Digitale Mobilität erfordert eine nachhaltige Datenkultur

Digitalisation of mobility requires a sustainable data-culture

Kurztitel

Nachhaltige Datenkultur

Autoren

Karl Teille, Katharina Jahn, Thomas Waschke, Christoph Wust, Yulika Zebuhr, Klaus Markus Hofmann

Supplementarische Information $\mathbb{SI}$ (1.1)
zum Kapitel «Mobilität und vernetzte Räume»

Klaus Markus Hofmann (Universität Freiburg) , Susanne Hanesch (TU-Darmstadt), Meike Levin-Keitel (TU Dortmund), Florian Krummheuer (detecon), Wolfgang H. Serbser (European College of Human Ecology), Karl Teille (Auto-Uni), Christoph Wust (Ford-Deutschland)

In: R.W. Scholz, et al. (Hrsg.) Weißbuch: Orientierungen zum verantwortungsvollen Umgang von digitalen Daten. N.N. Verlag, N.N. Ort

Daten sind ein soziales Phänomen für dessen Entstehung und Verwertung keine natürlichen Gesetzmäßigkeiten gelten. Um eine schädlichen Umgang mit Daten, die im Zusammenhang mit Mobilität von Menschen und Gütern anfallen, zu verhindern sind sozial robuste Institutionen zu entwickeln und im Sinne einer nachhaltigen und sicheren Datenkultur für alle Akteure im Rahmen der Erhebung, Speicherung und Verwendung vom mobilitätsspezifischen Daten umzusetzen.

Fahrzeuge und Verkehrsinfrastruktur verwenden kontinuierlich mehr datengesteuerte Systeme. Zunehmende Rechnerleistung bei sinkenden Kosten (Mooresches Gesetz) ermöglicht bis dato immer komplexere Elektronik, die unter Nutzung bisher nie vorhandener Datenmengen und Qualität völlig neue Anwendungen erlaubt, zunehmend automatisiert und mit Unterstützung von KI-Systemen.

Verschiedene Mobilitätskonzepte werden von Kommunen und Industrie in Projekten mit Namen wie „Autonomes Fahren“, „Grüne Mobilität“ oder „Smart City“ entwickelt und erprobt. Datengetriebene Businessmodelle im Umfeld der „Neuen Mobilität“ werden im Wettbewerb zu entscheidenden Erfolgsfaktoren. Die zentrale Frage für Nutzer und Hersteller wird eine sichere Datenkultur sein, die den Zugang zu Daten, die im Betrieb des Fahrzeugs anfallen, von den Insassen erzeugt werden oder Resultat von Interaktionen zwischen Fahrzeugen (Car2Car) oder von Fahrzeugen mit der Infrastruktur (Car2X) sind, zwischen Akteuren zukünftig ausgewogen, zuverlässig sowie markt- und rechtskonform gestaltet. Das Recht an den eigenen Daten und die Teilhabe an deren Nutzung dabei gesellschaftlich offen zu diskutieren und gesetzlich zu regeln. Fahrzeuge kommunizieren automatisch mit z.B. Ampeln, Verkehrszeichen oder Parkplätzen. Der Schienenverkehr wechselt europaweit auf ein elektronisches Leit- und Sicherungssystem (ETCS), welches sämtliche Zugbewegungen in Echtzeit steuert. Airlines vertrauen darauf, dass der Autopilot Flugzeuge zuverlässig lenkt und sicher landet. Neben der fortgeschrittenen Digitalisierung des Vertriebs von Fahrzeugen und Mobilitätsleistungen über das Internet, gewinnt auch auf der Straße die digitale Optimierung des Betriebes für alle Mobilitätsformen an Bedeutung. Einzelne Programme können, bei aller Komplexität qualitätsgesichert von Unternehmen optimiert werden, während der Zugang zu den relevanten Daten von Verkehrsteilnehmern und mobilen Objekten stärker mit den ausgehandelten Schutz- und Zugriffsmöglichkeiten der verschiedenen Akteure sowie den Businessmodellen verbunden ist. Der Wert dieser Daten liegt zum einen in gezielter Kundenansprache und -bindung, zum anderen in verbesserten Echtzeit- und prognosebasierten Analyse und Steuerungsmöglichkeiten wie neuronale Netzen. Daraus resultiert ein intensiver Wettbewerb um die Möglichkeit, mobile Daten aus den technischen Systemen, von Sensoren und letzt- endlich von den NutzerInnen selbst und über ihr Mobilitätsverhalten zu gewinnen und nutzen zu können für den bisher eine international verlässliche Datenkultur für einen nachhaltigen und sozial robusten Umgang mit bis dato unbekannten digitalen Werten, Rechten und Risiken fehlt. Auch kann weder die Steuerung dieser neuen digitalen Möglichkeiten allein dem Wechselspiel des Marktes überlassen werden noch die öffentliche Teilhabe eingeschränkt werden. Jenseits von Marktmechanismen unterliegt eine nachhaltige Datenkultur der Verantwortung der nationalen und europäischen Gesetzgeber.

Beschreibung der Unseens einer sicheren Datenkultur

Kennzeichen des Wettbewerbs von Automobilhersteller und Zulieferern, der durch zunehmende Konkurrenz von IT-Firmen und Plattformanbietern verstärkt wird (Alphabet, Apple, Tesla, UBER, Amazon), sind disruptive Innovationen, die zu erheblichen Unsicherheiten bei Herstellern, Anbietern und NutzerInnen von digitalen Mobilitätsleistungen führen. Die in Tabelle 1 aufgeführten Anwendungsbereiche entfalten jeder für sich und in der Kombination zukunftsweisende Formen von individuell organisiertem Transport. Mobilität, die über die Bewegung von A nach B hinausgehen und nicht länger ein eigenes Fahrzeug voraussetzt für deren Gestaltung eine verlässliche Datenkultur erst zu entwickeln ist.

Funktion/ Basistechnologie	Fahrsicherheit/ Supportsysteme	Information/ Entertainment	Steuerung/ Fahrzeugbetrieb
On Board IT-Systeme	Bordcomputer mit Kamera- und Assistenzsystemen, die die Fahrer z.B. mit Infrarot oder Augmented Reality unterstützen	Infotainment-Angebote mit Möglichkeit von stationären Updates der Datenbestände (Navigation, Text, Bild, Musik, Video)	Embedded Systems im Bereich Motorsteuerung, Getriebeautomatik, Sensorik, ABS, adaptives Fahrwerk, Tempomat, Airbag, …
Vernetzte Bordsysteme	Assistiertes Fahren mit dynamischem Routing, mit individuellen Profilen zur Überwachung von Aufmerksamkeit und Gesundheit des Fahrers (Level 2 - 3)	Dynamische Integration von Internet und Umfelddaten, z.B. Stau- und Verkehrswarnung, Verbrauchsanzeige, Intermodaler Wechsel, Emissionsrechner etc.	Software basierte Upgrades für Motor-Leistung oder Fahrverhalten eines Fahrzeuges, die modular „as a Service“ gegen Entgelt bezogen werden.
Netzgestützter Systembetrieb	Hochautomatisiertes Fahren in dynamischen Umfeld auf Straße und Schiene (Level 4). Echtzeitübertragung vom Fahrzeug zu Infrastruktursystemen und anderen Verkehrsteilnehmern	Gamification, Angebote auch mit Augmented Reality (Apps oder in Verbindung mit Beacons) für value added Services und Unterhaltung, Mobilitätssubstitution durch virtuelle Präsenz	Autonomes Fahren im Connected Vehicle (Level 5), Digital orchestrierter Individualverkehr für motorisierte und nicht-motorisierte Verkehrsteilnehmer

Tabelle 1: Vernetzung von Fahrzeugfunktion (Quelle: Eigene Darstellung)

Unsichtbare Systembarrieren

Das Internet wird als „Demokratisches Werkzeug“ verstanden, welches durch seinen diskursiven Charakter politische Meinungs- und Willensbildung ermöglicht, demokratischen Diskurs verstärkt und damit demokratische Prozesse unterstützt. Dieser optimistischen Techniksicht stehen im Umfeld der digitalisierten Mobilität bei der Daten- und Systemnutzung folgende Aspekte entgegen:

- Zugang zum Netz steht nicht allen Akteuren und Verkehrsteilnehmern bzw. Partizipanten an vernetzten Räumen in gleichem Maße offen. Angebote setzen Mobilfunkversorgung und Zugang zu Endgeräten voraus, sind entgeltabhängig oder an einen Mobilitätsanbieter gekoppelt.
- Kommunikation von Verkehrsteilnehmern wird durch Systemanbieter ermöglicht oder versagt. Dieses gilt umso mehr, als den rivalen Nutzungsmöglichkeiten beschränkte Bandbreiten zur Datenübertragung gegenüberstehen.
- Heterogenität der kommerziell angebotenen Lösungen, für die es bisher keine vorgegeben Standards gibt.
- Komplexe Systeme, die mit KI-Unterstützung programmiert, getestet und überwacht werden sowie mit Machine-Learning trainiert werden, hinsichtlich bestimmter Gruppen oder Problem einen Bias aufweisen, weil Stimuli selbst einem Bias unterliegen können.

Intransparente Datengenerierung, Rechte für Datenzugang und -Nutzung

Kein Computer Programm ist ethisch neutral, da bei jeder moralischen Bewertung potentielle Einsatzmöglichkeiten der Gesamtsysteme mitbetrachtet werden müssen.
Dieses Grunddilemma kann auf Daten, genauer, zukünftige Datensammlungen im Verkehrssektor übertragen werden.
Verschiedene Arten von Mobilitätsdaten müssen in der Governance nach differenzierten Regeln behandelt werden.

1. Anonymisierte Daten, von mobilen Objekten (Fahrzeuge, Drohnen, Anlagen u.a.)
2. Anonymisiere Daten, die sich auf öffentlich zugängliche Räume beziehen (Smart City, Verkehrsfluss, Infrastruktur u.a.)
3. Daten, im Kontext mit Menschen erhoben werden und die Rückschlüsse auf einzelne Personen zulassen.

Für personenbezogene Mobilitätsdaten kommt ein entscheidendes Merkmal hinzu.

Daten, die im Kontext von Mobilität erhoben, gespeichert und weiterverwendet werden, sind inhärent mit der Identität der Person verbunden. Datenschutzrechtlich sind verschiedene Kategorien zu unterschieden:

a. Daten, die nur indirekt mit Personen in Beziehung stehen
b. Daten, die in Beziehung mit klar umrissenen Gruppen stehen
c. Daten, die von einem oder sehr wenigen Individuen stammen
d. Daten, die unauflöslich mit einer Person verbunden sind

Kritikalität im Hinblick auf Datenschutz nimmt mit der Nähe zur Identität einer konkreten Person zu. Unter Punkt d. werden zumeist biologische oder medizinische Daten betrachtet, die einem Individuum zumindest für einen längeren Zeitraum inhärent eigen sind und nicht veränderbar sind. Fakt ist, dass Fahrzeuge zunehmend auch biometrische Daten von FahrerInnen erfassen und weiterleiten können. Daten, die nach DSGVO[1] eines besonderen Schutzes bedürfen sind: Fingerabdruck, Netzhautmuster, Bedien- und Reaktionsverhalten, chronische Krankheiten, körperliche Merkmale zumal Fahrzeuge zunehmend auch biometrische Daten erfassen. Aber auch juristische Daten wie Name oder Adresse gehören zu einer neu auszuhandelnden Privatsphäre. Jede Form von personenbezogenen Mobilitätsdaten ist als besonders schützenswert zu be- trachten.
Im Rahmen eine sicheren Datenkultur sind Institutionen für den Umgang mit personenbezogenen Daten verlässlich zu gestalten, egal ob diese vom Staat oder aus der Privatwirtschaft im Mobilitätssektor erhoben, verarbeitet und gespeichert werden. Maßgeblich ist dafür auch die Organisation der Speicherung. Datenminimierung, Anonymisierung und zentrale Serverstrukturen oder eine dezentrale, individualisierte Speicherung sind diskurspflichtige technische Speicherkonzepte.

Digitale Black-Box und Monopole ermöglichen Datenmissbrauch

Missbrauch von Daten im Mobilitätsumfeld muss ausgeschlossen werden. Auch für Mobilitätsdaten gilt die Forschererfahrung, dass Menschen grundsätzlich das tun, was technisch machbar ist. Um den technisch unbegrenzten Missbrauchsmöglichkeiten Grenzen zu setzten sind Rechte und Pflich-

[1] Art. 9

ten für Mobilitätsakteure dynamisch zu regeln. Inhärent für Missbrauch ist, dass er von den Missbrauchenden nicht als solcher benannt wird. Für Mobilität können zwei Formen von Datenmissbrauch unterschieden werden. Zum ersten kriminelle Aktivitäten, bei denen Daten legal oder illegal beschafft werden und diese über das Internet manipuliert oder missbraucht werden. Zum zweiten sind dies Datenpools, die seitens der Privatwirtschaft, Verwaltung oder Organen mit Sicherheitsaufgaben angelegt werden, um mit Hilfe dieser Daten legale Geschäfts- und Überwachungsprozesse zu unterstützen. Dazu zählt auch die visuelle Überwachung öffentlicher Räum. Auch bei diesen Datenpools oder Mobilitätsdatenplattformen besteht Missbrauchsgefahr, besonders insofern die Nutzung über den ursprünglichen Zweck hinaus geht oder unberechtigte Dritte Datenzugang erhalten. In Folge von Missbrauch könnte auch die Freiheit von Einzelnen stark einschränkt oder Grundlagen des Rechtsstaats gefährdet werden.

Ursachen und Erklärung zur Entstehung dieses Unseens

Unsichtbare Systembarrieren

Die technischen Lösungen basieren auf kommerziellen Modellen, die zwar BenutzerInnen oder Benutzern eine höhere Verkehrssicherheit und einen höheren Komfort bei Wegfindung, Zielrichtung, Kommunikation und Infotainment bieten, deren primäres Interesse aber der Verkauf von Dienstleistung ist, welche auf gesam- melten und zur Verfügung gestellten Daten und den dazugehörigen Programmen ba- sieren. Darüber hinaus basieren Bandbrei- ten und Rechenleistung in den peripheren Einheiten (z.B. Fahrzeugen) auf kosteninten- siver Hardware und Infrastruktur[2].

Komplexität und Kosten erzeugen inhärente Barrieren des Zugangs und der Nutzung

[2] Zu beachtende Basistechnologien und Konzepte sind IoT (Internet of Things), Cloudcomputing, Big-Data, Edge Computing, OTA (Over-the-Air Update), KI (Künstliche Intelligenz), Blockchain und Echtzeitverarbeitungsfähigkeit.

Wachsender Digitaler Fußabdruck

Mobilitätsdaten gehören zu den relevanten Datenvolumina des Digitalen Fußabdrucks. IT-Systeme in Fahrzeugen haben einen hohen Grad an Komplexität erreicht, bei deren Programme bis zu 100 Mio. Lines of Code enthalten. Die Datenmenge wird für autonome Fahren weiter ansteigen. Um ein autonom agierendes Fahrzeug sicher durch den Verkehr führen zu können, fallen bis zu 300 Gigabyte pro Fahrzeug/Stunde an. Die absehbar wesentlichen Systeme der Digitalisierung sind Bausteine des maschinellen Lernens bzw. der sog. „schwachen künstlichen Intelligenz“ und das automatisierte Internet der Dinge (Internet of Things). Während letzteres den autonomen Datenaustausch zwischen technischen Systemen ermöglicht, sind erstere in der Lage Muster zu erkennen, automatisch zu verarbeiten und aus daraus logische Sachverhalte zu erschließen. Die für digitale Mobilitätssysteme zum Einsatz kommenden Neuronalen Netze basieren auf Milliarden von Datensätzen, die synchron verarbeitet werden können. Diese Daten stehen in direkten Bezug zum Mobilitätsverhalten der NutzerInnen (Trajektorien, Modalpräferenzen) und fallen damit auch unter die personenbezogene Daten. Weitere relevante Datenquellen sind die mobilen Geräte der NutzerInnen vom Smartphone bis hin zu sonstigen Wearables.

Entscheidend ist hierbei, dass die Daten, so sie an einem Punkt zusammengeführt und verdichtet werden können, die Anonymität, die für die einzelne Quelle möglicherweise noch gegeben war, verlieren.
Andererseits basieren viele digitale Optimierungsansätze und Geschäftsmodelle gerade auf dem Erhalt und der Nutzbarmachung solcher Daten (von individualisiertem Routing, Rettungseinsätzen bis zu Werbung, Buchungs- und Bezahldiensten). Daneben steht die Frage, inwiefern mobilitätsbezogene Daten dauerhaft anonymisierbar sind und personenbezogene Daten geschützt bleiben.

Netzwerkeffekte fördern Monopole für skalierbarer Datendienstleistungen

In keinem Wirtschaftszweig entstehen monopolartige Strukturen so kostengünstig und schnell wie im Bereich von Dienstleistungen über das Internet, der digitalen Plattformökonomie. Da das Ausweiten der Nutzerkreise einer Plattform skaliert dort, wo die Nutzer einen Vorteil durch die Anzahl der Mit-Nutzer erreichen und die Kosten jeder Lösung in direkter Relation zur Anzahl der Nutzenden sinken. So erfahren

die Betreiber eine positive Rückkopplung (sog. Netzwerkeffekte), innerhalb kurzer Zeit entstehen so weltweite de facto-Monopole (Beispiele Kommunikationsplattformen wie Facebook, Twitter, WhatsApp) denen mit regulatorischen Maßnahmen (Transparenz- und Anti-Trust Regelungen, EU-Datenschutzverordnung Steuern) Grenzen zu setzen sind, (Kersting 2012, 2017).
Eine höhere Zahl der Nutzer führt erstens zu höheren Einnahmen über Gebühren oder Werbung und zweites über Rückschlüsse über Interaktion von Nutzer mit Systemen, wodurch eine präzise Analyse der Benutzerwünsche und ihres zukünftigen Mobilitätsverhaltens ermöglicht wird. So können digitale Mobilitätsplattformen einfach und kontinuierlich optimiert werden. Damit werden NutzerInnen an die jeweilige Plattform gebunden und Neukunden gegenüber der Konkurrenz schneller gewonnen. (Beispiele: Google, Amazon, Apple, Microsoft, Spotify, Skype)

Vorsorgeprinzip bei Datensammlung
Die Effizienz einer digitalen Verwaltung lässt Behörden und Organe mit Sicherheitsaufgaben massive Anstrengungen unternehmen, um Verwaltungsprozesse skalierbar zu digitalisieren und damit verbunden Datenarchive von relevanten Informationen anzulegen. Diese analog entstandenen Rechte gelten selbstverständlich nicht nur in Bezug auf den Staat, sondern noch viel mehr in Bezug auf Wirtschaftsunternehmen, die direkt oder mittelbar auf die wachsende Menge von digital verfügbaren Mobilitätsdaten zugreifen. Mit neuen technischen Möglichkeiten wächst die rechtliche Grauzone zwischen innovativem Neuland und Missbrauch von Daten oder Marktdominanz einzelner Anbieter, da Gesetze, als geronnene Politik, bislang immer erst im Nachhinein aus realen Erfahrungen entstanden sind.

Daten von NutzerInnen liefern den Rohstoff für innovative Geschäftsmodelle und mutieren zu einem verdeckten Zahlungsmittel. Begünstigt wird diese Entwicklung dadurch, dass die aktuellen Hardwareentwicklungen immer mehr Bauteile hervorbringen, die via eingebetteten Mikrocontrollern gesteuert werden. Dadurch können diese sich mit anderen Fahrzeugen und Systemen vernetzen. Sämtliche mechanischen Vorgänge im Verkehrssektor werden sukzessive digitalisiert und erzeugen in transparenten und geschlossenen Systemen ein virtuelles Pendant.

Der häufig gegenüber KundInnen genutzte Terminus „Bezahlen mit Daten“ ist insofern irreführend wohingegen bei herkömmlichen Währungen, der Wert und die sich damit ergebenden Möglichkeiten für alle Geschäftspartner offensichtlich sind. Der Gegenwert ist bei der digitalen de-facto Währung „Persönliche Daten“ kaum nachvollziehbar und nicht immer gleichwertig, zumal weder Art und Qualität der individuellen Daten noch die Dauer der Nutzung transparent sind.

Dysfunktionaler Transfer von Rechten
Grundlegende Werte unserer Demokratie sind die Unverletzlichkeit der Wohnung, das Fernmeldegeheimnis, die freie Wahl des Wohnorts und das Recht auf Mobilität. Will der Staat überwachend eingreifen, bedarf dies eines konkreten Anlasses und eines richterlichen Beschlusses. Diese analog entstandenen Rechte gelten selbstverständlich nicht nur in Bezug auf den Staat,

sondern noch viel mehr in Bezug auf Wirtschaftsunternehmen, die direkt oder mittelbar auf die wachsende Menge von digital verfügbaren Mobilitätsdaten zugreifen.
Im Zuge der zunehmenden Digitalisierung geraten diese Grundwerte zum Schutz von Informationen über den Einzelnen zunehmend in Gefahr. Es gilt sicher zu stellen, dass die vorhandenen Rechte und Pflichten auch für die Akteure in der digitalen Mobilitätswelt ihre Gültigkeit behalten und gesetzlichen Grundlagen auch international entsprechend den neuen Möglichkeiten angepasst werden.

Eine Ursache der Erosion von analogen Rechten liegt an inhärenten Eigenschaften der Digitalisierung. Einen wesentlichen Schutz des Briefgeheimnisses bedingte der hohe Aufwand, der betrieben werden musste, um einen Brief unbemerkt zu öffnen und wieder zu versiegeln. Dagegen ist eine E-Mail für Diensteanbieter ungeschützt mit geringem Aufwand kopier- und auswertbar. Während in der analogen Welt eine natürliche Hürde ein hoher Aufwand zur Gewinnung von Informationen betrieben werden musste, gilt in der digitalen Welt auch für Massendatenauswertung geradezu das Gegenteil. Die Nutzung digitaler Errungenschaften generiert automatisch Daten, die auch benutzerspezifisch interpretiert werden können. Dem gegenüber sind erhebliche Anstrengungen erforderlich, um den Datenschutz entsprechend der Gesetzeslage beispielsweise für mobilitätsspezifsiche Betriebsdaten zu realisieren. Das sich hieraus ergebende Ungleichgewicht durch unterschiedliche Nutzung und einen Mangel der Sensibilisierung für Belange des Datenschutzes wird dramatisch zunehmen. Im internationalen Vergleich wird deutlich, dass in verschiede- nen Ländern nicht nur andere Standards gelten, sondern oft auch ein grundlegend anderes gesamtgesellschaftliches Ver- ständnis Schutzwürdigkeit von Daten und individuellen Rechten herrscht. So sind sowohl für die pragmatische Managementmentalität des „just do it“ als auch gegenüber dem totalitären Anspruch autoritärer Einparteiensysteme die freiheitlichen Institutionen der europäischen Aufklärung und die individuellen Freiheitsrechte fremd. Positiv anzumerken sind hier die Anstrengungen hin zu einem gleichen Verständnis von Datenschutz zumindest in der Zusammenarbeit demokratischer Rechtsstaaten, die in Fachkreisen in Amerika und Asien erste Früchte zeigen (z.B. California Consumer Privacy Act).

An welchen Zielen orientiert sich ein Umgang mit dem Unseen

Systemzugang sicherstellen
Von der Möglichkeit der Steigerung der Effizienz und des Komforts durch digitale Mobilitätssysteme darf grundsätzlich niemand ausgeschlossen werden. Die Mobilität des Einzelnen muss ein Grundrecht bleiben, diskriminierungsfrei zugänglich und bezahlbar. Der Schutz von Leib und Leben hat uneingeschränkte Priorität, darüber hinaus sind Persönlichkeitsrechte und Datenschutz im Sinne der DSGVO und der ePrivacy zu gewährleisten.

Transparente Datengenerierung
Empfehlungsrahmen für Gesetzgebung und Industrie ermöglicht die sichere und ethisch abgesicherte Entwicklung zukünftiger datenbasierter Systeme im Mobilitätssektor bei Gewährleistung des Datenschutzes, Wahrung der Persönlichkeits- rechte und Offenlegung der wesentlichen Algorithmen und der vewendeten Daten. Gesellschaftliche Akzeptanz („Li- cence to operate“) und Vertrauen der Nut- zerInnen sind durch garantierte Standards und transparente Rechte für Erhebung und Verwertung von Mobilitätsdaten zu fördern.

Prävention von Datenmissbrauch Der System- und Datenzugang bei Nutzung der Mobilitätsangebote muss sicher sein. Sowohl der Datenschutz im Sinne der DSGVO resp. ePrivacy als auch die Datenintegrität, Datensouveränität und Schutz vor Datenmissbrauch durch Dritte sind in der vernetzten Mobilitätskette zu gewährleisten. Basierend auf international festgelegten Standards über Nutzungsmöglichkeiten, Transparenz und Eingriffsmöglichkeiten der jeweiligen Datenschutzbehörden, sind Missbrauchsmöglichkeiten, durch robuste Mechanismen, zu verhindern, aufzudecken und über nationale Grenzen hinweg zu sanktionieren (EU vs. Google).

Entwicklung adäquater Institutionen zur Nutzung digitale Mobilitätsdaten
Demokratische Freiheitsrechte müssen auch in einem digital vernetzten Mobilitätssektor geschützt bleiben. Hierzu sind individuelle Rechte aus der analogen Welt in ihrem Wesenskern mutatis mutandis verbindlich für die digitale Mobilitätswelt mit multiplen Akteuren, KI-basierten Entscheidungen und international agierenden Konzernen zu adaptieren und übertragen.

Im Sinne einer universell zugänglichen Mobilität sind netzunabhängige, analoge Rückfallebenen für Datensicherheit und bei Datenverlust von öffentlichen und nicht-öffentlichen Verkehrssystemen zu definieren und zu implementieren.
Wesentliche Stakeholder bei der Entwicklung der Digitalen Infrastruktur sind Investoren und die digitale Industrie. Hierbei gilt es frühzeitig darauf zu achten, dass der digital unterstützte Öffentliche Verkehr, die urbanen Mobilitätssysteme und die digitalen Plattformen nicht zu Lasten des Gemeinwohls monopolisiert werden.

Welche Maßnahmen sind für welche Ziele sinnvoll

Absenken von Systembarrieren

Sensibilisierung aller Akteure für Disruption und für den Einsatz neuer Technologien im Mobilitätssektor.

- Es ist sicherzustellen, dass Mobilitätssysteme und Mobilitätsdaten diskriminierungsfrei zur berechtigten Nutzung Jedermann zur Verfügung gestellt werden.

Die sog. „Digitale Spaltung“ mit ungleichen Zugangschancen Einzelner oder ganzer Gruppen darf sich nicht vergrößern.

- - Der offen geführte Diskurs und akzeptierte gesetzliche Grundlagen schaffen die Bereitschaft des Einzelnen zur Weitergabe seiner Daten, wenn das Recht an der Teilhabe der Datennutzung Nutzung als fair empfunden geregelt ist.
- Internationale Standards zur Sicherstellung von Transparenz bei technischen Lösungen und den zugrunde gelegten Geschäftsmodellen, sind zu beachten und stetig weiter zu entwickeln.
- Kompetenzvermittlung bei Bedienung, Nutzung und Aufbau der digitalen Systeme.

- Einhaltung der Datenschutzaspekte insb. im Hinblick auf die Zweckbindung im Sinne der Datenschutzgrundverordnung (DSGVO, ePrivacy) und darüberhinausgehend eine stetige Sicherstellung ethischer Grundprinzipien bei Erweiterung der technischen Möglichkeiten.

Transparente Systeme verhindern Missbrauch

Transparenz über die Prozesse und den Datenverkehr ist systemseitig vorzusehen und gegenüber Berechtigten offen zu legen. Modelle der Datengenerierung, der - Speicherung sowie der - Nutzung sind zu prüfen ggfs. zu simulieren, um aus gewonnenen Erkenntnisse konkrete Maßnahmen abzuleiten. Fragen der Verwertbarkeit von Daten und der Weitergabe an Dritte sind im Grundsatz festzulegen, und mit angemessener Sensibilität für jeweils konkreten Situationen bedarfsweise durch die Akteure sinngemäß zu regeln._Wesentlichen Algorithmen und die jeweils verwendeten Daten sind offenzulegen; dabei ist zwischen den Interessen der Industrie (Geschäftsgeheimnisse) und dem Wunsch des Einzelnen nach Transparenz abzuwägen. Die muss auf Basis und in Form von festen Regeln (Gesetzen und Verwaltungsvorschriften) geschehen.

Gewährleistung von Daten- und Funktionssicherheit

Die DSGVO und ePrivacy, geben den aktuellen gemeinsamen Datenschutzrahmen innerhalb der Europäischen Union vor. Ergänzt wird diese durch die so genannte JI-Richtlinie für den Datenschutz im Bereich der Justiz.

- Regelungen der DSGVO und der ePrivacy sind im Mobilitätssektor zu gewährleisten.
- Standards für (offene) Plattformen zur wirksamen Prävention von Missbrauch

sind darauf basierend zu entwickeln und durchzusetzen.
- Die sich dynamisch entwickelnden Anforderungen der Datensicherheit sind stetig zu überprüfen und deren Einhaltung ist sicherzustellen.

Verhinderung von Monopolbildungen

Frühzeitig sind die „Spielregeln“ seitens der europäischen Gesetzgeber festzulegen, die bei der Übernahme von Aufgaben durch private Investoren übernommen werden. Da die öffentliche Hand weder über die Flexibilität noch über die notwendigen Finanzmittel verfügt sind unter Beachtung der informationellen Selbstbestimmungen Partnerschaften zwischen staatlichen Organisationen und Unternehmen vorzusehen. Wettbewerb muss dabei gewährleistet werden und Monopole im Bereich der digital unterstützten Mobilität oder dem Aufbau urbaner Mobilitätssysteme sind frühzeitig zu verhindern. Entscheidende infrastrukturelle digitale Basissysteme, wie z.B. die digitalen Plattformen müssen im Sinne von modernen Commons-Systemen organisiert werden, die einer angemessenen Kontrolle durch die öffentlichen Hand unterliegen.

- Fehlerprüfverfahren und Validierung sind zur Sicherstellung der Datenintegrität und Resilienz im notwendigen Maße vorzusehen.
- Grundsätzlich ist sicherzustellen, dass eine Mobilitätsleistung netzunabhängig erbracht werden kann. besonders im Fall technischer oder anderweitiger Systembeeinträchtigungen.
- Parallel zu digitalen Lösungen sind analoge Verfahren für Mobilitätseingeschränkte und Non-Digital-NutzerInnen zu prüfen, sicherzustellen und netzunabhängige Rückfalllösungen zu gewährleisten.

Grundsätze ethischer Datengenerierung und Verwertung für Mobilität

- Entwicklung von international gültigen Regeln Maßnahmen zur nachhaltigen Qualitätssicherung von dezentralen und zentralen Datenquellen, -speichern, Daten und der relevanten Verfahren sowie zu Haftungsrisiken.
- Sicherstellung von Transparenz gegenüber NutzerInnen über Erfassung, Speicherung und Verarbeitung ihrer Daten in zentralen und dezentralen Systemen.
- Fortlaufende Beobachtung der De-Anonymisierbarkeit von Daten, unter Einbeziehung interdisziplinärer Experten.
- Gesellschaftliche Diskussion ethischer Aspekte, die mit der sog. Künstlicher Intelligenz aufkommen und Transfer für Daten im Mobilitätssektor.
- Praktische Hinweise zum Umgang mit dem sog. Trolley-Problem[3] .

[3] MIT Moral Machine Experiment 2017 Aktuelle Einschätzung: Durch Maschinen zu treffende Entscheidungen können nicht ausschließlich aufgrund technischer und juristischer Regeln erfolgen, sondern im kulturellen Kontext sind ethische Regeln zu berücksichtigen.

Begründung für die Orientierung

Der Umgang mit Mobilitätsdaten erfordert sozial robuste Mechanismen im Sinne einer nachhaltigen Datenkultur die Erhebung, Speicherung und Verwendung von mobilitätsbezogenen Daten zwischen öffentlichen und privaten Akteuren regeln. Zur sicheren Datenkultur gehören der diskriminierungsfreier Zugang zu Mobilitäts-Plattformen und relevanten Daten, die Einhaltung der europäischen Datenschutzanforderungen (insb. DSGVO) sowie netzunabhängige Rückfallebenen zur Gewährleistung von Mobilität. Nachhaltige Datenkultur kann zum Spitzenprodukt europäischer Kultur werden.

Die Stakeholder der Mobilität sind zu bestimmen und ihre jeweiligen Rollen und Verantwortlichkeiten zu beschreiben. Hierunter fallen: Systemhersteller, Mobilitätsanbieter, Zulieferindustrie, Softwareanbieter, Infrastrukturbetreiber, Kommunen und Behörden und die Nutzer der verschiedenen Generationen (X, Y, Z, …), im Rahmen von dezentralen organisierten digitalen Netz- bzw. Mobilitätsinfrastrukturen.

Da weder für den Einzelnen noch für Unternehmen oder Behörden offensichtlich ist, welche Daten gespeichert werden und in welcher Form sie genutzt werden, wächst ein vielfach berechtigtes Misstrauen über das, was mit diesen Daten geschieht. Nichtsdestotrotz nutzt eine Vielzahl der AnwenderInnen aus Gründen der Bequemlichkeit und aus Mangel an Alternativen (Smartphone-Betriebssysteme) oder praktikablen Opt-Out Optionen (AGB-Dilemma) die scheinbar kostenfrei angebotenen Lösungen.

Sicherheitsstandards, die im analogen Verkehr ihre Gültigkeit haben, sind als minimale untere Schranke für Sicherheitsstandards, Datenschutz und Verwendungsmöglichkeiten der Digitalen Mobilitätssysteme zu sehen. Dort, wo eine Erprobung in Experimentierräumen unter realen Bedingungen (Reallabor) nicht möglich oder zu gefährlich ist, sind mit statistischen Verfahren und digitalen Simulationen realitätsnahe Simulationen zur Erprobungen vorzunehmen.

Literatur zu den wesentlichen Aussagen

Courtland, R. (2015). Gordon Moore: The man whose name means progress. Gordon Moore: The man whose name means progress. *IEEE Spectrum, March 30, 2015*.

Scholz, R. W. (2016). Sustainable digital environments: What major challenges is humankind facing? *Sustainability, 8*(8), 726.

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.

Zhirnov, V. V., & Cavin, R. K. (2013). Future microsystems for information processing: limits and lessons from the living systems. *IEEE Journal of the Electronic Devices Society, 1*(2), 29-47. doi:10.1109/jeds.2013.2258631

Aryaa, Vikas; Sethib, Deepa; Paul Justin: Does digital footprint act as a digital asset? – Enhancing brand experience through remarketing in International Journal of Information Management Volume 49, December 2019, Seiten 142-156

Herrmann, Andreas; Brenner, Walter: Die autonome Revolution; Frankfurter Allgemeine Buch; Frankfurt am Main; 2018; Seite 18

Hofmann, Jeanette; Norbert Kersting; Wolf Schünemann; Claudia Ritzi (eds) 2019: Politik in der digitalen Gesellschaft: Zentrale Problemfelder und Forschungsperspektiven. Bielefeld: Transcript

Kersting, Norbert (ed.) 2012: Electronic democracy. Opladen: BB publisher. IPSA series: The World of Political Sience

Kersting, Norbert 2020: Digitale Ungleichheiten und digitale Spaltung in: Klenk, T. et al 2020: Handbuch Digitalisierung in Staat und Verwaltung. Springer

Kersting, Norbert 2017: Open data, Open Government und Online Partizipation in der Smart City. Vom Informationsobjekt über den deliberativen urn zur Algorithmokratie? In: Burh, Lorina, Hammer, Stefanie und Schlözel, Hagen (eds.) 2017: der Staat, Internet und digitale Gouvernementalität. Wiesbaden: Springer VS: 87-104

Moore, Gordon: Formulierte Gesetzmäßigkeit, welches eine Verdopplung der Transistordichte alle 12-24 Monate prognostiziert; vgl. https://www.intel.de/content/www/de/de/it-managers/moores-law-evolution.html

Rammler, Stephan 2015: Schubumkehr – Die Zukunft der Mobilität, Fischer Taschenbuch, Frankfurt am Main, 2. Auflage

Herrmann, Andreas, Brenner, Walter, 2018: Die autonome Revolution, Frankfurter Allgemeine Buch; Frankfurt am Main, Seite 18

Siedschlag, Alexander, Rogg, Arne, Welzel, Carolin, 2002: Digitale Demokratie - Willensbildung und Partizipation per Internet; Springer

Bessette, Joseph M. 1980: Deliberative Democracy - The Majority Principle in Republican Government in How democratic is the constitution?; American Enterprise Institute for Public Policy Research, ISBN 0844734004, Seiten 102-116

Habermas, Jürgen, 1990: Strukturwandel der Öffentlichkeit - Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft; Surkamp Taschenbuch

Verordnungen (EU) 2016/679 Des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

Viale Pereira, et al.: Electronic Government, 19th IFIP WG 8.5 International Conference, EGOV 2020, Linköping, Sweden, August 31 – September 2, 2020, Proceedings; Springer; 2020

Weizenbaum, Joseph, 1987: Kurs auf den Eisberg - Die Verantwortung des Einzelnen in der Diktatur der Technik, Serie Piper, 3. Auflage, 19. Tsd.

Aryaa, Vikas; Sethib, Deepa; Paul Justin, 2019: Does digital footprint act as a digital asset? – Enhancing brand experience through remarketing in International Journal of Information Management, Volume 49, Seiten 142-156

Lin-Hi, Nick, 2020: "Licence to operate" in https://wirtschaftslexikon.gabler.de/definition/licence-operate-51612, Springer Gabler

European Commission, 2018: A New Deal for Consumers: Commission strengthens EU consumer rights and enforcement; Presse Mitteilung vom 11. April, Brüssel

Shi-Kupfer, Kristin; Chen, George G. 2017: Massenhaft Nutzer – mangelhafter Datenschutz; Zeit – Online, 20. August; [https://www.zeit.de/politik/ausland/2017-08/china-datenschutz-digitalisierung-gesetze]

Vertiefende Anmerkungen

Gelöscht: ¶
¶
¶
¶
18¶

Verzeichnis Endnoten