Autonomes Fahren und Recht

Herausgegeben von

Dr. Iris Eisenberger
Universitätsprofessorin
Universität für Bodenkultur Wien

Dr. Konrad Lachmayer
Universitätsprofessor
Sigmund Freud Privatuniversität

RA Dr. Georg Eisenberger
Universitätsprofessor
Karl-Franzens-Universität Graz

Wien 2017
MANZ'sche Verlags- und Universitätsbuchhandlung

Gerhard Kunnert

„Autonomes Fahren“ aus datenschutzrechtlicher Sicht*)

*) Die dem Beitrag zu entnehmenden Wertungen spiegeln ausschließlich die persönliche Meinung des Autors wider. Aus Gründen der Textökonomie in geschlechtsspezifischer Form verwendete Bezeichnungen sind geschlechtsneutral zu verstehen.

I. Einleitung

A. Begriffsklärungen

Im gegebenen Kontext sieht sich der Jurist zunächst mit einer relativen Unschärfe bzw Mehrdeutigkeit des Begriffs „*autonomes Fahren*" konfrontiert. Dieser wird in der Alltagssprache oftmals undifferenziert gebraucht. Autonomie im philosophischen Sinne bedeutet bei Kant vereinfacht die menschliche Fähigkeit zur „(Selbst)Gesetzgebung" durch das vernünftige Ich im Rahmen eines übergeordneten Sittengesetzes.[1]) In Verbindung mit der hier interessierenden motorisierten Fortbewegung drückt Autonomie die Fähigkeit eines technischen Systems zur selbständigen Bewältigung von Aufgabenstellungen aus, ohne dass es eines menschlichen Zutuns bedürfte.[2]) Insbesondere mit Blick auf sog Dilemma-Situationen[3]) besteht insofern ein Konnex zu genuin menschlichen Wertentscheidungen, als Sittengesetze quasi in die Programmlogik autonomer Fahrzeuge implementiert werden müssen.[4])

Synonym zum „autonomen Fahren" wird in der Fachliteratur auch von „*automatisiertem Fahren*" gesprochen.[5]) Zu beachten ist aber, dass es – technisch gesehen – verschiedene Automatisierungsstufen gibt.[6]) Schon heute kön-

---

[1]) Vgl *Schöndorf*, Autonomie, Heteronomie in *Brugger/Schöndorf* (Hrsg), Philosphisches Wörterbuch (2010) 52; *Feil*, Antithetik neuzeitlicher Vernunft (1987) 51 ff.

[2]) Vgl *Häußling,* Techniksoziologie (2014) 89.

[3]) Dazu bspw *Lin*, Why Ethics Matters for Autonomous Cars, in *Maurer et al* (Hrsg), Autonomes Fahren (2015) 69 (70 ff, 74 ff); s auch *Gasser*, Grundlegende und spezielle Rechtsfragen für autonome Fahrzeuge, in *Maurer et al* (Hrsg), Autonomes Fahren (2015) 544 (554 ff).

[4]) Vgl dazu mwN *Hilgendorf*, Automatisiertes Fahren und Recht, in 53. Dt Verkehrsgerichtstag (VGT) 2015, 55 (68 ff); *Lin* (FN 3), Ethics, in *Maurer et al* (FN 3) 69 ff; *Gerdes/Thornton,* Implementable Ethics for Autonomous Vehicles, in *Maurer et al* (FN 3) 87 ff; *Cacilo et al,* Hochautomatisiertes Fahren auf Autobahnen – Industriepolitische Schlussfolgerungen, Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO. Dienstleistungsprojekt 15/14 (2015) 137 f; *Krieger-Lamina,* Vernetzte Automobile. Datensammeln beim Fahren – von Assistenzsystemen zu autonomen Fahrzeugen, ÖAW ITA Projektbericht Nr 2016-02 (2016) 60 ff.

[5]) Vgl bspw *May*, Automatisiertes Fahren – Betrachtung aus verbraucherrechtlicher Sicht, in 53. VGT 2015, 81 ff; *Lenninger,* Der Weg zum automatisierten Fahren – eine evolutionäre Entwicklung, in 53. VGT 2015, 73 ff. Kritisch zu dieser Begriffsverwendung *Hilgendorf* (FN 4) in 53. VGT 2015, 55 (56).

[6]) Insofern unpräzise § 102 Abs 3a KFG idF RV 1192 BlgNR 25. GP (33. KFG-Novelle), der von „automatisierten […] Fahrsystemen" spricht. In den Erl hierzu ist dezidiert vom „automatisierten Fahren" die Rede (Besonderer Teil – Zu Z 1 [§ 102 Abs 3a und 3b]). Ebendort werden diese Begriffe allerdings nicht synonym zu „autonomem Fah-

nen sog fortschrittliche *Fahrerassistenzsysteme* (FAS; ADAS[7])) in bestimmten Situationen einzelne Aufgaben unabhängig vom Lenker ausführen.[8]) Zu nennen sind hier Anwendungen wie „Antiblockiersystem“ (ABS)[9]), „Adaptive Geschwindigkeitsregelung“ (AGR; ACC[10])), „Elektronische Stabilitätskontrolle“ (ESP; ESC[11]) oder „Spurhalteassistent“ (LDP[12]) oder LDW[13]); mit aktivem Lenkeingriff: LKAS[14])). Charakteristisch für solche Systeme ist, dass sie den Fahrer zwar punktuell bei der Bewältigung der Fahraufgabe entlasten, ihn aber nicht aus seiner Verantwortung für die permanente Systemüberwachung entlassen. Zudem wird von ihm je nach Fall (Bsp: ACC) die jederzeitige Bereitschaft zur (Rück-)Übernahme der Fahraufgabe verlangt. Durch die Kombination bereits verfügbarer Assistenzsystemkomponenten lassen sich Funktionen realisieren, die als „*teilautomatisiert*“ bezeichnet werden.[15]) Zu verweisen ist hier etwa auf den sog „Autobahnassistenten“, welcher mittels Kombination von LDP/LDW und ACC Längs- und Querführung des Fahrzeugs für einen bestimmten Zeitraum oder bestimmte Situationen übernehmen kann.[16]) Auch solche teilautomatisierte Systeme erfordern noch eine dauerhafte Überwachung durch den Fahrer samt jederzeitiger Bereitschaft zur vollständigen Rückübernahme der Fahrzeugführung.[17]) Beim „*hochautomatisierten Fahren*“ dagegen („Stauchauffeur“, „Spurwechsel-Chauffeur“ und „Autobahnchauffeur“)[18]) entfällt das Erfordernis der permanenten Überwachung durch den Fahrer und es steht diesem nach Aufforderung durch das System eine gewisse Zeitreserve zur Rückübernahme der Fahraufgaben zur Verfügung.[19]) Darauf kann auf der Stufe des „*vollautomatisierten Fahrens*“ (Bsp: „Autobahnpilot“) verzichtet werden, da hier der Fahrroboter alle sog Systemgrenzen erkennen und das Fahrzeug in allen Situationen ohne menschliches Zutun selbständig in einen risikominimieren-

---

ren“ gebraucht, sondern entsprechen am ehesten der Kategorie des „teilautomatisierten Fahrens“ (s bei FN 15), da eine ständige Überwachung der Fahrsysteme durch den Lenker gefordert wird (vgl § 102 Abs 3b Satz 2 KFG idF RV 1192).

7) Für „Advanced Driver Assistance Systems“.

8) S als Überblick *Cacilo et al* (FN 4) 19 ff; zur historischen Entwicklung *Lenninger* (FN 5) in 53. VGT 2015, 73 (76).

9) Für „Anti-lock Braking System“.

10) Für „Adaptive Cruise Control“.

11) Für „Electronic Stability Control“.

12) Für „Lane Departure Prevention“.

13) Für „Lane Departure Warning“.

14) Für „Lane Keeping Assist System“.

15) IdS die Einteilung in Automatisierungsstufen bei *Gasser* (Projektgruppenleitung) *et al,* Rechtsfolgen zunehmender Fahrzeugautomatisierung, Berichte der Bundesanstalt für Straßenwesen. Fahrzeugtechnik Heft F 83 (2012) 9.

16) Vgl ebenda, 9.

17) Vgl ebenda, 9, 11 f.

18) Vgl dazu näher *Cacilo et al* (FN 4) 31 ff.

19) Vgl *Gasser* (Projektgruppenleitung) *et al* (FN 15) 9, 12. S aber die davon abweichende Nomenklatur der Society of Automotive Engineers International (SAE), welche auf der Stufe des hochautomatisierten Fahrens („high automation“) den Fahrer nicht mehr als Rückfallebene vorsieht (vgl *Cacilo et al* [FN 4] 5 ff [7]).

den Zustand überführen kann.[20]) Nur bei Erreichung dieses Automatisierungsgrades kann genau genommen von einem (voll)*autonomen Fahren* gesprochen werden.[21]) Dieses Begriffsverständnis wird auch dieser Untersuchung zugrunde gelegt. Übernimmt ein Fahrroboter sämtliche Fahraufgaben vom Start bis zum Ziel („Robotertaxi") kann man ergänzend vom „*fahrerlosen autonomen Fahren*" sprechen.[22])

Die Begriffe „*Autonomie*" und „*Vernetzung*" bilden im spezifischen Kontext des autonomen Fahrens nur scheinbar ein Gegensatzpaar. Schon heute besteht eine weitgehende Vernetzung von im Fahrzeug eingebauten Sensoren (Bsp: Reifendrucksensor, Bedientaste, Gaspedal) und Aktoren (Bsp: Relais, Antriebsmotor des Fensterhebers, Einspritzventil) mit elektronischen Steuergeräten (ECUs[23])). Letztere setzen mithilfe entsprechender Software die erhaltenen Sensordaten in entsprechende Steuerbefehle an die Aktoren um. Die Verbindung zwischen Sensoren und Aktoren erfolgt über sog „Datenbusse".[24]) Das sind vereinfacht gesagt „Sammelleitungen", die von einer Mehrzahl von Komponenten gemeinsam zur Datenübertragung genutzt werden. Aufgrund unterschiedlicher Anforderungen an die Übertragungskapazität und Sicherheit werden in Fahrzeugen heute verschiedene Bussysteme mit jeweils unterschiedlichen Kommunikationsprotokollen nebeneinander eingesetzt (Bsp: CAN[25])-Bus; LIN[26])-Bus).[27]) Solche Bussysteme können wiederum miteinander vernetzt werden. Wird diese fahrzeuginterne Vernetzungsarchitektur um ein Kommunikationsmodul (TCU)[28]) ergänzt, eröffnet sich die Möglichkeit der *Vernetzung* des Fahrzeugs *mit externen Komponenten* bzw *Akteuren*.[29]) Die WLAN[30])-basierte[31]) Vernetzung der Fahrzeuge untereinander wird mit C2C[32]) (V2V[33])), jene von Fahrzeugen mit straßenseitiger/straßennaher Infrastruktur (mittels intelligenter Funkbaken; IRS[34])) mit C2I[35]), V2I[36]) oder C2R[37]) umschrieben. Für die draht-

---

20) Vgl *Gasser* (Projektgruppenleitung) *et al* (FN 15) 9, 12; *Cacilo et al* (FN 4) 32.

21) IdS die Auswahl der Anwendungsfälle bei *Wachenfeld et al*, Use Cases des autonomen Fahrens, in *Maurer et al* (FN 3) 10 (12 ff).

22) idS *Cacilo et al* (FN 4) 8 f.

23) Für „Electronic Control Units".

24) Vgl einführend *Reif*, Automobilelektronik. Einführung für Ingenieure[3] (2009) 1 ff, 13 ff.

25) Für „Controller Area Network" (va zur Vernetzung von Steuergeräten untereinander bzw mit einfachen Echtzeitanwendungen).

26) Für „Local Interconnect Network" (va zur Vernetzung mechatronischer Komponenten).

27) Näheres bei *Reif* (FN 24) (2009) 13 ff.

28) Für „Telematics Control Unit".

29) Vgl *Lawson*, The Connected Car: Who is in the Driver's Seat? Published by the British Columbia Freedom of Information and Privacy Association (2015) 27.

30) Für „Wireless Local Area Network".

31) Vgl *Cacilo et al* (FN 4) 94.

32) Für „Car to Car".

33) Für „Vehicle to Vehicle".

34) Für „Intelligent Roadside Stations".

35) Für „Car to Infrastructure".

lose (idR mobilfunkbasierte)[38]) Anbindung an diverse zentralisierte Dienstanbieter (Hersteller, Werkstätten, Internetdienstanbieter etc) wird der Terminus „Car2Backend“ gebraucht. Als Überbegriff für die genannten Vernetzungsformen werden C2X[39]) bzw V2X[40]) verwendet.

C2C und C2I werden aktuell zwar nicht als integraler Bestandteil des autonomen Fahrens gesehen,[41]) könnten aber künftig im Rahmen sog *intelligenter Verkehrssysteme*[42]) (IVS; ITS[43])) bzw deren Weiterentwicklung („kooperative IVS“; C-ITS[44]); „direkte Abstimmung des Fahrverhaltens zwischen Fahrzeugen“) eine bedeutende Rolle spielen.[45])

Reine „Infotainmentanwendungen“ (aus Modulen wie Radio, CD, Video, Telefonie, Navigation etc) bilden *kein betriebsnotwendiges Merkmal* autonomen Fahrens.[46]) Tatsächlich aber forcieren sowohl Fahrzeughersteller als auch andere Dienstanbieter aus vorwiegend ökonomischen Motiven (Kundenbindung, Zusatzprofite, Produktentwicklung, Big Data) sog Telematikkonzepte, die von einem permanenten Datenaustausch zwischen dem Fahrzeug und einem vom Dienstanbieter/Hersteller betriebenen externen Rechner (sog „Backend“) ausgehen („Connected Car“[47]*);* oder „Extended Vehicle“[48])).

B. Offene Fragen aus technisch-regulatorischer Sicht

Die datenschutzrechtliche Beurteilung eines technischen Sachverhaltes setzt die Kenntnis der diesem zugrundeliegenden informationstechnischen Grundlagen bzw Funktionalitäten voraus. Deren Recherche und Aufbereitung stoßen im Falle des teil- oder vollautonomen Fahrens allerdings auf gewisse Grenzen.

---

36) Für „Vehicle to Infrastructure“.

37) Für „Car to Roadside“.

38) Vgl *Cacilo et al* (FN 4) 96.

39) Für „Car to X“.

40) Für „Vehicle to X“.

41) IdS *Lawson* (FN 29) 42; *Cacilo et al* (FN 4) 48, 94 f; *C-ITS-Platform – WG-4,* Data Protection & Privacy for Cooperative Intelligent Transport Systems (C-ITS). Analysis of Data Protection & Privacy in the context of C-ITS (2016) 14 (= Annex zu *C-ITS-Platform,* Final Report [January 2016]) (Quelle: http://ec.europa.eu/transport/themes/its/c-its_en.htm); aA *Lenninger* (FN 5) in 53. VGT 2015, 73 (78).

42) Zur Definition s Art 4 Nr 1 RL 2010/40/EU ABl 2010 L 207, 1 (4) bzw § 2 Nr 1 IVSG; als Überblick s bspw *BMVIT*, Verkehrstelematikbericht 2016 (30. 6. 2016) 20 ff; *ders,* IVS-Aktionsplan Österreich (2011); s auch *Krüger,* Architektur Intelligenter Verkehrssysteme (IVS) (2015).

43) Für „Intelligent Transportation System“.

44) Für „Cooperative Intelligent Transportation System“; vgl dazu *C-ITS Platform*, Final Report (January 2016) 17 ff, 39 ff (Internetquelle wie in FN 41).

45) Vgl *Cacilo et al* (FN 4) 94 f; *Lawson* (FN 29) 15 f, 42 f; idS auch die Pkt I.a der Amsterdamer Erklärung der EU-Verkehrsminister vom 14./15. 4. 2016 (abrufbar unter https://english.eu2016.nl/documents/publications/2016/04/14/declaration-of-amsterdam).

46) Vgl idS *Wachenfeld/Winner,* Lernen autonome Fahrzeuge? in *Maurer et al* (FN 3) 10 (28); *Cacilo et al* (FN 4) 19; *Lawson* (FN 29) 42.

47) S als Überblick über mögliche Anwendungen *Lawson* (FN 29) 32 ff; *Johannig/Mildner,* Car IT kompakt (2015) 25 ff.

48) Vgl die aktuellen Standardisierungsarbeiten unter ISO 20077-20078.

Einerseits sind viele für die künftige autonome Fahrzeugführung erforderliche technische *Einzelkomponenten* auf Ebene der Sensorik (Bsp: Kameras, Radar) und Aktorik (Bsp: „elektronisches Gaspedal", Automatikgetriebe) bereits verfügbar und im Rahmen von Assistenzsystemen im Einsatz.[49]) Andererseits gibt es noch keine feststehende *Gesamtarchitektur*. Eine Mehrzahl von diesbezüglichen Grundsatzentscheidungen muss erst getroffen werden. In welche Richtung sie fallen werden, hängt sowohl von technischen Forschungsergebnissen als auch von regulatorischen Entscheidungen ab.

Bereits im Vorabschnitt angesprochen wurde die aus Datenschutzsicht sehr wichtige Frage der Ergänzung der Fahrzeugsensorik um *informatorischen Input aus einer Vernetzung* (C2C; C2I; C2Backend). Zu denken ist weiters an Ansätze zur Implementierung einer „Selbstlernfähigkeit" von Fahrzeugen während des Betriebs („maschinelles Lernen") samt Transfer des erlernten Wissens an ein anderes Fahrzeug (Nutzerwechsel) bzw dessen Bereitstellung im Rahmen gemeinsamer Plattformen.[50]) Nicht unerheblich aus Datenschutzperspektive ist auch, welche Rolle dem *menschlichen Fahrer* während einer autonomen Fahrt zugewiesen wird. Soll er aus Sicherheitserwägungen (Erreichung der „Systemgrenze") in irgendeiner Form *als Rückfallebene* fungieren („Verfügbarkeitsfahrer"), könnte sich die Frage einer automatisierten Überwachung der tatsächlichen Rückübernahmebereitschaft des Fahrers stellen. Wieder anders zu beurteilen ist der Fall fahrerloser Robotertaxis. Hier kommen die Fahrgäste als potenzielle Überwachungsobjekte in Betracht („Insassensicherheit", „Vandalismus"). Von Relevanz für den Datenschutz ist auch, wie sich das *Zusammenspiel „betriebsnotwendiger" Fahrzeugkomponenten* mit *Internetdienstanbietern* (Google, Facebook etc) im Rahmen sog Infotainmentsysteme gestalten wird. Wird der bestimmende Einfluss beim jeweiligen Fahrzeughersteller oder bei Dienstanbietern liegen, die primär das Sammeln von Nutzerdaten im Fokus haben?

Die vorstehend genannten Sachverhalte unterliegen grundsätzlich dem *Einfluss staatlicher bzw überstaatlicher Regulierung.* Sie kann bspw festlegen, welche Daten im Rahmen von C2C bzw C2I ausgetauscht werden, nach welchem technischen Standard dies passiert und ob sich künftig zuzulassende Fahrzeuge an diesem Austausch ggf zwingend beteiligen müssen. Auch die Frage der Erstellung und Zugänglichkeit hochgenauer und hochaktueller digitaler Straßenkarten bedarf einer näheren Analyse unter regulatorischen Gesichtspunkten. Analoges gilt für die Rolle des Fahrers als „Rückfallebene" (Stichwort: erlaubte „Nebentätigkeiten"). Auch obliegt es dem Gesetzgeber zu entscheiden, ob er autonomes Fahren nur auf Autobahnen oder auch auf Landstraßen und im urbanen Bereich gestattet. Je nach Fall steigen oder sinken die jeweiligen technischen Anforderungen bzw die Qualität und Quantität der zu verarbeitenden Daten. Die schon heute unter dem Titel „Connected Car" angebotenen Zusatzdienstleistungen (Ferndiagnose, Fernsteuerung bestimmter Funktionen etc) be-

---

[49]) Vgl als Überblick *Cacilo et al* (FN 4) 19 ff, 47 ff.

[50]) Dazu etwa *Wachenfeld/Winner* (FN 46) Lernen, in *Maurer et al* (FN 3) 465 ff (485).

dürfen einer kritischen Überprüfung anhand geltenden Rechts (Datenschutz und va auch Daten*sicherheit*!). Schließlich wird der Gesetzgeber sich der Frage einer allfälligen zwingenden Datenspeicherung zwecks Aufklärung von Unfallursachen zu stellen haben. Das autonome Fahren wirft auch hier neue Fragen auf (Bsp: menschliche Übersteuerung des Fahrroboters als Unfallursache?).

II. Eingrenzung des Untersuchungsgegenstandes

Für den Zweck dieser Untersuchung wird primär auf die Variante des autonomen bzw (voll)automatisierten Fahrens abgestellt. Dieses dürfte aus heutiger Sicht zunächst in der Ausprägung des *Autobahnpiloten* (mit „Verfügbarkeitsfahrer“) (Szenario 1) realisiert werden.[51]) Miteinbezogen in die Betrachtung wird die Situation des Verlassens der Autobahn, welche in die *Rückübernahme* der Fahraufgaben durch den Fahrer mündet. Mit Blick auf letzteren Aspekt besteht eine gewisse Überlappung mit dem Konzept des Autobahnchauffeurs. Innerstädtisch sind am ehesten *fahrerlose Robotertaxis* (Szenario 2), die sich im unteren Geschwindigkeitssegment bewegen, vorstellbar.[52]) Im Lichte der im Vorabschnitt diskutierten Unsicherheit in Bezug auf die konkrete künftige Ausgestaltung von Technik und Regulierung des autonomen Fahrens bedarf es gewisser Vorannahmen. In Bezug auf die Vernetzung autonomer Fahrzeuge soll grundsätzlich eine Konzentration auf die für die autonome Fahrfunktion erforderlichen Aspekte erfolgen.[53])

III. Szenario 1 – „Autobahnpilot“

A. Zum Technischen Sachverhalt

1. Kernkomponenten und -funktionen

a) Fahrzeugsensorik einschließlich Ortungsfunktionen

Aus der Fachliteratur ist erschließbar, dass mehrere Komponenten zusammenspielen müssen, um sicheres autonomes Fahren zu ermöglichen. Unzweifelhaft bedarf es einer entsprechenden Ausstattung des Fahrzeuges mit *Sensoren* (auch: „Detektoren“). Diese setzen physikalische oder chemische Größen

---

[51]) Vgl näher bei *Wachenfeld et al* (FN 21) Use Cases, in *Maurer et al* (FN 3) 12 ff.

[52]) Vgl ebenda, 19 ff; *Biker*, Implementierung eines selbstfahrenden und individuell abrufbaren Personentransportsystems, in *Maurer et al* (FN 3) 287 ff.

[53]) Näheres zur Vernetzung unter Datenschutzgesichtspunkten abseits des autonomen Fahrens bei *Kremer*, Connected Car, intelligente Kfz, intelligente Verkehrssysteme, intelligenter Datenschutz? RDV 240 ff; *Kunnert,* Das vernetzte Automobil aus datenschutzrechtlicher Sicht, ZVR 2015, 481 ff; *ders*, Die datenschutzkonforme Vernetzung des Automobils, CR 2016, 509 ff.

in elektrische (digitale) Signale um und fungieren damit quasi als „Sinnesorgane“ des Fahrzeugs.[54]) Ermittelt werden können so Fahrzeugzustände („Eigendiagnose“; Bsp: Raddrehzahl), Fahrumfeld (Bsp: andere Verkehrsteilnehmer, Hindernisse, Verkehrszeichen) sowie die Situation im Fahrzeuginnenraum (Insassenzustand, insbesondere Fahrerzustand).[55])

Ein wichtiger Unterfall eines Sensors ist ein Gerät zum Empfang von Signalen von Navigationssatelliten (Bsp: GPS-Empfänger[56])) Aus den Signalen mehrerer Satelliten kann jeweils die (absolute) globale Position eines Fahrzeuges errechnet werden. Da nicht immer eine Sichtverbindung zu den Satelliten besteht (Bsp: Tunnelstrecke), bedarf die *Fahrzeug-Ortungstechnik* der Ergänzung um fahrzeuginterne (relative) Ortungssysteme, die auf Odometrie („Messung von Radumdrehungen“) oder Inertialsensoren („Trägheitsnavigationssystem“; Messung von Beschleunigungen und Drehraten) basieren.[57])

b) Hochgenaue digitale Karten

Insbesondere bei einem Spurwechsel (Bsp: Autobahnkreuzung), bei Spurverengungen oder in komplexen urbanen Verkehrssituationen erfordert autonomes Fahren eine sehr genaue („spurgenaue“) Eigenlokalisierung des Fahrzeuges.[58]) Fehlt es an eindeutigen Fahrbahnmarkierungen oder Verkehrsschildern oder ist das GPS-Satellitensignal zu schwach, reichen die vorgenannten Ortungstechniken iVm herkömmlichen digitalem Kartenmaterial, auf welches für die Positionsbestimmung zurückgegriffen wird, ggf nicht mehr aus.[59]) Als Lösung wird angestrebt, auf *hochgenaue digitale Karten* zurückzugreifen, in denen insbesondere die globale Position sog *Landmarken* (Verkehrszeichen oder sonstige charakteristische topographische Objekte [Türme etc]) verzeichnet sind. Durch die fahrzeugseitige (kamerabasierte[60]) oder Lidar[61])-basierte) Detektion von in hochgenauen digitalen Karten verzeichneten Landmarken samt automatisiertem Abgleich mit (im Fahrzeug verfügbarem) digitalem Kartenmaterial („Multilateration“) könnte eine ausreichend genaue Eigenlokalisierung bewerkstelligt werden.[62])

---

[54]) Näheres bei *Reif et al,* Sensoren im Kraftfahrzeug, in *Reif* (Hrsg), Sensoren im Kraftfahrzeug[2] (2012) 10.

[55]) Vgl als Überblick *Cacilo et al* (FN 4) 49 ff.

[56]) Neben dem bekannten GPS-System (USA) gibt es noch die Systeme Beidou (China), GLONASS (RF) und Galileo (EU). Mehrfachempfänger können zwecks Ergebnisoptimierung Signale verschiedener Systeme verarbeiten.

[57]) Vgl überblicksmäßig *Cacilo et al* (FN 4) 83.

[58]) Vgl *Cacilo et al* (FN 4) 82, 84.

[59]) Vgl ebenda, 47, 84, 88.

[60]) Vgl ebenda, 56 ff.

[61]) Für „Light Detection and Ranging“. Damit wird ein Verfahren umschrieben, bei dem die Laufzeit von Lichtwellen zwischen Aussenden und Empfang gemessen wird (vgl mwN *Cacilo et al* [FN 4] 51 ff).

[62]) Vgl *Cacilo et al* (FN 4) 82, 84, 85; sa *Rauch et al,* Autonomes Fahren auf der Autobahn – Eine Potentialstudie für künftige Fahrerassistenzsysteme, Tagung Fahrerassistenz München (2012) 4 f; *Krzikalla et al,* Mehr Sicherheit durch Positionsbestim-

Hochgenaue digitale Karten ermöglichen im Übrigen nicht nur die präzise Selbstortung, sondern auch die Kompensation der (heute) begrenzten Reichweite der zur Umfelderfassung eingesetzten Sensorik (va Lidar-, Radar[63])-, Ultraschall[64])- und Videosensoren). Erst der so mögliche „*Vorausblick*“ des Fahrroboters kann ggf den nötigen Zeitpolster schaffen,[65]) der dem Fahrer nach einer entsprechenden Aufforderung zur Rückübernahme der Fahraufgabe (vgl oben bei FN 17 und 32) verbleiben muss.[66])

Der *Qualität* des Kartenmaterials kommt zentrale Bedeutung für die Verkehrssicherheit zu. Insofern erscheint es plausibel, dass dieses einer behördlichen Freigabe/Kontrolle unterworfen sein wird und zur betriebsnotwendigen Mindestausstattung von „autonomen“ Fahrzeugen gehören wird. Es wäre konsequent, die Bereitstellung solcher Karten als (kostenfrei zugängliche) öffentliche Dienstleistung bzw als Dienstleistung des Autobahnbetreibers bzw -erhalters zu gestalten.[67])

Es versteht sich von selbst, dass die besagten hochgenauen Karten auch eine entsprechende Aktualität aufweisen müssen. Hinsichtlich der *Aktualisierungsintervalle* erscheint eine differenzierte Herangehensweise angezeigt.[68]) Topographische Informationen (hier: Autobahnspuren bzw Landmarken entlang einer Autobahn) weisen grundsätzlich eine gewisse Stabilität auf. Selbst Baustellen werden aufgrund ihrer Auswirkung auf den Verkehrsfluss längerfristig geplant.[69]) Eine Aktualisierung in Intervallen erscheint insofern ausreichend und eine dauernd aktive Funkverbindung zum Server eines Kartendienstanbieters unnötig. Nicht zuletzt mit Blick auf potenzielle Ausfälle der Netzverbindung erschiene eine Abhängigkeit der Einsatzfähigkeit der autonomen Fahrfunktion von einer durchgängigen Funkverbindung zu einem sog „Backend“ übrigens nicht zweckmäßig bzw wünschenswert (Ausfallsicherheit, Signallaufzeit!).[70]) Anbieten würde sich bspw eine manuell ausgelöste Aktualisierungsanfrage unmittelbar vor Antritt einer Fahrt mit beabsichtigter Nutzung des Autobahnpiloten.

Die auf hochgenaue Autobahnkarten fokussierte Datenmenge ließe sich im Übrigen ohne weiters im Fahrzeug selbst speichern und verarbeiten (dh ohne Rückgriff auf externe Rechner in der „Cloud“). Angemerkt sei, dass etwa mit Blick auf die Komplexität der Fahraufgabe im urbanen Umfeld der Rückgriff auf hochgenaue digitale Karten als Zusatzmittel zur Lokalisierung wegen

---

mung mit Satelliten und Landmarken, in *Siebenpfeiffer* (Hrsg), Vernetztes Automobil (2014) 20 ff.

63) Für „Radio Detection and Ranging“; s mwN *Cacilo et al* (FN 4) 50 f.

64) Vgl *Cacilo et al* (FN 4) 54 f.

65) Vgl ebenda, 47.

66) Vgl idS *Gasser* (Projektgruppenleitung) *et al* (FN 15) 16, 25; *Cacilo et al* (FN 4) 76 ff, 81.

67) IdS ErwGr 9 iVm Art 8 Abs 2 lit b Delegierte VO (EU) 886/2013 ABl 2013 L 247, 6.

68) Vgl idS bspw auch *Cacilo et al* (FN 4) 96.

69) IdS *Cacilo et al* (FN 4) 87.

70) IdS *Cacilo et al* (FN 4) 106.

der Aktualisierungsproblematik mitunter kritisch gesehen und stattdessen die Verbesserung der Sensorik gefordert wird.[71])

Informationen über *kurzfristige Verlegungen* von Fahrspuren, *Sperren* oder *Umleitungen*, etwa infolge eines Unfalls oder Wetterereignissen, ließen sich zeitnah am besten mittels Funkverbindung in das Fahrzeug übertragen (via C2C, C2I).[72]) Ob die angesprochenen Ad-hoc-Informationen rechtzeitig und in einer Form angeboten werden könnten, die eine direkte Einbindung in eine digitale hochgenaue Karte erlaubt, kann hier nicht beurteilt werden. Im Sinne einer Risikominimierung läge es allerdings nahe, solche kurzfristig entstehenden Gefahrenbereiche gar nicht für die Benutzung im Modus „(voll)autonomes Fahren" freizugeben.

In diesem Kontext ist auch die Einbeziehung der Gesamtheit vernetzungsfähiger Fahrzeuge als Datenlieferanten nach dem Muster von sog „Floating Car Data (FCD)"-Modellen einzelner Fahrzeug- oder Navigationsgeräteherstellern denkbar. Dabei werden Sensordaten (Stichworte: Regensensor, Geschwindigkeitsmesser, Bremssensoren) über Funk an eine zentrale Stelle übermittelt, welche diese aggregiert/anonymisiert, zu Verkehrslage- bzw Straßenzustandsmeldungen weiterverarbeitet und über einen „Rückkanal" den Fahrzeugnavigationssystemen zur Verfügung stellt[73]) und/oder Verkehrsleitmaßnahmen setzt[74]). Die Laufzeit der Information ist hier naturgemäß länger als bei C2C.[75])

Dieser Ansatz wird im Übrigen auch zur Aktualisierung und Weiterentwicklung digitalen Kartenmaterials in Erwägung gezogen.[76])

c) Steuergeräte und Software

Vor ihrer Umsetzung in Steuerbefehle an die Aktorik bedürfen die Sensordaten einer Interpretation durch entsprechende Software.[77]) Während aktuell in Fahrzeugen bis zu über 100 (dezentrale) Steuergeräte im Einsatz sind, zeichnet sich mit Blick auf das künftige autonome Fahren deren Reduktion bzw eine Konzentration auf zentrale Steuereinheiten ab.[78]) Dort soll auch die erforderliche hohe Rechenleistung erbracht werden.[79])

Die Funktion der Software besteht zunächst darin, nach der Vorverarbeitung der Sensor-Rohdaten eine Analyse und Kategorisierung (Bsp: Objekterkennung und -klassifikation) ebendieser zu unternehmen („*Perzeption*").[80]) Anschließend erfolgt die Zusammenfassung der Daten aus allen Sensortypen zu

---

71) IdS *Dietmayer*, Prädiktion von maschineller Wahrnehmungsleistung beim automatisierten Fahren, in *Maurer et al* (FN 3) 420 (423).

72) Vgl *Cacilo et al* (FN 4) 94 f.

73) Vgl *Cacilo et al* (FN 4) 77, 87, 90 ff.

74) Vgl ebenda, 93.

75) Vgl *Cacilo et al* (FN 4) 94 f; *C-ITS Platform* (FN 44) Report, 78 f.

76) Vgl ebenda, 92 f; man spricht hier auch von „crowd sensing"; dazu *Dubitzky*, Das Fahrzeug als Sensor, ATZelektronik 2015, H 2, 38 ff.

77) Vgl ebenda, 68.

78) Vgl ebenda, 68, 70 f.

79) Vgl ebenda, 70.

80) Vgl *Cacilo et al* (FN 4) 69.

einem umfassenden Situationsbild bzw (Fahrzeug-)Umfeldmodell („*Datenfusion*“).[81]) Letzteres wird mit verfügbarem Zusatzwissen (bspw statische Umfeldinformationen aus digitalen Karten) angereichert.[82]) Auf Grundlage des solcherart gewonnenen Umfeldmodells werden dann alle erkannten Einzelelemente (Verkehrszeichen, andere Verkehrsteilnehmer) in Beziehung zueinander gesetzt und unter Rückgriff auf zuordenbare bekannte Verhaltensmuster von Verkehrsteilnehmern wird quasi ein *maschinelles Szenenverständnis* errechnet („*Kognition*“).[83]) Auf der nächsten Stufe, der *Situationsvorhersage* („*Prädiktion*“), werden dann verschiedene mögliche zeitliche Entwicklungen der besagten Szene („Episoden“) vorausberechnet und hinsichtlich ihrer Eintrittswahrscheinlichkeit bewertet.[84]) Daraus wiederum entwickelt ein darauf aufbauendes Softwaremodul eine entsprechende *Handlungsplanung* (auch: Fahrmanöverplanung, Fahrstrategie; Bsp: Umfahren eines Hindernisses).[85]) Als Entscheidungsmaßstäbe stehen primär Sicherheit sowie sekundär Komfort und Effizienz im Fokus.[86]) Die ausgewählte Fahrstrategie wird dann mittels Steuerbefehlen an die Fahrzeugaktorik umgesetzt.[87])

Die spezifische Problematik der Situationsvorhersage besteht – abgesehen von systembedingten Grenzen maschineller Wahrnehmungsleistung (Defizite/Ausfälle der Sensoren; Bsp: Blendung von Videosensoren)[88]) und dem Erfordernis der ständigen Anpassung an das tatsächliche Verhalten anderer Verkehrsteilnehmer[89]) – va in der potenziellen Vielzahl möglicher Episoden[90]). Ohne eine – die menschliche Erfahrung simulierende – hinterlegte Wissensbasis über wahrscheinliche Episodenentwicklungen stößt die maschinelle Prädiktion heute an Grenzen.[91])

d) Mensch-Maschine-Schnittstelle

Die Stelle, an der ein Mensch mit einer Maschine zum Zwecke ihrer Nutzung bzw Bedienung in Kontakt tritt, wird als „Mensch-Maschine-Schnittstelle“ (MMS; HMI[92])) bezeichnet. Im Falle des Automobils besteht eine Mehrzahl solcher Schnittstellen (va Lenkrad, Schalthebel, Armaturenbrett, Mittelkonsole, Pedalerie). Beim autonomen Fahren muss die MMS uU einige zusätzliche spezifische Anforderungen erfüllen. So muss das System bei der Ausprägung „Autobahnpilot“ den Fahrer beim Verlassen der Autobahn, ggf zusätzlich bei Erkennen

---

81) Vgl ebenda, 47, 69, 70.
82) Vgl ebenda, 69.
83) Vgl *Dietmayer* (FN 71), Prädiktion, in *Maurer et al* (FN 3) 420 (421).
84) Vgl ebenda, 421.
85) Vgl ebenda, 421.
86) Vgl *Cacilo et al* (FN 4) 70; *Dietmayer* (FN 71) in *Maurer et al* (FN 3) 420 (421).
87) *Cacilo et al* (FN 4) 47, 61 ff.
88) Dazu näher ebenda, 49 ff.
89) Vgl *Dietmayer* (FN 71), Prädiktion, in *Maurer et al* (FN 3) 420 (421).
90) Vgl ebenda, 420 (434).
91) Vgl ebenda, 420 (434 ff).
92) Für „Human Machine Interface“.

von Systemgrenzen (zu komplexes Umfeld [Baustelle oÄ]), rechtzeitig *zur Rückübernahme der Fahraufgabe auffordern.*[93]) Dabei ist ua das Szenario mit zu berücksichtigen, dass der Fahrer nach einer längeren autonomen Fahrt nicht (mehr) zur (rechtzeitigen) Rückübernahme der Fahraufgabe bereit ist (Schlafzustand, Ablenkung oÄ). Um solches festzustellen und zutreffendenfalls eine Weckfunktion zu aktivieren (bei normaler Fahrt) oder die Fahrstrategie entsprechend auszurichten (Anhalten des Fahrzeugs noch vor Verlassen der Autobahn), könnte in den Fahrzeugen eine entsprechende Sensorik zum Einsatz kommen, die den *Fahrerzustand permanent überwacht* (bspw Videodetektion der Lidschlagfrequenz [auch: „Eyes-on-Erkennung"][94]), des Gesichtsausdrucks, der Körperhaltung; Messung Herzschlagfrequenz uam).[95])

Aus Datenschutzsicht kommt der konkreten Gestaltung der MMS im Übrigen auch im Zusammenhang mit für das autonome Fahren – je nach Fall – permanent, periodisch oder ad hoc erforderlichen Kommunikationsvorgängen wie C2C, C2I bzw C2Backend und daraus für/in Bezug auf den Fahrer resultierender Handlungs- bzw Informationsnotwendigkeiten Bedeutung zu.

e) Unfalldatenspeicher und Protokollierung des Betriebsmodus

Schon für konventionelle Fahrzeuge wird seit langem ein verpflichtender Einbau von Unfalldatenspeichern (UDS; EDR[96])) zwecks erleichterter Rekonstruktion von Unfallhergängen sowie künftiger Unfallverhütung diskutiert.[97]) Verunfallt ein zum autonomen Fahren geeignetes Fahrzeug, könnte fraglich sein, ob zum Zeitpunkt des Unfalls bzw im unmittelbaren zeitlichen Vorfeld eines solchen die Fahraufgabe vom Fahrroboter oder vom menschlichen Fahrer wahrgenommen worden ist, ob Letzterer – sofern überhaupt technisch möglich – den Fahrroboter manuell übersteuert hat oder ob eine frühere Rückübernahme zumutbar gewesen wäre. Je nach Beantwortung dieser Frage(n) ergeben sich deutlich unterschiedliche Konsequenzen aus haftungsrechtlicher und strafrechtlicher Sicht.[98]) So muss in einer Phase des vollautonomen Fahrens eine Haftung des Fahrers (vom Fall der Übersteuerung abgesehen) typischerweise ausscheiden.[99]) Ebenso außer Betracht hat hier eine strafrechtliche Verantwortlichkeit

---

[93]) Vgl *Cacilo et al* (FN 4) 76; *Wachenfeld et al* (FN 21) Use Cases, in *Maurer et al* (FN 3) 10 (29 ff).

[94]) Vgl *Bartels/Ruchatz,* Einführungsstrategie des Automatischen Fahrens, in at – Automatisierungstechnik Bd 63 H 3, 168 (175).

[95]) Vgl mwN *Cacilo et al* (FN 4) 29 f, 47, 74, 75 f, 81; *Rannenberg,* Erhebung und Nutzbarmachung zusätzlicher Daten – Möglichkeiten und Risiken, in *Maurer et al* (FN 3) (516) 519.

[96]) Für „Event Data Recorder".

[97]) S als Überblick *Frisoni et al*, Technical Development and Implementation of Event Data Recording in the Road Safety Policy (2014) (= Dok PE 529.071); s auch *Petersen/Ahlgrimm*, Nutzen/Kosten-Analyse des obligatorischen Einsatzes von Unfalldatenspeichern, Methodik und Ergebnisse, ZVS 2014, 101 ff; *Cacilo et al* (FN 4) 156 ff.

[98]) Vgl näher *Cacilo et al* (FN 4) 142 ff (145 ff, 150 ff).

[99]) Vgl ebenda, 141, 142, 146; *Borges*, Haftung für selbstfahrende Autos, CR 2016, 272 (273).

des Fahrers zu bleiben.[100]) Sinngemäßes gilt für als Verwaltungsstraftaten zu ahndende Verkehrsübertretungen (Bsp: Tempoüberschreitung).[101]) Um zweifelsfrei feststellen zu können, in welchem Modus („menschlicher Fahrer“, „Fahrroboter“) ein Fahrzeug im Zeitpunkt eines Unfalls oder einer Verkehrsübertretung in Betrieb stand, wird daher eine entsprechende Protokollierung – etwa in einem UDS – als Zulassungsvoraussetzung für autonome Fahrzeuge gefordert.[102]) Darüber hinaus sollen in der Phase des vollautonomen Fahrens gewisse beweiserhebliche Parameter[103]) jedenfalls vom UDS aufgezeichnet werden, um die Verantwortlichkeit des Herstellers für allfällige Fehlfunktionen (Produkthaftung)[104]), aber auch die Legitimität und Wirkung eines allfälligen manuellen Übersteuerns klären zu können.[105])

f) „Freigabefunktion“

Als ein weiteres Thema ist die allfällige Vorabüberprüfung einer vom Fahrer in Aussicht genommenen Autobahnstrecke auf deren *Freigabe für autonomes Fahren* anzusprechen.[106]) Denkbar wäre hier bspw ein Verfahren, das bei Eingabe eines Fahrziels in ein festeingebautes Navigationsgerät automatisiert anhand digitalen Kartenmaterials und/oder ergänzender Ad-hoc-Informationen des Autobahnbetreibers eine entsprechende Abklärung vornimmt und den Fahrer über die „Mensch-Maschine Schnittstelle“ über das Ergebnis informiert (Freigabe ja/nein). Alternativ zur Kommunikation mit dem Autobahnbetreiber wird auch an die Anbindung an von Herstellern betriebene Backends gedacht.[107])

2. Zusatzkomponenten

Die bereits angesprochene *Kommunikationsform C2C* zielt einmal auf eine Erweiterung des normalen Wahrnehmungshorizonts des einzelnen Fahrzeuges („Blick um die Ecke“, Glatteiswarnung, Kollisionswarnung etc) und folglich eine vorausschauende Steuerung (Bsp: sanftes Abbremsen etc) ab.[108]) *C2I* wiederum legt die Basis für höherentwickelte aktive Verkehrsmanagementlösungen (bspw „Vorausblick“ über größere Distanzen in Form von Stauwarnung;

---

[100]) Es sei denn, man ginge bspw von einer Sorgfaltswidrigkeit des Lenkers wegen mangelnder Rückübernahmebereitschaft nach entsprechender Aufforderung aus. Vgl *Cacilo et al* (FN 4) 150 f.

[101]) Vgl ebenda, 159 f.

[102]) Vgl ebenda, 147, 159, 160; *Gasser* (FN 3), Rechtsfragen, in *Maurer et al* (FN 3) 544 (569); *May* (FN 5) in 53. VGT 2015, 82 (92).

[103]) Wie bspw Geschwindigkeit, Blinkerfunktion, Fahrtrichtungswechsel etc; zum Datenumfang s näher *Schmidt-Cotta et al,* VERONICA – Project Final Report (29. 11. 2006) 31 ff (35), 53 f; *Schmidt-Cotta,* VERONICA – II. Final Report (6. 10. 2009) 76; mwN *Cacilo et al* (FN 4) 67.

[104]) Dazu näher mwN *Cacilo et al* (FN 4) 141 f; *Borges* (FN 99) CR 2016, 272 (274 f).

[105]) IdS ebenda, 145, 147.

[106]) Vgl ebenda, 87, 92 f, 106.

[107]) Vgl *Cacilo et al* (FN 4) 47 f, 92, 100.

[108]) Vgl ebenda, 94 f.

Tempolimitwarnung uam). Zwecks Gewährleistung einer entsprechenden Interoperabilität der für C2C und C2I verwendeten Kommunikationseinrichtungen wurde ein eigener WLAN-Standard geschaffen (WLANp)[109]). Unter dem Gesichtspunkt angestrebter (kooperativer) intelligenter Verkehrssysteme (IVS) wurden zudem eine Reihe technischer Standards entwickelt.[110])

Nach aktuellem Diskussionsstand auf EU-Expertenebene ist für C2C bzw C2I ua vorgesehen, dass Fahrzeuge unverschlüsselt[111]) neben anlasslos gesendeter Basisdaten (Eigenposition, Geschwindigkeit, Fahrtrichtung; sog CAMs)[112]) anlassbezogene sensorgenerierte Ad-hoc-Meldungen über Störungen/Gefahren (Stau, Glatteis etc; DENM[113])-messages) an straßenseitige Empfänger und andere Fahrzeuge aussenden.[114]) Auf Basis Letzterer sollen insbesondere automatisierte Warnmeldungen in jeweils anderen Fahrzeugen generiert und eine Verkehrssteuerung in Echtzeit ermöglicht werden.

Um die Echtheit (Authentizität) und Unverfälschtheit (Integrität) der besagten Meldungen sicherzustellen, ist vorgesehen, diese mit einer Sicherheitskopfzeile („security header") und digitalen Signaturen zu versehen. Mit Letzteren sind Daten gemeint, die anderen digitalen Daten beigefügt oder logisch mit ihnen verknüpft sind und der Bestätigung der ausschließlichen Zuordnung zu einem Unterzeichner dienen[115]) („Echtheitsbestätigung"). Um dies zu bewerkstelligen, soll eine „Public-Key-Infrastruktur" (PKI) eingerichtet werden. Diese übernimmt Ausstellung, Verteilung, Prüfung und ggf Widerruf der sog digitalen PKI-Zertifikate.[116]) Letztere sind elektronische Bescheinigungen, mit der Signaturprüfdaten einer Person, einer Stelle oder einem Gerät zugeordnet werden und so deren Identität bestätigen.[117])

Für den Bereich der IVS wurde ein spezifisches PKI-Konzept entwickelt.[118]) Demzufolge soll jedem Fahrzeug bereits auf der Produktionsstufe ein Zertifikat für dessen gesamten Lebenszyklus fest zugeordnet werden, etwa auf

---

[109]) Entspricht ETSI ITS-G5 (basierend auf IEEE 802.11p). Vgl *C-ITS Platform* (FN 44) Report, 10, 93 ff; *Cacilo et al* (FN 4) 99.

[110]) Vgl ITS Standardization Activities of ISO/TC 204. 2016 (September 2016) (Quelle: http://www.iso.org/iso/iso_technical_committee%3Fcommid%3D54706).

[111]) Vgl *C-ITS Platform* (FN 44) Report, 57; *C-ITS-Platform – WG-4* (FN 41) Analysis, 16.

[112]) Für „Cooperative Awareness Messages".

[113]) Für „Dezentralized Environmental Notification Messages".

[114]) Vgl *C-ITS Platform* (FN 44) Report, 51 f; *C-ITS-Platform – WG-4* (FN 41) Analysis, 17, 22 f.

[115]) Vgl idS Art 2 Nr 1 RL 1999/93/EG ABl 2000 L 13, 12 idF VO (EG) 1137/2008 ABl 2008 L 311, 1.

[116]) Vgl dazu einführend *Buchmann et al,* Introduction to Public Key Infrastructures (2013).

[117]) IdS Art 2 Nr 9 RL 1999/93/EG.

[118]) Vgl ETSI – TS 103 097 – V1.1.1 – Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats; s auch *Bißmeyer*, A Generic Public Key Infrastructure for Securing Car-to-X Communication, 18th World Congress on Intelligent Transport Systems. Proceedings (2011); *C-ITS-Platform – WG-4* (FN 41) Analysis, 4 ff, 27 ff.

Basis der Fahrzeug-ID[119]) („long term certificate“; kurz: LTC). Sämtliche Fahrzeug-IDs mit zugehörigen LTCs sollen in einem zentralen Verzeichnis erfasst werden.[120]) Unter Rückgriff auf ein LTC soll sich ein Fahrzeug im C-ITS-System anmelden, worauf es von einer entsprechend autorisierten Stelle ein Paket temporärer Zertifikate („temporary certificates“; kurz: TCs) zugeteilt erhält.[121]) Mittels TC sollen dann jeweils die vom Fahrzeug abgesetzten Meldungen (CAMs, DEMNs) signiert werden.[122]) Durch laufenden Wechsel der TCs soll die genaue Identität des Fahrzeugs gegenüber anderen Fahrzeugen bzw straßenseitigen Empfangsstationen verborgen bleiben.[123]) Allerdings soll protokolliert werden, welche TCs-Pakete jeweils welchem durch ein LTC bestimmtes Fahrzeug zur Verfügung gestellt werden.[124]) Dies ermöglichte es, bei Bedarf jenes LTC, mit dem (infolge Korrumpierung des Systems) inhaltlich falsche CAMs/DEMNs signiert werden, zu ermitteln, auf eine Sperrliste („Blacklist“) zu setzen und von der weiteren Vergabe von TCs und damit vom C-ITS auszuschließen.

Der *Kommunikation „C2Backend“* (via Mobilfunkverbindung, etwa GSM[125]), UMTS[126]) etc) kommt unter dem Gesichtspunkt des autonomen Fahrens primär Bedeutung im Zusammenhang mit der *Aktualisierung von digitalem Kartenmaterial* bzw der Prüfung der *Freigabe von Autobahnabschnitten* für autonomes Fahren zu.

Technische Voraussetzung für eine bezügliche Kommunikation zwischen Fahrzeug und dem Server eines Kartendienstes ist das Vorhandensein eines Kommunikationsmoduls im Fahrzeug, welches mit einer sog SIM[127])-Karte ausgerüstet ist und wie ein Mobiltelefon (auch Mobilfunkstation; kurz: MS[128])) über das Mobilfunknetz kommunizieren kann. Der Zugang zu einem Mobilfunknetz erfolgt vereinfacht ausgedrückt über sog „Luftschnittstellen“ (auch: „Funkschnittstellen“).[129]) Damit wird ein standardisiertes Verfahren zur Datenübermittlung zwischen MS und sog Basis-Sende- und Empfangsstationen (kurz: BTS[130])) umschrieben. Eine BTS sendet kontinuierlich ein Signal aus, welches von den MS (hier: Einbaugeräte in Autos), die sich in Reichweite einer BTS befinden, erkannt wird. In Reaktion auf das besagte Signal tauscht die MS bestimmte Informationen mit der BTS aus und sendet zur Authentisierung die auf der SIM-

---

119) Vgl *C-ITS-Platform – WG-4* (FN 41) Analysis, 25, 28, 29.
120) Vgl ebenda, 25.
121) Vgl ebenda, 25.
122) Vgl ebenda, 23.
123) Vgl ebenda, 27, 29.
124) Vgl ebenda, 25.
125) Für „Global System for Mobile Communications“.
126) Für „Universal Mobile Telecommunications System“.
127) Für „Subscriber Identity Module“.
128) Für „Mobile Station“.
129) Die folgende technische Skizzierung bezieht sich primär auf den GSM-Standard; s mwN *Bundesamt für Sicherheit in der Informationstechnik (BSI)*, Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte (2008) 9 ff. Zu UMTS bietet infolge kleinerer Zellgrößen präzisere Ortungsmöglichkeiten (s *BSI,* ebenda, 35 ff).
130) Für „Base Transceiver Station“.

Karte gespeicherte internationale Mobilteilnehmerkennung (IMSI)[131]) gemeinsam mit weiteren Daten (Endgerätenummer [IMEI][132]), Rufnummer (MSISDN)[133])) an die BTS. Letztere leitet diese Information über eine zentrale Steuerungseinheit (BSC)[134]) an die Vermittlungszentrale (MSC)[135]) weiter. Dort wird die IMSI mit weiteren Daten wie Rufnummer und Aufenthaltsbereichskennung (kurz: LAI[136])) in das sog Visitor Location Register (VLR) eingetragen. Die LAI bezeichnet einen geographischen Bereich, in dem eine Mehrzahl von BTS und damit die von Letzteren generierten Funkzellen, die zur selben MSC gehören, zusammengefasst sind. Die geographische Ausdehnung eines Aufenthaltsbereiches (LA)[137]) steht in Abhängigkeit von der Netzdichte (Zahl der Funkzellen). Wechselt eine MS nicht nur von einer Funkzelle zur nächsten, sondern passiert zugleich die Grenze zwischen zwei LAs, findet automatisch eine Aktualisierung der LAI im VLR statt (sog „Location Update"). Unabhängig davon meldet sich die MS im Standby-Modus periodisch im Netz an. Das Netz kennt somit stets den groben Aufenthaltsbereich einer MS. In welchem VLR die aktuelle LAI gespeichert ist, kann wiederum dem sog Home Location Register (HLR) eines Providers entnommen werden.

Die funkzellengenaue Lokalisierung einer MS ist erst beim Aufbau einer aktiven Gesprächs- oder Datenverbindung zwischen verschiedenen MS oder zwischen MS und sonstigen Endgeräten erforderlich. Jeder Basis-Sende- und Empfangsstation (BTS) oder auch jeder Antenne auf einer BTS ist eine Mobilfunkzellenkennung (kurz: „Cell-ID"[138]) oder „CID"; auch „Cell of Origin" [„COO"]) zugeordnet. Gemeinsam mit der LAI bildet eine CID die weltweit eindeutige Global Cell-ID (GCID). Da ein Endgerät (MS) ständig die Signalstärke der nächstgelegenen BTS misst, um den optimalen Empfang sicherzustellen, dh bei Bedarf einen Funkzellenwechsel zu initiieren, ist der MS die aktuelle CID stets bekannt. Baut eine MS eine aktive Netzverbindung auf, teilt sie dem Netz die CID jener Funkzelle mit, in welcher sie sich gerade befindet. Sinngemäßes passiert bei einem ankommenden Gespräch, SMS etc. Um dieses zu einer bestimmten MS leiten zu können, stellt das Netz zunächst mittels VLR fest, in welchem Aufenthaltsbereich (LA) sich die angerufene MS befindet und ruft diese dann über alle der LA zugeordneten BTS an. Bei entsprechender Rückmeldung, die wiederum ua die CID enthält, erfährt das Netz den funkzellengenauen Standort und kann eine Verbindung mit der in Betracht kommenden BTS und damit mit der MS aufbauen. Mit netzseitiger Zusatzausrüstung, etwa zur Messung der Laufzeit des Funksignals zwischen BTS und MS („Timing Ad-

131) Für „International Mobile Station Identity".

132) Für „International Mobile Equipment Identity". Im UMTS-Netz wird die IMSI verschlüsselt übertragen („Extended Encrypted Mobile Subscriber Identity" [XEMSI]).

133) Für „Mobile Subscriber ISDN Number".

134) Für „Base Station Controller".

135) Für „Mobile Switching Center".

136) Für „Location Area Identity", bestehend aus Mobile Country Code (MCC), Mobile Network Code (MNC) und dem Location Area Code (LAC).

137) Für „Location Area".

138) Für „Cell Identification".

vance“ [TA]), können auch genauere Ortungen der MS erfolgen. Daneben kann ua auf Methoden der Funkpeilung oder Signalstärkemessung zurückgegriffen werden.[139]) Bei UMTS sind Funkzellen kleiner als bei GSM, was von vornherein eine genauere Ortung erlaubt.[140])

Unabhängig von einem Anruf oder SMS kann das GSM-Netz den aktuellen Standort einer MS übrigens unbemerkt auch durch Versand sog stiller SMS (auch: „Stealth Ping“ oder „Silent SMS“) ermitteln, auf welche die MS automatisch antwortet.[141]) Wer Zugriff auf die Ortungsfunktionen des Netzes hat, kann (technisch gesehen) bei Kenntnis von IMEI oder IMSI Bewegungsprofile zu einzelnen Nutzern anlegen.[142])

Zu *nicht betriebsnotwendigen* Car2Backend-basierten Komponenten und Funktionen (sog „Infotainmentfunktionen“) ist ergänzend anzumerken, dass ein gewisser Zusammenhang mit betriebsnotwendigen Komponenten insofern besteht, als etwa die Frage, ob und wieweit der Fahrer als Rückfallebene fungieren soll, naturgemäß Einfluss auf die potenzielle Reichweite erlaubter Nebentätigkeiten und damit auf die Gestaltung von Infotainmentsystemen und deren technisch-funktionelles Zusammenspiel mit betriebsnotwendigen Komponenten autonomen Fahrens hat.[143])

B. Datenschutzrechtliche Beurteilung

1. Datenschutz als Verfassungs- bzw Grundrecht

Im österreichischen Verfassungsrecht[144]) wie auch in dt Landesverfassungen[145]) ist das Recht auf Datenschutz als *grundrechtliche Gewährleistung* verankert. Diese soll sicherstellen, dass der Einzelne grundsätzlich selbst über die Preisgabe und Verwendung auf ihn bezogener Daten bestimmen kann.[146]) Die dt Rsp hat ein „Recht auf informationelle Selbstbestimmung“[147]) sowie ein „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“[148]) entwickelt. Letzteres soll gegen den staatlichen Zugriff auf in vernetzten privaten IT-Systemen gespeicherte Datenbestände schützen.[149]) Als

---

[139]) Vgl *BSI,* Mobilfunknetze (FN 130) 104 ff.

[140]) Vgl ebenda, 104.

[141]) Vgl ebenda, 66, 69.

[142]) Vgl ebenda, 112.

[143]) IdS *Cacilo et al* (FN 4) 79 f, 82, 130 ff.

[144]) Vgl § 1 Abs 1 DSG 2000.

[145]) Vgl bspw Art 4 Abs 2 VfNRW; Art 21b LV-Berlin.

[146]) IdS BVerfGE 65, 1 (42 f) zum vergleichbaren dt „Recht auf informationelle Selbstbestimmung“, welches auch der VfGH in seiner Rsp zitiert (VfSlg 19.892/2014, Abschn III Pkt 2.3.11.2).

[147]) Vgl Art 2 Abs 1 iVm Art 1 Abs 1 GG iVm BVerfGE 65, 1 (43, 44, 71); dazu *Rudolf in Merten/Papier*, Handbuch Grundrechte. Bd IV (2011) § 90 Rn 9 ff; *Simitis* in *Simitis*, BDSG-Kommentar[8] Einl Rn 27 ff (31) § 1 Rn 26 ff.

[148]) BVerfGE 120, 274; dazu bspw *Hornung*, Ein neues Grundrecht, CR 2008, 299 ff; *Rudolf* in *Merten/Papier* (FN 148) § 90 Rn 73 ff.

[149]) Vgl BVerfGE 120, 274.

bereichsspezifische Ausformung des Datenschutzgrundrechts ist im gegebenen Kontext ergänzend auf das Fernmeldegeheimnis zu verweisen.[150]) Dieses schützt während eines Telekommunikationsvorganges anfallende Daten, seien es Inhalte[151]), seien es nähere Umstände (Zeit, Ort, Kontaktnummern etc)[152]).

Die grund- bzw verfassungsrechtliche Verankerung des Datenschutzrechts und des Kommunikationsgeheimnisses haben typischerweise zur Konsequenz, dass *staatliche Beschränkungen* derselben jeweils einer *ausreichend genauen*[153]) *gesetzlichen Ermächtigung* bedürfen, welche zudem *verhältnismäßig*[154]) sein muss. Hinzu kommt, dass die Rsp aus dem Datenschutzgrundrecht auch gewisse *staatliche Pflichten* zum vorbeugenden Schutz der Privatsphäre im Verhältnis zwischen Privaten („positive Gewährleistungspflicht") ableitet.[155]) Die Zulässigkeitsregeln für die Datenverarbeitung durch Private in (allgemeinen) Datenschutzgesetzen können als eine (Teil)Erfüllung dieser Pflichten gesehen werden.

Die aktuell in Konkretisierung der Vorgaben des Verfassungsrechts, aber auch der EU-Datenschutzrichtlinie (DSRL)[156]) bestehenden einfachrechtlichen Datenschutzbestimmungen[157]) werden ab Mitte 2018[158]) weitestgehend durch die Erlaubnistatbestände und allgemeinen Datenschutzgrundsätze der EU-Datenschutz-Grundverordnung (DSGVO)[159]) ersetzt werden. Diese wiederum ist durch den EuGH am Maßstab der EU-Grundrechtecharta (GRC) auszulegen,

---

150) Vgl Art 8 Abs 1 EMRK (vgl EGMR 29. 6. 2006, 54934/00, Weber/Saravia, Rn 77); § 93 TKG.

151) Vgl Art 8 EMRK iVm EGMR 6. 9. 1978, 5029/71, Klass ua, Rn 41; 2. 8. 1984, 8691/79, Malone, Rn 64; § 93 Abs 1 und 3 TKG.

152) Vgl Art 8 Abs 1 EMRK iVm EGMR 2. 8. 1984, 8691/79, Malone Rn 84, 89; § 93 Abs 1 und 3 TKG.

153) IdS Art 8 Abs 2 EMRK iVm EGMR 26. 4. 1979, 6538/74, Sunday Times, Rn 49; 25. 3. 1983, 5947/72, Silver, Rn 88; 12. 1. 2010, 4158/05, Gillian und Quinton, Rn 80 ff; § 1 Abs 2 Satz 1 letzter Satzteil DSG 2000 iVm VfSlg 16.369/2001, 18.146/2007, 19.657/ 2012, 19.738/2013, 19.892/2014; zu Art 7, 8 GRC s auch EuGH 8. 4. 2014, verbRs C-293/12 u C-594/12, DRI, Rn 62, 65, 66.

154) Vgl Art 8 Abs 2 EMRK iVm EGMR 4. 12. 2008, 30562/04 u 30566/04, Marper, Rn 112, 119; § 1 Abs 2 letzter Satz DSG 2000 iVm VfSlg 18.643/2008, 19.657/2012, 19.738/2013, 19.892/2014; Art 8 iVm Art 52 Abs 1 GRC iVm EuGH verbRs C-92/09 u C-93/09, Schecke, Rn 50, 65; 8. 4. 2014, verbRs C-293/12 u C-594/12, DRI, Rn 38, 45, 69.

155) IdS (zu Art 8 EMRK): EGMR 13. 6. 1979, 6833/74, Marckx, Rn 31; 2. 4. 2015, 27148/12, Ribić, Rn 89; VfSlg 14.301/1995; *Wiederin,* in *Korinek/Holoubek* (Hrsg), Bundesverfassungsrecht (1999 ff) Art 8 EMRK Rn 11; *Grabenwarter/Pabel*, EMRK[5] § 22.I.6 Rn 53 ff; *Ennöckl,* Die Zulässigkeit von Informationseingriffen in der Rechtsprechung des EGMR, in FS Machacek/Matscher (2008) 81 ff; *Adamovic et al*, Österr Staatsrecht[2] Bd 3 Rz 41.078 ff (41.086); (zu Art 2 Abs 1 iVm Art 1 Abs 1 GG): BVerfGE 96, 56 (64); *Rudolf* in *Merten/Papier,* HdB Grundrechte. Bd IV (2011) § 90 Rn 27.

156) RL 95/46/EG ABl L 281, 31.

157) Vgl va § 7 Abs 1, § 8 Abs 1 DSG 2000; s auch § 28 Abs 1 Nr 1 u 2, Abs 6 Nr 1 BDSG.

158) Mit 25. 5. 2018 (vgl Art 99 Abs 2 DSGVO).

159) VO (EU) 2016/679 ABl 2016 L 119, 1.

va anhand Art 7 („Privat- und Familienleben“) und 8 („Datenschutz“)[160]). Im Ausmaß inhaltlicher Überschneidungen[161]) Letzterer mit Art 8 EMRK wird auch die bezügliche EGMR-Rsp[162]) beachtlich.[163]) Davon unabhängig bildet die EMRK einen Bestandteil der allgemeinen Rechtsgrundsätze der EU.[164])

Wie die DSRL, so wird im Übrigen auch die spezifisch dem Schutz der Vertraulichkeit der elektronischen Kommunikation im Rahmen öffentlich zugänglicher Kommunikationsnetze bzw -dienste dienende sog „Telekom-DSRL“[165]) mittelfristig überarbeitet und durch eine unmittelbar anwendbare Verordnung neu geregelt werden.[166])

Alle vorzitierten Gewährleistungen haben gemein, dass sie nur bei der Verarbeitung „*personenbezogener*“ Daten eingreifen.[167])

2. Zum Datenschutzbezug des autonomen Fahrens

a) Zum Begriff des „personenbezogenen Datums“

Um von einem „*personenbezogenen*“ Datum sprechen zu können, muss sich dieses entweder *zur direkten* (Bsp: Name) oder *indirekten Identifizierung* einer Person („Bestimmbarkeit“) *eignen* (Bsp: TelefonNr).[168]) Umstritten ist, wo genau die Grenze der „Bestimmbarkeit“ und damit des Schutzbereiches des Grundrechts bzw der DSRL (bzw künftig der DSGVO) liegt. Die restriktivere Auffassung geht dahin, zu prüfen, ob ein konkreter Datenverwender über vernünftige, dh legale und mit verhältnismäßigem Aufwand realisierbare,[169]) Möglichkeiten zur Herstellung eines Bezugs zu einer bestimmten Person verfügt („*relativer Personenbezug*“)[170]). Verneinendenfalls soll der Verwender nicht

---

[160]) Vgl näher bei *Bernsdorff* in *Meyer* (Hrsg), Charta der Grundrechte der Europäischen Union[4] Art 7 Rn 14 ff, Art 8 Rn 12 ff.

[161]) Vgl bspw EuGH 5. 10. 2010, Rs C-400/10, McB, Rn 53; 15. 11. 2011, Rs C-256/ 11, Dereci, Rn 70.

[162]) Zum Gehalt des Art 8 EMRK s *Grabenwarter/Pabel*, EMRK[5] § 22.I.3 Rn 9 ff, 27, 33 ff; *Ennöckl* (FN 156) in FS Machacek/Matscher (2008) 95 ff.

[163]) IdS Art 52 Abs 3 GRC iVm Erl zu Art 8 GRC (ABl 2007 C 303, 17 [20]); s auch BVerfGE 130, 001 (024, 030 f).

[164]) Vgl Art 6 Abs 3 GRC.

[165]) Vgl Art 1, 5 ff RL 2002/58/EG ABl L 201, 37 idF RL 2009/136/EG ABl L 337, 11.

[166]) Vgl *EU-Kommission*, Pressemitteilung: „Ein digitaler Binnenmarkt für Europa: Kommission stellt 16 Initiativen zur Verwirklichung vor“, IP/15/4919 (Brüssel, 6. 5. 2015) 2 Pkt 12; Mitteilung KOM (2015) 192 endg vom 6. 5. 2015 der Kommission […]: Strategie für einen digitalen Binnenmarkt für Europa, 14 (15).

[167]) Vgl Art 1 Abs 1 DSGVO.

[168]) Vgl Art 4 Abs 1 iVm ErwGr 26 DSGVO; *Art 29-Gruppe*, Stn 4/2007 (WP 136) 14 ff; EuGH 6. 11. 2003, Rs C-101/01, Lindqvist, Rn 27; VfSlg 18.146/2007; VfGH 9. 12. 2008, B 1944/07; VwSlgNF 16.330 A/2004; s auch ISO/IEC 29100:2011(E) Pkte 2.5, 2.9, 2.10, 4.2.1, 4.4.

[169]) IdS *Dammann* in *Simitis,* BDSG-Kommentar[8] § 3 Rn 26 f; idS auch ISO/IEC 29100:2011(E) Pkt 4.4.

[170]) Vgl *Art 29-Gruppe*, Stn 4/2007 (WP 136) 18, 23; *dies*, Stn 5/2014 (WP 216) 11; hA in Dtl: s bspw *Gola/Schomerus*, BDSG[11] § 3 Rn 10; mwN *Dammann* (FN 169) Rn 21, 24, 32; *Roßnagel,* Datenschutz und Straßenverkehr, in 44. VGT 2006, 143.

den Datenschutzvorschriften unterfallen, uzw selbst dann nicht, wenn ein Dritter den Bezug noch herstellen könnte.[171]) Die Daten sollen insofern wie anonyme Daten behandelt werden.[172]) Die weitere Auffassung dagegen bejaht die Anwendbarkeit der Datenschutzvorschriften auf alle Fälle, in denen auch nur ein Dritter den Personenbezug herstellen kann („*absoluter Personenbezug*")[173]).[174]) Auch die Vertreter der restriktiven Deutung der „Bestimmbarkeit" weisen aber zu Recht darauf hin, dass ein und dieselbe Datenart (Bsp: IP-Adressen) je nach Kontext (spezifische Befugnisse des Empfängers) einmal bestimmbar und einmal nicht bestimmbar sein kann.[175]) Und neue technische Möglichkeiten (Bsp: „Big Data"; neue Entschlüsselungstechnologien) können vermeintlich „anonyme" Daten wieder zu personenbezogenen mutieren lassen[176]). Diesfalls sollen sämtliche datenschutzrechtliche Restriktionen wieder eingreifen. Auch auf der Stufe nicht personenbezogener Daten können insofern entsprechende Datensicherheitsmaßnahmen geboten sein (Schutz vor Weiterübermittlung).[177]) Beachtlich ist solch ein „Re-Identifizierungsrisiko", solange nicht sämtliche Identifikatoren beseitigt wurden, dh pseudonyme Daten vorliegen.[178])

b) Autonomes Fahren als Anwendungsfall

Wie aus Abschn III.A.1.a hervorgeht, erfasst beim autonomen Fahren die Fahrzeugsensorik eine ganze Reihe von Daten (Fahrzeugzustandsdaten, Fahrdynamikdaten, Daten aus der Fahrzeuglokalisierung), die vordergründig als rein technische Parameter erscheinen. Infolge der Speicherung der ein Fahrzeug identifizierenden Merkmale (ua Fahrzeug-ID) gemeinsam mit Kennzeichen und Halterdaten (Name, Adresse etc) in der zentralen Zulassungsevidenz[179]) können sie aber letztlich von staatlichen und privaten Akteuren zumindest mit der Person des Halters in Verbindung gebracht werden.[180]) Daher sind Fahr-

---

171) Vgl *Scholz* in *Simitis,* BDSG-Kommentar[8] § 3 Rn 219a.

172) Vgl mwN *Scholz* (FN 171) Rn 217a, 219a.

173) IdS Erl zu § 4 Z 1 RV 1613 BlgNR 20. GP, 36; VwGH 28. 3. 2011, 2010/17/0170-6; *Kotschy,* Das Grundrecht auf Geheimhaltung personenbezogener Daten, in JB Datenschutz 2012, 27 (51 f) (unter Berufung auf ErwGr 26 RL 95/46/EG); für Dtl: *Sachs*, Datenschutzrechtliche Bestimmharkeit von IP-Adressen, CR 2010, 547 (551); *Weichert* in *Däubler et al*, BDSG[4] § 3 Rn 13, 15; *Kremer* (FN 53) RDV 240 (244).

174) S als Überblick *Bergt,* Bestimmbarkeit als Grundproblem des Datenschutzes, ZD 2015, 365 ff.

175) Vgl *Art 29-Gruppe*, Stn 4/2007 (WP 136) 18; *Dammann* (FN 169) § 3 Rn 21, 34.

176) IdS *Art 29-Gruppe*, Stn 4/2007 (WP 136) 18; *dies*, Stn 5/2014 (WP 216) 9 f 10; *Dammann* (FN 170) Rn 34 f; („potentiell personenbezogene" Daten): Rn 36 ff.

177) IdS *Art 29-Gruppe*, Stn 5/2014 (WP 216) 11; *Dammann* (FN 169) Rn 36, 38.

178) Vgl *Art 29-Gruppe*, Stn 4/2007 (WP 136) 21; *dies*, Stn 5/2014 (WP 216) 10 f; *Weichert*, Datenschutz im Auto, in 52. VGT 2014, 285 (295); speziell im Kontext der standortbezogenen Daten s *OECD International Transport Forum – CPB*, Big Data and Transport. Understanding and assessing options (2015) 33 ff (45 ff).

179) Vgl § 47 Abs 1 KFG bzw für Dtl § 33 Abs 1 („Fahrzeugregister") StVG.

180) Je nach Befugnissen des Datenverwenders (vgl [für Behörden]: § 47 Abs 1a ff KFG 1967; § 31 ff StVG; [für Private]: § 47 Abs 2a, 3 KFG 1967, § 31a Abs 4 KHVG; § 39 Abs 1 StVG).

zeugkennzeichen schon für sich als personenbezogen zu behandeln.[181]) Videodaten aus der Umweltsensorik können bei ausreichender Qualität (Erkennbarkeit von Kennzeichen, Gesichtern) potenziell ebenfalls Individuen zugeordnet werden.[182]) Auf eine tatsächliche Zuordnung kommt es für die Bejahung des Personenbezuges gar nicht an.[183]) Sinngemäßes gilt für Daten aus der Fahrerüberwachung. Kommunikationsdaten, die mittels registrierter Mobilfunkeinrichtungen generiert werden, können jedenfalls vom jeweiligen Dienstanbieter einem Kunden zugeordnet werden.[184]) Bei Nutzung diverser Apps mittels Smartphone trifft dies darüber hinaus auf eine Vielzahl kommerzieller Drittanbieter zu.[185]) Auch bei der Kommunikation C2C bzw C2I wird – zumindest auf Stufe der Datengenerierung – grundsätzlich von einem Personenbezug ausgegangen.[186]) Insgesamt sprechen die besseren Argumente daher dafür, sämtliche durch ein Fahrzeug beim autonomen Fahren generierte Daten als personenbezogene Daten iwS zu behandeln.[187])

---

[181]) ISd *Art 29-Gruppe*, Stn 4/2004 (WP 89) 15; DSB 30. 6. 2010, K121.359/0009-DSK/2010; VwGH 28. 3. 2011, 2010/17/0170-6; 12. 9. 2016, Ro 2015/04/00117; *Kunnert*, Die abschnittsbezogene Geschwindigkeitsüberwachung (Section Control) aus datenschutzrechtlicher Sicht, ZVR 2006, 78 (81 vor FN 39); *ders,* Die fahrleistungsabhängige Maut nach dem Bundesstraßen-Mautgesetz 2002 („elektronische LKW-Maut“) aus der Perspektive von Art 8 EMRK und § 1 DSG 2000, in JB Datenschutz 2009, 117 (150); *ders* (FN 53) ZVR 2015, 481 (482); *ders* (FN 53) CR 2016, 509 (510); zu Dtl: BVerfGE 120, 378 (396 ff, 400); BVerwG 22. 10. 2014, 6 c 7.13 Rn 23; AG Coburg 7. 11. 2012, 12 C 179/12; *Payer,* Datenschutz und Verkehrsrecht, in 33. VGT 1995, 211 ff (212); *Graeger,* Unfalldatenspeicher, in 41. VGT 2003, 227; *Arzt*, Rechtsfragen der automatisierten Kennzeichenerkennung, SVR 2004, 323; *Dammann* in *Simitis,* BDSG-Kommentar[8] § 3 vor Rn 29; *Roßnagel*, Fahrzeugdaten – wer darf über sie entscheiden, SVR 2014, 281 (284); *Buschbaum/Rosak*, Kfz-Kennzeichenerfassung in Parkhäusern, ZD 2015, 354 (355).

[182]) IdS *Art 29-Gruppe*, Stn 4/2004 (WP 89) 6; DSK K120.854/0002-DSK/2005; DSB 10. 8. 2015, DSB-D202.152/0002-DSB/2015; VfSlg 18.987/2010; BVwG 30. 1. 2015, W214 2011104-1; *Kotschy,* Datenschutzrechtliche Rechtsfragen zur Videoüberwachung, in FS Machacek/Matscher (257) 260; BVerfGE 120, 378 (399, 426 f); EuGH 11. 12. 2014, Rs C-212/13, Ryneš, Rn 22; EGMR 28. 1. 2003, 44.647/98, Peck, Rn 60 ff; 24. 6. 2004, 59.320/00, Hannover, Rn 53; *Rannenberg* (FN 95), Risiken, in *Maurer et al* (FN 3) 516 (518, 519).

[183]) Vgl DSK K507.515/-021/0004-DVR/2005; *Art 29-Gruppe*, Stn 4/2007 (WP 136) 19.

[184]) Vgl § 92 Abs 3 Z 3 iVm § 96 Abs 1, 2 TKG 2003; EuGH 8. 4. 2014, verbRs C-293/12 u C-594/12, DRI, Rn 26 f.

[185]) Vgl *Rothmann et al,* Aktuelle Fragen der Geodaten-Nutzung auf mobilen Geräten, ÖAW ITA-Projektbericht Nr A63 (2012) 4, 16 ff.

[186]) Vgl *C-ITS Platform* (FN 44) Report, 13, 47, 49, 53, 58; *C-ITS Platform – WG4* (FN 41) Analysis, 5, 26, 48; ErwGr 12, Art 10 Abs 1 RL 2010/40/EU; s auch ErwGr 9 Delegierte VO (EU) 2015/962 ABl 2015 L 157, 21.

[187]) IdS *Europäischer Datenschutzbeauftragter*, Stn zur Mitteilung der Kommission über einen Aktionsplan zur Einführung intelligenter Verkehrssysteme, ABl 2010 C 47, 6 Pkt 8, 26, 36; *BfDI,* 25. TB (2013/14) Z 14.1; Anfragebeantwortung durch dt BReg vom 29. 4. 2014 BT-Drs 18/1362 (zu Frage 11); *Datenschutzkonferenz des Bundes und der Länder (DSBK)*, Entschließung vom 8./9. 10. 2014 (DS im Kfz) (= BT-Drs 18/5300, 261); *Weichert*, Big Data und Datenschutz, ZD 2013, 251 (257); *Hornung*, Verfügungsrechte an personenbezogenen Daten, DuD 2015, 359 (361 f); *Lüdemann*, Connected

3. Risiken aus Datenschutzsicht

a) Privatsphäre

aa) Daten aus der Eigenlokalisierung

Unterstellte man eine *Speicherung* von Daten aus der Eigenlokalisierung zum Zwecke späterer Nutzung, ließe sich aus diesen Daten – va wenn man nicht nur die Phase der autonomen Autobahnfahrt einbezöge – ein *Bewegungsprofil* erstellen, aus welchem *detaillierte Rückschlüsse* auf die Lebensweise des Fahrers ableitbar wären (Bsp „Work-Life-Balance"; spezifische Freizeit- bzw Konsuminteressen; Arztbesuche; Lokale uvm).[188]) Je nach Wohnform bzw Siedlungsdichte wäre zusätzlich die genaue Wohnadresse und ggf der Arbeitsplatz erschließbar. Schon mit Blick auf diesen Umstand käme solchen Profilen eine identifizierende Wirkung zu,[189]) uzw unabhängig von der Verknüpfung mit einem bestimmten Fahrzeug. Es wäre nämlich ein Leichtes, die präzisen Standortdaten einer Adresse zuzuordnen und mittels dieser in einem allgemein zugänglichen digitalen Telefonbuch die Identität des Fahrers mit großer Wahrscheinlichkeit zu ermitteln. Besagte Bewegungsprofile geben im Übrigen auch Aufschluss über das Fahrverhalten des Lenkers bzw seine „Rechtstreue" (Stichwort Pausen, Geschwindigkeitsübertretungen). Naturgemäß wecken sie auch das Interesse von Polizei- und Strafverfolgungsbehörden, aber auch von Versicherungen und diversen Dienstanbietern (Bsp: ortsbasierte Direktwerbung, fahrverhaltensbasierte Rabattmodelle von Versicherungen, Navigationsdienste etc).[190])

Für den Fahrer/Halter selbst wäre die unkontrollierte Zugänglichkeit zu seinen Bewegungsdaten überdies mit schwer abschätzbaren *Sicherheitsrisiken* behaftet (bequeme Planbarkeit von Fahrzeugdiebstahl, Wohnungseinbrüchen, Überfällen, Erpressung [„Standort Rotlichtviertel"] etc).[191])

Kontextabhängig („Rotlichtviertel"; „Spital"; „Politische Veranstaltung") können besagte Daten hohe Sensitivität[192]) erlangen und ggf sensible Daten auch

---

Cars, ZD 2015, 247 (249 f, 254); *Roßnagel*, Grundrechtsausgleich beim vernetzten Automobil, DuD 2015, 353 (355); *Rannenberg* (FN 95), Risiken, in *Maurer et al* (FN 3) 516 (518); *Hinrichs*/*Becker*, Connected Car vs Privacy – Teil 1, ITRB 2015, 164 (167, 168); aA *Rieß/Greß*, Privacy by Design für Automobile auf der Datenautobahn, DuD 2015, 391 (395); *VDA*, Datenschutz-Prinzipien für vernetzte Fahrzeuge (3. 11. 2014), Pkt III.1; *VDA/Datenschutzaufsichtsbehörden*, Muster-Information über Datenspeicher im Fahrzeug (Februar 2012) (http://www.datenschutz.sachsen-anhalt.de/service/formulare-und-merkblaetter/formulare-nicht-oeffentliche-stellen/).

188) Vgl idS („Persönlichkeitsprofilbildung") auch *DSBK,* Entschließung vom 8./9. 10. 2014 Einleitung; *OECD International Transport Forum – CPB* (FN 178) 49; *Lawson* (FN 29) 65.

189) Vgl idS *Hansen*, Das Netz im Auto & das Auto im Netz, DuD 2015, 369 vor Abschn 3.2; implizit auch *Dammann* in *Simitis,* BDSG-Kommentar[8] § 3 Rn 69.

190) Vgl idS *Rannenberg* (FN 95), Risiken, in *Maurer et al* (FN 3) (516) 523 f; s auch die Übersicht bei *Krieger-Lamina* (FN 4) 50.

191) So auch *Lawson* (FN 29) 63.

192) IdS etwa *Rannenberg* (FN 95), Risiken, in *Maurer et al* (FN 3) 516 (519, 529); *Lawson* (FN 29) 65.

iSd Legaldefinition der DSGVO[193]) sein. Standortdaten wird daher zu Recht von unabhängigen Datenschutzbehörden und Rsp eine hohe Sensibilität und Schutzwürdigkeit bescheinigt.[194]) Dass die Daten anlässlich der Teilnahme am *öffentlichen* Straßenverkehr anfallen, tut diesem Befund keinen Abbruch, da nach der Rsp auch außerhalb der eigenen vier Wände gelebte „äußere“ Beziehungen zu anderen Menschen „geheimschutzfähig“ sind.[195])

Je dichter ein Bewegungsprofil, desto individueller wird sein Charakter.[196]) Diese Eigenschaft ist insbesondere für eine allfällige *spätere Weiterverwendung* solcher Daten in „aggregierter Form“ – etwa für Zwecke der Verkehrssteuerung – von hoher Relevanz. Die Vielzahl der für Dritte sonstigen zugänglichen Nutzerdaten (Bsp: zu einem bestimmten Zeitpunkt von einer bestimmten Person an einem bestimmten Ort abgesetzte „Twittermeldung“; Filmrezension in Internetforum uÄm) erhöht das *Risiko* einer *Re-Identifizierung* solcher bloß aggregierter Standortdaten enorm.[197]) Eine *wirksame Pseudonymisierung* oder *Anonymisierung* hochindividueller Profile bedarf insofern des Einsatzes ausgefeilter Techniken.[198])

Unabhängig vom vorstehend skizzierten Szenario könnten Standortdaten auch *als Folge* von *Kartenaktualisierungen* oder bei manuellen oder automatisierten *Anfragen,* ob *Autobahnabschnitte fürs autonome Fahren freigegeben* sind, anfallen, wenn dies via Mobilfunk erfolgte.

Die Eigenheit der beim Mobilfunk zur Anwendung kommenden Vermittlungstechnik (dazu oben nach FN 126) bedingt, dass – solange eine Mobilfunkeinheit im Fahrzeug „eingeschaltet“ ist – dem Netzbetreiber, mit dessen SIM-Karte diese bestückt ist, stets der grobe Aufenthaltsort des betreffenden Fahrzeuges bekannt ist (dh die sog Location Area). Schon daraus ergäbe sich im Falle einer Speicherung ein grobes Bewegungsprofil mit ähnlichen Implikationen wie bereits oben im Kontext der „Selbstortung“ von Fahrzeugen diskutiert. Im Falle einer permanenten Verbindung zu einem Kartenserver fallen funkzellengenaue Standortdaten an.

Standortdaten fallen zwar wie Inhaltsdaten unter das Kommunikationsgeheimnis.[199]) Auch ist den Providern selbst die Speicherung und Auswertung von im Mobilfunknetz anfallenden Standortdaten – vorbehaltlich der Einwilligung der betroffenen Nutzer[200]) – grundsätzlich verboten, soweit dies nicht

---

[193]) Vgl 9 Abs 1 DSGVO.

[194]) IdS *International Working Group on Data Protection in Telecommunications,* (2001) Pkt 7; BVerfGE 120, 378 (401, 404 ff); EuGH 8. 4. 2014, verbRs C□293/12 u C□594/12, DRI, Rn 26 f, 66.

[195]) Vgl EGMR 16. 12. 1992, 13.710/88, Niemietz, Rn 29; 16. 2. 2000, 27.798/95, Amann, Rn 65.

[196]) Vgl *Lawson* (FN 29) 67.

[197]) Dies belegen diverse wissenschaftliche Versuche (vgl wieder *Lawson* [FN 29] 67).

[198]) Vgl dazu *Art-29-Gruppe*, Stn 5/2014 (Anonymisierungstechniken) 9 ff; *OECD International Transport Forum – CPB* (FN 178) 52 ff.

[199]) Vgl § 93 Abs 1–3 iVm § 92 Abs 3 Z 6 TKG 2003; Art 5 Abs 1 iVm Art 2 lit b, c RL 2002/58/EG.

[200]) Vgl § 96 Abs 2 TKG 2003; Art 9 Abs 1 und 2 RL 2002/58/EG.

unmittelbar für die Erbringung des Mobilfunkdienstes erforderlich ist.[201]) Zugleich bestehen in der EU aber in einer Mehrzahl von Mitgliedstaaten trotz gegenläufiger EuGH-Rsp[202]) gesetzliche Pflichten zur sog *Vorratsdatenspeicherung* von Mobilfunkdaten für Strafverfolgungszwecke, welche in gewissem Ausmaß auch Standortdaten umfassen.[203]) In Verbindung mit der Unmöglichkeit, absoluten Schutz gegen unrechtmäßigen Zugang zu solchen Daten zu garantieren, besteht insofern ein erhebliches Risiko für eine enorme Zahl Betroffener. Davon abgesehen ist an die Befugnisse der Strafverfolgungsbehörden zur geheimen Echtzeitüberwachung von Standortdaten zu erinnern.[204]) Für die Ortung spielen insbesondere sog „stille SMS" (s oben nach FN 140) eine wichtige Rolle.[205])

Im Falle eines automatisierten Kartenupdates, welches auf jene geographische Region fokussierte, in der sich ein Fahrzeug aktuell aufhielte, müsste dem Kartendienstanbieter zwecks Auswahl und Übermittlung des relevanten Kartenmaterials auch die Eigenposition übermittelt werden. Standortdaten bzw Bewegungsprofile fielen folglich zusätzlich beim Kartendienstanbieter an. Weithin unklar ist heute, ob Lenker beim autonomen Fahren auf den Betriebsmodus (aktiviert, deaktiviert) der für Kartenaktualisierungen genutzten On Board-Mobilfunkfunktion und damit auf die Update-Frequenz überhaupt Einfluss nehmen können werden.

Auf im Rahmen der Eigenlokalisierung neben Standortdaten ebenfalls anfallenden *Bilddaten* aus der Videodetektion (va von Landmarken) wird im nächsten Abschnitt Bezug genommen.

bb) Sonstige Daten aus der Umweltsensorik

Der kamerabasierte Teil der Umweltsensorik autonomer Fahrzeuge liefert digitales Bildmaterial über die unmittelbare Fahrzeugumgebung. Insofern kommt potenziell auch die Erfassung personenbezogener Daten über andere Verkehrsteilnehmer, seien es *Fahrzeugkennzeichen,* seien es *Gesichter* von Lenkern oder Fußgängern in Betracht.[206])

Datenschutzrisiken entstünden hier – eine entsprechende Bildauflösung vorausgesetzt – wiederum vorwiegend dann, *wenn* es zu einer *Speicherung* im oder außerhalb des Fahrzeugs käme. Motiviert könnte eine solche durch das

---

[201]) Vgl § 96 Abs 1, 2 TKG 2003; Art 6 Abs 1, 2 iVm Art 2 lit b, c RL 2002/58/EG.

[202]) Vgl EuGH 8. 5. 2014, verbRs C-291/12 u C-594/12, DRI; dazu bspw *Kunnert,* EuGH zur Vorratsdatenspeicherung: Außer Spesen nichts gewesen? DuD 2014, 774 ff.

[203]) Vgl bspw § 113b dTKG idF Art 2 G v 10. 12. 2015 dBGBl I 2218 (2222).

[204]) Vgl § 134 Abs 2, § 135 Abs 2 StPO iVm § 3 Abs 2 Z 9 Überwachungsverordnung – ÜVO.

[205]) Zur Praxis in Dtl s mwN *Krüger,* Die sogenannte „stille SMS" im strafprozessualen Ermittlungsverfahren, ZJS 5/2012, 606 ff. Für Ö eine Anwendung ausschließend dagegen die Anfragebeantwortungen der BMI vom 13. 3. 2012 (10349/AB vom 30. 3. 2012 zu 10489/J [XXIV. GP]) und vom 8. 9. 2014 (2109/AB vom 15. 9. 2014 zu 2231/J [XXV. GP]).

[206]) So auch *Rannenberg* (FN 95), Risiken, in *Maurer et al* (FN 3) 516 (518).

Ziel der Beweissicherung in Unfallsituationen sein. Schon heute wird in der Praxis auf nachträglich im Fahrzeug installierte Unfallkameras (auch: „Dashcams“) zurückgegriffen.[207]) Dem *Beweissicherungsinteresse* des Fahrers oder Dritter (Bsp: Versicherungen, Behörden) steht hier das legitime Interesse der jeweils Erfassten anderen Verkehrsteilnehmer auf Wahrung ihrer *Privatsphäre* entgegen.[208]) Letzteres speist sich ua aus dem Umstand, dass sich aus dem Bildmaterial ggf auch der genaue Zeitpunkt und Ort der jeweiligen Aufzeichnung ergeben. Hinsichtlich der potenziellen Sensibilität von Standortdaten im Allgemeinen kann an dieser Stelle auf die Ausführungen im Vorabschnitt verwiesen werden. Mittels spezieller Software kann digitales Bildmaterial im Übrigen gezielt nach bestimmten Kennzeichen oder Personen (Gesichtserkennung) durchsucht werden. Hinsichtlich der Frage des Zugangs zu den Daten stellen sich im Prinzip ähnliche Fragen wie bei Unfalldatenschreibern (dazu unten Pkt dd).

Davon abgesehen ist für andere Verkehrsbeteiligte idR entweder gar nicht ersichtlich, dass sie einer Bildaufzeichnung unterworfen werden oder es fehlt an Kenntnis der technischen Spezifik (permanente oder anlassbezogene Aufzeichnung? Erkennbarkeit von Passanten? etc).[209]) Schon diese Ungewissheit infolge fehlender *Transparenz* kann uU negative Wirkung auf die Ausübung von Grundrechten haben.[210])

cc) Daten zum Verhalten und Zustand des Fahrers

Soweit man dem Fahrer auch in autonomen Fahrzeugen noch eine aktive (Rest-)Rolle zubilligte (Rückübernahme bei Verlassen der Autobahn bzw Erreichen der „Systemgrenze“), erscheint es nicht ganz abwegig, fahrzeugseitig eine automatisierte Feststellung der Rückübernahmebereitschaft vorzusehen. Solange entsprechende Sensordaten nur während der Fahrt in flüchtigen Speichern verarbeitet würden, stellten sich primär philosophische Fragen („Will der Mensch vom Fahrzeug überwacht werden?“) bzw Fragen zur *Datensicherheit* (Online-Zugriff durch Unbefugte).

---

[207]) Zur Funktion s *Bachmeier*, Dash-Cam & Co – Beweismittel der ZPO? DAR 2014, 15 (16).

[208]) Vgl VwGH 12. 9. 2016, Ro 2015/04/00117; *Thiele,* Videoüberwachung aus Fahrzeugen – Datenschutzrechtliches zu Dashcams, in JB Datenschutz 2014, 235 (247); zur Diskussion in Dtl s (kein überwiegendes Beweissicherungsinteresse): Düsseldorfer Kreis am 25./26. 2. 2014 („Dashcams“) 1; VG Ansbach 12. 8. 2014, AN 4 K 13.01634; AG München 13. 8. 2014, 345 C 5551/14; LG Heilbronn 17. 2. 2015, Az I 3 S 19/14; LG Memmingen 14. 1. 2016, Az 22 O 1983/13; *Bihari Vass,* Minikamera am Pkw zu Beweiszwecken – rechtliche Einordnung, DAR 2010, 504 (507); *Lachenmann/Schwiering*, Datenschutzrechtliche (Un-)Zulässigkeit des Betriebs von Videokameras in PKW, NZV 2014, 291 (297); aA AG Nienburg, 20. 1. 2015, 4 Ds 155/14 ua; *Klann,* Zur Zulässigkeit der Verwendung privater Verkehrsüberwachungskameras zu Beweiszwecken, DAR 2015, 188 (190 f); *Greger*, Kamera on board – Zur Zulässigkeit des Videobeweises im Verkehrsunfallprozess, NZV 2015, 114 (116 f).

[209]) IdS *Bachmeier* (FN 207) DAR 2014, 15 (19 f); *Weichert* (FN 178) in 52. VGT 2014, 285 (309 f); s aber die Informationspflichten nach Art 13 DSGVO; s auch *Art 29-Gruppe*, Stn 4/2004 (WP 89) 22.

[210]) Vgl BVerfGE 65, 1 (43); EuGH 8. 4. 2014, verbRs C-293/12 u C-594/12, DRI, Rn 28, 37.

Spätestens dann, wenn solche Systeme das Verhalten des Fahrers etwa in den Phasen der Rücknahmeaufforderung bis hin zur tatsächlichen Rückübernahme aufzeichnen und analysieren sollten, um bei späteren Fahrten anhand von „Mustererkennung" die Rückübernahmebereitschaft besser beurteilen zu können, wird es sehr kritisch. Eine allfällige zwingende staatliche Anordnung solcher Überwachungstechniken stellte nicht zuletzt mit Blick auf die Sensibilität der Daten („Gesundheitsdaten") zweifelsohne einen gravierenden Eingriff in das Datenschutzgrundrecht des jeweiligen Fahrers dar. Hinzu kämen absehbare Begehrlichkeiten auf die *Weiterverwendung* solcher Daten zur Unfallklärung, zu einer damit in Verbindung stehenden Strafverfolgung des Lenkers, zur Beurteilung der Fahrtüchtigkeit und Zuverlässigkeit des Lenkers im Allgemeinen usw. Insgesamt ginge somit jede Form der Speicherung der hier interessierenden Daten mit einem sehr hohen Risiko für das Datenschutzgrundrecht der Betroffenen einher.

dd) Unfalldatenspeicher

Die im Kontext des autonomen Fahrens ins Treffen geführten Argumente für den zwingenden Einsatz von digitalen Unfalldatenschreibern (UDS) erscheinen auf den ersten Blick durchaus plausibel. Dessen ungeachtet werfen UDS aus Datenschutzsicht eine Reihe von Problemen auf. Zunächst stellt sich die Frage nach *Art/Umfang* (Fahrdynamikdaten, Fahrerdiagnosedaten, Insassendaten, Umweltdaten?), *zeitlicher Reichweite* (Daueraufzeichnung? Start ab „Rückübernahmeaufforderung"?) und *Ort* (im Fahrzeug, „Sicherheitskopie" in der Cloud?)[211]) der Datenspeicherung. Je nach Beantwortung ergibt sich ein höheres oder geringeres Risikopotenzial im Falle eines späteren Datenzugriffs. Welche Risiken sich dann konkret verwirklichen können, hängt entscheidend von der *Befugnisregelung für den Zugriff* auf die Daten im UDS ab. Dies einmal deshalb, da deren Offenlegung gegenüber Unfallgegnern oder Dritten (Versicherung), sei es durch „freiwillige" Herausgabe (Bsp: Werkstatt),[212]) sei es infolge gerichtlicher Anordnung[213]), für den Fahrer erheblich nachteilig sein kann (Regressforderung wegen Verschuldens), ohne dass er dies aber vor der Datenauswertung wissen bzw abschätzen kann[214]). Hinzu kommt die Gefahr der Belastung durch Daten aus dem eigenen Fahrzeug im Strafprozess[215]) als Folge behördlicher/gerichtlicher Zwangsmaßnahmen[216]). Weiters können aus der Erfassung

---

[211]) Vgl *Cacilo et al* (FN 4) 67.

[212]) Vgl etwa § 7 Abs 2 iVm § 8 Abs 1 Z 4 iVm Abs 3 Z 1 DSG 2000; § 28 Abs 2 Nr 2 lit a BDSG.

[213]) „Beweisbeschlüsse" (vgl §§ 303ff, 369 ZPO).

[214]) IdS bspw *Mielchen,* Verrat durch den eigenen PKW – wie kann man sich schützen? in 52. VGT 2014, 241 (249, 254).

[215]) Unterlaufen des Verbots von Zwang zur Selbstbezichtigung (vgl Art 6 EMRK; Art 90 Abs 2 B-VG; § 7 Abs 2, § 157 Abs 1 Z 1 StPO; EGMR 17. 12. 1996, 19187/91, Saunders, Rn 68; 21. 12. 2000, 34720/97, Heaney and McGuinness, Rn 40; VfSlg 10.291/1984; 14.988/1997; 18.164/2007); s auch *Müller*, EuGRZ 2001, 546 ff; *Grabenwarter/Pabel,* EMRK[5] § 24 Rn 123; *Mielchen* (FN 214) in 52. VGT 2014, 241 (249, 251 f).

[216]) „Sicherstellung" bzw „Beschlagnahme" (vgl § 109 ff StPO).

sonstiger Fahrzeuginsassen iVm überschießenden Beweisbeschlüssen[217]) nicht intendierte Nebeneffekte („Beziehungskrise“; Scheidung) resultieren.

Rein technisch wäre auch eine Funkübertragung der für die Unfallklärung interessanten Daten an einen externen Rechner („Cloud“) realisierbar. Ein Argument könnte die zentralisierte Auswertbarkeit im Interesse der künftigen Unfallvermeidung sein. Dass dies erhebliche Zusatzprobleme auf der Ebene der *Datensicherheit* mit sich brächte, liegt auf der Hand. Eine weitere Variable mit Relevanz für die Risikoabschätzung stellt naturgemäß die Speicher*dauer* dar. Kein besonderes Risikopotenzial wäre in der bloßen Protokollierung des Betriebsmodus („menschlicher Fahrer“, „Roboter“) zu erblicken.

cc) Daten aus Kommunikationsvorgängen (C2C, C2I, C2Backend)

Abseits des teil- bis vollautomatisierten Fahrens käme den im Rahmen von C2C und C2I kommunizierten Meldungen *rein informatorischer* bzw *Warn-Charakter* zu. Es läge jeweils am Fahrer, auf die Hinweise entsprechend zu reagieren. Im Falle des autonomen Fahrens dagegen kann es nicht bei der bloßen Visualisierung oder akustischen Signalisierung bleiben, wenn das Potenzial von C2C und C2I ausgeschöpft werden soll. Die empfangenen Verkehrslage- bzw Warnhinweise müssten vielmehr Eingang in das im Fahrzeug in der zentralen Steuerungseinheit generierte sog Umfeldmodell finden und letztlich zu entsprechenden *Steuerbefehlen* (Bremsmanöver etc) an die *Fahrzeugaktorik* führen. Daraus folgt die erhöhte *(Daten-)Sicherheitsrelevanz* von Echtheit und Richtigkeit besagter Meldungen, uzw sowohl aus Betriebs- als auch aus Verkehrssicherheitsperspektive. Denkbar wäre bspw ein Hackerangriff mit dem Ziel, durch Falschmeldungen den Verkehrsfluss zu stören oder gar Unfälle auszulösen. Aber auch aus Sicht der Akzeptanz solcher Meldungen für menschliche Fahrer spielt deren Qualität eine nicht zu unterschätzende Rolle. Bereits an früherer Stelle wurde auf das *aktuell* für C2C bzw C2I *diskutierte Sicherheitskonzept* („Public-Key-Infrastruktur“ [PKI]) Bezug genommen. Dieses Konzept unterbindet in seiner aktuellen Ausgestaltung nicht ausreichend sicher die Möglichkeit der Erstellung von Bewegungsprofilen der beteiligten Fahrzeuge bzw die Weiternutzung der Daten für ggf unerwünschte andere Zwecke als Verkehrssicherheit und -steuerung. Die einer oder mehreren zentralen Stellen bekannte fixe Verknüpfung von Langzeitzertifikaten (LTCs) mit eineindeutigen Merkmalen bestimmter Fahrzeuge (Fahrzeug-ID) iVm dem zeitlich nicht näher spezifizierten Rhythmus des Wechsels temporärer Zertifikate (TCs), der unklaren Zahl an TCs pro Paket, der Protokollierung, welche TCs jeweils mit welcher LTC angefordert wurden, und der ständige Online-Austausch der Schlüssel bergen *hohe Risiken* zur Nutzung der C2C- bzw C2I-Kommunikation *zur identifizierenden Überwachung* und *stellen* den *Nutzen* der angedachten *Pseudonymisierung* mittels wechselnden TCs *in Frage*[218]). Hinzu kommt, dass die von Fahrzeugen lau-

---

[217]) Vgl §§ 303 ff, 369 iVm § 305 ZPO.

[218]) Dazu *Wiedersheim et al,* Privacy in Inter-Vehicular Networks: Why Simple Pseudonym Change is Not Enough, in Wireless On-demand Network Systems and Services (WONS) 2010 (Conference Paper) 176 (182 f).

fend versendeten Basismeldungen (sog CAMs) *nicht verschlüsselt* werden sollen und daher potenziell von einer unbestimmten Zahl von Akteuren empfangen und für beliebige Zwecke weiterverarbeitet werden könnten.[219]) Die bloße Markierung von CAMs und DENMs („Consent markers") zwecks Erlaubnis/Unterbindung der Verarbeitung durch andere[220]) bietet keine ausreichende Absicherung.

Zur *Kommunikation C2Backend* wiederum ist anzumerken, dass das von dieser ausgehende Risiko (va Angriff auf die Fahrzeugsteuerungseinheit) bei Nutzung in nur eingeschränkter Form, etwa zur Aktualisierung von digitalen Straßenkarten in gewissen Abständen oder zur Vorabfreigabe einer bestimmten Autobahnstrecke für autonomes Fahren, eingrenzbar wäre. Eine darüber hinausgehende Nutzung/Gestaltung von Car2Backend als (SIM-Karten-basierte) „Always-On-Anwendung" iSd Generierung und Übermittlung von „Echtzeitmeldungen" an das Backend eines Herstellers zwecks Aufbereitung und Rückverteilung an „Flottenfahrzeuge" oder andere würde unweigerlich personenbezogene Bewegungsprofile entstehen lassen.

Die meisten der *bereits heute* von den Herstellern iVm anderen Dienstleistern – etwa unter dem Titel „*Connected Car*" – *angebotenen Telematikdienste* (Bsp: Fernwartung, Ferndiagnose[221]), Fernsteuerung einzelner Funktionen wie der Heizung, „Telematiktarif" von Versicherungen) bringen zwar keinerlei Mehrwert für das autonome Fahren als solches, bergen freilich umso *größere Risiken* für die Privatsphäre. Die Hersteller zielen mit diesen Diensten insbesondere darauf ab, einen permanenten Zugriff auf Fahrzeugzustands- bzw Fahrdynamikdaten und Standortdaten zu erhalten, welche sie zur Produktentwicklung („Big Data"), zur gezielten Ansprache und Bindung der Kunden (Werbung, Aufforderung zum „Werksservice"), deren Selektierung (Bsp: Garantieverlust für aggressive Fahrer) sowie zum Weiterverkauf an Dritte (ortsbasierte Dienste etc) nutzen wollen. Auf diese Weise entstehen auf den „Backends" der Hersteller *weitreichende Nutzerprofile,* die wiederum potenziell dem Zugriff durch Polizei- und Strafverfolgungsbehörden, aber auch dem Risiko unbefugten Zugriffs durch Kriminelle unterliegen. Es stellen sich damit ähnliche Probleme, wie sie bereits in Vorabschnitten (va „Eigenlokalisierung" und „Unfalldatenspeicher") diskutiert worden sind. Hinzu kommen gravierende Sicherheitsrisiken durch mögliche Angriffe auf die Steuerungseinheit, wie sie bereits oben bei C2C und C2I angedeutet wurden.

b) Informationssicherheit (Cybersicherheit)

Betrachtet man alle vorstehend angesprochenen Kommunikationskanäle in ihrer Gesamtheit, zeigt sich, dass ein breitflächiger Angriff auf ebendiese – etwa im Wege massenhafter Verbreitung von Schadsoftware via C2C bzw C2I[222])

---

[219]) IdS *C-ITS-Platform – WG-4* (FN 41) Analysis, 18, 23 f, 39 f

[220]) So der Vorschlag in *C-ITS Platform* (FN 44) Report, 58; *C-ITS Platform – WG-4* (FN 41) Analysis, 44 ff, 48 f.

[221]) Vgl ISO/AWI 20080 – Road vehicles – Information for remote diagnostic support – General requirements, definitions and use cases.

[222]) IdS *Dittmann et al*, Elektronische Manipulation von Fahrzeug- und Infrastruktursystemen, BASt Fahrzeugtechnik H F 78 (2011) 76 ff.

– massive Auswirkungen auf das Straßenverkehrssystem insgesamt haben könnte. Insofern ist auch die Thematik der Informationssicherheit (Cybersicherheit) angesprochen.[223])

4. Ausreichende Risikobegrenzung durch geltendes Datenschutzrecht?

a) Voraussetzungen rechtmäßiger Datenverwendungen nach der DSGVO

Nach der DSGVO ist eine Verarbeitung personenbezogener Daten durch *staatliche Stellen* allgemein nur *zulässig,* wenn eine unionsrechtliche oder mitgliedstaatliche *gesetzliche* Grundlage besteht und damit auf *verhältnismäßige* Weise ein im öffentlichen Interesse liegendes Ziel verfolgt oder öffentliche Gewalt ausgeübt wird.[224]) Die *Datenverarbeitung durch Private* wiederum kann sich auf eine Mehrzahl von Erlaubnistatbeständen stützen, die die DSGVO im Wesentlichen unverändert von der DSRL übernimmt.[225])

Neben der auf einer „freien“ und „informierten“ Entscheidung des Betroffenen beruhenden Einwilligung[226]) sind im vorliegenden Kontext va die Erforderlichkeit zur Vorbereitung oder Erfüllung eines Vertrages, dessen Partei der Betroffene ist,[227]) sowie die Erforderlichkeit zur Wahrung „berechtigter Interessen“ des für die Verarbeitung Verantwortlichen oder eines Dritten, welche nicht von schutzwürdigen Interessen oder Grundrechten des Betroffenen überwogen werden,[228]) zu nennen.[229]) Von zentraler Bedeutung für die Gewährleistung einer „*informierten*“ Einwilligung ist die Herstellung von ausreichender *Transparenz* durch Bereitstellung von Informationen durch den für die Verarbeitung Verantwortlichen.[230]) Für *jeden* Verarbeitungs*zweck* ist eine *separate Einwilligung* zu ermöglichen.[231])

Neben der damit angesprochenen Rechtmäßigkeit müssen auch alle anderen *allgemeinen Datenschutzgrundsätze* („Treu und Glauben“, „Zweckbindung“, „Erforderlichkeit“ [bzw „Datenminimierung“], „Richtigkeit“ und „Speicherbegrenzung“) gewahrt werden.[232])

---

[223]) Vgl zur Sicherheit von C2X *Glas et al,* Echtzeitfähige Car-to-X-Kommunikationsabsicherung und E/E-Architekturintegration in *Siebenpfeiffer* (Hrsg), Vernetztes Automobil (2014) 70 ff.

[224]) Vgl Art 6 Abs 1 lit e iVm Abs 3 und Art 8 Abs 2 GRC.

[225]) Zur Rechtslage nach der DSRL s *Dammann/Simitis*, EG-Datenschutzrichtlinie (1997) Art 7 Rn 3 ff; *Ehmann/Helfreich*, EG-Datenschutzrichtlinie (1999) Art 7 Rn 17 ff.

[226]) Vgl Art 6 Abs 1 lit a iVm Art 4 Nr 11 DSGVO; *Art 29-Gruppe*, Stellungnahme 15/2011 (WP 187) 11, 15 f, 20, 23 ff, 41 f.

[227]) VglArt 6 Abs 1 lit b DSGVO.

[228]) Vgl Art 6 Abs 1 lit f DSGVO; *Art 29-Gruppe*, Stellungnahme 6/2014 (WP 217) 30 ff.

[229]) Vgl *Buchner*, Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, DuD 2016, 155 (157 f).

[230]) Vgl idS Art 7 Abs 2 iVm Art 12 und 13 f DSGVO.

[231]) Vgl idS Art 7 Abs 2 DSGVO.

[232]) Vgl Art 5 Abs 1lit a–e DSGVO. Dazu *Buchner* (FN 229) DuD 2016, 155 (156 f); im Kontext des autonomen Fahrens *Rannenberg* (FN 95) in *Mauer et al* (FN 3) 516 (526 ff).

Zu den obzitierten allgemeinen Grundsätzen gesellt sich als weiteres zentrales Strukturprinzip die *Datensicherheit,* welche auf die Gewährleistung von Integrität und Vertraulichkeit der Daten abzielt.[233]) Schließlich werden in der DSGVO die präventiv wirkenden Grundsätze des Datenschutzes „durch Technik" („*Privacy by Design*") bzw „durch datenschutzfreundliche Voreinstellung" („*Privacy by Default*") ausdrücklich verankert.[234])

b) Ergänzende rechtliche Vorgaben mit Bezug zum Thema

Aus Art 8 EMRK hat die Rsp abgeleitet, dass es einen Anspruch auf Bewegung im öffentlichen Raum ohne systematische Beobachtung gibt[235]). In Konkretisierung des Menschenrechts auf Privatsphäre bzw des Datenschutzgrundrechts kann insofern von einem „*Recht auf anonyme Nutzung von Verkehrsinfrastruktur*"[236]) oder – spezifischer – von einem *Recht auf* eine „*spurenfreie Mobilität*"[237]) gesprochen werden. Auch verschiedene EU-Sekundärrechtsakte mit Bezügen zur vorliegenden Thematik (Telekommunikation, Intelligente Verkehrssysteme) betonen die Bedeutung der Möglichkeit zur anonymen oder pseudonymen Nutzung öffentlicher Infrastruktur.[238])

c) Zur Steuerungswirkung der Normen im vorliegenden Fall

Betrachtet man die aktuellen Angebote der Fahrzeugindustrie auf dem Sektor des „vernetzten Fahrens" sowie die zahlreichen geodatenbasierten Internetdienste, hat man – vorsichtig formuliert – *nicht* den Eindruck, dass sich diese strikt *an den allgemeinen Datenschutzgrundsätzen oder den Grundsätzen Privacy by Design/by Default orientieren.*[239]) Auch mit der *Datensicherheit* ist es nicht allzu weit her, wie jüngere Untersuchungen zeigen.[240]) Dies mag auch daran liegen, dass mit Datenschutzgrundsätzen konfligierende, aber profitträchtige Geschäftsmodelle (Bsp: Facebook) auf zu wenig Widerstand der Gesellschaft im Allgemeinen und eine unzureichende Kontrolle durch Datenschutzaufsichts-

---

[233]) Vgl Art 5 Abs 1 lit f iVm Art 32 DSGVO.

[234]) Vgl Art 25 iVm ErwGr 78 DSGVO.

[235]) Vgl EGMR 4. 5. 2000, 28341/95, Rotaru, Rn 43 f; 28. 1. 2003, 44647/98, Peck, Rn 59 ff; *Art 29-Gruppe*, Stn 4/2004 (WP 89) 6; *Achelpöhler/Niehaus*, Videoüberwachung öffentlicher Plätze, DuD 2002, 731 f; *Arzt* (FN 181) SVR 2004, 323 f; *Grabenwarter/Pabel,* EMRK[5] § 22.I.3 Rn 9.

[236]) IdS *Kunnert,* Big Brother in U-Bahn Bus und Bim, Juridikum 2006/1, 42 (46); *ders* (FN 181) in JB Datenschutz 2009, 117 (187).

[237]) IdS *DSBK*, Entschließung vom 9./10. 3. 1995 (Automatische Erhebung von Straßennutzungsgebühren); *Weichert* (FN 178) in 52. VGT 2014, 285 (289).

[238]) Vgl idS ErwGr 9 und 33 RL 2002/58/EG; ErwGr 13 und Art 10 Abs 3 RL 2010/40/EU; ErwGr 9 Delegierte VO (EU) 305/2013 ABl 2013 L 91, 1; ErwGr 8 Delegierte VO (EU) 886/2013; ErwGr 21 VO (EU) 2015/758 ABl 2015 L 123, 77; ErwGr 9, 10 Delegierte VO (EU) 2015/962, 21; s auch § 3 Satz 2 IVSG.

[239]) Vgl dazu bspw für Kanada die umfassende Analyse der Unternehmenspraxis bei *Lawson* (FN 29) 46 ff, 90 ff; *Krieger-Lamina* (FN 4) 45 ff.

[240]) IdS etwa „Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk" (US Senate, „Markey-Report"; Februar 2015); *Cacilo et al* (FN 4) 101 f.

behörden und Gerichte im Besonderen stoßen.[241]) Das typische Machtgefälle zwischen dem einzelnen Betroffenen und potenten Dienstanbietern (Oligopole oder Monopole) tragen das ihre dazu bei, dass oftmals Funktionen implementiert werden, die überwiegend dem Datensammelinteresse des Dienstanbieters (Bsp: umfassende Weiterleitung von Fahrdynamikdaten an Hersteller) und weniger dem Nutzen des Kunden (Wartung) dienen.[242])

Zahlreiche Probleme stellen sich im Privatbereich schon bei der *Handhabung der Rechtsgrundlagen* „Einwilligung“ und „berechtigtes Interesse“. Erstere erfüllt oftmals durch gezielte Intransparenz des Dienstanbieters nicht das Kriterium der „Informiertheit“[243]) und/oder es fehlt infolge fehlender Alternativen bzw ökonomischen Drucks an der „Freiwilligkeit“[244]). Der Tatbestand des „berechtigten Interesses“ wiederum eröffnet nicht zuletzt durch inkonsistente bzw zu pauschal formulierte Erwägungsgründe der DSGVO[245]) große Auslegungsspielräume. Das Machtgefälle wirkt hier in der Praxis wiederum oftmals zu Lasten Betroffener. Ein weiteres Problem bildet die Relativierung des aus Datenschutzsicht zentralen Zweckbindungsgrundsatzes durch die DSGVO selbst. So kommt eine Weiterverwendung auch für einen vom Ausgangszweck verschiedenen, aber damit „zu vereinbarenden“ Zweck in Betracht.[246]) Trotz von der DSGVO bereitgestellter Kriterien zur Abschätzung der „Vereinbarkeit“ von Erst- und Zweitzweck („Kompatibilitätstest“)[247]) birgt diese Konstruktion ein hohes Maß an Rechtsunsicherheit in sich.

Keine Rolle scheint im Übrigen der Gesichtspunkt des Anspruchs auf *anonyme Nutzung öffentlicher Straßenverkehrsinfrastruktur* zu spielen – weder bei privaten noch bei öffentlichen Akteuren.

Anzumerken ist schließlich, dass im gegebenen Kontext auch die *Begrenzung behördlicher Grundrechtseingriffe* nicht voll befriedigt. Die Sicherstellungs-[248]) und Beschlagnahmebefugnisse[249]) lassen insbesondere in Bezug auf massenhafte Datenverarbeitung einen differenzierenden, begrenzenden Regelungsansatz völlig vermissen – sieht man einmal von den Sonderfällen der Bankverbindungen bzw Briefe und Telekommunikation ab[250]). Erschwerend kommt hinzu, dass selbst rechtswidrig erhobene bzw verarbeitete Daten im Strafverfahren keinem generellen Beweisverwertungsverbot unterliegen.[251])

---

241) Vgl *Weichert,* Zur Kontrolle von Datenerhebung und -nutzung durch global agierende soziale Netzwerke und sonstige Internet-Unternehmen, in Datenschutz im digitalen Zeitalter – global, europäisch, national (2015) 151 (159 ff, 162 ff).

242) IdS *Krieger-Lamina* (FN 4) 45 f (46).

243) Vgl Art 4 Nr 11 DSGVO; s auch *Krieger-Lamina* (FN 4) 47, 54.

244) Vgl ebenda.

245) Vgl ErwGr 47–50.

246) Vgl Art 6 Abs 4 iVm ErwGr 50 DSGVO.

247) Vgl ebenda.

248) Vgl 110 ff StPO.

249) Vgl 115 ff StPO.

250) Vgl §§ 116, 138 StPO.

251) Arg e contrario aus § 123 Abs 6 f, § 140 StPO; OGH 2. 7. 1992, 15 Os 3/92-8; OGH 13. 5. 2015, 11 Os 48/15s; weiters *Schmoller*, Unvertretbares Beweismaterial im Strafprozeß, in Strafprozeß- und Vollzugsreform, Schriftenreihe des BMFJ Nr 45,

Auch an eine freiwillige Übermittlung von Daten durch Vertragspartner des Betroffenen an die Strafjustiz ist zu denken.[252]) Von Privaten (außerprozessual) rechtswidrig erlangte Beweismittel (Bsp: heimliche Videoaufnahme) sind zudem weder im Strafprozess[253]) noch im Zivilprozess[254]) als solche von einer Verwertung ausgeschlossen. Angesichts der relativ weit konzipierten Ermächtigungsgrundlagen der DSGVO besteht zudem das Risiko der Übermittlung rechtmäßig ermittelter Daten (Bsp: Dienstanbieter) ohne Zutun des Betroffenen an einen Zivilprozessgegner.[255])

5. Schlussfolgerungen

a) Regelungserfordernisse

Die Erwägungen im Vorabschnitt zeigen, dass es aktuell sowohl an steuerungswirksamen Regeln als auch an darauf Bezug habender Kontrollaktivität der Aufsichtsbehörden fehlt. Umso wichtiger erscheint es, in einer Phase mit noch relativ offener technischer Entwicklung auf Basis der generellen Datenschutzvorgaben konkrete Anforderungen zu formulieren. Diese sollten in letzter Konsequenz nach internationaler Abstimmung[256]) in generellen EU-Rechtsakten va auf den Feldern IVS (ITS; C-ITS) und „Fahrzeugzulassung“[257]) verbindlich verankert werden.

b) Vorgaben zur Datenschutzkonformität autonomen Fahrens

Auf Basis der bisherigen Ausführungen lassen sich – geordnet nach technisch-funktionellen Gesichtspunkten – nachstehende Anforderungen ableiten.

aa) Kernkomponenten

(1) Selbstortung und digitale Karten sowie Streckenfreigaben

Angesichts der unbestreitbaren Sensibilität der Standortdaten darf die „Standardeinstellung“ eines Fahrzeugs *nicht auf* deren *Aufzeichnung gerichtet* sein. Anderes gilt nur zugunsten der Funktion „Unfalldatenschreiber“ (dazu unten).

---

130 (156 f, 180, 206, 225); für Dtl S auch BGH, 11. 11. 1998 – 3 StR 181/98, BGHSt 44, 243, 249; BGH 18. 4. 2007 – 5 StR 546/06; BGHSt 51, 285 Rn 20; (Bußgeldverfahren): BVerfG, Kammerbeschluss 20. 5. 2011 – 2 BvR 2072/10, NJW 2011, 2783 Rn 12; OLG Stuttgart, Beschluss 4. 5. 2016, Az 4 Ss 543/15.

252) Vgl idS § 7 Abs 2 iVm § 8 Abs 3 Z 1 bzw Abs 4 Z 2 DSG 2000; § 28 Abs 2 Nr 2 lit b BDSG.

253) Vgl OGH 2. 7. 1992, 15 Os 3/92-8; s auch EGMR 12. 7. 1988, 10862/84, Schenk Rn 51, 53.

254) StRsp; vgl bspw OGH 29. 1. 2008, 1 Ob 172/07m mwN. Zur Diskussion in Dtl am Bsp „Dashcam“ s bspw *Greger* (FN 208) NZV 2015, 114 (116).

255) Vgl Art 6 Abs 1 lit f DSGVO („zur Wahrung der berechtigten Interessen eines Dritten erforderlich“); s auch § 180 Abs 2, 183 ff ZPO; vgl § 371 dZPO; *Mielchen* (FN 214) in 52. VGT 2014, 250, 252.

256) Vgl als Überblick zum Rechtsrahmen *Cacilo et al* (FN 4) 111 ff

257) Vgl RL 2007/46/EG ABl 2007 L 263, S iVm Vorschlag KOM (2016) 31 endg vom 27. 1. 2016 betreffend Anforderungen an die Kfz-Typgenehmigung.

Um den Anfall von Orts- bzw Bewegungsdaten anlässlich von Anfragen an einen externen Rechner zwecks *Kartenupdates via Mobilfunk* zu vermeiden, müssten solche auf eine unbedingt erforderliche *niedrige Frequenz* begrenzt werden bzw in die Disposition des Fahrers gelegt werden. Aktualisierungen via C2I mittels WLAN, welche keine Identifizierung mittels SIM-Karte erforderten, wären – auch mit Blick auf kürzere Signallaufzeiten – zu bevorzugen. Dies umso mehr, als Kartenupdates als kostenloses Service des Straßenerhalters gestaltet werden sollten (vgl oben bei FN 67). Für Anfragen betreffend die Freigabe einer Strecke für automatisiertes Fahren gelten die Erwägungen sinngemäß.

(2) Innen- und Umweltsensorik

Videobasierte Umweltsensorik wäre so zu konzipieren, dass fremde Kennzeichen oder Gesichter von Fahrzeuginsassen, Passanten etc erst gar nicht erfasst oder während der Verarbeitung zum Situationsbild in der Steuerungseinheit unkenntlich gemacht werden. Eine automatisierte laufende Kontrolle des *Fahrerzustands* wäre angesichts potenziell nachteiliger Folgen bei Weiterverwendung durch Dritte[258]) als zwingende Funktion nur ohne Speicherung denkbar und hinsichtlich der erfassten Daten auf ein Minimum zu beschränken. Alternativ könnte – quasi in Analogie zu bestehenden Ansätzen im Bereich des Infotainment (Speicherung lenkerspezifischer Einstellungen [„Klimatisierung“, „Lieblingssender“ uam]) – eine Ablage von Daten in einem portablen Speicher angedacht werden, der in der alleinigen Verfügung des Lenkers verbleibt und so Schutz vor Zugriffen als auch einen fahrzeugunabhängigen Einsatz ermöglichte.[259]) Eine akustische Überwachung muss wegen schädlicher Nebenwirkungen auf andere Grundrechte (Kommunikationsgeheimnis) außer Betracht bleiben.[260])

(3) Unfalldatenspeicher (UDS)

UDS wären so zu konzipieren, dass die zu erfassenden Datenarten *auf* ein für die Unfallrekonstruktion/-forschung *erforderliches Minimum beschränkt* bleiben und infolge laufender automatischer Überschreibung („Ringspeicher“) nur für einen kurzen Zeitraum vor, während und nach einem Unfallereignis verfügbar sind.[261]) Zudem muss die Datenintegrität gewährleistet („digitale Signierung“)[262]) und der (physikalische) Zugang schon auf technischer Ebene auf (zertifizierte) Sachverständige beschränkt werden[263]). Zu beachten ist hier auch

---

[258]) Kritisch bspw *Rannenberg* (FN 95), Risiken, in *Maurer et al* (FN 3) (516) 526.

[259]) IdS *Rannenberg* (FN 95) in *Mauer et al* (FN 3) 516 (533).

[260]) Allein aus der Gesichtsmimik kann aber ggf sogar auf den psychischen Zustand von Personen geschlossen werden (vgl idS *Wüst*, Die Vermessung des Wüterichs, Spiegel Online, 43/2009; http://www.spiegel.de/spiegel/a-656024.html).

[261]) Vgl 41. VGT 2003 AK V Pkt 1; *Schmidt-Cotta et al*, 2006 (FN 103) 46 f; *Schmidt-Cotta,* 2009 (FN 103) 182 f, 10.

[262]) 41. VGT 2003 AK V Pkt 3; *Schmidt-Cotta,* 2009 (FN 103) 182 f, 184; *Frisoni et al* (FN 97) 32.

[263]) IdS *Schmidt-Cotta et al,* 2006 (FN 103) 35, 36 f; *Brenner/Schmidt-Cotta,* Der Einsatz von Unfalldatenspeichern unter dem Brennglas des Europarechts, SVR 2008,

die komplementäre Funktion der Protokollierung des Fahrmodus („autonom“ oder „herkömmlich“). Von Letzterem müsste die Zulässigkeit des *Zugriffs auf den UDS* abhängig gemacht werden. Käme es während einer vom Lenker selbst pilotierten Fahrphase zu einem Unfall, dürfte der Zugang zu UDS-Daten gegen den Willen des Lenkers aus Verhältnismäßigkeitsgründen nur bei schwerem Personenschaden oder Todesfolge erlaubt sein.[264]) Anderes hätte mit Blick auf Produkthaftungsfragen wohl für vollautonome Fahrphasen zu gelten.[265]) Eine Sicherungsspeicherung der vorgenannten Daten außerhalb des Fahrzeuges wäre sowohl mit Blick auf Zugriffsschutz als auch Datensicherheit abzulehnen. Vor einer Weiterverwendung für Unfallforschungszwecke muss jedenfalls eine Anonymisierung stattfinden.[266])

bb) Zusatzkomponenten

(1) Einbettung in intelligente Verkehrssysteme (IVS) (C2C, C2I)

Insbesondere im Fall der ggf zwingend angeordneten Einbettung autonomen Fahrens in kooperative IVS müsste gewährleistet sein, dass das *Bemühen* um *Echtheit* und *Unverfälschtheit* von Verkehrsmeldungen (CAMs; DENMs) mittels Public-Key-Infrastruktur *nicht* das Prinzip der „*anonymen Fahrt*“ *in Frage stellt.* Deshalb darf bspw keine Verbindung zwischen einem Langzeitzertifikat (LTC), welches einem einzelnen Fahrzeug zugewiesen wird, und einer dieses eindeutig identifizierenden personenbezogenen Kennung (Fahrzeug-ID, Kennzeichen oÄ) hergestellt werden.[267]) Die zur Kommunikation C2C und C2I vorgesehenen „pseudonymen“ Kurzzeitzertifikate (TCs) müssten zudem in zu definierender Weise möglichst häufig gewechselt und deren (sicherheitstechnisch bedingte) temporäre Zuordnung zu einem mittels LTC bestimmten Fahrzeug möglichst kurz gehalten werden[268]). Sinngemäßes gilt für LTC-Sperrlisten.[269]) Andere Speicherungen von TCs müssten verboten werden.[270]) Um die unkontrollierte/unerwünschte Sammlung von Positionsdaten durch andere als am Verkehr teilnehmende Fahrzeuge und die öffentliche Straßeninfrastruktur

48; *Schmidt-Cotta,* 2009 (FN 103) 10, 182 f, 185; *ders,* VKU 2010, 317; ähnlich („Vier-Augen-Prinzip“ beim Zugriff) *Rannenberg* (FN 94), Risiken, in *Maurer et al* (FN 3) 535.

[264]) Vgl dazu 17. VGT 1979 AK VII Pkt 4; 18. VGT 1980 AK I Pkt 6; 41. VGT 2003 AK V Pkt 3; 44. VGT 2006 AK V Pkt 3.

[265]) Vgl *Cacilo* (FN 4) 143.

[266]) IdS 45. VGT 2007 AK VII Pkt 1; *Schmidt-Cotta,* 2009 (FN 103) 37, 82.

[267]) Vgl iSd anonymen Nutzbarkeit von Verkehrsinfrastruktur 44. VGT 2006 AK V Pkt 2 und 3; *Herrtwich et al,* Datenschutz und Straßenverkehr, in 44. VGT 2006, 132 (141); *Roßnagel* (FN 170) in 44. VGT 2006, 143, 155; *BfDI,* 25. Tätigkeitsbericht (2013/14) Z 14.1; *Art 29-Gruppe,* Stn. 8/2014 (WP 233) Pkt 6.1 (im Kontext Internet der Dinge); *Pohle/Zoch*, eCall = Der gläserne Fahrer, CR 2014, 409 (411); *VDA*, Datenschutz-Prinzipien für vernetzte Fahrzeuge (3. 11. 2014) Pkt 2; *Weichert* (FN 178) in 52. VGT 2014, 294.

[268]) IdS auch *C-ITS Platform* (FN 44) Report, 60; *C-ITS-Platform – WG-4* (FN 41) Analysis, 49.

[269]) Vgl *C-ITS-Platform – WG-4* (FN 41) Analysis, 49.

[270]) IdS *C-ITS Platform* (FN 44) Report, 59.

zu unterbinden, wäre zu prüfen, wieweit dies über eine Verschlüsselung der mit CAMs bzw DENMs verbundenen Inhaltsdaten erreichbar wäre.[271]) Spezifische verbindliche[272]) Verwendungsregeln wären ergänzend festzulegen (Bsp: keine auf Identifizierung gerichtete Verarbeitung für Verkehrslenkungszwecke; Weitergabe an Dritte nur in anonymisierter Form; Verbot der Speicherung in Fahrzeugen; raschestmögliche Datenlöschung im sonstigen System; begrenzte Gültigkeitsdauer von LTCs; keine Nutzung von CAMs/DENMS zur Mauterhebung[273])). Ob die Erfüllung dieser Anforderungen tatsächlich die anonyme Fahrt gewährleisten kann und C2C bzw C2I dann noch funktionellen Mehrwert brächten, kann hier nicht abschließend beurteilt werden.

An den besagten Anforderungen würde auch die Stützung der Teilnahme an C2C bzw C2I auf die *Einwilligung* der Lenker im Grunde nichts ändern. Eine solche Konzeption indizierte vielmehr technisch ungelöste Problemlagen und wäre zutreffendenfalls in punkto Freiwilligkeit zu hinterfragen. Anzumerken ist zudem, dass eine Einwilligung als Opt-in- und nicht bloß als Opt-out-Option gestaltet sein müsste, da die DSGVO für eine gültige Einwilligung eine *aktive Willensbetätigung* fordert[274]).[275]) Eine Opt-out-Lösung käme insofern nur in Betracht, um Einzelnen die Möglichkeit zu geben, sich einer generell durch Gesetz angeordneten Datenerhebung zu entziehen. Eine solche Option zieht aber zugleich die Legitimität des Eingriffs, dh die Erforderlichkeit der grundsätzlichen generellen Erhebung, in Zweifel.

Unter dem Gesichtspunkt der Gesamtarchitektur sei angemerkt, dass grundsätzlich Lösungen, die primär auf die direkte Kommunikation C2C (via WLAN) abzielen, solchen vorzuziehen wären, bei denen die Informationen stets den Umweg über eine Verkehrszentrale nehmen müssen.[276]) Verkehrszentralen sollten im Übrigen öffentliche Dienstleister sein, die Daten direkt aus der Kommunikation der Fahrzeuge mit öffentlicher straßenseitiger Infrastruktur beziehen und nicht auf einer zusammenfassenden Verarbeitung von Daten auf Backends Privater (Hersteller ua)[277]) angewiesen sein.[278])

(2) Sonstiges („Infotainmentdienste“ uÄ)

Sollen die oben skizzierten Datenschutzziele erreicht werden, müssen sonstige fahrzeugseitige, herstellerseitige oder von Dritten bereitgestellte Infotainmentkomponenten strikt von den hier diskutierten Kern-Funktionen des autono-

---

[271]) Vgl dazu *Dubitzky*, Das Fahrzeug als Sensor, ATZelektronik 2015, H 2, 38 (42).

[272]) Codes of Conduct wären nicht ausreichend (aA *Eck*, Digital, sicher, vernetzt, individuell, Internationales Verkehrswesen 2015 H 1, 16 [17]; *C-ITS Platform* [FN 44] Report, 60; *C-ITS-Platform – WG-4* [FN 41] Analysis, 49).

[273]) Vgl dagegen das problematische Bsp in *C-ITS Platform* (FN 44) Report, 53.

[274]) Vgl Art 4 Nr 11 iVm ErwGr 32 DSGVO. IdS auch *Buchner* (FN 229) DuD 2016, 155 (158).

[275]) Anders aber die Konzeption in *C-ITS Platform* (FN 44) Report, 13, 48, 56 f, 75; *C-ITS-Platform – WG-4* (FN 41) Analysis, 44 f.

[276]) IdS im Kontext des autonomen Fahrens *Rannenberg* (FN 95), Risiken, in *Maurer et al* (FN 3) 516 (533).

[277]) Vgl dazu *C-ITS Platform* (FN 44) Report, 81.

[278]) Unkritisch dagegen *Cacilo et al* (FN 4) 93.

men Fahrens getrennt bleiben und auf rein freiwilliger Nutzung beruhen.[279]) Keine Lösung bilden Pauschaleinwilligungen. Für jeden Verarbeitungszweck müssen Legitimität und die Begrenzung der verarbeiteten Daten auf den erforderlichen Umfang gewährleistet werden.[280]) Im spezifischen Kontext des automatisierten Fahrens ist insofern entscheidend, dass Nutzer nicht über die (fehlende) Relevanz von Datenverarbeitungen für die Kernfunktionen des autonomen Fahrens getäuscht werden dürfen.[281]) Generell ist zu bemerken, dass Anwendungen, die darauf abzielten, einen ständigen, dem Fahrzeug zuordenbaren Datenstrom aus diesem heraus an einen externen Rechner („Cloud") zu generieren und damit das Fahrzeug quasi permanent „an die digitale Leine" zu nehmen, naturgemäß den im Vorabschnitt diskutierten Datenschutzanforderungen zuwiderlaufen würden. Rechtspolitisch wäre daher anzustreben, die bereits bestehenden herstellerspezifischen, nicht datenschutzfreundlichen (SIM-Karten-basierten) und auch langsameren[282]) Car2Backend-Lösungen für Echtzeit-Verkehrsinformation[283]) mittelfristig durch öffentlich organisierte bzw bereitgestellte C2C bzw C2I-Lösungen abzulösen. Dies gilt sinngemäß für flottenbasierte Systeme zur Aktualisierung von digitalem Kartenmaterial. Schließlich sollte es keinerlei Zwang geben, die Funktion „automatisiertes Fahren" zu verwenden. Fahrzeuge müssten also so konzipiert werden, dass sie auch völlig ohne Datensammlung und -weitergabe sicher betrieben werden können.[284])

IV. Szenario 2 – „Robotertaxi"

A. Zum technischen Sachverhalt

Vom Szenario „Autobahnpilot" (mit „Verfügbarkeitsfahrer") unterscheidet sich das *Robotertaxi* zunächst wesentlich darin, dass es keinerlei menschlichen Fahrer mehr gibt. Daraus folgt, dass es im Fahrzeug keiner herkömmlichen „Mensch-Maschine-Schnittstelle" (Lenkrad etc) mehr bedarf.[285]) Gleichwohl wird aus Sicherheitserwägungen – ähnlich wie in öffentlichen schienengebun-

---

[279]) IdS *Europäischer Datenschutzbeauftragter,* zsf Stn zu eCall, ABl 2014 C 38, 8 Pkt 65; *Bönninger/Schüppel*, Vertrauen erhalten – Datenschutz und Datensicherheit bei modernen Fahrzeugen, ZVR 2015, 474 (479); *Römmele,* Automatisiertes Fahren erfordert sichere Netze, ATZelektronik 2015, H 28 (32).

[280]) Vgl idS Art 5 Abs 2, Art 6 Abs 1 lit a, Art 7 Abs 2 und 4 iVm ErwGr 32 DSGVO; s auch *Rannenberg* (FN 95) *in Mauer et al* (FN 3) 516 (526 ff); *DSBK,* Entschließung vom 8./9. 10. 2014 (DS im Kfz); *Buchner* (FN 229) DuD 2016, 155 (157).

[281]) Zutreffend *Rannenberg* (FN 95) *in Mauer et al* (FN 3) 516 (529); *DSBK*, Entschließung vom 8./9. 10. 2014 („Datenschutz im Kfz").

[282]) Die Signallaufzeit bei mobilfunkbasierten Backend-Lösungen ist länger als im für C2C bzw C2I entwickelten ITS G5-Standard (WLANp) (vgl *Cacilo et al* [FN 4] 99).

[283]) Vgl Bsp bei *Cacilo et al* (FN 4) 90 f.

[284]) Vgl *Kunnert* (FN 53) ZVR 2015, 481 (483); *ders* (FN 53) CR 2016, 509 (511); ähnlich iS eines „Datensammel-Opt-outs" *Krieger-Lamina* (FN 4) 77.

[285]) Vgl *Winner/Wachenfeld,* Auswirkungen des autonomen Fahrens auf das Fahrzeugkonzept, in *Maurer et al* (FN 3) 265 (280).

denen Verkehrsmitteln – eine Art *Notbremse* verfügbar sein müssen, um in definierten Ausnahmesituationen (Bsp: gesundheitliche Probleme eines Fahrgastes, Unfall) das Anhalten bzw Verlassen des Fahrzeugs zu ermöglichen.[286]) Es liegt nahe, dass im Falle der Betätigung der Notbremse eine Sprechfunkverbindung, ggf auch eine Videoverbindung zu einer Taxizentrale und/oder einer Notrufzentrale aufgebaut würde.[287]) Plausibel wäre es, daneben eine Art *Alarmknopf* für Fälle vorzusehen, dass es zwischen Fahrgästen zu Problemen kommen sollte (Bsp: aggressives Verhalten) – ebenfalls verbunden mit der Öffnung eines Sprech- bzw Videokanals zu einer „Sicherheitszentrale“. Weiters könnte das Interesse der Robotertaxi-Betreiber bestehen, zwecks Vorbeugung gegen bzw zwecks erleichterter Aufklärung mutwillige(r) Sachbeschädigungen auf technische Mittel zur *Überwachung der Fahrgäste* (bspw Videoaufzeichnung) zurückzugreifen. Eine zentrale Komponente eines Robotertaxidienstes würde im *Reservierungs- bzw Bezahlsystem* bestehen. Vermutlich würden die Betreiber neben festen Rufeinrichtungen an Haltestellen auf die Reservierung/Bezahlung mittels Smartphone („Mobile App“) setzen[288]) und neben der Angabe des Abfahrtsorts auch jene des Fahrziels verlangen. Auch eine Anbindung an soziale Netzwerke iSd automatisierten Routenplanung auf Basis dort geposteter Mobilitätswünsche ist denkbar.[289]) Weiters ist davon auszugehen, dass es im Interesse der Effizienzmaximierung (gleichmäßige Verteilung, Wartungsoptimierung) eine Art automatisiertes *Flottenmangement* auf Basis von laufend an einen zentralen Rechner gesendeten Positionsdaten geben wird.[290]) Solcherart wäre jedes Fahrzeug jederzeit lokalisierbar. Denkbar wären ergänzende Infotainmentangebote für die Fahrgäste (Bsp: WLAN in der Fahrgastzelle). Sieht man von der hier nicht näher diskutierten komplexen Kommunikation zwischen Robotertaxi und nicht motorisierten anderen Verkehrsteilnehmern (Fußgänger, Aufsichtspersonal)[291]) oder von erhöhten Anforderungen an das digitale Kartenmaterial (urbane Zonen!)[292]) ab, dürften sich die sonstigen im Szenario 2 erforderlichen Komponenten (Eigenlokalisierungsfähigkeit, UDS etc) mit jenen des Szenario 1 decken.

B. Datenschutzrechtliche Beurteilung

1. Risiken aus Datenschutzsicht

Aus den im Vorabschnitt getroffenen Annahmen ergibt sich eine Mehrzahl von Risiken für die Privatsphäre von Fahrgästen. Zu verweisen ist einmal an

---

[286]) IdS *Biker* (FN 52), Personentransportsystem, in *Maurer et al* (FN 3) 291, 302; *Wachenfeld et al* (FN 21) Use Cases, in *Maurer et al* (FN 3)10 (20, 21, 34); *Gasser* (FN 3), Rechtsfragen, in *Maurer et al* (FN 3) 554 (559).

[287]) IdS *Biker* (FN 52), Personentransportsystem, in *Maurer et al* (FN 3) 291, 293, 302.

[288]) IdS ebenda, 291.

[289]) Vgl *Wachenfeld et al* (FN 21) Use Cases, in *Maurer et al* (FN 3) 10 (20).

[290]) IdS *Biker* (FN 52), Personentransportsystem, in *Maurer et al* (FN 3) 302; *Gasser* (FN 3), Rechtsfragen, in *Maurer et al* (FN 3) 554 (561 ff).

[291]) Näheres bei *Färber,* Kommunikationsprobleme zwischen autonomen Fahrzeugen und menschlichen Fahrern, in *Maurer et al* (FN 3) 127 ff (137 ff).

[292]) Vgl *Cacilo et al* (FN 4) 88.

eine technisch *mögliche lückenlose Video- und Audioüberwachung* im Fahrgastraum unter Berufung auf Eigentumsschutz (Stichwort: „Vandalismus“) und „Fürsorgepflichten“ gegenüber den Fahrgästen. Dies bedrohte nicht nur Datenschutzrechte, sondern potenziell auch das *Telekommunikationsgeheimnis* von Fahrgästen (Stichwort „Mobiltelefonie im Fahrgastraum“). Im Falle personalisierter Bestell- und Abrechnungssysteme würden die Betreiber von Robotertaxidiensten im Unterschied zu heutigen Funktaxizentralen zusätzlich zu Telefonnummer und Abfahrtsort des Bestellers auch die genaue Fahrtroute zentral erfassen. Damit ließen sich wiederum *Bewegungsprofile* erstellen, auf deren generelle Problematik bereits im Szenario 1 eingegangen wurde. Die Bereitstellung von WLAN in den Fahrgastzellen eröffnete den Betreibern potenziell auch die *Kontrolle über genutzte Internetdienste* (aufgerufene Seiten etc).[293]) All diese Aspekte werfen auch Fragen der praktischen Herstellung datenschutzrechtlich geforderter *Transparenz* auf. Das bereits im Szenario 1 angesprochene Risiko eines Angriffs auf die zentralen Steuergeräte, welches aus der Vernetzung der Fahrzeuge resultiert, kann sich auch im Szenario 2 realisieren und gravierende Folgen nach sich ziehen (Entführung von Fahrzeugen, Herbeiführung eines Unfalls etc).

2. Schlussfolgerungen aus Datenschutzsicht

Um den vorstehend skizzierten Risiken vorzubeugen bzw diese zu mindern, bedürfte es einer *konsequenten Ausgestaltung* von Robotertaxidiensten unter Zugrundelegung der Grundsätze „*Privacy by Design*“ und „*Privacy by Default*“. So sollten die Nutzer die Möglichkeit haben, sich auf einschlägigen Plattformen von Taxidiensten *pseudonym/anonym* zu *registrieren* und die Bezahlung mittels *vorausbezahlter Wertkarten* vorzunehmen. Mittels zusätzlicher Schutzmaßnahmen auf Seite der Kunden (Verschleierung der IP-Adresse) könnten entstehende Nutzerprofile dann nicht ohne weiteres konkreten Personen zugeordnet werden. Jedenfalls müssten nach erfolgter Bezahlung und Ablauf einer (kurzen) Reklamationsfrist *sämtliche ortsbezogenen Daten* aus den beim Dienstanbieter für buchhalterische Zwecke aufbewahrten Datensätzen *entfernt werden.* Nur so könnte das Risiko späterer Re-Identifizierungen begrenzt werden. Analoges bietet sich für personalisierte Bezahlvarianten an. Auch das Risiko der späteren Zweckentfremdung (Behördenzugriff, Kommerzialisierung, Kriminalität) entstehender personenbezogener Bewegungsprofile würde so begrenzt. Eine *akustische Überwachung* der Fahrgastzellen *müsste* mit Blick auf Seiteneffekte auf andere Grundrechte *jedenfalls unterbleiben.* Die *nachträgliche Nutzung* allfälliger Video*aufzeichnungen* müsste durch generelle Regeln *strikt* auf bestimmte legitime Fälle *begrenzt* werden und technischen (Verschlüsselung!) und verfahrensrechtlichen (Einbindung des betrieblichen Datenschutzbeauftragten usw) Sicherungen unterliegen. Für Fälle von Cyberangriffen auf die Fahrzeugsteuerung müsste Vorsorge getroffen werden, dass bspw *Nothaltewünsche* von Fahrgästen den *Autopiloten jedenfalls automatisch übersteuern.*

---

[293]) Vgl *Lawson* (FN 29) 63, 64.

V. Resümee

Wiewohl heute auf dem Felde des autonomen Fahrens noch einiges an technischer Entwicklungsarbeit bevorsteht und unklar ist, ob und wann ein wirklich sicheres System einsatzbereit sein wird, zeichnen sich gewisse Szenarien ab. Deren vorläufige Evaluierung zeigt *erhebliche Risikopotenziale aus Grundrechtssicht* auf. Sollen diese bewältigt werden, bedarf es nicht nur eines intensiven Dialogs zwischen Technikern und Rechtsexperten, sondern wohl auch gewisser *funktioneller Beschränkungen,* die infolge widerstreitender Interessenlagen nicht auf Verständnis aller Akteure stoßen werden. Nur wenn der Fokus klar auf die Kernfunktionen, die für Verkehrs-, Betriebs- und Datensicherheit zwingend erforderlich sind, gelegt wird und gleichzeitig von einer Verquickung mit rein kommerziellen Weiterverwendungsinteressen abgesehen wird, bestehen Chancen auf eine grundrechts- und insbesondere datenschutzkonforme Realisierung.[294]) Weitgehend *ungelöst* ist insbesondere die Frage des *wirksamen Schutzes vor* der *Ausspähung und Kommerzialisierung* des *Mobilitätsverhaltens* im Kontext der Vernetzung von Fahrzeugen (C2C, C2I, C2X). Unabdingbar erscheinen zudem bereichsspezifische zwingende gesetzliche Vorgaben auf EU-Ebene.[295]) Nicht nur wegen der grenzüberschreitenden Dimension der Thematik (Einheitlichkeit der Standards)[296]), sondern auch wegen stark divergierender Interessenlagen unterschiedlich mächtiger Akteure bzw Betroffener, die aus heutiger Sicht ihren „gerechten“ Ausgleich nicht im Wege des freien Spiels der Kräfte finden werden.

---

[294]) Anders aber Pkt II.b der Amsterdamer Erklärung (FN 45).
[295]) Diesbezüglich unambitioniert ebenda, Pkt IV.c.
[296]) IdS ebenda, Pkt II.a und V.c–d.