnische Täuschungsmöglichkeit zu stärken. Sie dienen als Ausgangspunkt zur Formulierung von *Sozial Robusten Orientierungen* (nach Roland Scholz), die dem vierfachen Anspruch genügen sollen, *verständlich* zu sein, dem Stand des akzeptierten, *wissenschaftlichen Wissen* zu entsprechen, *Erfahrungswissen mit Wissenschaftswissen* zu verbinden sowie *Unsicherheiten und Beschränkungen* zu benennen.49 Zur Operationalisierung dieser vier Orientierungen werden zudem soziotechnische Innovationen und Maßnahmen zur ihrer Lancierung skizziert. Sie alle sind vorläufig und lediglich als Diskussionsvorschläge gedacht, die durch die in dem Projekt DiDaT versammelten Stakeholder als auch durch die Unterzeichner noch genauer geprüft werden sollen.

**1) Die Rückverfolgung von einer Information zur Informationsquelle sollte gewährleistet sein.** Aus der begrifflichen Klärung des Verhältnisses von Vertrauenswürdigkeit und Zeugenschaft ergibt sich, dass mit letzterer eine konkrete Person gemeint ist, die einen Sachverhalt selbst dokumentiert hat oder (und das ist wichtig!) die die Richtigkeit ihrer Dokumentation bezeugen kann und dafür einsteht. Als vernünftiges Wesen muss diese Person als verantwortlich und als rechenschaftspflichtig für die Information gelten. In der technischen Dimension bedeutet das, dass z.B. ein Realitätstreue beanspruchendes Foto den unverfälschten Rohdaten einer ganz spezifischen Kamera verlässlich zugeordnet werden kann. Diese Zuordnung muss nach vernünftigen, hinreichenden Kriterien, die in der jeweiligen Kommunikationsgemeinschaft geteilt werden (Standards). Dafür müssen nicht nur Normungsprozesse für solche Standards in etablierten europäischen und internationalen Foren wie CEN / CENELEC, ISO, IEC, ITU usw. vorangetrieben werden Im Streitfall müssten (soziale) Medien dazu gebracht werden, diese Zuordnung gemäß diesen Standards zu leisten, was womöglich nicht nur gesetzlicher Verankerung bedarf, sondern auch Aufklärungsarbeit in der (digitalen) Öffentlichkeit und ein Werben unter zivilgesellschaftlichen Anspruchsgruppen.

**2) Die Informationsquellen brauchen eine Identität, ohne dass der bürgerrechtliche Anspruch auf Quellenanonymität gefährdet wird.** Das setzt wahrscheinlich eine soziale und technische Infrastruktur für Pseudonyme voraus. Dabei muss sichergestellt sein, dass eine natürliche Person je Medium/sozialen Netzwerk nur eine begrenzte Anzahl pseudonymisierter

49 Roland Scholz (2011): Environmental Literacy in Science and Society: From Knowledge to Decisions; Cambridge University Press: New York; S. 373-404

| | | | | | | |
|---|---|---|---|---|---|---|
| **Unseens (behandelt werden hier die „negativen unerwünschten Folgen“)** | Herkunft und Vertrauenswürdigkeit von Information nicht mehr klar | | Misstrauen und Rückzug aus dem konstruktiven demokratischen Diskurs | Desorientierung und erzwungene Unmündigkeit des Einzelnen (Vertrauensverlust, Reality Apathy, Zynismus) | Beeinträchtigung oder sogar Zusammenbruch review-basierter Plattformen, insb. in der Sharing Economy | Die Öffentlichkeit vertraut dem staatlichen Rechtssystem nicht mehr. |
| **Ursachen/ Kausalitäten/ Entstehungsprozesse der Unseens** | → Herkunft und Vertrauenswürdigkeit von Information nicht mehr klar | | | | | |
| | Erweiterte technische Möglichkeiten zur Fälschung | | | | | |
| | Schwere Erkennbarkeit von Fälschungen; nur mit immer ausgefeilteren Tools (Wettrüsten Erkennung<->Fälschung) | | | | | |
| | Überflutung und Schnelligkeitsdrang von Informationen | | | | | |
| | Erweiterte techn, Möglichkeiten zur schnellen Verbreitung von Informationen | | | | | |
| | Kommerzielle Anreize, bevorzugt skandalisierende, extreme und/oder emotional erschütternde Nachrichten zu verbreiten | | | | | |
| | Staatliche und nicht staatliche Akteure, die bürgerliche Öffentlichkeit, Politikbetrieb und Medienwelt destabilisieren wollen | | | | | |
| | Politische bzw. soziokulturelle Polarisierung in den liberalen Demokratien | | | | | |
| | Zahlreiche Menschen, die aus privaten, malignen Intentionen Falschinformationen verbreiten | | | Zahlreiche Menschen, die aus privaten, malignen Intentionen Falschinformationen verbreiten | | |
| **Maßnahmen möglicher sozio-technologischer Innovationen zur Mitigation** | Standards für die 1zu1-Zuordnung von Informationen zu einer Person/ Organisation als Urheber:<br>-> Normungsprozesse in etablierten Foren wie CEN, ISO, IEC, ITU<br>-> Gesetzliche Unterstützung der Standards<br>-> Öffentlichkeitsarbeit zum Sinn solcher Standards etablieren | - Nutzung vorhandener kryptografischer Funktionen in ID-Cards<br>- Erforschung alternative Blockchain-basierter Lösungen, wo staatlicher Vertrauensanker nicht akzeptabel ist | Protokolle und Reputationstools, zur Visualisierung der Vertrauenswürdigkeit eines Online-Akteur<br>- Implementierung umfangreicher Pilotprojekte<br>- Entwicklung/erforschung theoretischer Modelle für Online-Verhalten<br>Implementierung von Pilotprojekten (um der Öffentlichkeit Vorteile solcher Tools zu demonstrieren und um Optimierungsmöglichkeiten auszuloten) | | | Strafbarkeit für die absichtliche Erstellung und Verbreitung von Fälschungen, die nicht als Satire oder Fiktion erkennbar sind |
| | | | Entwicklung / Verbreitung von Alternativen zum "Gefällt mir"; Beispiele:<br>- "Gefällt mir" auf erfolgreiche Dialoge<br>- Online-Reputationsgewinne durch erfolgreiche Kompromissbildung | Bildungsprogramme zur Identifizierung von Erkenntnisbarrieren & Perspektivverzerrungen sowie zu Know-How, sich Informationen auf umsichtige und kritische Weise | | Etablierung von auch für Nichttechniker plausiblen Notariatsmechanismen |
| **Ziele** | In der (inter-)nationalen Kommunikationsgemeinschaft soll die Herkunft und die Vertrauenswürdigkeit für das Gemeinwohl relevanter Informationen gewährleistet sein | Gewährleistung der moralischen (nicht unbedingt der juristischen) Verantwortlichkeit bei der Urheberschaft von Informationen | Stärkung eines gesellschaftlichen Klimas zur fairen demokratischen Auseinandersetzung und erkenntnisorientiertem Diskursverhalten | Stärkung der Urteilsfähigkeit des mündigen Bürgers | | Gewährleistung der Nachvollziehbarkeit der Rechtsprechung und Aufrechterhaltung des Rechtfriedens |
| **Sozial robuste Orientierungen zum Umgang mit Unseens** | **Gesellschaftlich verfügbare und verbreitete Instrumente zur Rückverfolgung von Information zur Informationsquelle etablieren** | **Nachrichtenquellen müssen identifizierbar sein, ohne den bürgerrechtlichen Anspruch von Quellenanonymität zu gefährden** | **Aufbau und Verbreitung soziotechnischer Strukturen zur Förderung von Konsens und Kompromiss** | **Vertrauenswürdigkeit von Bezeugung für breite gesellschaftliche Gruppen verstehbar, reflektierbar, einsehbar und kritisierbar zu machen** | | **Rechtswesen, den Bedingungen des digitalen Zeitalter anpassen** |

Identitäten besitzt. Die Pseudonymisierung muss garantiert werden, damit sie vor dem Zugriff (auch vor dem Staat) zuverlässig im Sinne des Persönlichkeitsrechts geschützt ist.

Diese eineindeutige Zuordnung bedeutet also nicht die Möglichkeit zur Identifizierung im Sinne eines Klarnamens. Ob sich dafür die kryptografischen Funktionen von Personalausweisen oder Blockchain-basierten Lösungen so eignen50, dass das Recht auf Meinungsfreiheit und das Recht auf informationelle Selbstbestimmung nicht gefährdet werden, müsste geprüft werden.

**3) Um die Urteilsfähigkeit des mündigen Bürgers zu stärken, sollte die Vertrauenswürdigkeit von Bezeugung gesellschaftsweit verstehbar, reflektierbar, einsehbar und kritisierbar gemacht werden.** Natürlich bieten sich dazu schulische und erwachsenenpädagogische Bildungsangebote an, in denen man sowohl lernt, sich Informationen auf umsichtige und kritische Weise zu beschaffen als auch eigene Erkenntnisbarrieren und Perspektivverzerrungen zu identifizieren. Auch technische Hilfsmittel, die Vertrauenswürdigkeit mit Reputation verbinden, sind hilfreich – sofern man damit nicht der Versuchung erliegt wird, Vertrauen auf ein technisches Problem zu reduzieren.51 So sollten allen Teilnehmern des digitalen Öffentlichkeitsraums Protokolle und Reputationswerkzeuge zur Verfügung stehen, mit denen man bewerten und (grafisch, auditiv etc.) veranschaulichen kann, wie viel Vertrauen ein Online-Akteur verdient hat, jedoch so, dass die Sichtbarkeit unterschiedlicher Ansichten und Einschätzungen über einen bestimmten Akteur gewahrt bleibt. (Pilotprojekte könnten der Öffentlichkeit die Vorteile solcher Tools demonstrieren und zugleich eine Gelegenheit zu haben, Optimierungsmöglichkeitein auszuloten. Einsatzgebiete dafür könnten Online-Publikationen und Soziale Netzwerke sein, die auf lokale oder regionale Nachrichten Angelegenheiten beschränkt sind.) In wissenschaftlicher Perspektive korrespondiert dies mit der Anwendung und Entwickelung relevanter theoretischer Modelle für das Verhalten von unterschiedlichen Online-Akteuren voraus (z.B. z. aus der Spieltheorie). Ansätze, die eigene Urteilskraft zu reflektieren, können zudem daran ansetzen, die Evolution von Informationen einschätzen zu lernen.52 Aus der Biologie sind grafische Darstellungen von Nachfolgebeziehungen in Form Evolutionsbäumen bekannt. Ähnlich könnten zur Bewertung von Informationen (vielleicht automatisiert erstellte) Evolutionsbäume helfen, die ihren

50 Hinsichtlicher der Blockchain-basierten Lösungen müssen komplexe Fragen der Nachhaltigkeit beachtet werden, Siehe dafür Julio Lambing (2018): Sense of balance? Nachhaltigkeitspolitische Fragen an die Distributed Ledger Technologie und Smart Contract Systeme; Reflexionspapier zur Distributed Ledger Technologie (Nr. 2 – 10/2018); Hrsg. v. Verein zur Erforschung zukunftsfähiger Lebensweisen e.V.

51 Vgl. zur Darstellung bisheriger technischer Lösungsansätze und der Bewertung ihrer Leistungsfähigkeit: Andreas Kaminski (2019): Begriffe in Modellen. Die Modellierung von Vertrauen in Computersimulation und maschinellem Lernen im Spiegel der Theoriegeschichte von Vertrauen; in: Nicole J. Saam, Michael Resch und Andreas Kaminski (Hg.): Simulieren und Entscheiden. Entscheidungsmodellierung, Modellierungsentscheidungen, Entscheidungsunterstützung; Wiesbaden: Springer, S. 167-192.

52 Vorschlag aus dem Sociopolitical Advisory Board des Höchstleistungsrechenzentrum Stuttgart

Ursprung, ihre Selektion (werden sie rezipiert und weiterverbreitet oder nicht), die Variation (werden sie verändert) sowie ihre Stabilisierung in bestimmten Umwelten (in welchen Milieus gedeihen sie, wo sterben sie aus) darstellen.

**4) Es sollten soziotechnische Strukturen zur Förderung von Konsens und Kompromiss aufgebaut werden.** Sie können zugleich als Leuchtturmprojekte für die in den ersten drei Empfehlungsvorschlägen angedachten Anliegen und Instrumenten dienen. Dies könnte z.B. bedeuten, dass Alternativen zur weit verbreiteten "Gefällt mir"-Bewertungsfunktion für Online-Kommentierungen oder -Berichte entwickelt und implementiert werden – etwa die Möglichkeit, mit "Gefällt mir" nicht einzelne Posts zu kennzeichnen, sondern ganze Dialoge, die als gelungen betrachtet werden, zu bewerten. Zudem sollte die Möglichkeit bestehen, dass Online-Akteure sichtbare und digital verwertbare Reputation dadurch gewinnen können, dass sie an einer Kompromissbildung unter Akteuren beteiligt waren, die anfänglich gegensätzliche Ansichten vertreten haben. (Dies allerdings nur in Ergänzung zu anderen Bewertungsmechanismen, um keinen Anreiz für triviale Einigungen oder exzessiv radikale Einstiegspositionen zu geben und um in grundrechtlicher Perspektive „Unverhandelbarem“ keinen Raum zu geben. Eine geeignete Pilotanwendung könnte lokale oder fachspezifischen Arenen im digitalen Raum sein, in denen politische Entscheidungsträger mit Betroffenen diskursiv verhandeln.)

## 2 Erweiterter Vorschlag für Vertiefungsforschung

Im Rahmen des VR06 werden soziotechnische Lösungsansätze erarbeitet, die den beteiligten Stakeholdern sowohl aus Sicht der Praxis als auch aus Sicht der Wissenschaft plausibel erscheinen. Darüber hinaus wird es möglich sein, die rein technischen Komponenten dieser Lösungsansätze mit hoher Zuverlässigkeit einzuschätzen, insbesondere hinsichtlich ihrer Machbarkeit und ihres Umsetzungsaufwands, da für die erwarteten soziotechnischen Lösungsansätze voraussichtlich kein technisches Neuland betreten werden muss, sondern vorhandene technische Möglichkeiten verfeinert, neu kombiniert und in neuen Kontexten genutzt werden können. – Anders sieht es jedoch bei den nichttechnischen Aspekten der Lösungsansätze aus. Hier befinden wir uns sehr wohl im Neuland, insbesondere hinsichtlich der Nutzerakzeptanz und der Reaktion verschiedener Stakeholdergruppen auf diese Lösungsansätze. Daher ist es essenziell, dass die erarbeiteten Ergebnisse durch praktische Pilotierung geprüft und verfeinert werden.

Für den Gegenstandsbereich von VR6 sollten wir bedenken, dass es unklar ist, wie eine Infrastruktur für eine breit anerkannte, nicht staatlich beeinflusste Einschätzung von Informationsquellen aussehen könnte, insbesondere durch Reputationsträger und Autoritäten, die nicht bereits als „Marken“ aus dem Offline-Bereich bekannt sind. Die Vergabe von SSL-Zertifikaten für elektronische Signaturen kann ein Ausgangspunkt der Überlegungen sein, ist aber nur begrenzt

übertragbar und hat zahlreiche Schwächen. Wichtig ist auch, dass eine anonyme (bzw. irreversibel pseudonyme) Kommunikation möglich bleibt.

Es ist daher eine Vertiefungsforschung mit folgenden Schritten bzw. Elementen erforderlich:

- Prototypische Umsetzung eines Systems zur Vergabe pseudonymer Identitäten (idealerweise als Vorstufe einer umfassenden technischen Lösung, mindestens aber als ausreichend funktionsfähiger Demonstrator)
- Auswahl einer geeigneten Anwendungsnische mit ausreichender Interaktionsdichte sowie Experimentierbereitschaft der Nutzer (beispielsweise der Kommentarbereich eines Onlinemediums)
- Definition von Observablen anhand erwünschter und unerwünschter historischer Muster im Nutzerverhalten
- Partieller Roll-out und Beobachtung multipler Aspekte des Nutzerverhaltens, z.B. Verhaltensänderungen (Inhalte, Art der dialogischen Interaktion zwischen Nutzern etc.), Manipulationsversuche, Blasenbildung, Verhältnis von pseudonymen Identitäten gegenüber „herkömmlichen“, nicht verifizierten Nutzernamen etc.
- Beobachtung einer Evolution von Informationen
- Laufendes Nachsteuern des Prototyps zur explorativen Lösung auftretender Probleme. Dabei ggf. Anlehnung an Maßnahmen, die in der Vergangenheit in anderen Informationsökosystemen eingesetzt wurden (z.B. App-Ökosysteme (Google, Apple), Datenökosysteme im Industrie-4.0-Bereich (z.B. Bosch IOTA), Zertifikatökosysteme (SSL klassisch bzw. mit CaCERT), Digitale Währungen oder Peer-to-Peer-Dateiaustausch-Ökosysteme (z.B. BitTorrent)).
- Sondierung von Möglichkeiten zur Simulation des Nutzerverhaltens

Für die obigen Elemente ist Vertiefungsforschung im Umfang von **mindestens 1 Personenjahr erforderlich.** Darüber hinaus halten wir es für sinnvoll, parallel zur prototypischen Exploration die Forschung zur gesellschaftlichen Wirkung von Deep Fake-Videos sowie zur Evolution von Nachrichten im Internet voranzutreiben. Um dieses begleitende theoretische Umfeld zu schaffen, müsste die Vertiefungsforschung jedoch auf **insgesamt 1,5 Personenjahre** aufgestockt werden.

# Vulnerabilitätsraum 07 (VR07)

# Cybercrime/-security in Cyberspace und digitale Daten

## „Schwerpunktstaatsanwaltschaft als Bearbeitungsformat für Cybercrime-Delikte“

DiDaT Feinplanung für den Vulnerabilitätsraum 07 (VR07)

# *Cybercrime / Cyber Security*

*Eike Albrecht (BTU), Andriy Panchenko (BTU), Dirk Labudde (HS Mittweida), Pavel Gladyshev (UC Dublin), Dirk Marx (BTU), Dr. Heralt Hug (BTU / CMS Hasche Sigle Kanzlei Leipzig), Larissa Kätker (BTU), Marcel Mönch (BTU); Practice: Haiying Wu (Huawei), Dirk Nagel (Vodafone), Veselko Hagen (BTU), Bernhard Brocher (StA Cottbus), Bernhard Otupal (Dell)*

## 1. Gegenstand, Ziele und Leitfrage

Das Forschungsprojekt DiDaT (Laufzeit 11/2019 bis 10/2021) beinhaltet sieben Arbeitsgruppen als dementsprechende Vulnerabilitätsräume (VRs). Diese Teilbereiche des Gesamtprojektes spiegeln gesellschaftliche und funktionale Forschungsschwerpunkte wider. Dabei wird ein den VR bestimmender thematischer Rahmen und eine theoretische Struktur so aufgestellt, dass mit Hilfe einer Leitfrage transdisziplinäre Forschung möglich wird.

Ein solcher Forschungsprozess ist durch die Erstellung eines Grob- und eines Feinplans sowie der Anfertigung eines Weißbuches mit Hilfe von Vertiefungs- und Folgeforschung gekennzeichnet. Im Rahmen der hier vorliegenden Feinplanung erfolgt zunächst die Eruierung von *Vulnerabilitäten* und *Unseens*, aus denen in einem weiteren Arbeitsschritt sozial robuste Orientierungen im Sinne des Transformationsprozesses. Vertiefungsforschung und eine Td-Lab[53]-Folgeforschung ermöglichen einen besseren Überblick und tieferen Einblick zu unerwünschten Nebenfolgen, den Rebounds und verbessern damit das Erkennen von Unseens.

Die vorliegende Ausarbeitung ist daher die Grundlage für das Erkennen spezieller Herausforderungen im Bereich von Cybercrime und Cyber Security (vgl. Rechavi u. Berenblum 2018).

Eine zunehmende Bedrohung für die öffentliche Sicherheit und Ordnung stellt die Nutzung digitaler Systeme im Cyberspace dar, die die Begehung von Straftaten einerseits erst ermöglicht und andererseits einen anonymisierten und entpersonalisierten Rahmen zur Verfügung stellt, der möglicherweise zu unrechtmäßigem Handeln verleitet (vgl.Falk 2017; Lentner, 2019). Der Cyberspace (das Internet) muss heute schon alleine aufgrund seiner immensen Bedeutung für Wirtschaf und Gesellschaft geschützt werden. Solche Schutzmaßnahmen können jedoch von Kriminellen missbraucht werden, wenn z.B. Verschlüsselungsverfahren missbräuchlich genutzt werden, um den rechtmäßigen Benutzer auszuschließen. Dolose (arglistig, trügerisch) Handlungen (vgl.

[53] Td-Lab: Transdisziplinäres Laboratorium als virtueller Raum, der im Sinne der Transdisziplinarität Vernetzung von Wissenschaftlern mit Interessengruppen der Wirtschaft, Industrie, öffentlichen Verwaltung und Zivilgesellschaft ermöglicht (vgl. https://www.donau-uni.ac.at/de/universitaet/fakultaeten/wirtschaft-globalisierung/forschung/lab-sustainable-digital-environments.html, abgerufen am 07.01.2020)

Siepermann, 2017) und alle anderen unrechtmäßigen Ausführungen im *Cyberspace* erfordern im Rahmen der Zuordnung *Cybercrime und Cyber Security*[54] spezielle Antworten auf Fragen, die wegen der Dynamik im Internet teils noch gar nicht gestellt sind (vgl. Goeken u. Fröhlich, 2018). Basierend auf dieser Erkenntnis ist das präventive Handeln eine äußerst ernst zu nehmende Aufgabe, die nur dann erfolgreich bewältigt werden kann, wenn sie in Verbünden bearbeitet wird. Hierbei spielen Kooperationen zwischen Akteuren, die unsichere und auffällige Daten im Rahmen ihres Geschäftsmodelles nutzen, die zentrale Rolle (Kathuria, 2019; Nieborg, 2015). Außerdem ist es notwendig, die datentechnische Infrastruktur, das Datenmanagement sowie die Geschäftsabwicklungsmethoden (beispielsweise bei Banken) im Rahmen der Bearbeitung dieses Vulerabilitätsraums konkret zu analysieren (vgl. Conti, Dehghantanha, Franke u. Watson, 2018). Weiterhin müssen die aktuellen Möglichkeiten der Strafverfolgung mit den Mitteln des Strafrechts betrachtet und ggf. existierende Lücken in den Gesetzgebungen herausgearbeitet werden sowie eine Qualifizierung der Strafermittlungsbehörden zu ermöglichen.

Hervorzuheben ist ferner das Phänomen *«Darknet»*, welches sich auf der einen Seite als „zunehmende Bedrohung“ darstellt, weil die klassische Kriminalität, wie z. B. Waffen- und Drogenhandel, partiell in den Cyberspace als virtuellen und somit versteckten Raum verlagert wird. Auf der anderen Seite bietet das Darknet auch Schutz vor staatlicher Repression, beispielsweise in weniger demokratischen Systemen.

Generell ist hervorzuheben, dass neue Anforderungen an die Datensicherheit und hier gerade auch durch die Einführung von externen Cloud-Computing und einen damit erhöhten Datentransfer, gestellt werden. Dies gilt gerade vor dem Hintergrund der zunehmend globalisierten und grenzüberschreitenden Datenspeicherung und der damit einhergehenden Fragestellung, welche Rechtsnormen welches Landes anzuwenden sind.

Der Einsatz neuer Technologien bedarf daher rechtlicher Anpassungen auf nationaler und auch internationaler[55] Ebene verbunden mit dem Ziel, eine Anpassung von Organisationsstrukturen und eine Änderung von Verhaltensweisen herbeizuführen die *Resilienz* der Gesellschaft und des Staates gegen die nachteiligen Auswirkungen der Digitali-

[54] *Cybercrime* umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels dieser Informationstechnik begangen werden (BKA, 2018). *Cyber Security* befasst sich mit Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der klassischen IT-Sicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein (BSI, 2019). *Cybersafety* bedeutet Internetsicherheit und wird im Rahmen dieser Arbeit unter Cyber Security subsummiert. Denn Cybersafety scheint begrifflich eine private Internetnutzung anzusprechen und nicht eine professionelle, so wie es Cyber Security eher zugeordnet wird. Diese Begriffsabgrenzung ist unscharf und führt dazu, dass Cybersafety als Begriff eines alltäglichen Sprachgebrauchs verwandt wird und somit inhaltlich mit Cyber Security gleichgesetzt werden kann und aus Gründen der Klarheit auch muss.

[55] Cybercrime Convention Budapest 2001 (Übereinkommen über Computerkriminalität) – erste internationale Vereinbarung über mittels Internet oder sonstiger Computer begangener Straftaten: https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/185 (abgerufen am 16.11.2019)

sierung zu erhöhen. Dabei ist es erforderlich, «*socially robust strategies*»[56] im Rahmen dieses Teilprojektes durch die Identifizierung von Vulnerabilitäten zu entwickeln. Dieser dynamische Prozess hat Auswirkungen in den folgenden **Bereichen der Nutzung digitaler Daten** und kann regulatorische
oder bestrafende Wirkung zur Folge haben. Unter Einbeziehung Dritter (Vorschriften zur Vorratsdatenspeicherung) kann dies zur Verpflichtung einer Datenanalyse führen. Somit könnte z. B. von Banken erwartet werden, **Massendaten** ihrer Kunden so **auszuwerten**, sodass u. a. eine Verfolgung und Unterbindung von Geldwäsche durch die Strafverfolgungsbehörden gelingen kann.

Es ist eine **Neuorganisation** der Strafverfolgungsbehörden erforderlich, die aufgrund der digitalen Herausforderungen sowohl vor rechtlichen als auch forensischen neuen Herausforderungen stehen.[57] Es ist zu hinterfragen, wie sich Computer- und Systemnutzung durch *Digitalität* von Manipulation, Korruption bis hin zur Sabotage kritischer Infrastrukturen und anderer krimineller Aktivitäten im Cyberspace abgrenzen lassen.

Zwei weitere Nutzungsbereiche digitaler Daten sind **digitale Infrastrukturanbieter**, die den Ausbau der Hardware sicherstellen sowie die digitalen Serviceanbieter, die **Provider**, die die Software und Datenflusstechnik zur Verfügung stellen, bilden zwei weitere Hauptbereiche ab.

Es geht somit im Weiteren unter Einbeziehung dieser vier Hauptbereiche (Auswertung von Massendaten, Neuorganisation der Strafverfolgungsbehörden, digitale Infrastrukturanbieter und Provider) darum, dass unbeabsichtigte Nebenwirkungen (sog. *Unseens*; abgeleitet von: unintended side effects[4]) als *Nebeneffekte* zu erkennen und zu akzeptieren. Dazu gehört eine bewusste, gesellschaftlich ausgehandelte Akzeptanz von nachteiligen Auswirkungen, z.B., wenn die positiven Folgen überwiegen oder die nachteiligen Folgen nicht sehr schwerwiegend sind. Die technologischen Entwicklungsgeschwindigkeiten, die zu temporären und lukrativen Markterfolgen führen können, werden durch den Markt reguliert, was als weiterer Überprüfungsmechanismus dient hohe Geschäftsrisiken einzugehen.

Eine solch *profitable* Ambivalenz erfordert die Abwägung zwischen verschiedenen Rechtsgütern wie Freiheit vs. Sicherheit und Gesellschaftskonzepten, Selbstverantwortlichkeit vs. staatlich-gesellschaftlich organisiertem Schutz sowie einer Gewichtung und Regulierung des gesellschaftlichen- und unternehmerischen Verhaltens. Eine Basis zur Aushandlung von Akzeptanz, vor allem vor dem Hintergrund nicht vorhersehbarer und nicht gewollter Nebeneffekte, scheint es transparent noch nicht zu geben. Es geht eher um reaktives Verhalten, wobei die staatliche Regulierung hinter der Privatwirtschaft regelmäßig zurückbleibt, wie das bei der Einführung neuer Technologien zu beobachten ist. (vgl. Scholz, 2019).

Cybercrime-Angriffe auf digitale Infrastrukturen und digitale Daten sind regelmäßig

[56] DiDaT Newsletter 01, Februar 2019, www.iass-potsdam.de (abgerufen am 05.05.2019)

[57] https://www.computerweekly.com/de/definition/Computerkriminalitaet-Cybercrime

strafbar aber schwer nachweisbar. Denn *digitale Spuren* können flüchtig sein und werden nicht in allen Fällen mit dem für den klassischen Strafrechtsbereich geltenden Beweisanforderungen (vgl. Miebach, 2016) belegbar sein. Ein Lösungsansatz ist die Etablierung von Kompetenzen und Technologien bei den sich mit Cybercrime befassenden Ermittlungseinheiten und Staatsanwaltschaften. Als Beispiel hierfür ist die Schwerpunktstaatsanwaltschaft für Cybercrime in Brandenburg (Staatsanwaltschaft Cottbus) zu erwähnen. Anzumerken ist, dass die organisatorische Antwort auf diese neuen Herausforderungen auch über andere Modelle realisiert werden kann (Referenz: Vorarlberg in Österreich). In Deutschland stellen sich die Strafverfolgungsbehörden in den verschiedenen Bundesländern dem sich dynamisch ändernden Kriminalitätsphänomen „Cybercrime“ durch unterschiedliche organisatorische Antworten.

Ausgehend von einer Analyse der Vulnerabilitäten werden positive und negative Options- und Handlungsräume betrachtet, die soziale- und technische Innovationen (transdisziplinärer Prozess) für einen verantwortungsvollen Umgang mit *digitalen Daten* zu *Cybercrime* und *Cyber Security* ermöglichen.

Die **Leitfrage** dieser Feinplanung[58] des VRs lautet daher: *Ist der derzeitige Rechts- und Organisationsrahmen der Straf- und Ermittlungsbehörden geeignet, gegenwärtige und zukünftige Herausforderungen der Digitalisierung in verhältnismäßiger Weise zu erkennen, zu bewältigen und zu verfolgen?*

## Definitionsraum

*1. «Cybercrime»* umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne)[59] oder die mittels dieser Informationstechnik begangen werden (Computerkriminalität). Aktuell verbreitete Erscheinungsformen von Cybercrime sind gekennzeichnet durch die Infektion und Manipulation von Computersystemen mit Schadsoftware, z.B. um persönliche Daten und Zugangsberechtigungen des Nutzers abzugreifen und missbräuchlich nutzen zu können (Identitätsdiebstahl), darauf befindliche Daten/Dateien des Nutzers mittels sog. Ransomware zu verschlüsseln, um "Lösegeld" zu erpressen, sie "fernsteuern" zu können, in sog. Botnetzen zusammenzuschalten und für weitere kriminelle Handlungen einzusetzen.

*Zusammengefasst* lassen sich die o.g. Definitionsräume zu Cybercrime wie folgt ausformulieren: «Cybercrime im **engeren Sinne** sind Straftaten, die sich gegen das Internet,

[58] Die zuvor genannten Hauptbereiche (Auswertung von Massendaten, Neuorganisation der Strafverfolgungsbehörden, digitale Infrastrukturanbieter und Provider) werden im Rahmen der Vertiefungsforschung aufgegriffen.

[59] „Cybercrime im engeren Sinne bezieht sich gemäß dem Deutschen BKA auf spezielle Phänomene und Ausprägungen dieser Kriminalitätsform, bei denen Elemente der elektronischen Datenverarbeitung (EDV) wesentlich für die Tatausführung sind.“: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2011.pdf;jsessionid=A914451065D1D0C8E5F1ED18FDFDEA9A.live0612?__blob=publicationFile&v=3

Datennetze, informationstechnische Systeme oder Daten richten» und «Cybercrime im **weiteren Sinne**

sind Straftaten, die mittels Informationstechnik begangen werden»[60]. Die letztgenannten Delikte sollen im Rahmen der Feinplanung allenfalls sekundär behandelt werden, geht es doch bei ihnen um althergebrachte Straftaten, die lediglich unter Nutzung neuer technischer Möglichkeiten begangen werden. Somit sind unter den Begriff Cybercrime viele Delikte subsumierbar. Klassische Straftaten nach dem Strafgesetzbuch unterscheiden sich von solchen Delikten jedoch (teils gravierend) dahingehend, als dass durch die Begehung von Cybercrime-Delikten im globalen Netz (kaum wahrnehmbare) Landesgrenzen überwunden werden und sich dadurch anders gelagerte Problemstellungen im Zusammenhang mit der Strafverfolgung des Täters ergeben können.

*Tabelle 2: Grundlage für die Verfolgung von Cybercrime im engeren Sinne nach dem Strafgesetzbuch*[61]

| Straftatbestände | Inhalt (Kurzbeschreibung) |
|---|---|
| **§ 202a StGB<br>Ausspähen von Daten** | Das unbefugte Verschaffen eines Zugangs zu Daten, die nicht für den Täter bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung. |
| **§ 202b StGB<br>Abfangen von Daten** | Das unbefugte Verschaffen von Daten aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage unter Anwendung von technischen Mitteln. |
| **§ 202c StGB<br>Vorbereiten des Ausspähens und Abfangens von Daten** | Das Vorbereiten einer o. g. Straftat durch das Herstellen, Verschaffen oder Zugänglichmachen von Passwörtern, Sicherheitscodes oder Computerprogrammen, deren Zweck die Begehung einer solchen Tat ist. |
| **§ 202d StGB<br>Datenhehlerei** | Das sich oder einem anderen Verschaffen, Überlassen, Verbreiten oder Zugänglichmachen von nicht allgemein zugänglichen und durch einen anderen aus einer rechtswidrigen Tat erlangten Daten mit der Absicht, sich oder einen Dritten zu bereichern oder einen anderen zu schädigten. |
| **§ 263a StGB<br>Computerbetrug** | Das Schädigen des Vermögens eines Andern durch Beeinflussung des Ergebnisses eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf. Des Weiteren das Vorbereiten einer solchen Tat durch Herstellung, Verschaffung, Veräußerung, Verwahrung oder Überlassung eines Computerprogramms, dessen Zweck die Begehung einer solchen Tat ist. |
| **§ 269 StGB<br>Fälschung beweiserheblicher Daten** | Das Speichern oder Verändern beweiserheblicher Daten zur Täuschung im Rechtsverkehr, sodass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder das Gebrauchen solcher Daten. |
| **§ 303a StGB<br>Datenveränderung** | Das rechtswidrige Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten. |
| **§ 303b StGB<br><br>Computersabotage** | Das erhebliche Stören einer Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, durch<br>1. Begehung einer Datenveränderung (§ 303a),<br>2. Eingabe oder Übermittlung von Daten in der Absicht, einem anderen einen Nachteil zuzufügen,<br>3. Zerstörung, Beschädigung, Unbrauchbarmachen, Beseitigen oder Verändern einer Datenverarbeitungsanlage oder eines Datenträgers. |
| | |

[60] Differenzierung des BKA im Bundeslagebild 2016 zur Thematik „Cybercrime im engeren und im weiteren Sinne“

[61] BKA, Cybercrime – Handlungsempfehlungen für die Wirtschaft

*2. «Cyber-Raum»* Sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik mit darauf basierender Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen.[62]

*3. «DarkNet»: Anonyme Verbindungen, die nicht öffentlich zugänglich und somit z.B.* nicht von normalen Suchmaschinen auffindbar sind. Der Begriff wird häufig als Synonym für das Tor-Netzwerk verwendet[63], das Verbindungsdaten anonymisiert[64]. Der virtuelle Raum wird häufig für den Handel mit illegalen Waren (z. B. Falschgeld, Betäubungsmittel, Waffen, usw.) genutzt.[65]

## Ziele

Die Datenerhebung und -analyse (Datenzugriff, Datenauswertung) auf den Ebenen von Anwendern, Providern oder der Strafverfolgung (am Beispiel einer „Schwerpunktstaatsanwaltschaft", konkret in Cottbus) machen Herausforderungen in dreierlei Bereichen der Verwendung digitaler Daten und deren Auswertungen soweit kenntlich, dass folgende Arbeitsvoraussetzungen für diesen VR aufzustellen sind.

**(Arbeitsvoraussetzung 1)** Die Qualität der Ausbildung der „spezialisierten" Staatsanwälte und Cybercrime-Ermittler (z. B. BKA, LKAs) in digitaler Forensik muss schnell erhöht und dynamisiert werden. Dies ist erforderlich, um einerseits krimineller Aktivität mindestens auf Augenhöhe begegnen zur können, aber auch, um das Risiko der Nutzung elektronischer Systeme zu reduzieren.

**(Arbeitsvoraussetzung 2)** Ebenso muss das Spektrum aus Wissen zu Veränderungen der Tatorte, beispielsweise in Bezug auf hinterlassene Spuren und der Tathergänge im Cyberspace musterhaft und schnell vergleichbar dokumentiert werden.

**(Arbeitsvoraussetzung 3)** Bewegungen im DarkNet müssen in Echtzeit forensisch sicher analysiert werden können.

**(Arbeitsvoraussetzung 4)** Um das zu ermöglichen, müssen Aufgaben zur Cybercrimeabwehr zwischen systemrelevanten Unternehmen so verteilt werden, dass Wissen, Erstzugang, Manpower und Legitimation Eingang in die Forschung finden. Weitere forschungsvertiefende Ansätze dieses VR`s zur Tatüberführung ergeben sich aufgrund digitaler, forensisch begutachteter Spuren die als belastbare Beweise für die Verwendung einer Gesamtanalyse herangezogen werden können. Die Weitergabe digitaler Informationen systemrelevanter Unternehmen, etwa Kundendaten von Internet- und Mobilfunkprovider, aber auch von Banken und Versicherungen, die zur Unterstützung staatlicher Ermittlungsarbeit aber auch für präventive Zwecke verwendet werden, müsste auf der Grundlage eines gesellschaftlichen Aushandlungsprozesses zumindest öffentlich transparent sein.

Die bisherige Interpretation aller digitaler Spuren führt zu einer Tathergangseinschätzung durch die Staatsanwaltschaft, die nur mit hohem Aufwand oder mit zu geringem Erfolg hergestellt werden kann.

[62] Bundesamt für Sicherheit in der Informationstechnik, o. J.
[63] Vgl. *Golem Media GmbH*, o. J.
[64] Vgl. *Wikimedia Foundation Inc.*, o. J.
[65] Vgl. *Bundeskriminalamt*, 2018, S. 25.

In verschiedenen Lagebildern, Studien und Veröffentlichungen wird auf Folgen aus Cybercrime-Delikten hingewiesen.

Zentral ist im VR07 eine Analyse des «Kampfes» gegen Cybercrime unter besonderer Berücksichtigung der Verfälschung und missbräuchlichen Nutzung von *digitalen Daten sowie* deren Manipulationen. Dieser VR untersucht, welche nicht intendierten Nebeneffekte mit solchen Delikten einhergehen.

Im Rahmen dieser **Feinplanung** wird als erster Teilschritt die organisationsrechtliche Frage der Errichtung spezialisierter Schwerpunktbehörden am Beispiel der Schwerpunktstaatsanwaltschaft für Internetkriminalität im Land Brandenburg (StA Cottbus) analysiert und der anders organisierten Staatsanwaltschaft im österreichischen Bundesland Vorarlberg gegenübergestellt.

Dabei sind die folgenden analytischen Schwerpunkte zu untersuchen:

**(Arbeitsvoraussetzung 5)** Neuordnung von Organisationsstrukturen innerhalb der Staatsanwaltschaft und ihrer Instrumentarien zur Strafverfolgung in Kooperation auch mit anderen behördlichen Akteuren.

**(Arbeitsvoraussetzung 6)** Die Analyse und kritische Beurteilung geltenden Rechts als Voraussetzung für die Strafverfolgung in Deutschland und der EU.

**(Arbeitsvoraussetzung 7)** Ausbildung zur Anwendung und Durchsetzung des Rechts auf den unterschiedlichen Ebenen der Staatsanwaltschaft und deren Organisationsstrukturen. Durch Überführung von z.B. Handlungsempfehlungen zur *«Cyber Security»* wird eine Prävention insoweit möglich, dass zentrale Wirtschafts- und Finanzakteure, wie die Stakeholder der Grobplanung (Deutsche Bank, Vodafone und Huawei) eine relevante Aufgabe bei der Abwehr von Cybercrime zugewiesen bekommen. Darüber hinaus tragen sie im Rahmen der Kooperation (oder auch des Zwanges) mit der Staatsanwaltschaft dazu bei, durch gegenseitiges Feedback und fortwährendes Lernen ein *Handlungsspektrum* zu entwickeln in dem gemeinsame Anwendungen genutzt werden können. Zudem wird es den Unternehmungen ermöglicht, vorhandene und auch nur mögliche Vulnerabilitäten dabei selber zu erkennen, sodass man sich in die Lage versetzt sieht, konkrete Optionen zur Verbesserung des eigenen Geschäftsbereichs anzuwenden.[66] Aus einem Bericht von Risk Based Security geht hervor , dass 34 % der bekannten Vulnerabilitäten des ersten Halbjahres 2019 bis zum 23.08.2019 nicht behoben werden konnten[67]. Dieser Bericht verdeutlicht den Forschungsbedarf sowie die Schaffung von Handlungsangeboten in diesem Bereich.

Cyber Security und Cybercrime stehen in gegenseitiger Wechselwirkung, da Cyber Security sich grundsätzlich und regelmäßig

[66] „Das BSI publiziert in unregelmäßigen Abständen verschiedene Dokumente mit Hinweisen zu Themen der Cyber-Sicherheit. Dabei handelt es sich beispielsweise um Konfigurationsempfehlungen für Software-Produkte, Analysen von häufig verwendeten Angriffsmustern oder Hilfsmittel zur Detektion von Angriffen auf die eigene Organisation.“ https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/empfehlungen_node.html;jsessionid=C6EF59FA3225F81A6BD9C50259090FF2.1_cid341 (abgerufen am 23.10.2019)

[67] Halbjahresbericht: https://www.riskbasedsecurity.com

im Vorfeld mit der Thematik «Unseens» befasst. Cyber Security kann somit die Grundlage für die Beurteilung der Strafbarkeit von Dekikten im Cyberspace sein und kann darüber hinaus verschiedene Hilfsmittel zur Verfolgung von Cybercrime-Delikten bereitstellen.

**2. Welche nicht intendierten, unbeabsichtigten Nebenfolgen sind von Interesse und warum?**

*Box 1: Grundsatzerörterung zur Datenverwendung*

**1. Grundsätzliche Fragestellungen**

- Warum wird Cybercrime akzeptiert?
- Gelernte «evolutionäre» Hilflosigkeit? (Bedeutung: Nichts oder sehr wenig über das Problem oder die Problemlösung wissen?)

**2. Einstellung zum Cybercrime**

- Die Mehrheit ist davon überzeugt, dass „Cyberkriminelle“ nicht der Strafverfolgung zugeführt werden bzw. werden können
- Cyberkriminelle sind gesichtslos, anonym, da diese oftmals aus anderen Ländern kommen bzw. von dort aus operieren

**3. Recht – Rechtsgrundlagen (National und EU)**

- Aktuelles Recht (National und EU)
- Nationale Priorität in Bezug auf Cybercrime?!
- Strafbarkeit einzelner Delikte
- (Straf-) Gesetze beinhalten einen Schutzzweck. Dies können die menschliche Gesundheit, das Vermögen, aber auch die Sicherheit digitaler Infrastrukturen und Systeme sein. Wird dies auf den „Cyberspace“ übertragen, dann spräche man von den Computern/Servern/IoT (Internet of Things), die verletzlich sind oder sein könnten (also geschützte Rechtsgüter sein können?).

**4. Fehlende Rechtsgrundlagen, Beweismittel**

- Besondere Herausforderung:
  - Verlust von Beweismaterial im Cyberspace – meist nur temporär verfügbar (auch Cloud)
- Wo ist der Tatort? Ist das Delikt dort (geografischer Tatort) auch mit Strafe geahndet – subsidiäre Strafverfolgung (Erhebung des Kriteriums des deliktischen Schwerpunkts)?
- Mangelndes Unrechtsbewusstsein
- Cybercrime – konventionelle Straftaten:
  - Wirtschaftskriminalität
  - Waffen-, Drogen- und Menschenhandel
  - Im Internet organisierter politischer Extremismus
  - Das Verbreiten illegaler Inhalte im Netz
- Haftungsdilemma:
  - Apple Malware
  - Provider
  - Google-Play-Store

Um den mit der Internetnutzung einhergehenden unbeabsichtigten Nebenfolgen auf systematischer und inhaltlicher Ebene näherzukommen hilft es, die Grundsätze der

Box 1 aus Sicht der Bedürfnisse der Stakeholder zu betrachten.

Dabei werden dementsprechend unterschiedliche Datenverwendungen in den Fokus gestellt. Die Tabelle 2 zeigt die entwickelten „Unseens“ sowie die aus den Ursachen und Maßnahmen abgeleiteten sozial robusten Orientierungen.

### Unseens in Bezug auf digitale Daten

Cybercrime, insbesondere eine gesetzeswidrige Nutzung von digitalen Daten, beansprucht die Strafverfolgung in unterschiedlicher Qualität. Die Gründe hierfür liegen in der zunehmenden Professionalität der Täter sowie einer örtlichen Flexibilität, mit der Cyberangriffe verübt werden können.

Tatort und Taterfolgsort müssen nicht zwingend identisch sein und die Angriffe auf ausgewählte Ziele erfolgen zunehmend gut vorbereitet.[68] Die Errichtung von Schwerpunktstaatsanwaltschaften, wie etwa der StA Cottbus, ist ein Beispiel für eine organisationsrechtliche Reaktion im Feld der Strafverfolgung von Cyberdelikten. Ist die Schwerpunktstaatsanwaltschaft im Vergleich zu herkömmlich organisierten Staatsanwaltschaften, die ebenso Cybercrime-Delikte bearbeiten, bei der Strafverfolgung erfolgreicher? Spielen dabei noch andere Aspekte der staatsanwaltschaftlichen Arbeit und Sorgfalt eine Rolle? Ist eine Grenze zwischen der Bearbeitung von Cybercrime-Delikten in strafprozessualer Konkurrenz mit weiteren Delikten gezogen, oder werden bzw. können diese als „Hybrid-Delikte“ interpretiert werden? Tatsächlich ist festzustellen, dass derart gravierende organisationsrechtliche Vorhaben keinerlei empirischer Untersuchung erfahren haben.

[68] Vgl. Bundesministerium des Innern, für Bau und Heimat, o. J.

*Tabelle 3: Unseens, Ursachen und Maßnahmen zu sozial robusten Orientierungen*

| | 1. Unseens[69] | 2. Ursachen/ Kausalitäten/ Entstehungsprozesse der Unseens | 3. Maßnahmen möglicher sozio-technologischer Innovationen zur Mitigation | 4. Ziele | 5. Sozial robuste Orientierungen zum Umgang mit Unseens |
|---|---|---|---|---|---|
| | | **Kausalität aus Opferperspektive** | | | |
| 1 | Ausspähen von Daten | **Komplexität**<br>komplexe IT-Anlagen u. Software, falsche Konfiguration | **Präventive u. repressive Maßnahmen** | Verständnis, Awareness und Sicherheitslösungen schaffen (Updates und Anpassungen an neuste Entwicklungen); Zugang zu weiterentwickelten Produkten und Dienstleistungen erleichtern (Änderungsgeschwindigkeit) | **handeln und binden** |
| 2 | Abfangen von Daten | | | | |
| 3 | Vorbereiten des Ausspähens und Abfangens von Daten | **Vertrautheit**<br>Verwendung von allgemein zugänglichem Code, dessen Lücken bereits bekannt sind | **System-Kooperationen** | Verbünde schaffen und kritische Infrastrukturen (KRITIS) schützen | **verstehen** |
| 4 | Datenhehlerei | **Vernetzung**<br>je umfassender IT-Anlagen vernetzt sind, desto höher könnte das Risiko einer Verletzlichkeit sein, aber auch das Gegenteil ist denkbar | **Entscheidungsverlagerung** | Individuelle Handlungssouveränität schaffen | **umsetzen** |
| 5 | Computerbetrug | | **Cybersecurity**<br>Entwicklung eines IT-Grundschutzkatalogs (BSI) | Sensibilisierung und Vermittlung des IT-Grundschutzkatalogs (BSI) | **reagieren, schützen, abwehren** |
| 6 | Fälschung beweiserheblicher Daten | **Schlechtes Passwort-Management** | **Verlagerung von staatlichen Aufgaben auf Unternehmen / nicht staatliche Organisationen** | Entlastung der Staatsanwaltschaften und Behörden durch Datenverlagerung, Nutzung von externen Kompetenzen und Kapazitäten | **ausweichen** |
| 7 | Datenveränderung | **Fehler im Betriebssystem**<br>Gefahr der Infektion mit Viren, unerlaubter Zugang | **Digitale Forensik** | Spuren im Internet explorieren und zielgerichtet reagieren | **Forensisch analysieren**<br>neue Vollzugs- und Erfassungslogik durch forensische Analysen |
| 8 | Computersabotage | **Software-Fehler**<br>**Anwenderfehler**<br>die wohl größte Vulnerabilität dürfte der Anwender sein[70] | | | |

[69] Bundeslagebild Cybercrime 2018; Vgl. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2018.html

[70] Es gibt viele Definitionen von Verwundbarkeit:
(a) National Institute of Standards and Technology (NIST): Schwachstelle in einem Informationssystem, in den Systemsicherheitsverfahren, in den internen Kontrollen oder in der Implementierung, die von einer Bedrohungsquelle ausgenutzt oder ausgelöst werden könnte.

## 3. Welche Stakeholder sind von Bedeutung?

*Box 2: Erklärung der syllogistischen Struktur sozial-robuster Orientierungen im VR07*

1. Fragestellungen an Unternehmen als mögliche Stakeholder
   - Welche Missbräuche können Sie mit Ihren Mitteln identifizieren?
   - Handelt es sich bei den Auswertungsergebnissen um „Real-Time-Daten“ oder „Offline-Daten“?
   - Welche Maßnahmen kann das Unternehmen selbst und unmittelbar umsetzen? Sind diese Maßnahmen State-of-the-Art?
   - Verfügt das Unternehmen über ein Alarmierungssystem?
2. Verantwortlichkeiten
   - Grundsätzliche Frage:
     - Wer ist für den Schutz von was im Internet zuständig (Provider, Techniker, User)?
3. Wirtschaftsfaktor Sicherheit
   - Budgets für Cybersicherheit steigen (auch Auswirkungen als Folge der Datenschutzgrundverordnung)
   - Eigener Wirtschaftszweig
4. Paradigmenwechsel
   - Früher: Reaktionen auf Angriffe
   - Jetzt/Trend: Dynamische präventive Vorkehrungen im Rahmen von Cyber-Security. Angriff/Vorfall schnell erkennen und richtig darauf reagieren – Resilienz steigern
   - Man kann sich nicht vollständig vor Angriffen schützen – Reaktion (Zeit und Maßnahmen) sind wichtig!
     - Technische Vorkehrungen
     - Persönliche Sensibilisierung
   - Hack-back (moralisch und rechtlich vertretbar?)
   - Prävention statt Reaktion

Anhand der Beantwortung der Fragestellungen an Unternehmen, die in Box 2 enthalten sind, werden mögliche Stakeholder ausgewählt. Thematisch räumliche (an welcher Stelle im Internet findet einer *Spurenanalyse* statt) und inhaltliche (paradigmatische Nutzung des digitalen Raumes durch z. B. geschäftliche, private oder andere Inhalte/Daten) Zuordnungen können dabei systematisch erkannt werden. Eine konkrete Basis-Arbeitsgrundlage für die weitere Herangehensweise und Ergebnisermittlung wird mit den folgenden Verengungen der Fokusgruppe (Stakeholder) so dargestellt, dass *Unseens* optional im weiteren Verlauf sichtbar werden. Aufgrund der Diskussionen auf Stakeholderkonferenzen wurde eine Analyse über möglich „Unseens“ erstellt, die im Laufe der Arbeiten

(b) ISO 27005: Eine Schwachstelle eines Vermögenswerts oder einer Gruppe von Vermögenswerten, die durch eine oder mehrere Cyber-Bedrohungen ausgenutzt werden kann, wobei ein Vermögenswert alles ist, was für die Organisation, ihre Geschäftsabläufe und deren Kontinuität von Wert ist, einschließlich der Informationsressourcen, die die Mission der Organisation unterstützen.
(c) IETF RFC 4949: Ein Fehler oder eine Schwäche im Design, in der Implementierung oder im Betrieb und der Verwaltung eines Systems, die ausgenutzt werden könnte, um die Sicherheitsrichtlinie des Systems zu verletzen. https://www.upguard.com/blog/vulnerability (Zugriff am 01.01.2020)

im VR 07 zunehmen evaluiert und validiert wurden. Daraus resultiert eine Verschiebung der Vulnerabilitäten mit der Folge, dass anfangs zentrale Akteure nun eher nachgelagerte Bedeutung haben.

*Box 3: Gedanken zur Auswahl der Stakeholdergruppen*

Eine wesentliche Herausforderung von DiDaT besteht darin, sowohl auf der Seite der Praxis als auch auf der Seite der Wissenschaft ein ausgewogenes Spektrum von Repräsentanten zur Verfügung zu haben, welche die Interessens- und Wissensperspektiven angemessen vertreten. Um dieses zu gewährleisten und die Orientierungen des Weißbuches nicht wissens- oder wertemäßig zu verzerren, wird im Vulnerabilitätsraum eine sogenannte **"Unseens x Stakeholder-Tabellen"** erstellt (siehe S. 13). Diese soll nachvollziehbar machen, welche Perspektiven im Projekt direkt vertreten sind. Die Unseens beziehen sich in DiDaT auf als **negativ bewertete** (unbeabsichtigte Neben-) Folgen der Nutzung von digitalen Daten.
Bei der Identifikation, Beschreibung und Analyse dieser Unseens fließen somit normative Aspekte ein. Hierbei ist natürlich angemessen zu berücksichtigen, dass das, was von einer Seite als negativ betrachtet wird, von der anderen Seite **positiv gesehen** werden kann.
Um hier pragmatisch die wesentlichen Unseens zu identifizieren, wurden die Arbeitsgruppen in einem ersten Schritt angehalten, sich auf **Auswirkungen** der Digitalisierung, **welche zu Nachteilen oder negativen Veränderungen bei sensitiven Stakeholdergruppen oder in sensitiven Subsystemen der Bundesrepublik Deutschland führten**, zu beschränken. Bei dieser Erstidentifikation von Unseens wird nicht erwartet, dass relevante Stakeholdergruppen vollständig erfasst werden, da hier allein die Betroffenheit im Vordergrund steht. Deshalb erfolgt ein zweiter Schritt. Hier besteht die Möglichkeit, für jeden Unseen die davon **Betroffenen**, die **Verursacher** sowie die für einen Umgang mit dem Unseen relevanten Stakeholdergruppen (sog. **Regulatoren**) aufzulisten. In diesem Schritt können jedoch auch andere Perspektiven als Betroffene, Verursacher und Regulatoren in Betracht gezogen werden.
Zum Beispiel kann ein Ansatz gewählt werden, der sich auf die Stakeholdergruppen mit dem umfassendsten **Wissen** oder den stärksten **Interessen** bezieht. Dabei ist ein funktionalistisches wissens- und kompetenzbezogenes und ein **demokratisches, interessensbezogenes Vorgehen** zu unterscheiden (Mielke, Vermaßen u. Ellenbeck, 2017). **In DiDaT sollen die interessensbezogenen Perspektiven im Vordergrund stehen**. Im Grundsatz muss auf der Grundlage der erstellten Liste von Unseens auch eine gleiche Betrachtung der Repräsentation von Wissenschaftsgebieten vorgenommen werden. Um die Reliabilität und Balance der Interessen der Stakeholdergruppen in der Unseens x Stakeholder-Tabelle zu vergrößern, ist es sinnvoll, die Auswahl der zu betrachtenden Stakeholdergruppen von Vertretern verschiedener Stakeholdergruppen durchführen zu lassen bzw. einen diskursiven Prozess zur Bestimmung der jeweiligen Stakeholdergruppen vorzunehmen.

## Einbeziehung von Stakeholdern

Die Arbeiten von Mielke, Vermaßen und Ellenbeck (2017) zeigen, dass die Einbeziehung von Stakeholdern zu einer gängigen Praxis in inter- und transdisziplinären Forschungsprojekten geworden ist und dass es Gemeinsamkeiten gibt, wie diese durchgeführt werden sollten. Während ein breites Spektrum nicht-akademischer Akteure beteiligt ist, stehen Interessenvertreter aus Politik und Zivilgesellschaft im Vordergrund. Meistens werden die Stakeholder durch Workshops, Interviews oder kooperative Prozesse eingebunden. Bei der Betrachtung der methodologischen Ideale dient der Wissenschaftler hauptsächlich als Fazilitator (Moderator) des Dialogs. Das zu erlangende Wissen sowie dessen Verwendung basiert auf den Bedürfnissen und Werten der Stakeholder. Diese stimmen mit dem Hauptziel überein, die Perspektiven der von den Transformationen betroffenen Akteure in den Dialog zu integrieren oder zu inkludieren.

Wissenschaftler wollen mit der Einbeziehung von Stakeholdern ebenso die Wege für die Politik besser skizzieren. Die Befragten der von Mielke, Vermaßen und Ellenbeck durchgeführten Studie stimmten am stärksten darin überein, dass die Wissenschaft sich mit den gesellschaftlichen Bedürfnissen befassen und die Transformationen unterstützen sollte. Dennoch wurden die Unterschiede zwischen den Idealen der Wissenschaftler und ihrer Praxis in Bezug auf die Einbeziehung von Stakeholdern deutlich. Als Ergebnis der Befragung wünschen sich die Probanden richtungsweisende Maßnahmen auf politischer Ebene gleichwohl in Hinblick auf das eigene Pro-

jekt der Erfolg dieser Maßnahmen von vielen als gering eingeschätzt wird. Als Gründe hierfür wurden die zum Teil unterschiedlichen Erwartungen von Stakeholdern und Wissenschaftlern, mangelnder Motivation auf Seiten der Stakeholder, fehlende Finanzierung oder mangelnde Nachbereitung der Ergebnisse angeführt. Viele sehen auch einen Kompromiss zwischen ihren wissenschaftlichen Zielen und der Einbeziehung von Stakeholdern, da sie durch diese weniger Zeit finden, sich auf ihre akademischen Veröffentlichungen zu konzentrieren, sich über die wissenschaftliche Nutzbarkeit des gewonnen Wissens unklar sind und sich vor Beeinflussung und Abgabe wissenschaftlicher Autonomie schützen wollen.

Die Befragten gaben auch Verbesserungsbedarf an und hofften vor allem auf eine höhere Finanzierung, mehr Zeit und geeignetere Methoden. Diese Abwägungen und der Verbesserungsbedarf deuten auf einen Mangel an Konzeptualisierung in der Einbeziehung von Stakeholdern hin.

Da sich wissenschaftliche Praktiken und Konzepte im Laufe der Zeit ändern, sollten darüber hinaus die Auswirkungen auf Forschungsfragen, Codes, Sprache, Werkzeuge und Methoden, durch die ES besser reflektiert werden.

*Tabelle 4: Unseen x Stakeholder-Tabelle VR07*

| | Unseens (Unintended side effects; unbeabsichtigte Nebenfolgen der Nutzung digitaler Daten) | "Verursacher" | "Betroffene" | "Problemlöser /Regulatoren" |
|---|---|---|---|---|
| 1 | Ausspähen von Daten | z. B. systemrelevanter Anbieter | z. B. Endnutzer, vertreten durch die Bundesregierung | z. B. StA, Aufsicht |
| 2 | Abfangen von Daten | | | |
| 3 | Vorbereiten des Ausspähens und Abfangens von Daten | | | |
| 4 | Datenhehlerei | | | |
| 5 | Computerbetrug | | | |
| 6 | Fälschung beweiserheblicher Daten | | | |
| 7 | Datenveränderung | | | |
| 8 | Computersabotage | | | |
| | Als Verursacher, Betroffene und Problemlöser / Regulatoren kommen situativ folgende Stakeholder in Betracht: Staatsanwaltschaft (StA), Mobilfunkunternehmen, Unternehmensberatung, systemrelevante Anbieter (Banken), Systemausstatter und –ausrüster, Interpol, Zivilgesellschaft (z. B. CCC), Universitäten, Cybersecurity, Aufsicht (BSI & BfDI) | | | |

Tabelle 3 zeigt die Erfordernisse der Einbeziehung von Stakeholdern als Verursacher, Betroffene oder Problemlöser/Regulatoren, die somit in einem entsprechend besonderen Zusammenhang zu den Unseens stehen. Damit werden Verhältnisse prozessualer Beziehungsebenen einzelner Stakeholdergruppen und deren Vertreter zu digitalen Daten weiter aufgeklärt. Aus diesen Verhältnisse können die Themen der im nachfolgenden Kapitel beschriebenen Vertiefungsforschung abgeleitet werden.

Das derzeit geltende Recht scheint auf den ersten Blick in vielen Fällen keinen hinreichenden Vollzugsrahmen für Datenkriminalität zu haben. Zur Orientierung zu den Themen Cybercrime und Cybersecurity wurde in den Unternehmen aber auch bei

der Schwerpunktstaatsanwaltschaft ein erster analytischer Diskurs durchgeführt. Dabei hat sich gezeigt, dass ein Cyberabwehrzentrum bei der Deutschen Bank, das Cyber Security Transparency Center von Huawei in Brüssel sowie die Sicherheitseinrichtungen von Vodafone existieren.

Digitale Daten hinterlassen Spuren. Solche Spuren führen ggfs. zu Unseens, zu denen im Zuge der Td-Lab Folgeforschung weitere Erkenntnisse (Orientierungen) beigesteuert werden. Heute erfolgt eine erste Beurteilung zu beachtenden und weniger zu beachtenden Spektren von Anwendungen im Internet. Diese Nutzungen führen zu systematischen Herausforderungen, da Daten im Netz selber erstellt als auch von außen an das Netz herangetragen und als ***digitale Spuren*** gefunden werden können. Der bisherige Bezug zur Leitfrage wird mit Hilfe der Stakeholder-X-Tabelle und vor dem Hintergrund der Unseens weiter konkretisiert.

Erst Antworten auf Unseens ermöglichen es, robuste soziale Orientierungen und die dahinterliegenden Mechanismen offenzulegen.

Die noch mittels empirischer Daten durchzuführende analytische Betrachtung der Stakeholderperspektiven – hin zu den Vulnerabilitäten als Teil eines transdisziplinären Prozesses zur Verwendung von digitalen Daten mit dem klaren Bezug zu Cybercrime – würde zu erkennen geben, ob die bisherigen Zuordnungen der Stakeholder X Tabelle zutreffend sind.

## 4. Erwartete Ergebnisse und Folgeinitiativen als Vertiefungsforschung

Eine Herausforderung ist, die unterschiedlichen wissenschaftlichen und praktischen Ansätze zusammenzuführen. Eine Vertiefungsforschung als Schlussfolgerung dieses Feinplans erfolgt mit den VR07-Teilnehmern BTU (Forensic Sciences and Engineering), Schwerpunktstaatsanwaltschaft (StA Cottbus), UCD Dublin – DigitalFire Labs und Interpol Lyon. Dabei werden bilaterale und multilaterale Schnittmengen herausgearbeitet. Durch diese Vorgehensweise sollen Unseens komprimiert und so in den Fokus gestellt werden, dass diese eindeutiger zu identifizieren sind, als es bisher gelungen ist. Zur Auffindung der Vulnerabilitäten wurden in dieser Feinplanung Wenn-Fragen bearbeitet. Die dabei gefundenen Dann-Antworten stellen die Ergebnisse, die Basis dieser Forschungsarbeit und somit die erwünschte Arbeitsbasis zur empirischen Bearbeitung von Datennutzungen, Datenanalysen und Auswertungen bei der Schwerpunkt-Staatsanwaltschaft in Cottbus dar. Auf dieser Basis kann die Arbeitsgruppe des VR 07 Cybercrime/-security die nötigen Ergebnisse als Beiträge zum Weißbuch erarbeiten und darüber hinaus in Vertiefungsforschungsprojekten und in der Anwendung der Td-Labs einfließen lassen.

### Vertiefungsforschung *Cyber Security*

Eine notwendige Folge der Vertiefungsforschung zu Cyber Security ist die Analyse des ***DarkNet***, da in diesem Bereich die meisten ***kriminellen Aktivitäten als Dienste angeboten*** werden (Angriff als ein Service). Das DarkNet und das DeepWeb werden/sind gerade vor dem Hintergrund solcher

***Dienste*** ein besonderer Marktplatz für illegale Geschäfte.[71] Analysen dazu können helfen, das Ausmaß und die Vielfalt von Cybercrime zu untersuchen und besser zu verstehen[72]. Denn bei einer sog. Deep Packet Inspection (DPI) werden in Datenpaketen nicht nur Absender- und Empfängeradressen ausgewertet, sondern auch der Inhalt selbst. Das wiederum hilft, gezielte Maßnahmen zu erarbeiten, um solche Aktivitäten zukünftig durch Präventionsmaßnahmen und -strategien zu unterbinden (Cyber Security).

## Vertiefungsforschung *Cybercrime*

Die Kooperation zwischen der BTU (Studiengang Forensic Sciences and Engineering), der Hochschule UCD in Dublin/Ireland (Prof. Gladyshev) und Interpol in Lyon (Cybercrime) entfaltet vor dem Hintergrund des Projektes DiDaT eine *neue Perspektive*, die dazu einlädt, Vertiefungsforschung im VR07 wie folgt zu beginnen.

Der Wissensbedarf zum Thema "Digitale Forensik" ist in den Bereichen des Spurenbeweises sehr hoch. Bisherige Erkenntnisse aus diesem Bereich sind solche, die in Gerichtsverfahren den Verfahrensverlauf erfolgreich begleitet und zu einem entsprechend zuverlässigen Abschluss gebracht haben (Daten). Forensische Gutachten im digitalen Bereich und darüber hinaus in Bereichen der transdisziplinären Verständnisart ermöglichen es, einen dynamisch zu gestaltenden Lernprozess neuartig zu begründen. Das Tool für die Ausbildung von Staatsanwälten, Richtern und Ermittlern existiert bereits und erste Schulungen wurden im Rahmen der Arbeiten bei Interpol durchgeführt Es gilt eine erste *Vertiefungsforschung* im Hinblick auf Anwendbarkeit und Adaptierbarkeit, zusammen mit den vier Partnern (BTU, Schwerpunktstaatsanwaltschaft Cottbus, UCD und Interpol) unter dem Dach von DiDaT aktuell bis zum 15.12.2019 zu erreichen.

[71] Vgl. Bundeskriminalamt, 2018, S. 25

[72] Vgl. hierzu die Stellungnahme des Chaos Computer Club (CCC) an das Bundesverfassungsgericht zum BND-Gesetz und zur Ausland-Ausland Fernmeldeaufklärung, 1 BvR 2835/17, 11/2019

## Literatur

Banks, J. (2010): Regulating hate speech online, International Review of Law, Computers & Technology, 24:3, 233-239,

Bundesamt für Sicherheit in der Informationstechnik (o. J.): Cyber-Sicherheit. <https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html>, [Zugriff 2019-10-23]

Bundesamt für Sicherheit und Informationstechnik (o. J.): IT Grundschutz, Die Phasen des Sicherheitsprozesses. <https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchu-lung/OnlinekursITGrundschutz2018/Lektion_2_Sicherheitsmanagement/Lektion_2_02/Lektion_2_02_node.html>, [Zugriff 2019-10-23]

Bundeskriminalamt (2017): Cybercrime, Bundeslagebild 2017, S. 25.

Bundeskriminalamt (o. J.): Internetkriminalität/Cybercrime. <https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html>, [Zugriff 2019-10-23]

Bundesministerium des Innern, für Bau und Heimat (o. J.): Cyberkriminalität. <https://www.bmi.bund.de/DE/themen/sicherheit/kriminalitaetsbekaempfung-und-gefahrenabwehr/cyberkriminalitaet/cyberkriminalitaet-node.html> [Zugriff 2019-10-23]

Carraro, L., Castelli, L. (2011): Ideology is related to basic cognitive processes involved in attitude formation. Journal of Experimental Social Psychology, Vol. 47, Issue 5, S. 1013-1016.

Conti, M., Dehghantanha, A., Franke, K. & Watson, S. (2018). Internet of Things security and forensics. Challenges and opportunities. *Future Generation Computer Systems, 78,* 544-546.

Décary-Hétu, D., u. Dupont, B. (2012) The social network of hackers,
Global Crime, 13:3, 160-175,

Del Monte, A., Papagni, E. (2001): Public expenditure, corruption, and economic growth: the case of Italy. European Journal of Political Economy, vol. 17, issue 1, 1-16.

Ebert, H., Maurer, T. (2017): Cyber Security. In: Patrick James (ed.): Oxford Bibliographies in International Relations. Oxford University Press, New York.

Eckert, C. (2017): Cybersicherheit beyond 2020. Informatik-Spektrum 40 (2017), Nr. 2, S. 141-146.

Falk, M. (2017): Cyber Security. Der blinde Fleck auf der CEO-Agenda. Entscheidern fehlt das «Big Picture» in der Diskussion um Cyber-Risiken. www.klardenker.kpmg.de (abgerufen am 02.05.2019).

Freiling, F., Grimm, R., Großpiesch, K.-E., Keller, H.B., Mottok, J., Münch, I., Rannenberg, K., Saglietti, F. (2014): Technische Sicherheit und Informationssicherheit. Unterschiede und Gemeinsamkeiten. Informatik-Spektrum 37, Nr. 1, S. 14-24.

Godbole, S. (2016): From Information Security to Cyber Security. www.isaca.org (abgerufen am 02.05.2019)

Goeken, M., Fröhlich, M. (2018): Sicherheit im Cyberraum – Stand der Dinge, Herausforderungen, Lösungsansätze. IT-Governance 27, S. 3-9.

Golem Media GmbH (o. J.): Darknet. https://www.golem.de/specials/darknet/, [Zugriff 2019-10-23]

Kathuria, V. (2019). Greed for data and exclusionary conduct in data-driven markets. *Computer Law & Security Review, 35* (1), 89-102.

Lentner, G. M. (2019). *Comparative Legal Analysis on Digital Data as subject of the European/German, US-American and Hongkong Law*.

Mertens, P., Barbian, D., Baier, S. (2017): Digitalisierung und Industrie 4.0 – eine Relativierung. Springer Wiesbaden.

Miebach, K. (2016), § 261, Rn. 58 f., in: Knauer, C., Kudlich, H., Schneider, H. (Hrsg.), Münchener Kommentar zur StPO, Beck, München.

Mielke, J., Vermaßen, H., u. Ellenbeck, S. (2017): Ideals, practices, and future prospects of stakeholder involvement in sustainability science. Proceedings of the National Academy of Sciences, 114(50).

Nieborg, D. B. (2015). Crushing Candy. The Free-to-Play Game in Its Connective Commodity Form. *Social Media + Society, 1* (2).

Polizei (o. J.): Zentrale Ansprechstellen Cybercrime der Polizeien für Wirtschaftsunternehmen. https://www.polizei.de/Polizei/DE/Einrichtungen/ZAC/zac_node.html. [Zugriff 2019-10-23]

Pospisil, B., Gusenbauer, M., Huber, E., Hellwig, O. (2017): Cyber-Sicherheitsstrategien – Umsetzung von Zielen durch Kooperation. Datenschutz und Datensicherheit – DuD, Ausgabe 10.

Rechavi, A., Berenblum, T. (2018): The Scondary Global Market for Hacked Data, In: International Journal of Cyber Criminology, Open Access Journal.

Scholz, R. W., u. Kley, M. (2019): Stocks and Flows-based Stakeholder Analysis of Digital Data – Basic concepts, tools for analysis, data, and the role of digital data infrastructure providers. Kreuzlingen: STTM.

Siepermann, M. (2017): Stichwort «IT Security». In: Gabler Wirtschaftslexikon online. www. wirtschaftslexikon.gabler.de (Zugriff am 02.05.2019)

Von Solms, R., van Niekerk, J. (2013): From information security to cyber security. Computers u. Security, Vol. 38, 10/2013, S. 97-102.

Wikimedia Foundation Inc. (2019): Tor (Netzwerk). <https://de.wikipedia.org/wiki/Tor_(Netzwerk)> [Zugriff 2019-10-23]

Whitman, M., Mattord, H. (2012): Principles of Information Security. 4th ed., Boston


# Ende