Digitale Daten als Gegenstand eines transdisziplinären Prozesses

DiDaT
Leitungstreffen am 03. Dezember 2019

Zusammenstellung der überarbeiteten Grobpläne

IASS POTSDAM

DONAU UNIVERSITÄT KREMS

b-tu Brandenburgische Technische Universität Cottbus - Senftenberg

STIFTERVERBAND

Inhaltsverzeichnis

Zusammenstellung «Überarbeitete Grobpläne»

Vulnerabilitätsraum 01

Digitale Mobilitätssysteme und vernetzte Räume

DiDaT Grobplanung für Vulnerabilitätsraum 01

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.

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

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

A 4.1) Umweltzerstörungs-Brandbeschleuniger: Mehrverkehr und Emissionen durch Rebound Effekte

Die Digitalisierung im Mobilitätssektor könnte zu Rebound Effekten führen wie Mehrverkehr, zu negativen Umwelteffekten und einer Verschlechte-

[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."
https://akademie-der-polizei.hamburg.de/verschiedene-veranstaltungen/11592502/systemische-digitalisierung-a/

rung der öffentlichen Gesundheit (IT-Energieverbrauch, Schadstoffe, Lärm, Bewegungsmangel). Auch preisreduzierte Angebote (free oder flatrate Mobilität) können zu negativen Auswirkungen führen.

A 4.2) 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.

A 4.3) Verwundbarkeit durch Zunahme der internationalen Mobilität

Globale Frachtströme, Fernpendler in Arbeitsverhältnissen, Mobilie Nomaden.

A 4.4) 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:

A 8.1) 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,

A 8.2) 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)

A 10 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.

A 11) 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 Rechtsysteme	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. 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.

5. Erwartete Ergebnisse und Folgeinitiativen

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

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/

Vulnerabilitätsraum 02

DiDaT Groblanung zum Vulnerabilitätsraum 02

<<Gesundheit, Digitalisierung und digitale Daten im deutschen Gesundheitswesen>>

Heike Köckler, Lisa A. Rosenberger, Roland Scholz

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

1. Gegenstand (Was wird betrachtet?), Ziele und Leitfrage[5]

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 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 physischen und auch psychischen Faktoren bereit, ohne sicher zu gehen, dass diese in ihrem Sinne und 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 (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

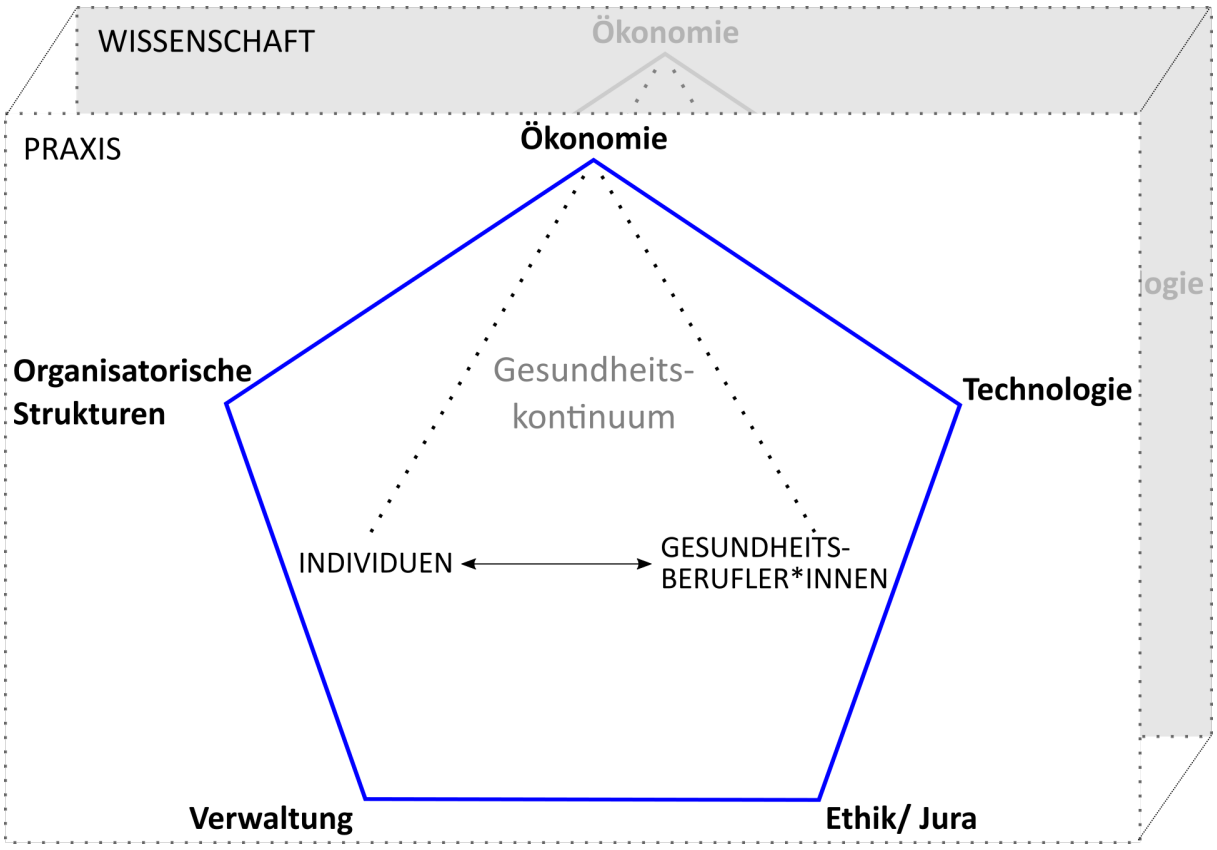
[5] Die positive und negative Wirkung der Digitalisierung im deutschen Gesundheitssystem wurde von den VR Gesundheit-Teilnehmern kritisch diskutiert und ist hier noch nicht ausgewogen beschrieben. Durch eine einseitige negative, oder einer einseitigen positiven Betrachtung besteht die Gefahr der Fehleinschätzung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

von Daten auf dem Endgerät der Individuen. Die Techniker 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 ePA auch unbeabsichtigte negative Effekte verbunden sein: Individuen können unter Umständen Arztbriefe nur unzureichend einordnen, die Digitalisierung kann in den einzelnen Praxen und Kliniken noch nicht ausreichend fortgeschritten 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 müssen zum Beispiel Lösungen entwickelt werden wie mit sensible Informationen in der Psychotherapie umgegangen wird, die entweder durch die Patient*innen oder die Ärzt*innen nicht protokolliert werden wollen. 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?*

Hierbei ist es das Ziel, unbeabsichtigte Nebeneffekte für das deutsche Gesundheitswesen zu systematisieren und 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 von der Rolle 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).

Begriffserklärung der Elemente des Systemmodells:

Individuen	Daten der Bürger*innen, Menschen, Personen, Patient*innen & Gesunden, sowie „Objekte der Rohdatenerzeugung“. Daten der Individuen beziehen sich zum einen auf digitale Informationen bzw. Messungen des Gesundheitszustands und zum Anderen auf die digitale Aufbewahrung von Gesundheitsdaten.
Gesundheitsberufler*innen	Daten der in Gesundheitsberufen Tätigen und Leistungserbringer*innen. Diese sind professionelle Datennutzer. Daten der Gesundheitsberufler*innen 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 (zB für Prävention und Diagnose) und dem Transfer digitaler Daten
Ethik/ Jura	Auf Daten und Gesundheit ausgerichtete Rechte und Pflichten der Individuen und Gesundheitsberufler*innen
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 Individuuum 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: Einschränkung der Möglichkeiten auf individuelle Entwicklung und Selbstbestimmung.

Gesundheitsberufler*innen:
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: Verlust der Qualität von Diagnostik und Therapie durch Einsatz von Algorithmen.

Forschungsmethodik:
Somit wären auch Forschende als eine sensitive Gruppe zu betrachten. Eine Datenmonopolisierung von Techunternehmen 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 den kontinuierlichen Daten über den Gesundheitszustand von Individuen verändert sich unser Verständnis von Gesundheit und Krankheit und müssen tägliche/ wöchentliche/ monatliche Fluktuationen erforscht werden um evidenzbasierte

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 Techunternehmen als Marktvorteil zur Konkurrenzfähigkeit genutzt (aber siehe auch www.patientslikeme.com). Diese Daten werden von den Techunternehmen (teilweiße) auch nicht aus Forschungsinteresse generiert (4P Kriterien - predictive, personalised, preventive, participatory).
Zudem bieten Algorithmen neue Analyseverfahren, die jedoch in ihrer Qualität bestehende Standards einer evidenzbasierten Medizin (randomisierte Kontrollstudien) nicht ersetzen dürfen.

UNSEEN: Epistemische Schwächen in Forschungsprozessen sowie Vernachlässigung der 4P Kriterien.

Ökonomie:
Die Generierung digitaler Daten kann durch die Nutzung digitaler Technologien bei Gesundheitsberufler*innen (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 Appentwickler und –betreiber auch eine Rolle.

UNSEEN: Verschlechterung der gesundheitlichen Versorgung durch eine auf ökonomische Effizienz gerichtete Digitalisierung

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 Gesundheitsapps, ist es aber nicht klar inwiefern diese auch tatsächlich bei der Prävention, Diagnose und Behandlung von Gesundheitsberufler*innen genutzt werden. Es besteht die Möglichkeit, dass die Integration der Gesundheitsapps in die berufliche Praxis der Gesundheitsberufler*innen 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 Gesundheitsberufler*innen ersetzen, und diese in Konkurrenz miteinander 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: Die gesundheitliche Versorgung wird durch die Nutzung von Apps verschlechtert, da deren positive Wirkung noch nachgewiesen werden muss.

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, Gesundheitsberufler*innen, 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 die Gefahr eines informatorischen Overflows der Gesundheitsberufler*innen beim Arztbesuch, welcher die Individuen – Gesundheitsberufler*innen Beziehung 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 Gesundheitsberufler*innen zu kommunizieren.

UNSEEN: Datenmissbrauch und Einschränkung des Rechts auf informationelle Selbstverwaltung.

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 Gesundheitsberufler*innen von den Unternehmen Zugang zu beiden Arten von Daten um diese für Diagnose oder Forschungszwecke nutzen zu können?

UNSEEN: Datenmissbrauch und Einschränkung des Rechts auf informationelle Selbstverwaltung und Selbstbestimmung.

Gesundheit:
Die Nutzung digitaler Medien hat ein hohes Suchtpotential (Andreassen, 2015). Es ist nicht klar inwiefern dies innerhalb von Gesundheitseinrichtungen und –behörden in Deutschland anerkannt wird und was für Gegenmaßnahmen erforscht beziehungsweiße angewandt werden.
Zusätzlich besteht die Möglichkeit, dass sich unser Verständnis von Gesundheit durch die kontinuierlichen Datenströme (siehe Beschreibung Forschung) verändert.

UNSEEN: unbalancierte Nutzung digitaler Medien macht krank.

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

UNSEEN: Technologieunternehmen verändern Rollenverteilung 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
Stakeholdergruppen			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		
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. 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 Gesundheitsberufler*innen – Gesundheitstechnologien)
- Besteht ein informatorischer Overflow bei Gesundheitsberufler*innen durch Dr.Google Verhalten der Individuen (Qualitätserkennung der Informationsquellen, Kommunikationsveränderung mit Gesundheitsberufler*innen)
- Systemveränderungen und Aufgabenverschiebung durch Techunternehmen im Gesundheitssystem

Technikfolgenabschätzung für ausgewählte Digitalisierungsprodukte – und prozesse
Systematisierung von Einzelelementen.
Case-based Learning

5. 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 (TK und einer weiteren Kasse) aus Sicht von Individuen, Ärzten sowie KV 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 Gesundheitsapps, 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.
- …

Literatur

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/

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

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).

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.

Vulnerabilitätsraum 03

KMU, Digitalisierung und Digitale Daten

DiDaT Grobplanung für Vulnerabilitätsraum 01

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 Inputs von

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

15.10.19 (Überarbeitung)

5. 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)6, 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 hinsichtlich 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).

[6] 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.

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.

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

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

	Vulnerabiltätsräume (abgleitet aus dem Mehrebenen-Modell)			
	Rahmen-Akteure	Markt-Akteure	Organisationale Akteure	Human Ressources
Trends: Threats/Opps (Ergebnis aus den Round Tables)	1 Neue, als Behinderung empfundene gesetzliche Regeln (DGVO)	4 Sharing Economy (Uber, AirBnB)	9 Umbau der Orga	10 Neue/andere Mitarbeiterqualifikation (auch in IT-Systemhäusern)
	2 Online Handel Plattformen (Amazon)	5 Industrie 4.0 Produktions-netzte	4 Sharing Economy (Uber, AirBnB)	11 Human Ressources surveillance (u.a. Kontrollangst der Mitarbeiter)
	3 Abhängigkeit von der Cloud (in Produkt, Preis, etc.)	6 IoT-isierung (system of systems)	5 Industrie 4.0 Produktions-netzte	
		7 Big Data Analytics	6 IoT-isierung (system of systems)	
			7 Big Data Analytics	
			8 Von „Lean Production" zu „Lean Collaboration	
	12 Datenhoheit			
	13 Surveillance Power			

Digitale Daten, Algorithmen und digitale Netzwerke als tragende Grundstruktur
(Digitale Grundstruktur)

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 be-

sitzt 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 soziotechnologischen 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.

6. 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[7]. 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

7. Welche Stakeholder sind für ein Verständnis und ein Management der „Unseens“ von besondererBedeutung? 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 Colla-boration" (agility based short time collaboration)*				Untern-Berater IT-Berater Strategie-Berater		
9. *Umbau der Organisation*			IHK	Untern-Berater		
10. *Neue/andere Mitarbeiterqualifika-tionen*			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 • IT-Systemhäuser und Unternehmensberater
	• IT-Infrastruktur-Provider	• Alle KMU, je kleiner desto eher abhängig	• Nationale und kleine Cloud-Anbieter • IT-Systemhäuser und Unternehmensberater
Repräsentanten	• NN	• Lothar Probst (IHK)	• Dr. Wolfgang Hofmann (Systemhaus) • NN

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

Stakeholder im Aktionsfeld „Organisationale Akteure“			
	Verursacher	**Betroffene**	**Problemlöser**
	• Plattformen • Automatisierer, KI-Provider • IT-Systemhäuser • IT-Provider • Unternehmenskunden	• Alle KMU insbesondere produzierende KMU im B2B	• Strategische Organisationsentwickler • Coaches und Trainer • IT-Systemhäuser und Unternehmensberater • Wirtschaftsverbände • Gewerkschaften
Repräsentanten	• Dr. Wolfgang Hofmann (Systemhaus) • NN	• Lothar Probst (IHK)	• Dr. Wolfgang Hofmann (Systemhaus) • NN

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

Noch fehlende Repräsentanten	• **Plattformen** • **IT-Infrastruktur-Provider** • **Automatisierer** • **KI-Provider** • **Topmanager**		• **Wirtschaftsverbände** • **Gewerkschaften**

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

8. 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.

9. 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

Landwirtschaft, Digitalisierung und digitale Daten

DiDaT Grobplanung für Vulnerabilitätsraum 04

Landwirtschaft, Digitalisierung und digitale Daten

Jana Zscheischler (ZALF), Elisabeth Behrens (NABU), 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)

10. 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[8]), 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[9] 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 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.

[8] 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.

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

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.[10]

Dazu bedarf es geeigneter gesellschaftlicher und gesetzlicher Rahmungen.[11]

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 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?

[10] 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).

[11] 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.

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” [12] lauten:

- Von welchem (negativen und positiven[13] 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?

[12] Hier geht es um die Qualität und Rückverfolgbarkeit der Argarprodukte (dies schliesst die Voraussetzungen für eine individualisierte Ernährung)

[13] Das Projekt DiDaT zielt auf den verantwortungsvollen Umgang mit Daten. Vor diesem Hintergrund stehen die Risiken und Vulnerabilitäten in DiDaT im Vordergrund.

11. 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 Nutzung digitaler Daten in der landwirtschaftlichen Produktionskette 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[14] 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 Land-

[14] 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.

wirtschaft von Gross-/Megabetrieben in Pflanzenbau und Tierproduktion.[15] 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.[16] [17] 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.

- **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.[18]

- **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

[15] 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.

[16] 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.

[17] 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.

[18] 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.

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.

- **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.

12. **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”	
	Repräsentanten von Stakeholdergruppen in DiDaT	Buitkamp (VDMA)		DLG			
1	Ökonomische Optimierung zu Ungunsten ökologischer Funktionen						
2	Beschäftigung und Akteursvielfalt im ländlichen Raum						
3	Marktkonzentration/ Datenrechte						
4	Wissensverlust						
5	Vollautomatisierung (Abhängigkeit und Manipulierbarkeit)						

6	Verlust an Wertschöpfung durch hohe Transparenz			
7	Ernährungssicherheit			

13. 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.

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

1. 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.

2. 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[19] sowie der Frage, inwieweit Wahrheit tatsächlich gewollt ist, auch mit Blick auf psychologische Mechanismen.

3. 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.

[19] unter Berücksichtigung der bereits vorhandenen philosophischen Erkenntnisse und Traditionen

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

Vulnerabilitätsraum 05

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

DiDaT Grobplanung für Vulnerabilitätsraum 05

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

Cornelia Sindermann (Universität Ulm), Felix Ebner (mecodia), Hanna Gleiss (Das NETTZ/BETTERPLACE LAB), Christian Montag (Universität Ulm), Lisa-Maria Neudert (Oxford University), Roland. W. Scholz (Donau Uni Krems), Leena Simon (Frieda Frauenzentrum – Anti-Stalking-Projekt), 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) • Professional network sites (e.g., LinkedIn, IBM's Beehive) • Chatboards & discussion fora • Social/Casual games (e.g., Farmville) • Wiki "Talk" pages • Tinder • Instagram • Wanelo • Yik Yak	• Online news services (e.g., *NYT* online, PerezHilton.com) • Wikipedia • Skype • Netflix • E-mail • Online news • SMS/Texts • Oovoo • Tumblr • Whisper

1.2 Ziele und Leitragen

Soziale Medien und Messengerapplikationen 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 Messengerdienst WhatsApp. Zusammen haben die drei Hauptprodukte 2,7 Milliarden angemeldete Nutzer*innen, wovon 2,1 Milliarden jeden Tag in einem der Dienste aktiv sind.[20] 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 Monetarisierungsmodell 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

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

dem Individuum helfen. Zudem sollen die Orientierungen helfen, soziotechnische Innovationen zu entwerfen. Die Orientierungen

sollen auch bezüglich gesetzlicher und gesellschaftlicher Regelungen 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.[21]

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/be-

[21] 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 Verhalten(smustern) der Einzelnen und ihrer Interaktion ergeben. Gleichermaßen nicht im Mittelpunkt stehen die spezifischen gesellschaftlichen Prozessen, Institutionen, demokratischen Abläufen 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.

wusste Meinungsbeeinflussung (Irreführung) im politischen und kommerziellen (Konsumenten-verhaltens-) Bereich.[22]

Werteperspektiven

WERTEPERSPEKTIVE (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)[23]

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.

[22] 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.

[23] 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“***[24]. 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 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

[24] 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/).

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.

WERTEPERSPEKTIVE (II): Soziale Medien und Demokratiefähigkeit

Demokratierelevante Aspekte aus der Sicht einzelner Bürger

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***“[25] (Vortkamp, 2013) ermöglichen. In der Rolle des „Bürger-Sein“ werden individualistische und egoistische Partikularinteressen mit sozialen Motivationen und einer Orientierung 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

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

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: Vulnerabilitäts/Unseen x Stakeholder Tabelle

			Stakeholder								
			Betroffene			Verursacher			Regulatoren		
Digitale Bedrohungen durch soziale Medien		Übernutzung	„Unregulierte“ soziale Medien -Nutzer	Soziales Umfeld Betroffener	Berufliches Umfeld Betroffener	Deutsche Internet-kultur	Social Media Provider		Thera-peuten	„LFK“	
	Digitale Gewalt	Hate-Speech									
		Cyber-Trolling									
		Cyber-Mobbing									
		Cyber-Stalking									
		...	Opfer	Soziales Umfeld der Opfer		Täter			Social Media Provider	Gesetzgeber	Therapeuten
	Reality-Shift		Jeder Nutzer von sozialen Medien	„Dumme“ Löschresistente		Deutsche Internet-gemeinschaft und -kultur	Social Media Provider	Politische, wirtschaftliche Akteure und Influencer	Politik und Gesetz-geber	Das geschulte Individuum (Bildungs-ämter)	
	(digitale soziale Kompetenzen)										
Auswirkungen											
	Wohlbefinden und Gesundheit										
	Demokratiefähigkeit										

4. Methodische Überlegungen zur Unterstützung von Kernaussagen

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.

5. 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

Vertrauenswürdigkeit und Zuverlässigkeit digitaler Daten und Informationen

DiDaT Grobplanung für Vulnerabilitätsraum 06

Vertrauenswürdigkeit und Zuverlässigkeit digitaler Daten und Informationen

Sebastian Hallensleben (VDE Frankfurt), Julio Lambing (Blockchain-Nachhaltigkeit)

14. Gegenstand, Ziele und Leitfrage

Wie können die Zuverlässigkeit digitaler Informationen sowie IT-gestützte Vertrauensinfrastrukturen in naher Zukunft[26] in Deutschland so gestaltet werden, dass ein fakten- und wertebasierter[27] 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 Verifizierung von Fakten unterstützt?

Wie kann auch künftig mündige politische Meinungsbildung ablaufen? Welche Anreizsysteme können vorgeschlagen werden, mit denen Wahrheitsfindung und -verbreitung präferiert werden? – Der Fokus liegt dabei auf der Information, unabhängig davon, wo sie im digitalen Raum vorliegt. In Abgrenzung zu VR05 betrachtet VR06 also nicht (oder nur am Rande) die Funktion und Struktur spezifischer Bereiche des digitalen Raums (z.B. Soziale Medien, klassische Nachrichtenmedien, Plattformen für nutzergenerierte Inhalte oder Fachpublikationen), sondern abstrahieren zur Information an sich sowie deren ursprünglicher Quelle. Es gilt die Hypothese, dass die grundsätzlichen IT-Voraussetzungen hierfür im Wesentlichen bereits vorhanden sind und nicht im Rahmen des Projekts entwickelt oder gefordert werden müssen.

Hintergrund: 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[28],[29],[30]) 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

[26] Zeithorizont ca. 5 Jahre
[27] „Werte“ meint hier v.a. Konsistenz, Verantwortung, und Veränderungsoffenheit.
[28] https://gizmodo.com/researchers-come-out-with-yet-another-unnerving-new-de-1828977488
[29] https://www.theregister.co.uk/2018/09/11/ai_fake_videos/
[30] https://www.youtube.com/watch?v=gLoI9hAX9dw

kann während des Programms gesteuert werden. Auch überzeugende „Fotos“ nichtexistenter Menschen sowie glaubwürdige Texte lassen sich mittlerweile mit minimalem Aufwand in großer Menge und mit zahlreichen Stellschrauben generieren[31].

Parallel zu dieser technologischen Entwicklung sinkt der Einfluss der traditionellen Massenmedien und ihrer Filter- und Verifizierungsfunktion für Informationen. Inhalte, egal, ob echt oder gefälscht, können sich rasend schnell verbreiten, teilweise gezielt vorangetrieben durch kommerzielle Dienstleister[32]. Die Werbewirtschaft und manche politischen Akteure haben sich bereits auf diese neuen Verbreitungsmöglichkeiten eingerichtet. Über gezielte Einflussnahmen beispielsweise der russischen „Internet Research Agency“ (IRA) [33] [34] sowie Wahlmanipulation durch Cambridge Analytica[35] ist ausführlich berichtet worden.

Eine Flut falscher Informationen hat das Potenzial, Fakten in der Wahrnehmung zu verdrängen. Dies geschieht nicht nur durch eine bewusste Entscheidung des Rezipienten, dieser oder jener Information eher zu vertrauen, sondern auch durch eine unbewusste Überlagerung bereits abgespeicherten Wissens[36].

Anmerkung: Es gibt Vorarbeiten für eine graphische Darstellung der vielfältigen Zusammenhänge; diese wird weiterentwickelt.

15. 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[37], der inzwischen auch an anderen Stellen aufgenommen wurde, allerdings bisher nur in Form einzelner Zwischenrufe an die breitere Öffentlichkeit gelangt ist [38] [39].

[31] https://www.theregister.co.uk/2018/12/14/ai_created_photos/ (man beachte auch das eingebettete Video im Artikel)
[32] https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf
[33] https://www.nytimes.com/2015/06/07/magazine/the-agency.html
[34] https://www.economist.com/briefing/2018/02/22/inside-the-internet-research-agencys-lie-machine
[35] https://www.bbc.com/news/av/world-43472347/cambridge-analytica-planted-fake-news
[36] https://www.researchgate.net/publication/8045738_Searching_for_the_neurobiology_of_the_misinformation_effect

(
[37] https://www.buzzfeed.com/charliewarzel/the-terrifying-future-of-fake-news
[38] https://www.wiwo.de/politik/deutschland/schlusswort-laesst-sich-die-infocalypse-noch-abwenden/20989742.html
[39] https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth

Traditionelle 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 Nachrichtenfluss (online) 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 Artikel 20, Absatz 2 des 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, darunter die Infragestellung der Zuverlässigkeit polizeilicher Untersuchungen oder Gerichtsprozesse durch die Fälschbarkeit von Informationen; Manipulation der Finanzmärkte mit realen Auswirkungen auf die Weltwirtschaft 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 (vgl. z.B. diese Tipps einer Werbeagentur[40]). 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. Die skizzierten unerwünschten Entwicklungen lassen sich unter folgenden Überschriften diskutieren:

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

Es wäre im VR außerdem zu klären, **welche positiven Entwicklungen** den nicht-intendierten und unbeabsichtigten Nebenfolgen möglicherweise gegenüberstehen, differenziert nach verschiedenen Nutzergruppen (Entwickler, Medien, Rezipienten). Es wäre hilfreich, eine explizite Beschreibung der intendierten Folgen (*benefits*) herauszuarbeiten, um diese dann den *unseens* gegenüber stellen zu können.

Benefits etwa wie: neue Form von Öffentlichkeit, Kommunikationsintensivierung mit Folgen für sozialen Zusammenhalt, usw. Auf technischer Seite beispielsweise die günstigere

[40] https://blog.hootsuite.com/de/facebook-algorithmus-organische-reichweite/

(

Filmproduktion u.a. Ambivalent zu diskutieren ist das Verständnis von Vertrauen: Vertrauen ist akzeptierte Vulnerabilität (Andreas Kaminiski). Insofern stellt sich die Frage, ob ein auf den ersten Blick eventuell naheliegendes Ziel, Vulnerabilität komplett zu eliminieren, tatsächlich sinnvoll und/oder wünschenswert wäre.

16. **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):

a. Schwerpunkt technische Perspektive: Experten für Künstliche Intelligenz, Deep Fakes, IT-Sicherheit, Zertifikatswesen, auch Datenwissenschaftler/ Bibliothekare
b. Schwerpunkt gesellschaftliche Perspektive: Publizisten wie Journalisten, Verlagsinhaber, Blogger, Medienwissenschaftler; Juristen für Internetrecht, Datenschützer, Normungsspezialisten; auch Politiker
c. Schwerpunkt philosophische Perspektive: Wissenschafts- und Technikphilosophen, Historiker; Psychologen
d. Schwerpunkt ökonomische Perspektive: Wirtschaftswissenschafter; Akteure im Online Marketing, Product Information Management, Content-Plattformen

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 gut willigen 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 Einordung nur eine grobe Orientierung sein kann: 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: Vulnerabilitäten/Unseens: X-Stakeholdertabelle

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
Politik und Gesellschaft				
Politikentwickler und Entscheider (MdBs, MEPs, Grundsatzabt. in Ministerien, Vordenker in Parteien etc.)	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
Internet-Juristen	B			B,L
Medien- und Kommunikationswissenschaftler, Medienpsychologen		L	L	
Sicherheits- und Prüfinstitutionen				
Polizei, Verfassungsschutz	B	B	B,L	B,L
Datenschutzaufsicht	L	L		B,L
Vertrauenswürdige neutrale Instanzen (z.B. Prüfer, Zertifizierer)	L	B	L	L

Zu den Systemgrenzen: Grundsätzlich sind sowohl die Betroffenheit durch die dargestellten Vulnerabilitäten als auch die Lösungsansätze 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 abgelegene Räume aus). Gleichzeitig würde es aber den Rahmen des Projekts sprengen, die Systemgrenzen entsprechend weit zu fassen, so dass sich die Frage stellt, wie hier sinnvoll eingeschränkt werden kann.

Angesichts der sich abzeichnenden Ateurskonstellation im Gesamtprojekt, der Sprachabhängigkeit von Onlineinformationen sowie der Jurisdiktionsbezogenheit von Lösungsansätzen wird zunächst Deutschland, fallweise auch die DACH-Region betrachtet. Es soll aber im Verlauf des Projekts herausgearbeitet werden, inwieweit sich Lösungen auch als Impulse bzw. Piloten für Europa (im Sinne der Europäischen Union) eignen.

Inhaltlich werden wirtschaftliche Aspekte vorerst ausgeklammert (daher auch keine entsprechenden Akteure in obiger Matrix). Allerdings bestünden hier durchaus Berührungspunkte, beispielsweise zur Frage der Vertrauenswürdigkeit von Produktreviews.

17. 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:
   Was ist philosophisch stringent und nachhaltig?
   Denkbar wäre eine Anwendung etablierter erkenntnis- und wissenschaftstheoretischer Ansätze auf die neuen Herausforderungen der Infokalypse.
4. Ökonomische Perspektive:
   Was ist finanzierbar oder langfristig lohnend?

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

der 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 für „Marken“, die nicht bereits aus dem Offline-Bereich bekannt waren. 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 **einem Personenjahr** eingeplant werden.

Dies kann auf insgesamt **1,5 Personenjahre** aufgestockt werden, um mehrere Informationsökosysteme parallel zu betrachten und Infrastrukturlösungen zu erarbeiten. 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 I-OTA), Zertifikatökosysteme (SSL klassisch bzw. mit CaCERT), Digitale Währungen oder Peer-to-Peer Dateiaustausch-Ökosysteme (z.B. BitTorrent).

5. Erwartete Ergebnisse und Folgeinitiativen

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 Akteur Auswahl sowie für die ersten Dialogschritte im Vulnerabilitätsraum dienen die folgenden Arbeitshypothesen zur Gestaltung des künftigen digitalen Raums. Die Liste ist naturgemäß unvollständig und wird laufend verfeinert und ergänzt:

4. 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.
5. 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.
6. 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.
7. 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.
8. 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[41]

[41] unter Berücksichtigung der bereits vorhandenen philosophischen Erkenntnisse und Traditionen

sowie der Frage, inwieweit Wahrheit tatsächlich gewollt ist, auch mit Blick auf psychologische Mechanismen.

9. 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.

Vulnerabilitätsraum 07

Schwerpunktstaatsanwaltschaft als Bearbeitungsformat für Cybercrime-Delikte

DiDaT (Grob-)Feinplanung für Vulnerabilitätsraum 07

Schwerpunktstaatsanwaltschaft als Bearbeitungsformat für Cybercrime-Delikte

Eike Albrecht (BTU Cottbus-Senftenberg), Dirk Labudde (HS Mittweida), Dirk Marx (BTU Cottbus-Senftenberg), Veselko Hagen (BTU Cottbus-Senftenberg), Larissa Kätker (BTU Cottbus-Senftenberg), Marcel Mönch (BTU Cottbus-Senftenberg) ; Practice: Haiying Wu (Huawei), Dirk Nagel (Vodafone), Bernhard Brocher (StA Cottbus), Hinrich Völcker (Deutsch Bank)

18. Gegenstand, Ziele und Leitfrage

Die Nutzung digitaler Systeme im *Cyberspace* kann zu führt Straftaten führen und ermöglicht es überhaupt erst, solche zu begehen. Dies stellt eine zunehmende Herausforderung für die öffentliche Sicherheit und Ordnung dar (Falk 2017; Lentner 2019). Zum einen braucht man Möglichkeiten, den Cyberspace zu schützen und zum anderen können solche Schutzmaßnahmen von Kriminellen missbraucht werden. Dolose (arglistig, trügerisch) Handlungen (nach Siepermann 2017) und alle anderen unrechtmäßigen Handlungen im *Cyberspace* erfordern im Rahmen der Zuordnung *Cybercrime und Cyber Security*[42] Antworten auf Fragen, die teils noch gar nicht gestellt sind (Goeken und Fröhlich 2018). Durch das Phänomen *«Darknet»*, welches sich als „zunehmende Bedrohung" darstellt, wird die klassische Kriminalität, wie z. B. Waffen- und Drogenhandel, partiell in den Cyberspace verlagert. Dabei ist hervorzuheben, dass neue Anforderungen an die Datensicherheit und hier gerade auch durch die Einführung von externen Cloud-Computing und einen damit erhöhten Datentransfer, notwendig machen. Der Einsatz neuer Technologien bedingt rechtlicher Anpassungen auf nationaler und auch internationaler[43] Ebene. Neue Gesetze – politische Situationen –, angepasste Organisationsstrukturen und geänderte Verhaltensweisen, verbunden mit dem Ziel, die *Resilienz* der

[42] *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). *Cybersafty* bedeutet Internetsicherheit und wird im Rahmen dieser Arbeit unter Cyber Security subsummiert. Denn Cybersafty 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 Cybersafty als Begriff eines alltäglichen Sprachgebrauchs verwandt wird und somit inhaltlich mit Cyber Security gleichgesetzt werden kann und aus Gründen der Klarheit auch muss.

[43] Cybercrime Convention (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

Gesellschaft und des Staates gegen die nachteiligen Auswirkungen der Digitalisierung zu erhöhen, machen es erforderlich, «*socially robust strategies*»[44] wertneutral im Rahmen dieses Teilprojektes zu entwickeln. Dieser dynamische Prozess stellt auch die Strafverfolgung vor neue Herausforderungen[45]. Wie aber kann sich Computer- und Systemnutzung durch *Digitalität* von Manipulationen, Korruption bis hin zur Sabotage kritischer Infrastrukturen und anderer krimineller Aktivitäten im Cyberspace abgrenzen? So abgrenzen, dass Rebounds als unbeabsichtigte Nebenwirkungen (sog. *Unseens*; abgeleitet von: uintended side effects[2]) erkannt und nicht als *Nebeneffekt* in Kauf genommen werden, weil beispielsweise nur hohe technologische Entwicklungsgeschwindigkeiten zu temporären, aber lukrativen Neben-Marktplätzen führen, die es abzuwehren aber bisher nicht lohnt, da das *Geschäft* doch ein reizvolles ist. Eine solche Ambivalenz erfordert die Abwägung zwischen verschiedenen Rechtsgütern (Freiheit vs. Sicherheit) und Gesellschaftskonzepten (Selbstverantwortlichkeit vs. staatlich-gesellschaftlich organisierter Schutz) sowie einer Gewichtung der gesellschaftlichen- und unternehmerischen Attribute zur Aushandlung, vor allem vor dem Hintergrund nicht vorhersehbarer und nicht gewollter Nebeneffekte (Scholz 2019). Cybercrime-Angriffe auf digitale Infrastrukturen und Daten sind regelmäßig strafbar, aber schwer nachweisbar. Denn *digitale Spuren* können flüchtig sein und werden nicht in allen Fällen mit dem für den klassischen Strafrechtsbereich geltenden Beweisanforderungen (Miebach 2016) belegbar sein. Ein Lösungsansatz ist hier Kompetenz und Technologie bei speziell für Cybercrime zuständiger Ermittlungsarbeit und Staatsanwaltschaften zu schaffen. Beispielhaft seien hier die Schwerpunktstaatsanwaltschaften für Cybercrime in Brandenburg (StA Cottbus) und andere Modelle zu nennen. Ganz anders erfolgt die organisatorische Antwort auf diese neuen Herausforderungen im Voralberg. Gegenwärtig stellen sich Strafverfolgungsbehörden dem sich dynamisch ändernden Kriminalitätsphänomen „Cybercrime“ durch die Institutionalisierung allen Bundesländern ein. Ausgehend von einer Analyse der Vulnerabilitäten werden Möglichkeiten- bzw. Options- und Handlungsräume betrachtet, die soziale- und technische Innovationen (einschließlich der dazu notwendigen Diskurse) für einen verantwortungsvollen Umgang mit *digitalen Daten* in einem ersten Blick auf die konzeptionelle Basis von *Cybercrime* und *Cyber Security* nehmen.

Definitionsraum

«Cybercrime» umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne)[46] 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 abgreifen und missbräuchlich nutzen zu können (Identitätsdiebstahl) darauf befindliche Daten/Dateien

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

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

[46] „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

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.[47] *Zusammengefasst* lassen sich obige aufgeführte Definitionsräume zu Cybercrime wie folgt ausformulieren: «Cybercrime im engeren Sinne sind Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder Daten richten» und «Cybercrime im weiteren Sinne sind Straftaten, die mittels Informationstechnik begangen werden»[48]. Unter dem Begriff Cybercrime sind 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 Landesgrenzen (kaum wahrnehmbar) 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 nach dem Strafgesetzbuch[49]

Straftatbestände	Inhalt (Kurzbeschreibung, Quelle Hagen)
§ 202a StGB 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 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 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 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 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 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 Datenveränderung	Das rechtswidrige Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten.
§ 303b StGB Computersabotage	Das erhebliche Stören einer Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, durch 1. Begehung einer Datenveränderung (§ 303a), 2. Eingabe oder Übermittlung von Daten in der Absicht, einem anderen einen Nachteil zuzufügen, 3. Zerstörung, Beschädigung, Unbrauchbarmachen, Beseitigen oder Verändern einer Datenverarbeitungsanlage oder eines Datenträgers.

«Cyber-Raum» Sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik mit darauf basierender Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen.[50]

«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-

[47] , o. J.
[48] Differenzierung des BKA im Bundeslagebild 2016 zur Thematik „Cybercrime im engeren und im weiteren Sinne"
[49] BKA, Cybercrime – Handlungsempfehlungen für die Wirtschaft
[50] Bundesamt für Sicherheit in der Informationstechnik, o. J.

Netzwerk verwendet[51] das Verbindungsdaten anonymisiert[52]. Der virtuelle Raum wird häufig für den Handel mit illegalen Waren (z. B. Falschgeld, Betäubungsmittel, Waffen, uvm.) genutzt.[53]

Ziel und Leitfrage

Ist der derzeitige Rechts- und Organisationsrahmen geeignet, in verhältnismäßiger Weise die Gesellschaft auf die gegenwärtigen und absehbaren zukünftigen Herausforderungen der Digitalisierung vorzubereiten?

Die Datenerhebung und -analyse (Datenzugriff, Datenauswertung) auf Arbeitsebenen der „Schwerpunktstaatsanwaltschaft in Cottbus“ wird Schlussfolgerungen zur Verwendung solcher Daten und deren Auswertungen soweit beschreiben, dass folgende Forderungen Arbeitsvoraussetzungen für diesen VR sind. *Die* Qualität der Ausbildung der „spezialisierten“ Staatsanwälte und Cybercrime-Ermittler (z. B. BKA, LKAs) in digitaler Forensik muss schnell erhöht und dynamisiert werden. Ebenso muss das Spektrum aus Wissen zu Veränderungen der Tatorte, hinterlassenen Spuren und der Tathergänge im Cyberspace musterhaft und schnell vergleichbar so gut dokumentiert werden, dass sogar Bewegungen im DarkNet in kurzer Zeit forensisch sicher analysiert werden können. Dies ist die Voraussetzung dafür, dass die Tatüberführung aufgrund digitaler forensischer Gutachten zu einem sicheren und belastbaren Beweis in der Gesamtanalyse und Interpretation aller Spuren führt und eine Tathergangsverantwortung durch die Staatsanwaltschaft somit sicher hergestellt werden kann. In verschiedenen Lagebildern, Studien und Veröffentlichungen wird auf Folgen aus Cybercrime-Delikten hingewiesen. DiDaT soll die Plattform bieten darüber hinaus zu untersuchen, welche nicht intendierten Nebeneffekte mit solchen Delikten einhergehen könnten. Zentral ist im VR07 dieser zweiten Phase eine Analyse des «Kampfes» gegen Cybercrime unter besonderer Berücksichtigung der Verfälschung und missbräuchlichen Nutzung von *digitalen Daten*, der Manipulationen und der missbräuchlichen Nutzungen etc.

<u>Blick auf die «Schwerpunktstaatsanwaltschaft» und der Betrachtung folgender Themen zur Regulation:</u>

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

(ii) Die Analyse und kritische Beurteilung geltenden Rechtes sowie Neubeurteilung des geltenden Rechts als Voraussetzung für die Strafverfolgung in Deutschland und der EU.

(iii) Ausbildung zur Anwendung und Durchsetzung des Rechts auf den unterschiedlichen Ebenen der Staatsanwaltschaft und deren Organisationsstrukturen «*Regulation*» und darauf basierend den *Gegenstand* als Anwendung so erkennen zu können, dass Handlungsempfehlungen als Arbeitsvorgaben zur Lokalisierung und Verfolgung von Cybercrime möglich werden. Die Staatsanwaltschaft ist „Vertreter“ und vertritt neben ihrer auch die gesellschaftlichen Positionen im Rahmen einer Abwägung dazu, wie das Gesetz vertreten und deren Auslegung vollzogen werden muss. Richter sind dabei die Instanz zur Bewertung und Beurteilung von Sachverhalten und der Bekanntmachung ihrer Einschätzung in dem ausgesprochenen Urteil.

[51] Vgl. *Golem Media GmbH*, o. J.
[52] Vgl. *Wikimedia Foundation Inc.*, o. J.
[53] Vgl. *Bundeskriminalamt*, 2018, S. 25.

Die individuelle Freiheit und gesellschaftliche Verantwortung finden hierdurch an dem zentralen Ort „Gericht“ eine Verfasstheit, die individuelle Freiheit bereit ist dort einzuschränken, wo das Gemeinwohl überwiegt.

Durch Überführung dieser Handlungsempfehlungen in Empfehlungen für *«Cyber Security»* wird eine Prävention insoweit möglich, dass zentrale Wirtschafts- und Finanzakteure, wie z.B. die Deutschen Bank, Vodafone oder Huawei ein Portfolio zur Abwehr von Cybercrime erhalten. Zudem wird es den Unternehmungen ermöglicht, vorhandene und auch nur mögliche Vulnerabilitäten zu erkennen, sodass man sich in die Lage versetzt sieht, konkrete Optionen zu verwenden[54]. Lt. einem Bericht von Risk Based Security, der sich mit Vulnerarbilitäten aus dem ersten Halbjahr 2019 befasst, wurden 34 % der bekannten Vulnerarbilitäten bis zum 23.08.2019 nicht behoben[55]. Cyber Security und Cybercrime stehen in gegenseitiger Wechselwirkung, da Cyber Security sich ureigenst bzw. bereits im Vorfeld mit der Thematik «Unseen» befasst, somit Grundlage für die Strafbarkeit von Delikten im Cyberspace sein kann und darüber hinaus Hilfsmittel zur Verfolgung von Cybercrime-Delikten bereitstellen kann.

[54] „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)

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

19. Welche nicht intendierten, unbeabsichtigten Nebenfolgen Cybercrime sind von Interesse und warum?

Box 1: Grundsatzerörterung zu Datenverwendung

1. Grundsätzliche Fragestellungen – Einstellung zum Cybercrime
   - Warum wird Cybercrime akzeptiert?
   - Gelernte «evolutionäre» Hilflosigkeit? (Bedeutung: Nichts oder sehr wenig über das Problem oder die Problemlösung wissen?)
   - 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
2. Recht – Rechtsgrundlagen (National und EU) – fehlende Rechtsgrundlagen, Beweismittel
   - Aktuelles Recht (National und EU)
   - Nationale Priorität in Bezug auf Cybercrime?!
   - Strafbarkeit einzelner Delikte
   - Durch Gesetze sind grundsätzlich Menschen, die verletzlich sind, geschützt. Wenn dies auf den „Cyberspace“ umgelegt wird, dann spräche man von den Computern/Servern/IoT (Internet of Things), die verletzlich sind oder sein könnten (Opfer?). Müssen Gesetze in Bezug auf Cybercrime demnach auch die verletzbaren Computer schützen?
   - Großes Problem:
     - 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 dieser Überschrift formulierten Nebenfolgen auf den Ebenen der Systematik und der Inhalte näherzukommen, hilft es, die Grundätze der Box 1 zu diskutieren. Dabei werden Daten aufgrund unterschiedlicher Bedürfnisse der Nutzung zur weiteren Klärung in den Fokus genommen.

Bekannte Vulnerabilitäten im Kontext zu Cybercrime-Delikten wären:

- **Komplexität** (komplexe IT-Anlagen u. Software, falsche Konfiguration)
- **Vertrautheit** (Verwendung von allgemein zugänglichem Code, dessen Lücken u. U. bereits bekannt sind)

- **Vernetzung** (je zahlreicher IT-Anlagen vernetzt sind, desto höher ist das Risiko einer Verletzlichkeit)
- **Schlechtes Passwort-Management**
- **Fehler im Betriebssystem** (Gefahr der Infektion mit Viren, unerlaubter Zugang)
- **Software-Fehler**
- **Anwenderfehler** (die wohl größte Vulnerabilität dürfte der Anwender sein)[56]

Die nachfolgende Tabelle zeigt die Vulnerabilitäten der entwickelt als "Wenn/Dann-Abwägungen" mit dem Schwerpunkt der Nutzung von Daten im Spektrum des Vulnerabilitätsraums Cybercrime/-security in Cyberspace (VR07).

Tabelle 3: Vulnerabilitäten der Phasen 1 und 2, 2019

Vulnerabilitäten (WENN)	Zuschreibungen (DANN)
Phase 1: Präventive u. repressive Maßnahmen ***Phase 2*: Verständnis, fehlende Awareness, Grenzen der Sicherheitslösungen (fehlende Updates und Anpassungen an neuste Entwicklungen)**	*Phase 1*: handeln ***Phase 2*: Präventive fortlaufende und repressive Maßnahmen**
Phase 1: System-Kooperationen ***Phase 2*: Leichte Verfügbarkeit (KRITIS) heute nicht abgeschottet**	*Phase 1*: binden ***Phase 2*: System-Kooperationen**
Phase 1: Änderungsgeschwindigkeit ***Phase 2*: Marktteilnahme (Dienstleistung., Produkte)**	*Phase 1*: verstehen ***Phase 2*: Sicherheit zweitrangig**
Phase 1: Verlagerung als Entpersönlichung ***Phase 2*: Zensur, Nudging, überfürsorglich. Upload-Filter (wird gar nicht hochgeladen obwohl zugestimmt), automatisierte Entscheidungen**	*Phase 1*: entrechten ***Phase 2*: Widersprechen, ignorieren, bekommen das gar nicht mit! (Entpersönlichung), Schleichender paternalistischer Staat**
Phase 1: Ein (An-)griffe von außen – Cybersecurity ***Phase 2*: IT- Grundschutzkatalog vermitteln**	*Phase 1*: reagieren, schützen ***Phase 2*: abwehren**
Phase 1: Verlagerung von staatlichen Aufgaben auf Private ***Phase 2*: Datenverlagerung**	*Phase 1*: ausweichen ***Phase 2*: Verlagerung von staatlichen Aufgaben auf Private**
Phase 1: Tatnachweise neu justieren – Cybercrime ***Phase 2*: Spuren im Internet**	*Phase 1*: neue Vollzugs- und Erfassungslogik durch *forensische Analysen* ***Phase 2*: Tatnachweise neu justieren (geringeres Maß an Überzeugungskraft)**

Die Aussagen der Tabelle 1 machen es möglich, Erörterungen so darzustellen, dass Vulnerabilitäten als in den unterschiedlichen Projektstadien von DiDaT (Erstellung des Grobkonzeptes und 2. Stakeholder-Konferenz) erkannt werden. Die erste Phase bezieht sich auf die Erstellung des Grobplanes vor der Stakeholderkonferenz im Juni 2019; die zweite Phase beginnt

[56] https://www.upguard.com/blog/vulnerability

nach dieser Stakeholderkonferenz. Der bisherige Bearbeitungsstand zeigt qualitative Unterschied, als Arbeitsergebnisses dieser Phasen. Die thematische Auseinandersetzung erfolgte im Rahmen von Diskussionen, dem Kickoff-Meeting und der ersten Stakeholderkonferenz, der Literaturarbeit und des erfolgten Reviews des Grobplanes, der mit diesem Text als Übergang von *Grob-* zum *Feinplan* entwickelt ist. Thematische Verdichtungen aus der "Wenn/Dann - Abwägungen" zu den jeweils in den Kästen der Tabelle 1 gegenüberliegenden Räumen werden so geführt, dass Antworten zu den folgenden Steuerungsfragen dazu befähigen, einen qualitativen Stakeholder-Diskurs fortzuführen. Die damit einhergehende Stakeholder-Analyse, ist in Umfang und zuletzt verfasster Zuordnung transparent erklärbar, so dass eine methodologische Ausrichtung thematisch keine willkürliche „räumliche" Zuordnung vorliegt.

Unseens in Bezug auf digitale Daten"

Cybercrime, insbesondere eine Gesetze verletzende Nutzung von digitalen Daten, überfordert die Strafverfolgung. Grund hierfür liegt in der zunehmenden Professionalität der Täter sowie der 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.[57] Eine Schwerpunktstaatsanwaltschaft, wie die in Cottbus, ist ein Beispiel dafür, dass sie sich bei der Strafverfolgung von Cyberdelikten immer dem technischen Entwicklungstand gegenüber herausgefordert sieht. Ist die Schwerpunktstaatsanwaltschaft denn ein gutes Beispiel dafür, dass z.B. Ermittlungsquoten hoch sind und wie ist dies mit herkömmlich organisierten Staatsanwaltschaften zu vergleichen, wenn überhaupt? Oder spielen dabei noch andere Aspekte der staatsanwaltschaftlichen Arbeit und Sorgfältigkeit eine spezifische Rolle und wenn ja, welche? Ist eine Grenze zwischen der Bearbeitung von Cybercrime-Delikten in strafprozessualer Konkurrenz mit weiteren Delikten gezogen, oder wird diese bzw. kann diese bei „Hybrid-Delikten" dynamisch interpretiert werden?

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

20. Welche Stakeholder sind für ein Verständnis und ein Management der Unseens von besonderer Bedeutung? Welche wissenschaftlichen Wissensbereiche sind relevant?

Box 2: *Vier* Übergangsfragen zur Klärung von Vulnerabilitäten und deren Zuordnungen

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 setzen? Sind diese Maßnahmen State-of-the-Art?
   - Verfügen Sie über ein Alarmierungssystem für das Unternehmen?
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 – https)
   - 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
   - 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 Repression

Die Begründung der Stakeholder-Auswahl erfolgt mit der Zusammenfassung der ersten Beantwortungen der vier Zuordnungen in Box 2 als Herleitung, die prozessual transdisziplinär entstand. Dabei ist zu erkennen, dass 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 systematisch erkannt werden. Eine konkrete Arbeitsgrundlage als Basis zur weiteren Herangehensweise und Ergebnisermittlung, wird mit folgend dargestellten Verengungen der Fokusgruppe, bestehend aus Stakeholdern, so ermöglicht, dass *Unseens* optional im weiteren Verlauf sichtbar werden.

Warum wurden diese Stakeholder ausgewählt? Bis zu welcher Stelle der Diskussion war es hilfreich und ab wann weniger und evtl. sogar eine Sackgasse?

- Konzeptionelle Herangehensweise
- Brainstorming und Zugangsmöglichkeiten
- Erörterung der Teilnahmekriterien an einem zu identifizierenden Markt

Stakeholder-Kreuztabelle

Tabelle 4: **Phase 1** Stakeholdergruppen VR Cybercrime/-security in Cyberspace, 2019

Stakeholdergruppe	Geschäftsfeldbeziehungen: Concerns/Competences/Threats/Sensitivities (Bedenken, Kompetenzen, Bedrohungen, Sensitivitäten)				
	Rechtsrahmen	Organisations-bezogene Fragen	Privatisierung staatlicher Aufgaben	Automatisierte Verfahren (KI)	Abwehrverhalten / digitale Resilienz
Staatsanwaltschaft Internetkriminalität	S	S	S	S	S
Mobilfunkunternehmen	M, G	M, G	M, G	M, G	M, G
Telekommunikations-ausrüster	M, G	M, G	M, G	M, G	M, G
Unternehmensberatung	A	A	A	A	A
System- (Ausstatter u. Ausrüster)	M, G	M,G	M, G	M, G	M,G
Bundespolizei (A)	S	S	S	S	S
Interpol	S	S	S	S	S
Universität Cybersecurity / Forensic Sciences	A, K, S, KI	A, K, S, KI	A, K, S, KI	A, K, S, KI	A, K, S, KI

Awareness; A / KRITIS; K / Markt; M / automatisch; KI / Grundschutzkatalog; G / Datenverlagerung; D / Spuren im Internet; S

Das Ergebnis der Stakeholderanalyse in Folge der ersten Phase (bis zur ersten Stakeholder-Konferenz) lautet wie folgt: Eine erste Sprachfindung konnte erfolgen.

Das derzeit vorhandene Recht erlaubt keinen hinreichenden Zugriff auf digitale Datenkriminalität. Zur Einsicht der Themen Cybercrime und Cybersecurity wurde in den Unternehmen aber auch spezifisch bei der Staatsanwaltschaft – theoretisch - eine IST-Analyse durchgeführt. Die daraus resultierenden Ergebnisse und Perspektiven sind „faktisch“ das Cyberabwehrzentrum bei der Dt. Bank, das Cyber Security Transparency Center von Huawei in Brüssel und die Sicherheitsbedürfnisse von Vodafone.

Es konnte jedoch eine spezifische Logik zur begründeten Beachtung und Nichtbeachtung von digitalen Daten im Spektrum der Anwendung und Nutzung von und zu systematischen Herausforderungen von innen und von außen kommender Daten insgesamt mit ***Spuren*** gefunden werden. Der bisherige Bezug zur Leitfrage konnte qualifiziert werden, so dass Antworten erhalten werden können. Aus diesem Grunde ist eine Verengung der Stakeholder-Gruppe notwendig geworden, die sich mit Tabellen 3 und 4 darstellt. Zuvor muss der Inhalt der Box 3 insofern noch diskutiert werden, da dies eine Begründung dazu ersichtlich werden lässt, warum eine entsprechend veränderte Stakeholder-Auswahl vorgenommen wurde.

Box 3: Perspektiven-Wechsel

4. Paradigmenwechsel
- Früher: Reaktion auf Angriff
- Jetzt/Trend: Dynamische präventive Vorkehrungen im Rahmen von Cyber-Security. Angriff/Vorfall schnell erkennen und richtig darauf reagieren – Resilienz
- 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 Repression

Die mittels empirischer Daten durchgeführte analytische Betrachtung der Stakeholderperspektiven – hin zu den Vulnerabilitäten als Teil eines transdisziplinären Prozesses zur Verwendung von digitalen Daten mit dem klaren Bezug zu Cybercrime – gibt zu erkennen, dass nicht alle bisherigen Zuordnungen fokussiert (siehe die Durchstreichungen in Tabelle 4) angewendet werden.

21. Methodische Überlegungen zur Unterstützung von Kernaussagen

Stakeholder-Auswahl (zur Vertiefung)

Tabelle 4: **Klärung** zur Stakeholdergrupp im VR Cybercrime/-security (Phase II) in Cyberspace, 2019

Stakeholdergruppe	Geschäftsfeldbeziehungen: Concerns/Competences/Threats/Sensitivities (Bedenken, Kompetenzen, Bedrohungen, Sensitivitäten)				
	Rechtsrahmen	Organisations-bezogene Fragen	~~Privatisierung staatlicher Aufgaben~~	Automatisierte Verfahren (KI)	~~Abwehrverhalten / digitale Resilienz~~
Staatsanwaltschaft Internetkriminalität					
Interpol					
BTU, UCD und DiDaT					

Tabelle 5: **Ergebnis** zur Auswahl der Stakeholdergruppe im VR Cybercrime/-security (Phase II) in Cyberspace, 2019

Das System	Recht	Orga. u. Struktur	Anwendung digitale Forensik	KI-Verfahren
Staatsanwaltschaft				
Interpol				
BTU, UCD, DiDaT				
Bürger				
Privat, Körperschaft				
Täter				

Schlussfolgernd kann es nun erst möglich werden, die Bedarfsargumente als Vulnerabilitäten (i) zu erfahren, deren (ii) spezifische Notwendigkeit zu verstehen und (iii) den Umgang damit im Rahmen eines festen Systems und der dortigen Nutzung von Daten gegebenenfalls auch zu erkennen

Erwartete Ergebnisse und Folgeinitiativen als *Vertiefungsforschung*

Eine Herausforderung ist, die unterschiedlichen wissenschaftlichen und praktischen Ansätze zusammenzuführen, so dass deren jeweilige Bedeutung und Wichtigkeit anerkennt werden kann, um notwendige Maßnahmen zu setzen.

Je verdichteter die Vertiefungsforschung gemeinsam mit den Teilnehmern BTU Cottbus Forensic Sciences and Engineering, Schwerpunkt-Staatsanwaltschaft (StA Cottbus), UCD Dublin – DigitalFire Labs und Interpol Lyon betrieben wird, desto deutlicher können gegenseitige (bilaterale und multilaterale) Schnittmengen herausgearbeitet werden. Durch diese Vorgehensweise sollen Unseen's komprimiert und so in den Fokus gestellt werden können, dass diese eindeutig zu identifizieren sind. In dieser Feinplanung sind Ergebnisse diejenigen Aussagen, die anhand der Bearbeitung zu den Wenn-Fragen als Suche nach Vulnerabilitäten durch die Dann-Antwort sich insofern ergeben haben, sodass eine Basis dieser Forschungsarbeit vorhanden ist. Dieser Feinplan stellt 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 VR07 Cybercrime/-security in Cyberspace die nötigen Ergebnisse als Beiträge zum Weissbuch und darüber hinaus Vertiefungsforschung und die Anwendung der Td-Lab erarbeiten.

Vertiefungsforschung *Cyber Security*

Die Analyse des ***DarkNet*** ist notwendige Folge, 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.[58] Analysen dazu können helfen, das Ausmaß und die Vielfalt von Cybercrime zu untersuchen und besser zu verstehen. Das wiederum hilft, gezielte Maßnahmen zu erarbeiten, um solche Aktivitäten zukünftig durch Präventionsmaßnahmen und -strategien zu unterbinden (Cybersecurity).

[58] Vgl. *Bundeskriminalamt*, 2018, S. 25

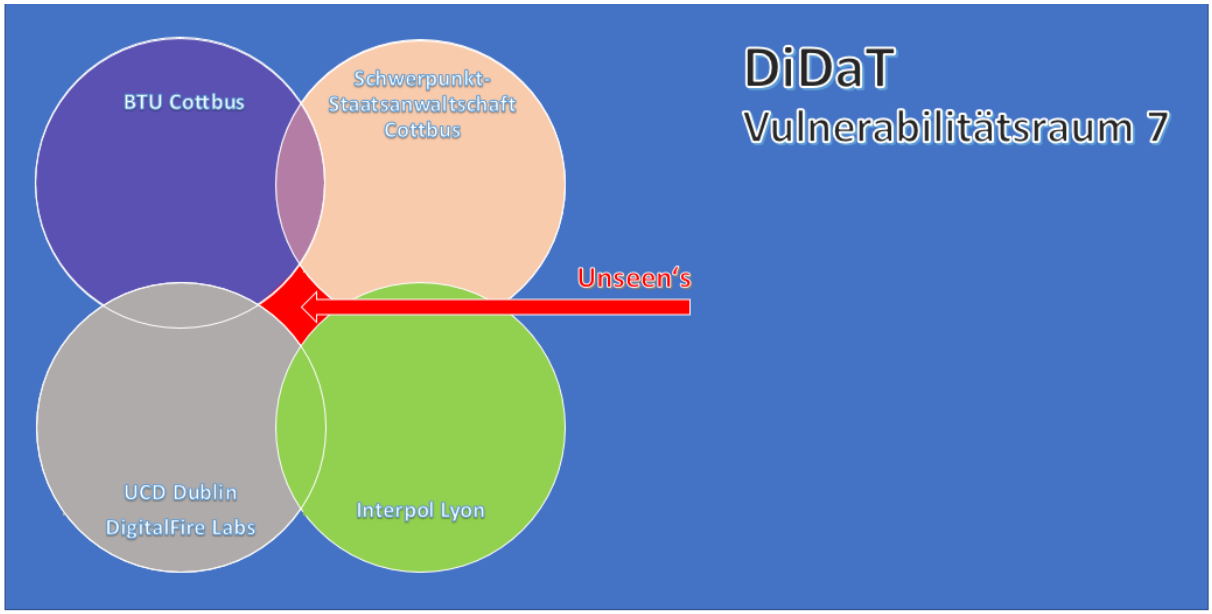


Abbildung 2: Vertiefungsforschung „digitale Spuren“

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 guten 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, Schwerpunkt-Staatsanwaltschaft Cottbus, UCD und Interpol) unter dem Dach von DiDaT aktuell bis zum 30.11.2019 zu erreichen.

Literatur

Albrecht, E., Küchenhoff, B. (2015): Staatsrecht, 3. Aufl. E. Schmidt, Berlin.

Albrecht E., Woll, R. (2010): Modelle, Methoden und Werkzeuge zum Risikomanagement, BTU, Bericht.

Albrecht, E. (2008): Risikomanagement nach REACH, StoffR (2), S. 64-69.

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.

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]

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.

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.

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 (abgerufen 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.