Lokationsdaten in der Digitalmobilität

7. No-Spy Konferenz

Literaturhaus Stuttgart, 16. Juni 2016

Dr. Dieter Klumpp

Institut für Kommunikationsforschung e.V.

Zu Beginn das bekannte „Lassen-Sie-mich-zunächst …“

… die „Lokationsdaten in der Digitalmobilität“ im **Kontext der Digitalisierung** darstellen**.**

Was? Die **Digitalisierung** mit ihren zahlreichen Unterpunkten – von **Digitalarbeit** über **Digitalordnung** bis **Digitalwaffen** – kann in der globalisierten gesellschaftspolitischen Diskussion gar **nicht mehr** zu einer **übersichtlichen Chefsache** werden.

Wie? Die Stakeholder von Wirtschaft bis Zivilgesellschaft, von Bundesregierung bis Landesministerien und nicht zuletzt von Partei zu Partei, stehen vor der Tatsache, dass **kein systematischer zeitstabiler Diskurs** in Gang kam, nicht einmal hinsichtlich der **sachlichen interdisziplinären Basisinformationen** war ein regelmäßiger Austausch zwischen den Akteuren untereinander sowie mit den Nutzern möglich.

Warum? In Wissenschaft, Wirtschaft, Politik und Verwaltung ist seit 15 Jahren ein **struktureller Partikularismus** prägend, der aus den **völlig unzureichenden Arbeitskapazitäten** und **Finanzressourcen** heraus die jeweiligen Aktivitäten auf gegebene **Zuständigkeiten** bzw. vorab festgelegte **Projektergebnisse** begrenzt.

Diskussionsfortschritt heißt seit 30 Jahren oft nur Schlagwortwechsel

Digitalhistorie 1987: „Datenschutz – mehr Licht im Datenschatten“

„Ein GAU der IT träfe die Wirtschaft, daher muß sie helfen, ihn zu verhindern!
In der Diskussion über den Ausbau unserer TK-Netze mit der Vision eines optoelektronischen Universalnetzes geht es auch um das Themenfeld ***Datenschutz, Datensicherheit und Persönlichkeitsschutz***.
Eine **Gesamtschau, die juristische, technische, wirtschaftliche und gesellschaftspolitische Aspekte** umfassen sollte, liegt bis heute nicht vor.
Modische Schlagworte wie **Digitalisierung,** ISDN und **Glasfasernetz** lösen bei Herstellern, Netzbetreibern und Technologiepolitikern aller Parteien Pawlow‘sche Reflexe aus. **Chancen** werden in kühnen Szenarien skizziert, wenngleich natürlich (!) die **Risiken** nicht übersehen, sondern ***"in den Griff bekommen"*** werden müssen.
Konträr dazu die Sicht der Datenschützer, der kritischen Sozialwissenschaftler und Gesellschaftspolitiker, die unter der Wirkung dieser Stichworte ebenso reflexartig das **"digitale Denken**", den **"Glasfaserstaat**“ und den "**entmündigten Menschen**" plastisch vorausmodellieren, ohne natürlich (!) die **Chancen** der Kommunikations- und Informationstechnik ganz *außer acht zu lassen“*.

Klumpp, D., Datenschutz - Mehr Licht im Datenschatten. Ein GAU der Informationstechnik träfe die Wirtschaft. Daher muß sie helfen, ihn zu verhindern, in: ***Neue Medien, Hamburg 4/1987, S.78f****.*

Diskussionswandel : Risiken werden Herausforderungen, Chancen bleiben

Digitale Gegenwart 2018

Die **dystopischen Daten-GAUs** sind in den letzten Jahrzehnten **allesamt eingetreten**, der **Datenschatten** erfasst **alle Online-Wirtschaft**, **alle Nutzer** und **jedwede Privacy.**

Statt **multilateraler Sicherheit** entstanden **hochautomatisierte Kontrollen:** Der Steinmüller-Workshop 2015 diagnostizierte bereits „**Big Data: Auf dem Weg in die Datendiktatur**“, die NOSPY 2015 zeigte „**Big Data – All Data: Wunschtraum von Regimes in aller Welt“** auf.

Die **milliardenfache Akzeptanz** des „Internet-Smartphones“ konfligiert mit einer **Akzeptabilität der Rahmenbedingungen** hinsichtlich **einer rechts-, wirtschafts- und sozialverträglichen Gestaltung**.

Digitalpioniere kritisieren „**kranke Geschäftsmodelle**“ mit **völlig unzureichendem Datenschutz.** Wegen des Umgangs mit **Nutzerdaten** und das Einspielen von **Werbung** scheidet am 12. Juni der **Whatsapp-CEO Jan Koum** aus Facebook aus. **Digitalpionier Jaron Larnier** warnt (Cebit 2018) vor den **negativen Auswirkungen der sozialen Netzwerke** und eindringlich dazu geraten, Facebook, Twitter & Co. zu verlassen.

Wer wird zukünftig für verträgliche Akzeptabilität „by design“ sorgen?

Digitale Zukunft: Datenschutz-Prinzipien Google für KI-Systeme

Zum Inkrafttreten der EU-Datenschutzgrundverordnung erklärt Google:
5. Privacy design principles. We will incorporate **our privacy principles** in the development and use of our AI technologies. We will give opportunity for notice and consent, encourage architectures with privacy safeguards, and provide **appropriate transparency and control over the use of data.** *(Google-Chef Sundar Pichai, sieben Regeln für alle KI-Projekte des Unternehmens)*

5. Datenschutz-Design-Prinzipien. Wir werden **unsere Datenschutz-Prinzipien** bei der Entwicklung und Nutzung unserer **KI-Technologien** einbauen. Wir geben die Gelegenheit zur Benachrichtigung und Zustimmung, wir **unterstützen Architekturen mit Datenschutzmaßnahmen** und bieten **angemessene** Transparenz sowie Kontrolle der Daten. *(Übers. Harry Elhardt, Brüssel)*

➡ **Höchstmögliche „Flexibilisierung“: Mit „Angemessenheit“** werden nicht nur in USA **Datenschutz und KI-Technologien** in praktisch **beliebigem Umfang** beim **Design neuer Systeme** berücksichtigt oder nicht; das heißt **praktisch: unberechenbar.**

➡ **Der Internetrechtler Thomas Hoeren** ironisierte schon immer die auch typisch deutsche Juristen-Vereinfachung aller Gesetze mit dem alleinigen Satz:
„Wer sich unangemessen verhält, wird angemessen bestraft“

Erkenntnisstand zu Big Data: Zwiespältigkeit offenkundig

„Am offenkundigsten zeigt sich die **Zwiespältigkeit von ‚Big Data'** im öffentlichen Diskurs bislang auf dem Feld der **mobilen Endgeräte. Smartphones, Tablets und Smartwatches** haben den medialen Erfahrungsraum individueller Nutzer erneut deutlich erweitert und **erleichtern deren Alltag durch massendatenbasierte Echtzeitanwendungen**.
Gleichzeitig führt die **Anbieterkonzentration** auf diesem Markt aber zu einer medienhistorisch bis dato **singulären Bündelung privatwirtschaftlicher Verfügungsmacht über Interaktionsdaten**, mit der letztlich eine **Privatisierung des Schutzes persönlicher Daten** einhergeht. Denn obgleich bislang keine der vorgestellten Prophetien und Prognosen in ihrer Radikalität empirisch eingelöst worden sind, erfüllen Sie in ihren **jeweiligen Anwendungskontexten** zentrale kommunikative Funktionen: Sie **erzeugen öffentliche Aufmerksamkeit** für neue technologische Möglichkeiten sowie die **damit verbundenen Chancen und Risiken,** kanalisieren den Diskurs und dienen nicht zuletzt als **Legitimationsgrundlage in wirtschaftlichen oder politischen Entscheidungsprozessen"**.
(*Jan-Felix Schrape, ‚Big Data' als Erwartungsraum, SoWi Stuttgart, Okt.2016)*

Tendenz zur Privatisierung des Datenschutzes mit Anbieterkonzentration

Digitalmobilität: Zielkonflikte bei Lokationsdaten

Die Lokationsdatenverarbeitung bringt seit Beginn der Mobiltelefonie generell Zielkonflikte mit sich: „Wir sehen für die **Mobilitätsdaten** ein besonderes Risiko für die **informationelle Selbstbestimmung**. Es gibt viele Dienste, bei denen Lokalisierungsdaten ganz **praktisch** sind, zum Beispiel Navigationsdienste. In der Tat ist für einen **GPS-Empfang keinerlei Personalisierung des Navigationsgeräts erforderlich**, es gleicht die Signale mit einer ggf. geräteinternen digitalen Karte ab. Aber **jedwede Vernetzung** dieses Navigationsgeräts führt **unweigerlich zu Lokationsdatenübertragung** an den Betreiber“*(SLH-Datenschutzbeauftragte Marit Hansen, zit. in: DIVSI 2016).*

Die **Zustimmung des Nutzers** für **„genaue Ortsbestimmung“** ist als Opt-In✓erforderlich, viele US-Eltern veranlassen bereits seit langem die Kinder, dies **permanent** zu tun.

Lokationsdaten sind für viele nutzernahe Services absolut erforderlich, aber deren **nachträgliche oder „echtzeitkritische“ Auswertung** führt schnell über die Personalisierung der Daten zu allseits *unerwünschten bzw. verbotenen Profilbildungen*.

Auch ohne Zustimmung des Nutzers ist genaue Ortsbestimmung möglich

Metadaten Lokation Mobiltelefon

Zitat NOSPY 2015 (ironisch):

LAC könnte **„Location Area Code“ (Funkzelle)** bedeuten, aber LAC 5233 ist keine Postleitzahl, die Nachbarzellen C1 und C2 sind für **rein technische Zwecke angegeben (z.B. Trigonometrie**).

NOSPY 2018 (ohne Ironie):

Mit den Metadaten der Nachbarzellen C1 und C2 werden mobilfunktechnisch schon immer die Zellenwechsel organisiert, aber zugleich lässt sich damit trigonometrisch auch der Standort immer bestimmen. **Gerätidentifikation** erst mit **der IMEI-Nummer**, **Personenbezug** erfolgt erst u.a. mit der **SIM-Karte.**

Bewegungsprofile aufgrund Lokationsdaten systemimmanent

Bewegungsprofile aus Lokationsdaten

Ein **Bewegungsprofil** ist ein durch Datensammlung und -verknüpfung erstellter Datensatz, der es ermöglicht, die Bewegungen (ggf. sogar Handlungen) einer Person nachzuvollziehen und dadurch überwachen zu können.

Indem man **personenbezogene Daten aus verschiedenen Quellen chronologisch** miteinander verknüpft, kann man zurückverfolgen, wann sich eine Person an welchem Ort aufhielt, was sie z.B. dort kaufte und welche Telefongespräche geführt wurden.

Quellen können hierbei die **Mobilfunknetzwerke (Funkzellen)** sein, mit denen beispielsweise ein Handy vom Netzanbieter relativ genau geortet werden kann. Mit GPS funktioniert eine Ortung bis auf wenige Zentimeter, auch mit WLAN oder Bluetooth lassen sich Positionsdaten ermitteln.
Bewegungsprofile mit personenbezogenen Daten sind **nur mit Zustimmung der Betroffenen erlaubt und an gesetzliche Vorgaben** gebunden. ***(Wikipedia; „Bedarf einer Überarbeitung“)***

Gestaltungsmöglichkeiten für Digitalmobilität sind noch unklar

Diskussionsstand zur Digitalmobilität

Die interdisziplinäre Diskussion in der Wissenschaft ist überwiegend auf **längerfristige Szenarien 2030-2045** (z.B. Autonomie, Elektromobilität, ÖPNV-Ausbau, Smart Cities etc.) hin ausgerichtet. Die Nachrichtenlage dominiert der sich exponentiell steigernde Diesel-Skandal. Das Obsoleszenzprinzip von Software wird zunehmend deutlich.

So wird schon von zuständigen Gremien relativ deutlich formuliert, nach welchen ethisch begründeten Prinzipien sich ein *KI-gestütztes autonomes Fahrzeug* verhalten soll,. Hingegen liegen für **kurzfristig anstehende Regelungen** für den bereits rasch wachsenden *Mischverkehr von fahrergesteuerten und hochautomatisierten Fahrzeugen* der Automatisierungsstufen bislang nur wenige Vorschläge vor.

Grundsätzliche Entscheidungen über die Fragen der **Vernetzung** (u.a. nach Schutz „kritischer Infrastruktur“) samt der dafür notwendigen Standards/Normen/Services (G5) sind stakeholderübergreifend ebenso wenig erfolgt wie über die von Stakeholdern der Fahrzeughersteller genannte Möglichkeit der komplett **fahrzeugautarken Digitalisierung** mithilfe umfangreicher Sensorik und Aktorik.

Weltweit werden verschiedene Technologiemodelle *parallelteuer* verfolgt

Technologieoptionen für Lokationsdaten im Fahrzeug

Lokationsdaten sind unabdingbar: **Fahrzeugautarke Systeme können zur prinzipiellen Vermeidung eines Tracking ohne Rückmeldung ans Netz aktuelle** Geodatensignale verarbeiten.
Bekannt vom „Navi“ im Auto: **GPS/Galileo** sendet die **Geodaten, die im Fahrzeug mit** dem dort gespeicherten (periodisch zu aktualisierendem) **Kartenmaterial abgeglichen werden.**
Auch ohne Rückkanal: Über **DAB+** könnten z.B. Stauwarnungen/Gefahrenpunkte mit **genauen Geodaten** (Quellen :Staumeldungen von Nutzern, Sensordaten von Fahrzeugflotten und von Messgeräten entlang von Straßen) aktuell versendet werden.
UKW-Lösungen werden in Deutschland nicht verfolgt.
Parallellösungen von Energieversorgern mit **450-MHz-Netzen** sind nach 20 Jahren seit 2016 wieder in Diskussion, zunächst im Kontext der Elektromobilität.
Als **Ergänzung zu GPS** könnte ein **RFID-Locationer** eine trassenseitige Ausbringung von passiven Bauelementen die jeweiligen Geodaten auf einen fahrzeugseitigen Funkimpuls hin (z.B. Bluetooth) im Bordcomputer des Fahrzeugs (Geodatenausleser) und speziell im Navigationssystem des Fahrzeugs verarbeiten.

Ein ‚Privacy-Oriented Vehicle Inboard Assistant System for Safety & Navigation’ könnte entstehen, aber wenige Stakeholder stehen für fahrzeugautarke Lokationsdatenverarbeitung

Datengovernance für Digitalmobilität

In Forschungsprogrammen wie BMVI/mFUND mit Begleitforschung werden noch 2018 Lösungsmöglichkeiten auch für das **Lokationsdatendilemma** untersucht.

Für die angestrebte **Datengovernance** werden offene Fragen zu **Datenschutz, Privacy, Datensicherheit, Datenbesitz und Datenhandel** erforscht, um die Minima der **Datenansprüche der jeweiligen Stakeholder** festzustellen und zu bewerten.

Unterschieden werden in der Expertenbefragung hierzu **Mobilitätsdaten,** die vom Betreiber **periodisch** bzw. in **Echtzeit** ausgelesen werden können und **Fahrzeugdaten**, die autark nur in der **Bordelektronik** verarbeitet werden sollen.

Infolge der aktuellen Grundsatzdiskussion, die weltweit um die *Facebook*-Missbräuche entstanden ist, liegt ein spezieller Fokus der **Datengovernance** auf der **regulierungsbedürftigen künftigen Betreiberorganisation**, die dann unter anderem im EU-Kartellrecht abgestimmt werden muss.

Datenschutzoptimierte Treuhänder-Organisation für Lokationsdaten?

eCall-Service: Wiki-Status

eCall (Idee 1999) bedingt unter anderem die Ausstattung von Fahrzeugen mit einem **Galileo- und GSM-Modul**, einer **Antenne** sowie einem zusätzlichen **Steuergerät**.
Die Verordnung sieht vor, dass parallel oder aufbauend auf **dem bordeigenen eCall-System umfangreiche Zusatzdienste** angeboten werden können. Auch für Mobilfunkanbieter ergeben sich dadurch **neue Geschäftsfelder**, da die für eCall **nötige SIM-Karte optional auch kostenpflichtige Telematikdienste** ermöglichen könnte.
Die Einwahl in ein Mobilfunknetz im europaweit geplanten eCall-System erfolgt erst unmittelbar nach dem Unfall, so dass **keine Bewegungsprofile** von Fahrzeugen anfallen, die **ggf. auf Basis der Telekommunikations-Überwachungsverordnung gespeichert** würden. >>En mode de **fonctionnement normal** relatif au système eCall basé sur le numéro 112, ne sont **pas traçables** et ne font pas l'objet d'une **surveillance constante.**<<
Über die komplette **Funktionsweise und Finanzierung des Systems** herrscht bisher aber noch **keine Klarheit,** da die Entwicklung noch nicht abgeschlossen ist.

Netzverfügbarkeit zum Unfallzeitpunkt nicht flächendeckend garantiert

Nur für den Standarddienst eCall ist konstante Überwachung ausgeschlossen

Kritik an ecall (Wikipedia)

„Das seit April 2018 von der EU vorgeschriebene **eCall-System steht in der Kritik**, trotz angeblich guter Intentionen möglicherweise die technische Grundlage für eine **EU-weite Überwachungsinfrastruktur** zu schaffen. Des Weiteren besteht die Möglichkeit, dass Fahrzeughersteller die **verpflichtend vorhandene Technik auch für kommerzielle** Zusatzdienste nutzen werden, die möglicherweise **zusätzliche Datenschutzprobleme** erzeugen (beispielsweise ‚Pay-As-You-Drive'-Versicherungsverträge, Mauterfassung)". In Wiki-Spanien sogar Hoffnung: „se **espera que se desarrollen otros servicios telemáticos** basados en las funcionalidades de posicionamiento", dort wird Datenschutz bzw. Tracking gar nicht erwähnt..

„In den **Zusatzdiensten** liegt die eigentliche Gefahr für die **informationelle Selbstbestimmung**, denn die **strengen Datenschutzbestimmungen** der Verordnung gelten **ausschließlich für den eCall-Notruf in seiner Basisfunktion**, die Zusatzdienste werden hiervon nicht erfasst. Insbesondere die **privaten eCall-Systeme** sind vor diesem Hintergrund bedenklich. Eingebettet in die modernen Bordsysteme ist bei entsprechender Gestaltung praktisch die **gesamte automobile Wertschöpfungskette in der Lage, unbegrenzt Daten über das Fahrzeug und das Fahrverhalten zu gewinnen".**

Ohne „sonstige Services" Lokationsdatensendung erst beim 112-Anruf?

Mobilitätsdatenauswertung – Kommerzialisierung als „Trends“

Teralytics-Mitgründer Georg Polzer: „Wir erfassen anonymisiert die Bewegungen von hunderten Millionen **Mobiltelefon-Nutzern** in Europa, Asien und den USA und stellen **diese Informationen Kunden** wie den **Verkehrsmittelbetreibern, Planern** und **Autoherstellern** zur Verfügung. Aus den Daten geht hervor, dass es einen **Trend zu Shared Mobility** gibt, also zu gemeinsam genutzten Verkehrsmitteln. Die Bewegungen der Menschen sind noch ziemlich **unorchestriert** – sie fahren mit **Autos herum, in denen vier Sitzplätze unbesetzt** sind. Das dürfte sich schon in den nächsten **fünf Jahren** ändern. Der Reiz an **heutigen Städten** liegt darin, dass sie **kurze Wege** bieten – wenn nicht gerade Stau ist. Im **Jahr 2050** wird es aber ganz neue Möglichkeiten für die Verkehrsanbindung geben, und **mit unseren Daten** ist es möglich, sie entsprechend des **Bedarfs** zu realisieren. Denken Sie an **Hyperloops, Drohnen oder fliegende Autos**“.

In der Tat sind heute im Stadtraum auch Lieferfahrzeuge, Taxis, Busse, Straßenbahnen oft nicht voll besetzt, weil der **individuelle Bedarf** sich nur schwer in **synchronen Gruppenbedarf** und damit **Shared Mobility** transformieren lässt. Dies gilt auch für künftige Hyperloops, Drohnen und Flugautos. In Kalifornien gibt es bereits in separaten Diamond Lanes seit 15 Jahren Stundenlöhner als „Beifahrer“. **Auslastungsflexible und zugleich nachhaltige ÖPNV-Systeme** sind auch am Standort erst in der Ideenphase.

Datenhandelswert ist bislang trotz/wegen Pseudo-Exaktheit gering

Wertsteigerung Lokationsdaten mit Big-Data-Mustererkennung

Big-Data-Analysen ermöglichen tatsächlich, mit Parallel Processing nur aus Mustern von **Mobilitätsdaten vollautomatisch** Datenlisten zu erstellen , die als **Prädiktionsdaten** für weitere Marketing- und Kontrollzwecke für alle Interessierten zwar **datenwertsteigernd** sind, aber zu **dystopischer Maschinenautonomie** führen (**http://futureoflife.org**)

Beispiel Marketing: Allein aus der maschinellen Algorithmen-Kombination **wiederholter zeitnaher Bewegungsdaten** z.B. zwischen exakten *Wohnorten und Einkaufsorten* entstehen vollautomatisch immer präzisere **Werbekundenlisten,** die jeweils den **Klickwert** im Datenhandel erhöhen.

Beispiel Kontrolle (fiktiv): Die Kombination **wiederholter zeitnaher Bewegungsdaten** z.B. zwischen *Bargeldausgabeorten und Grenzübergängen* führt zu **Überprüfungslisten** von Digitalgeräten, die wiederum unter KI-unterstützter Herstellung von Personenbezug und Algorithmen zu einer **automatisch produzierten Anfangsverdachtsliste** führen.

Bei den mit ✓ völlig akzeptierten Onlinediensten kann der heutige Sachverhalt nur noch „gepatcht“ werden. In der Digitalmobilität *könnte* der Standort Europa im globalen Wettbewerb jedoch noch eine Leitbildfunktion übernehmen.

„Sichere“ Digitalmobilität 2018 nicht einmal mehr im High-Tech-Militär

China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare (Nakashima/Sonne, WP, June 8 2018)

Chinese government **hackers have compromised the computers** of a Navy contractor, **stealing 614 gigabytes of highly sensitive data** related to undersea warfare — **including secret plans to develop a supersonic anti-ship missile for use on U.S. submarines by 2020**, according to American officials. (The) contractor works for the Naval Undersea Warfare Center, that conducts research and development for submarines and underwater **weaponry or the project known as Sea Dragon**, as well as **signals and sensor data, submarine radio room** information relating to **cryptographic systems**. The **Washington Post agreed to withhold certain details about the contractor** at the request of the Navy, which argued that their release **could harm national security**.

➡ **Optimistische Perspektive: Der wohl letzte wirklich sichere Code dieser Welt liegt *analog* auf leicht vergilbtem Papier gesichert in einem Präsidenten-Aktenkoffer.**

➡ **Allerdings muss jetzt unbedingt für das Öffnen des Koffers neben dem geltenden *Zweischlüssel-Prinzip* zusätzlich noch das *Vieraugen-Prinzip und ein Tweetverbot* vorgeschrieben werden.**

Lokationsdaten in der Digitalmobilität

Mit zahlreichen **offenen Fragen zur Gestaltung der Digitalmobilität** ist dringend über das Ingangsetzen einer **Datengovernance** eine Entscheidungsvorbereitung auf einer **stakeholderübergreifenden Diskursbasis** erforderlich.

Mögliche **Fragen für Digitalmobilität**:

- Sollte ein Basisdienst für Lokationsdaten in einer **Treuhänderorganisation** unter Einbeziehung auch **staatlicher Geodatenämter**, **zivilgesllschaftlicher Open Street Map** und **Datenschützeraufsicht** entwickelt werden?

- Sollte ein **Datenhandel privater Anbieter** mit **Lokationsdaten** reglementiert oder sogar verboten werden?

- Sollte eine mit **Big Data und KI mögliche rechnerautonome Erzeugung von Anfangsverdachten** aufgrund **Lokations-Tracking** untersagt werden?

Die möglichen **Nachfragen** beziehen sich dann auf das **praktische „Wie?“.**