DATENSCHUTZ BEIM HOCHAUTOMATISIERTEN FAHREN DER ZUKUNFT

Yvonne Prieur / Andreas Sesing-Wagenpfeil / Christian Müller

Yvonne Prieur, Juristin sowie Gesundheitswissenschaftlerin und externe Dozentin an der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW), Elfenauweg 9, 3006 Bern, CH
yvonne.prieur@bluewin.ch

Dr. iur. Andreas Sesing-Wagenpfeil, Wissenschaftlicher Mitarbeiter und Geschäftsführer, Universität des Saarlandes, Institut für Rechtsinformatik, Campus A5 4, 66123 Saarbrücken, DE
andreas.sesing@uni-saarland.de, https://www.rechtsinformatik.saarland

Dr.-Ing. Christian Müller, Leiter des Kompetenzzentrums Autonomes Fahren am Deutschen Forschungszentrum für Künstliche Intelligenz, Stuhlsatzenhausweg 3, Saarland Informatics Campus D 3_2, 66123 Saarbrücken, DE
christian.mueller@dfki.de, www.dfki.de

Schlagworte: ***Datenschutz, hochautomatisiertes Fahren, künstliche Intelligenz***

Abstract: *Hochautomatisierte Fahrzeuge sind ohne die Verarbeitung von großen Datenmengen undenkbar. Dies beruht einerseits darauf, dass entsprechende Systeme auf Verfahren Künstlicher Intelligenz (KI) fußen und daher bereits die Entwicklung nicht ohne umfassende Trainingsdatensätze auskommen. Andererseits kann die Fahraufgabe nur dann hochautomatisiert bewältigt werden, wenn das Fahrzeug seine Umwelt möglichst detailgetreu wahrnimmt. Der Beitrag skizziert die technischen Rahmenbedingungen des hochautomatisierten Fahrens und beleuchtet aus europäischer, deutscher und schweizerischer Perspektive die datenschutzrechtliche Fragestellung des hochautomatisierten Fahrens unter Einbeziehung der aktuellen Gesetzgebung sowie laufenden Gesetzesrevisionen.*

1. Ausgangslage

Schon heute erzeugen neuere Fahrzeuge eine Fülle von Daten.[1] Beim hochautomatisierten Fahren der Zukunft (SAE-Stufe 4[2]) kommt zur ohnehin vorhandenen Datenmenge hinzu, dass das Fahrzeug seine gesamte Umgebung erfassen muss, um sich sicher auf der Straße bewegen zu können. Dabei stehen aus datenschutzrechtlicher Sicht eine Vielzahl von Fragen im Raum, beispielsweise, ob und wie das hochautomatisierte Fahrzeug (HAF) personenbezogene Daten von Fahrzeuginsassen sowie anderer Verkehrsteilnehmenden erfasst, verarbeitet und speichert – und insbesondere, ob all dies (datenschutz-)rechtlich zulässig ist.

Der nachfolgende Beitrag beschreibt zunächst die erforderlichen Datenverarbeitungsvorgänge beim Betrieb hochautomatisierter Fahrzeuge aus technischer Sicht (2.) und nimmt sodann eine rechtliche Einordnung der Vorgänge aus der Perspektive des deutschen und unionalen Rechts (3.) sowie des schweizerischen Rechts (4.) vor, wobei in die rechtlichen Überlegungen sowohl das Datenschutzrecht als auch das Straßenverkehrsrecht einbezogen werden.

---

1 ADAC-Bericht: „Welche Daten werden in aktuellen Autos erhoben, gespeichert, gesendet“, 2016.

2 Beim hochautomatisierten Fahren der SAE-Stufe 4 übernimmt ein Fahrautomatisierungssystem zeitweise die gesamte dynamische Fahraufgabe, s. hierzu *SAE*, Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems, abrufbar unter https://www.sae.org/standards/content/j3016_202104. Alle Internetquellen wurden zuletzt am 14.11.2021 abgerufen.

2. Datenverarbeitung aus technischer Sicht

Die Verarbeitung von Daten ist für das hochautomatisierte Fahren in verschiedener Hinsicht von Bedeutung. Der sichere Betrieb eines HAF erfordert – worauf nachfolgend der Fokus gelegt werden soll – einerseits eine laufende Verarbeitung von (Sensor-)Daten während des Betriebs (2.1.), anderseits ist die Verarbeitung von Daten auch ein essenzieller Bestandteil in der Entwicklung von entsprechenden Fahrzeugsystemen, soweit diese auf Verfahren des maschinellen Lernens basieren (dazu 2.2.).

2.1. Datenverarbeitung beim Betrieb eines HAF

Bezüglich der Frage, welche technischen Subsysteme eines HAF personenbezogene Daten während des Betriebs im Straßenverkehr verarbeiten, werden nachfolgend diejenigen Komponenten betrachtet, an denen sie erzeugt werden. Bei einem hochautomatisierten Fahrzeug sind dies vor allen Dingen die Sensoren (außen und innen). Es gibt darüber hinaus Datenquellen, die nicht unmittelbar für die Fahrautomatisierung benötigt werden, aber dennoch in HAF verstärkt zu erwarten sind.

2.1.1. Sensortechnik

Ein hochautomatisiertes Fahrzeug nimmt seine Umgebung über Sensoren wahr, zu denen die Sensoren Kamera, Lidar und Radar gehören.

2.1.1.1. Lidar

Lidar (light detection and ranging) ist eine Methode zur optischen Abstands- und Geschwindigkeitsmessung auf Basis von Laserstrahlen. Im Zusammenhang mit HAF werden zwei Arten von Lidar-Sensoren verwendet: rotierende Lidarsensoren und feststehende Lidarsensoren (solid state lidar). Rotierende Lidarsensoren sind in der Regel in Prototypen verbaut und werden hauptsächlich auf dem Dach befestigt. Ein sehr schnell rotierender Spiegel lenkt den sich fortbewegenden Laserstrahl ab und erzeugt dadurch eine so genannte Punktewolke. Die Punktewolke aus rotierenden Lidarsensoren kann als die informationsreichste Datenquelle zur Umgebungswahrnehmung automatisierter Fahrfunktionen angesehen werden. Allerdings gibt es eine Reihe von Argumenten, diese Systeme nicht für die Serienfertigung zu verwenden, angefangen von ihrem sehr hohen Preis bis hin zu Designaspekten („Pickel auf dem Dach“). Mit dem Ziel einer serientauglichen Lösung arbeiten einige Hersteller an Solid-State-Lidarsystemen (feststehenden Lidarsystemen), die keine beweglichen mechanischen Elemente enthalten. Hersteller von Scheinwerfern und Rückleuchten planen, die Sensoren in ihren Produkten zu verbauen.[3]

2.1.1.2. Radar

Das *Radarsystem* funktioniert ähnlich wie das Lidarsystem. Der hauptsächliche Unterschied besteht darin, dass es Radiowellen anstelle von Lasern verwendet. Radiowellen werden jedoch weniger absorbiert als Licht, wenn sie Objekte berühren. Somit können sie über eine relativ lange Distanz arbeiten. Das Radarsystem ist gegenüber den heutigen Lidarsystemen relativ kostengünstig und funktioniert auch bei allen Wetter- bzw. Umweltbedingungen wie Nebel, Regen, Schnee und Staub. Es ist jedoch weniger winkelgenau als Lidar, da es in Kurven die Sicht auf das Zielfahrzeug verliert. Es kann darüber hinaus zu falschen Ergebnissen kommen, wenn mehrere Objekte sehr nahe beieinander platziert werden, z.B. können zwei kleine Autos in der Nähe als ein großes Fahrzeug wahrgenommen und ein falsches Annäherungssignal gesendet werden.

[3] Vgl. https://www.hella.com/hella-com/en/press/Company-Technology-Products-08-01-2019-17627.html.

„Imaging Radar“ ist eine Radaranwendung zur Erzeugung von 2D-Bildern oder sogar 3D-Punktwolken unter Verwendung der reflektierenden Energie des Radars durch schnelle Erzeugung von Radarimpulsen. Dies wird seit Jahren in der Luft- und Raumfahrtindustrie für Anwendungen wie Landkartierung und Wetter verwendet. Es wurde bisher nicht für Kfz-Radar verwendet, möglicherweise aufgrund von Leistungs- und Verarbeitungsbeschränkungen, wird aber sicherlich im Fokus der Entwicklungsbestrebungen sein.

2.1.1.3. Kamera

Von allen genannten Sensoren ist die *Kamera* am ehesten in der Lage, personenbezogene Daten zu liefern, da die Umgebung zunächst einmal fotorealistisch abgebildet wird. Es ist also – wie bei anderen „Überwachungskameras“ auch – ohne weiteres möglich, Persönlichkeitsmerkmale zu erkennen oder die Identität von Personen festzustellen. Es können auch Kameras verwendet werden, die keine Echtfarbenbilder liefern, wie beispielsweise Wärmebildkameras. Diese erfassen nicht nur weniger Merkmale einer Person, sondern zeigen auch als Sensor zum Teil bessere Leistungen.

2.1.2. Unterschiedliche Datenschutzrelevanz verschiedener Sensortechnologien

Lidar- und Radarsensoren stellen traditionell ein wesentlich geringeres Problem dar, wenn es um den Datenschutz geht. Punktewolken sind eher grob aufgelöste Repräsentationen, aus denen zwar ersichtlich ist, ob es sich bei einem bestimmten Objekt um eine Person handelt oder nicht, die aber darüber hinaus keine Rückschlüsse zulassen. Beim Radar ist die Situation noch eindeutiger. Die gewonnenen Sensorabdrücke eines klassischen Radars sind nicht geeignet, um personenbezogene Daten zu erfassen.

Es sind inzwischen jedoch Lidarsensoren auf dem Markt verfügbar, die eine so hohe Auflösung ermöglichen, dass erfasste Personen erkannt werden könnten. Auch „Imaging Radars“ können, wie der Name bereits vermuten lässt, mehr Informationen transportieren. Es ist derzeit unklar, ob diese hochaufgelösten Lidar- und Radarsysteme tatsächlich in Serienfahrzeugen zum Einsatz kommen werden. Es ist sehr wahrscheinlich, dass in Zukunft Kameras, Lidar und Radar als Sensoren nebeneinander existieren werden. U.E. wird es bezüglich des Sensor-Setups keine Entweder-oder-Situation geben. Aber auch im Fahrzeug werden Kameras verbaut, um den Innenraum zu überwachen. Außerdem finden sich dort Mikrofone vor, die Sprache und andere akustische Ereignisse aufzeichnen. Als wichtige Datenquelle sollte schließlich noch die Standortbestimmung des Fahrzeugs genannt werden.

2.1.3. Datennutzung in Subsystemen eines HAF

Kommen wir nun zu den hauptsächlichen Subsystemen im HAF, die personenbezogene Daten verarbeiten. Die Umgebungswahrnehmung soll feststellen, wo sich Personen in der Umgebung des Fahrzeugs befinden und wie ihre angenommenen Trajektorien[4] sind. Persönlichkeitsmerkmale oder gar die Kenntnis der Identität einer Person werden nicht benötigt. Um zu verhindern, dass dennoch personenbezogene Daten weitergereicht werden, können diese Merkmale entfernt werden, z.B. durch eine „Verpixelung“ der Gesichter. Je sensornäher diese Maßnahme erfolgt, desto weniger Subsysteme kommen mit den personenbezogenen Daten in Berührung. Doch nicht nur Personen, die sich in der Umgebung der Fahrzeuge aufhalten, sind betroffen. Bei höheren Automatisierungsstufen ist es notwendig, eine oder mehrere Kameras in den Innenraum des Fahrzeuges zu richten, um überwachen zu können, dass insbesondere die Haltung und der Zustand des Fahrers den jeweiligen Fahrsituationen entsprechend ist. Andernfalls wäre nicht gewährleistet, dass eine Übergabe an den Fah-

[4] Eine Trajektorie ist der Weg, den ein Objekt mit bewegter Masse in Abhängigkeit von der Zeit durch den Raum zurücklegt.

rer beim Verlassen der ODD[5] (Level 4) oder bei kritischen Ereignissen innerhalb der ODD (Level 3) möglich ist. Unter anderem bei Tesla ist dies heute bereits Realität. Wenn die Fahrer die Innenraumkamera aktivieren, zeichnet sie laut Tesla die Momente vor einem Unfall oder der Aktivierung der automatischen Notbremsung auf und gibt sie weiter, um dem Autohersteller bei der „Entwicklung zukünftiger Sicherheitsfunktionen und Softwareverbesserungen" zu helfen, heißt es auf der Tesla-Website.[6] Teslas Ansatz steht im Gegensatz zu den so genannten Closed-Loop-Systemen, die von anderen Autoherstellern wie BMW, Ford, und GM verwendet werden. Diese zeichnen keine Daten oder Videos auf, sondern verwenden Infrarottechnologie, um die Augenbewegungen oder die Kopfposition des Fahrers zu erkennen. Solche geschlossenen Systeme weisen nicht die gleichen Datenschutzprobleme auf wie Systeme, die Daten oder Videos aufzeichnen oder übertragen.

Darüber hinaus werden Standortdaten in autonomen Fahrzeugen zwangsläufig zu Navigationszwecken erfasst und verwendet, z.B. Zielinformationen, Routeninformationen, Geschwindigkeit und Fahrzeit. Standortmerkmale werden auch in herkömmlichen Fahrzeugen verwendet, um zusätzliche Informationen für die Fahrt bereitzustellen, z.B. Echtzeit-Verkehrsdaten und interessante Punkte entlang der geplanten Route, und um Routenpräferenzen festzulegen, z.B. die Vermeidung von Autobahnen oder Mautstraßen. Ein Datensatz, der Standort- und Reisedaten (z.B. aktueller Standort, Zielort, Geschwindigkeit, Route, Datum und Uhrzeit) mit zusätzlichen Informationen über den Betreiber und den Fahrgast korreliert, könnte verschiedene Vorteile bieten. Ein solcher Datensatz kann beispielsweise bei der Verkehrsplanung, der Verringerung von Verkehrsstaus und der Verbesserung der Sicherheit helfen. Diese Art von kombinierten Datensätze können jedoch auch sensible Informationen über Einzelpersonen preisgeben, insbesondere wenn diese Informationen über einen längeren Zeitraum aufbewahrt werden.

Eine Anwendung, die in diesem Zusammenhang besondere Aufmerksamkeit verdient, ist das Spracherkennungs- und Steuerungssystem des HAFs. Verbrauchergeräte, die diese Art von Technologie nutzen, haben in der Öffentlichkeit bereits Besorgnis und Beschwerden über die Erfassung und Übertragung privater Kommunikation ausgelöst.[7] Diese Systeme verwenden häufig ein Aktivierungsstichwort („Alexa", „Hey google", usw.). Das Mikrofon ist demnach permanent offen, während das Spracherkennungssystem auf das Stichwort wartet. Zwar handelt es sich in dieser Phase ebenfalls um ein Closed-Loop-System, aber dennoch gibt es keine technische Hürde zur Übertragung sämtlicher aufgezeichneter Informationen.

Hochautomatisierte Fahrzeuge verarbeiten zahlreiche Daten, die – je nach eingesetztem Sensor – personenbezogene Merkmale von Personen im Fahrzeugumfeld sowie von Fahrzeuginsassen enthalten können. Im Fall einer Verknüpfung von Standortdaten mit den Daten der Innenraumsensoren sind dabei weitreichende Rückschlüsse auf das Verhalten einzelner Personen, insbesondere der Fahrzeuginsassen, möglich.

2.2. Datenverarbeitung bei der Entwicklung von HAF

Schließlich sollten wir noch Vorgänge betrachten, die sich nicht unmittelbar während der Fahrt abspielen. Hochautomatisierte Fahrzeuge brauchen Künstliche Intelligenz, d.h. lernende Systeme, die auf der Grundlage von zuvor gesammelten Daten antrainiert worden sind. Gerade die heute gängigen Verfahren der so genannten Tiefen Neuronalen Netze (Deep Neural Nets) brauchen eine sehr große Anzahl von Trainingsbeispielen, die möglichst situationsnah gesammelt bzw. erzeugt werden müssen. Bei diesem Vorgang fallen unter Umständen

5 Operationale Design Domäne (ODD) eines autonomen Systems beschreibt die Betriebsbedingungen, für welche es funktional ausgelegt ist. Dazu gehören zum Beispiel Verkehrsarten (Straßen-, Schienenfahrzeug), die Umgebungen, in denen es operiert (Autobahn, Landstraße, innerstädtisch, innerhalb eines geschlossenen Campus oder Bahndepots), lokale Einschränkungen (zum Beispiel auf bestimmte Städte, Vorstädte), Wetterbedingungen und viele mehr.

6 https://www.tesla.com/support/car-safety-security-features.

7 Bedenken äußerte bereits die frühere deutsche Bundesbeauftragte für den Datenschutz, Andrea Voßhoff, vgl. die Berichterstattung der Wirtschaftswoche vom 25. Mai 2016, abrufbar unter https://www.wiwo.de/unternehmen/it/google-home-datenschutzbeauftragte-warnt-vor-google-sprachassistent/13641366.html.

sehr viele personenbezogene Daten an, weil die rohen Sensorabdrücke der Fahrzeuge auf den Servern der Hersteller gespeichert werden.

Auch hier gibt es technische Möglichkeiten, den Personenbezug zu eliminieren, aber ob diese Möglichkeiten auch tatsächlich konsequent ausgeschöpft werden, ist eine große Frage. In der KI-Forschung wird derzeit unter dem Stichwort „Vertrauenswürdige KI" (Trustworthy AI oder auch TrustedAI) an Verfahren gearbeitet, die für dieselbe Leistung wesentlich weniger Daten benötigen. Des Weiteren beinhaltet Trusted AI auch Methoden zur Validierung wie auch zum Training von lernenden Systemen basierend auf synthetischen Daten. Dabei handelt es sich um möglichst situationsgetreue simulierte Szenarien, die auch menschliches Verhalten beinhalten. Die Mensch-Modelle wurden zwar zu einem bestimmten Zeitpunkt auch auf Basis von menschlichen Beispielen trainiert. Für diesen Vorgang werden jedoch erstens weniger Daten benötigt und zweitens handelt es sich dabei zumeist um systematische Aufzeichnungen mit eingeweihten Personen (statt Kameraaufzeichnungen direkt im Verkehrsgeschehen).

3. Regulatorischer Rahmen im europäischen und deutschen Recht

Der Rechtsrahmen für datenschutzrechtliche Fragestellungen im Hinblick auf hochautomatisiertes Fahren setzt sich im europäischen und deutschen Recht zusammen aus der sektorspezifischen Datenschutzbestimmungen im (nationalen) Straßenverkehrsrecht zum einen (3.1.) und der Datenschutzgrundverordnung (DSGVO) zum anderen (3.2.).

3.1. Datenschutzrechtliche Bestimmungen im deutschen Straßenverkehrsgesetz (StVG)

Bereits seit Inkrafttreten des Achten Gesetzes zur Änderung des Straßenverkehrsgesetzes vom 16.6.2017[8] enthält das StVG Vorschriften für die Zulässigkeit des Betriebs von Kraftfahrzeugen mit „hoch- oder vollautomatisierter Fahrfunktion". Bei der bisherigen Regelung hat sich der Gesetzgeber nicht an der international gängigen[9] Klassifizierung der Automatisierungsstufen der *SAE International* – der Taxonomie J3016[10] – orientiert, sondern an einer abweichenden Klassifizierung, die vom Runden Tisch Automatisiertes Fahren erarbeitet wurde.[11] Übertragen auf SAE-Kriterien soll dies nach teilweise vertretener Auffassung SAE-Level 3 und 4 entsprechen,[12] andere erachten die Differenzierung des bisherigen Rechts als „falsch gewählt".[13] Indem der Gesetzgeber bei der Schaffung von § 1a StVG eine andere Klassifizierung zugrunde gelegt hat, ist eine eindeutige Zuordnung der vom Gesetz erfassten Automatisierungsstufen zu den SAE-Levels nicht möglich, wobei aufgrund der stets erforderlichen Rückfallebene eines menschlichen Fahrzeugführers ein weitgehender Gleichlauf mit SAE-Level 3 naheliegt. Die bisherigen Regelungen haben sich hinsichtlich der datenschutzrechtlichen Regelungen darauf beschränkt, eine Aufzeichnung darüber, ob ein hoch- oder vollautomatisiertes Fahrzeug von einem menschlichen Fahrzeugführer oder von der Steuerungssoftware gelenkt wird, verbindlich vorzuschreiben (sog. „Fahrmodusspeicher"; vgl. § 63a Abs. 1 StVG). Dabei wurde der Fahrzeughalter durch das Gesetz als derjenige bestimmt, der die aufgezeichneten Daten bei der Verwicklung des Fahrzeuges in ein Unfallereignis an Dritte herauszugeben hat (§ 63a Abs. 3 StVG). Dies legt nahe, dass das Gesetz bis-

8 BGBl. I 2017, S. 1648.

9 Die *SAE*-Taxonomie liegt etwa der EU-Strategie für die Mobilität der Zukunft zugrunde, vgl. *Europäische Kommission*, KOM(2018) 283 final, S. 5.

10 Siehe den Nachweis oben sub 1.

11 BT-Drs. 18/11300, S. 12 f.; das zugrundeliegende Gutachten „Automatisiertes Fahren im Straßenverkehr" von April 2017 ist abrufbar unter https://www.bmvi.de/SharedDocs/DE/Anlage/G/wissenschaftlicher-beirat-gutachten-2017-1.pdf.

12 Beck, in: Münchener Anwaltshandbuch IT-Recht, 4. Aufl. 2021, Teil 9.2 Rn. 56.

13 Steege, SVR 2021, S. 128 (130).

lang den Fahrzeughalter als Verantwortlichen für die Datenverarbeitung ansieht,[14] wobei bezweifelt werden muss, dass der Fahrzeughalter ohne Inanspruchnahme fremder Hilfe überhaupt zur Erfüllung der Pflicht zur Datenherausgabe imstande ist.

Mit Wirkung vom 28. Juli 2021 ist das StVG durch das „Gesetz zum autonomen Fahren“[15] erweitert worden.[16] Gegenstand der Neuregelung sind ausweislich des § 1e Abs. 1 StVG Kraftfahrzeuge mit autonomer Fahrfunktion. Anders als das bislang geltende Recht orientiert sich die Neuregelung nunmehr hinsichtlich ihres Anwendungsbereichs dabei an der Klassifizierung der Automatisierungsstufen nach *SAE International* und adressiert Fahrzeuge der Automatisierungsstufe 4.[17] Zugleich hat der Gesetzgeber die Beschränkung des zulässigen Einsatzbereichs von HAF auf festgelegte Betriebsbereiche beschränkt, wobei es sich hierbei um örtlich und räumlich abgegrenzte Teile des öffentlichen Straßenraums handelt (vgl. § 1d Abs. 2 StVG). Mit dem technischen Einsatzbereich – der Operational Design Domain (ODD)[18] – ist der vom Gesetz verwendete Begriff der festgelegten Betriebsbereiche daher nicht deckungsgleich, da ODDs auch durch nicht-räumliche Kriterien wie Tageszeiten, Lichtverhältnisse, Wetterlagen oder besondere Verkehrssituationen definiert sein können.[19] Für Fahrzeuge mit autonomer Fahrfunktion besteht gemäß § 1g Abs. 1 StVG die Pflicht, zahlreiche Daten beim Betrieb des Fahrzeuges zu speichern, darunter etwa Positionsdaten, Systemüberwachungsdaten, Umwelt- und Wetterbedingungen oder die Geschwindigkeit des Fahrzeugs. Auch diese Pflicht adressiert – ähnlich wie die Pflicht zur Datenbereitstellung nach § 63a Abs. 3 StVG – einzig den Fahrzeughalter.

Auffällig ist, dass sowohl die bisherige als auch die 2021 neu geschaffene Regelung zahlreiche der oben beschriebenen Datenverarbeitungsvorgänge – etwa die Datenverarbeitung durch Sensoren – nicht adressieren. Auch die zur Entwicklung autonomer Fahrfunktionen erforderlichen Verarbeitungsvorgänge werden durch das Straßenverkehrsgesetz nicht geregelt. Überdies erscheint fraglich, ob die Festlegung auf den Fahrzeughalter als (einzigen!) Verantwortlichen mit den Grundwertungen der DSGVO vereinbar ist. Hierauf wird noch zurückzukommen sein.[20]

3.2. Allgemeine Grundsätze der Datenschutz-Grundverordnung (DSGVO)

Neben den sektorspezifischen Bestimmungen des Straßenverkehrsgesetzes ist, da die dortigen Regelungen stark fragmentarisch sind und die Datenverarbeitungen eines HAF nicht annähernd vollständig erfassen, die DSGVO für sämtliche datenschutzrechtlichen Fragestellungen ergänzend heranzuziehen.

3.2.1. Verarbeitung personenbezogener Daten

Wie bereits die technische Darstellung erahnen lässt, geht hochautomatisiertes Fahren mit der Verarbeitung (auch) personenbezogener Daten einher.[21] Maßgeblich ist insoweit die Definition des personenbezogenen Datums in Art. 4 Nr. 1 DSGVO. Insoweit soll bekanntlich bereits die Erkennbarkeit von Kfz-Kennzeichen anderer Verkehrsteilnehmer – etwa auf Kameraaufnahmen – den Anforderungen an die Identifizierbarkeit einer anderen natürlichen Person ausreichen, da nach Auffassung des EuGH für eine Identifizierbarkeit aus-

14 Sesing/Putzki, MMR-Aktuell 2017, 388288, sub II.5.

15 BGBl. I 2021, S. 3108 ff.

16 S. zum Gesetz im Überblick Haupt, NZV 2021, S. 172 ff.; Lutz, DAR 2021, S. 182 ff.; Roshan, NJW-Spezial 2021, S. 137 ff.; Schrader, ZRP 2021, S. 109 ff.; Steege, SVR 2021, S. 128 ff.

17 Begr. RegE zum Gesetzentwurf, BT-Drs. 19/27439, S. 15.

18 Dazu oben 2.1.3.

19 Sesing, DSRITB 2021, S. 571 (574).

20 S. unten 3.2.2.

21 Forgó, in: Oppermann/Stender-Vorwachs, Autonomes Fahren, 2. Aufl. 2020, Kap. 3.5 Rn. 16; Rossnagel, SVR 2014, S. 281 (284); s. ferner die Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA) vom 26.1.2016, S. 1 (abrufbar unter (https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKEntschliessungen/DSK_20160126_VernetzteKfz.pdf?__blob=publicationFile&v=3).

reicht, dass der Verantwortliche über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand von Zusatzinformationen bestimmen zu lassen, soweit hierfür ein rechtlich zulässiger Weg besteht.[22] Der Bundesgerichtshof (BGH) hat mit ähnlicher Argumentation – nämlich unter Verweis auf die Möglichkeit einer Halterabfrage – das Vorliegen personenbezogener Daten im Fall der Aufzeichnung des Straßenverkehrs mittels einer sog. „Dashcam" bejaht.[23] Auch die nach § 1g StVG aufzuzeichnenden Daten weisen mitunter Personenbezug auf, da – etwa bei Kenntnis der Insassen des Fahrzeuges – Rückschlüsse auf deren Fahrtziele möglich sind. Überlegungen der Literatur, die Möglichkeit zur Identifizierung natürlicher Personen bei „geschlossenen Systemen" – gemeint sind Systeme, bei denen die verarbeiteten Daten zu keinem Zeitpunkt das System verlassen und auch nicht aufgezeichnet werden – zu verneinen,[24] haben sich bislang nicht durchsetzen können, erscheinen jedoch nicht fernliegend.

Ebenso wie die Verarbeitung der Daten während des Betriebs stellt auch die Verwendung von Lerndaten zum Trainieren von KI-Modellen, die zur Fahrzeugsteuerung eingesetzt werden, eine datenschutzrechtlich relevante Handlung dar. Dies gilt insbesondere dann, wenn zum Training derartiger Modelle reale Kameraaufnahmen verwendet werden, auf denen Passanten oder andere Verkehrsteilnehmer zu sehen sind. Eine in der Literatur z.T. vorgeschlagene Strategie zur Vermeidung von personenbezogenen Daten stellt insoweit der Rückgriff auf synthetische Daten dar.[25]

3.2.2. Datenschutzrechtliche Verantwortlichkeit

Ein zentraler Aspekt der datenschutzrechtlichen Beurteilung des hochautomatisierten Fahrens ist die Bestimmung des Verantwortlichen für die verschiedenen Datenverarbeitungsvorgänge.[26] Gesetzlicher Ausgangspunkt ist insoweit die Definition in Art. 4 Nr. 7 DSGVO, wonach Verantwortlicher ist, wer – allein oder gemeinsam mit anderen – über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Für den Fall, dass die Zwecke und Mittel der Datenverarbeitung durch das Unionsrecht oder mitgliedstaatliches Recht vorgegeben sind, stellt Art. 4 Nr. 7, 2. Halbsatz DSGVO zudem klar, dass auch die Festlegung des Verantwortlichen bzw. der hierzu heranzuziehenden Kriterien ebenfalls durch Unionsrecht oder mitgliedstaatliches Recht erfolgen kann. Insoweit erscheint es überzeugend, dass eine entsprechende Regelung im Einklang mit den tatsächlichen Gegebenheiten stehen muss und sich nicht in Widerspruch zum Konzept der Verantwortlichkeit setzen darf, wie es der DSGVO zu entnehmen ist.[27] Soweit zwar die Zwecke und Mittel der Datenverarbeitung vorgegeben werden, eine Präzisierung im Hinblick auf den Verantwortlichen jedoch nicht erfolgt, ist die Verantwortlichkeit folgerichtig nach allgemeinen Grundsätzen zu bestimmen.

Das StVG lässt, wie bereits dargestellt, sowohl im Hinblick auf den Fahrmodusspeicher (§ 63a Abs. 1 StVG) als auch im Hinblick auf die nach § 1g StVG aufzuzeichnenden Daten keine ernstlichen Zweifel daran, dass der Fahrzeughalter Verantwortlicher ist, da dieser als Adressat von Herausgabe- und Speicherpflichten benannt wird.[28] Insoweit erscheint es jedoch zweifelhaft, einzig den Fahrzeughalter, nicht hingegen den Fahrzeughersteller in den Fokus zu nehmen; insbesondere im Hinblick auf Verbraucher als Fahrzeughalter erscheint dies wenig sachgerecht.[29] Näherliegend erschiene es, den Fahrzeughersteller – der faktisch über die

[22] So für den Personenbezug dynamisch vergebener IP-Adressen EuGH, NJW 2016, S. 3579 (3581), Rn. 47.

[23] BGH, NJW 2018, S. 2883 (2885), Rn. 21.

[24] Vgl. Schröder, ZD 2021, 302 (304); ähnlich Borges, Potenziale von Künstlicher Intelligenz mit Blick auf das Datenschutzrecht, Gutachten, 2021, S. 15 (abrufbar unter https://stiftungdatenschutz.org/fileadmin/Redaktion/Gutachten-Studien/Stiftung-Datenschutz_Gutachten-Georg-Borges-Potenziale-Kuenstliche-Intelligenz-Datenschutzrecht-2021-12.pdf), der sich gegen den Personenbezug von Daten ausspricht, die ausschließlich zum Zweck der Steuerung von Maschinen verwendet werden.

[25] Paal, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence, 2020, S. 427, 439; Raji, DuD 2021, S. 303 (305 ff.).

[26] Ähnlich die Einschätzung bei Paal, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence, 2020, S. 427 (440).

[27] Petri, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 4 Nr. 7 DSGVO Rn. 26.

[28] Steege, SVR 2021, S. 128 (136).

[29] Wagner, SVR 2021, S. 287 (289 f.).

konkret eingesetzten Instrumente zur Datenaufzeichnung bestimmt – mit dem Fahrzeughalter wenigstens[30] als gemeinsam Verantwortlichen zu bestimmen.[31]

Soweit auch zur KI-Entwicklung verwendete Trainingsdaten Personenbezug aufweisen, erscheint es angemessen, den Systemhersteller als Verantwortlichen anzusehen; in seinem Auftrag handelnden Dritte können insoweit ggf. als Auftragsverarbeiter gemäß Art. 28 DSGVO anzusehen sein.[32]

3.2.3. Rechtfertigung der Datenverarbeitung

Schließlich ist zur Beantwortung der eingangs aufgeworfenen Frage, ob und inwieweit Funktionen des hochautomatisierten Fahrens mit den datenschutzrechtlichen Bestimmungen vereinbar sind, der Blick auf die Rechtfertigung der einzelnen Datenverarbeitungsvorgänge zu richten. Maßgebliche Grundlage ist insoweit Art. 6 Abs. 1 DSGVO, der einen abschließenden Katalog von Erlaubnistatbeständen enthält. Insoweit ist zwischen den unterschiedlichen Erlaubnistatbeständen zu differenzieren.

Die Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) stellt regelmäßig kein probates Instrument zur datenschutzrechtlichen Rechtfertigung dar, da insbesondere die Einholung einer Einwilligung von Verkehrsteilnehmern beim Betrieb eines HAF nicht möglich ist. Auch im Hinblick auf reale Lerndaten ist eine Einwilligung kein praktikables Mittel, zumal diese jederzeit frei widerruflich ist.

Aufgrund der straßenverkehrsrechtlichen Verpflichtung zur Aufzeichnung bestimmter Daten in §§ 1g, 63a StVG kommt insoweit eine Rechtfertigung nach Art. 6 Abs. 1 lit. c) DSGVO in Betracht. Diese Vorschrift erlaubt Datenverarbeitungen, die zur Erfüllung einer rechtlichen Verpflichtung erforderlich sind, denen der Verantwortliche unterliegt. Die Reichweite dieser Erlaubnis geht jedoch nicht weiter als die im StVG vorgesehene Speicherpflicht, sodass insbesondere die Datenverarbeitung mithilfe von Sensoren sowie das Training von KI-Modellen nicht geregelt wird.

Damit verbleibt im Wesentlichen eine Rechtfertigung über das Instrument der Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO.[33] Hiernach ist eine Datenverarbeitung gestattet, wenn diese zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Sowohl an der Absicherung der Funktionalität eines HAF im laufenden Betrieb als auch im Rahmen der Entwicklung von hochautomatisierten Fahrfunktionen besteht naturgemäß ein berechtigtes Interesse, (auch) personenbezogene Daten zu verarbeiten, und die entgegenstehenden Interessen Betroffener – etwa als Bestandteil eines Lerndatensatzes – fällt nicht merklich ins Gewicht. Hinsichtlich der beim Betrieb erforderlichen Datenverarbeitung taugt die Interessenabwägung jedoch nur für private Stellen als Erlaubnistatbestand; Behörden hingegen können sich auf den Erlaubnistatbestand nicht berufen (vgl. Art. 6 Abs. 1 S. 2 DSGVO). Soweit öffentliche Stellen also Halter von HAF sind, ist eine datenschutzrechtliche Gestattung der Verwendung von Sensordaten ohne entsprechende gesetzliche Grundlage nicht gestattet.

Insgesamt lässt sich daher resümieren, dass die gesetzlichen Grundlagen für die beim hochautomatisierten Fahren erforderlichen Datenverarbeitungsvorgänge unvollständig sind. Präzisere Bestimmungen könnten hier zu mehr Rechtssicherheit beitragen.

---

30 Für eine Alleinverantwortlichkeit des Fahrzeugherstellers etwa Forgó, in: Oppermann/Stender-Vorwachs, Autonomes Fahren, 2. Aufl. 2020, Kap. 3.5 Rn. 23; Grigorian/Tribess, DSRITB 2020, S. 651 (660).

31 Zurückhaltend in diese Richtung auch Steege, SVR 2021, S. 128 (136); a.A. etwa Skistims, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence, 2020, S. 352 f. (Betreiber von KI-Systemen als datenschutzrechtlich Verantwortliche).

32 Ausführlich zur Auftragsverarbeitung im KI-Kontext Piltz/Zwerschke, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence, 2020, S. 403 ff.

33 Forgó, in: Oppermann/Stender-Vorwachs, Autonomes Fahren, 2. Aufl. 2020, Kap. 3.5 Rn. 36.

4. Neue Datenschutznormen für die Schweiz

Die Schweiz ist durch zahlreiche Abkommen ins internationale und europäische Straßenverkehrsrecht eingebunden, insbesondere was die technischen Anforderungen an Straßenfahrzeuge betrifft.[34] Im Gegensatz zu Deutschland[35] kennt die Schweiz in Bezug auf hochautomatisiertes Fahren bisher keine sektorspezifischen Datenschutznormen im Straßenverkehrsrecht. Deshalb wird nachfolgend der Fokus auf neue Rechtsentwick-lungen gerichtet, die das schweizerische Strassenverkehrsgesetz (SVG) (4.1.) und das Bundesgesetz über den Datenschutz (DSG; 4.2.) betreffen.

4.1. Die laufende Teilrevision des schweizerischen Strassenverkehrsgesetzes (SVG)

Mit der laufenden Teilrevision des SVG will der Gesetzgeber die Bedürfnisse des automatisierten Fahrens der SAE-Stufen (J3016, 2018) 3 und 4 regeln.[36] Dafür hat er eine Legaldefinition entwickelt: Fahrzeuge mit einem Automatisierungssystem sind danach in der Lage, die Fahraufgaben des Fahrzeugführers zumindest unter bestimmten Bedingungen dauerhaft und umfassend zu übernehmen (Art. 25*a* E-SVG). Dieser Begriff dient indirekt zur Unterscheidung zwischen einem Fahrzeug mit Automatisierungssystem und einem mit Fahrassistenten. Auch moderne Fahrzeuge, die kein Fahrautomatisierungssystem aufweisen, verfügen über eine komplexe Systemarchitektur. Nach dem Gesetzesvorschlag kann der Fahrzeugführer eines Fahrzeugs, welches der Legaldefinition entspricht, unter bestimmten Voraussetzungen[37] von seiner Aufmerksamkeits- und Beherrschungspflicht nach Art. 31 Abs. 1 SVG entlastet werden (Art. 25*b* E-SVG). Der Bundesrat soll die Kompetenz erhalten, dafür bestimmte Regelungen zu erlassen, sofern die Rahmenbedingungen wie die Einhaltung der Verkehrssicherheit, der Verkehrsregeln, der Datensicherheit und des Datenschutzes gewährleistet sind.[38]

Unter der datenschutzrechtlichen Perspektive sind die Bestimmungen zum Automatisierungssystem (Art. 25*e* E-SVG), zum Fahrmodusspeicher (Art 25e f. E-SVG) und zum Zugriff auf dessen Daten (Art. 25*g* E-SVG) näher zu betrachten. Diese Subsysteme werden von den Herstellern je nach Fahrzeugtypus in den verschiedensten Ausführungen auf den Markt kommen. Deshalb kann der Gesetzgeber keine Anforderungen an eine konkrete Systemarchitektur stellen, sondern beschränkt sich auf Anforderungen, welche die Hersteller dieser Subsysteme sowie die Fahrzeugführer und Halter zu erfüllen haben. Damit die Verkehrssicherheit aller Straßenbenützer nicht beeinträchtigt wird, ist in der Ausführungsverordnung sicherzustellen, dass die Verkehrsregeln beachtet werden können und die Automatisierungssysteme die Daten nur dann bearbeiten dürfen, wenn deren Richtigkeit und Integrität gewährleistet ist (Art. 25*e* Abs. 1 E-SVG).[39] Fahrzeuge mit einem Automatisierungssystem sind zwingend mit einem Fahrmodusspeicher auszurüsten (Art. 25*e* Abs. 2 E-SVG). Das Automatisierungssystem und der Fahrmodusspeicher müssen zudem gegen unbefugten Zugriff geschützt sein, damit deren Funktionalität ohne Datenmanipulationen gewährleistet ist (Art. 25*e* Abs. 3 E-SVG).[40]

In der Vernehmlassung[41] hatten viele Kantone gefordert, dass der Zugang zu privaten personenbezogenen Daten in den Fahrzeugen und die Pflicht zur Herausgabe der Daten an die Strafverfolgungsbehörden verbind-

[34] S. Verordnung über die technischen Anforderungen an Strassenfahrzeugen (VTS), Anhang 2.

[35] Dazu 3.1.

[36] Die Botschaft zur Änderung des Strassenverkehrsgesetzes (SVG-Botschaft) ist abrufbar unter www.astra.admin.ch seit dem 17. November 2021, aber noch nicht amtlich publiziert. Die Ausführungsverordnung liegt noch nicht vor.

[37] Die vorgesehenen Einsatzgebiete sind bestimmte Parkplätze (Art. 25*b* Abs. 2 E-SVG) und Fahrstrecken (Art. 25*c* E-SVG); zusätzlich betreffen sie Fahrzeuge mit geringen Dimensionen und niedriger Geschwindigkeit, die durch Operatoren beaufsichtigt werden (Art. 25*d* E-SVG).

[38] SVG-Botschaft, S. 33 f.

[39] SVG-Botschaft, S. 33 f und S. 65.

[40] SVG-Botschaft, S. 34.

[41] Vernehmlassungen sind Stellungnahmen der Kantone, Parteien und interessierter Kreise im Gesetzgebungsverfahren der Schweiz, vgl. https://de.wikipedia.org/wiki/Vernehmlassung.

lich auf Gesetzesstufe zu regeln sind.[42] Deshalb soll nun der Zugriff auf die zweckbezogene Verarbeitung der Daten des Fahrmodusspeichers umfassend in Art. 25*g* E-SVG geregelt werden. Danach hat der Fahrmodusspeicher aufzuzeichnen, ob einerseits das Automatisierungssystem funktioniert und andererseits, ob der Fahrzeugführer das Fahrzeug lenkt oder das Automatisierungssystem. Damit kann die Funktionstüchtigkeit der Subsysteme und ihren Auswirkungen auf die Verkehrssicherheit und den Verkehrsfluss beurteilt werden und, wer die straf- und haftungsrechtliche Verantwortung trägt: der Hersteller oder der Fahrzeugführer. Dem Fahrzeughalter wird das Zugriffsrecht auf seine selbst erzeugten Daten eingeräumt und bei berechtigtem Interesse auf eine Drittperson, welche das Fahrzeug lenkt (Art. 25*g* Abs. 1 E-SVG). In den Absätzen 3 bis 5 werden behördliche Zugriffsrechte geregelt. Mit den erhobenen Daten im Fahrmodusspeicher können keine Persönlichkeitsprofile[43] erstellt werden, hält die Botschaft explizit fest, und es würden auch keine Daten zur Umgebungserkennung und -überwachung erfasst.[44] Diese Aussage ist insofern zu relativieren, da ab Mitte 2024 neue Fahrzeugtypen mit einem Unfalldatenschreiber ausgerüstet sein müssen, mit oder ohne Automatisierungssystem.[45]

Die Bestimmungen zu den Datenverarbeitungen der Subsysteme legen den Fokus auf die Datensicherheit, der unbestrittenen ein hoher Stellenwert zukommt. Der Schutzmaßnahmenstandart für das Automatisierungssystem und den Fahrmodusspeicher sind nach dem Stand der Technik auszurichten, hält die Botschaft fest. Die Anforderungen an die Richtigkeit und Integrität der Daten bedinge auch, dass das Fahrzeug Situationen (z.B. Witterungsverhältnisse, Alterung der Sensoren) erkenne, in dem von ihm selbst erhobene Daten nicht zuverlässig seien.[46] Für Automatisierungssysteme haben die Hersteller nachzuweisen, dass die Anforderungen an Richtigkeit und Integrität der Daten sichergestellt sind. Jene Daten, die von außerhalb in das System eingespiesen werden, bezeichnet die Botschaft als besonders heikel. Den Herstellern wird zur Gewährleistung der Datensicherheit und des Datenschutzes deshalb empfohlen, die Zuverlässigkeit externer Daten zertifizieren zu lassen.[47] Auf eine konkrete gesetzliche Verpflichtung wird in der SVG-Teilrevision verzichtet.

Wie bereits im technischen Teil ausgeführt, verarbeiten die Systeme personenbezogene Daten. Somit sind die einschlägigen Bestimmungen des Bundesgesetzes über den Datenschutz (DSG) subsidiär anwendbar. Dies gilt auch für Sachdaten, sofern deren Verarbeitung nicht getrennt von personenbezogenen Daten erfolgen kann. Die Teilrevision des SVG beschränkt die Datenthematik auf zwei Subsysteme, wodurch nicht die gesamte Datenverarbeitung in einem HAF erfasst wird und deshalb das DSG ergänzend herangezogen werden muss.[48]

4.2. Datenschutzrechtliche Anforderungen nach DSG und revDSG

Private und Bundesorgane fallen bei der Verarbeitung personenbezogener Daten unter den Geltungsbereich des DSG (Art. 2). Für die nachfolgend erörterten rechtlichen Fragestellungen zum hochautomatisierten Fahren ist – über das geltende Recht hinaus – bereits das totalrevidierte Bundesgesetz über den Datenschutz (*rev*DSG) einzubeziehen, dessen Inkrafttreten auf den 1. Januar 2023 verschoben worden ist. Die Verordnung dazu wird derzeit überarbeitet.[49] Mit dem *rev*DSG soll u.a. sichergestellt werden, dass die Europäische Kom-

---

42 S. https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/dl/proj/6020/43/cons_1/doc_17/de/pdf-a/fedlex-data-admin-ch-eli-dl-proj-6020-43-cons_1-doc_17-de-pdf-a.pdf.

43 Zum Begriff Persönlichkeitsprofil s. Kap. 4.2.

44 SVG-Botschaft, S. 34.

45 SVG-Botschaft, S. 86.

46 In der SVG-Botschaft wird in den Ausführungen zu Art. 25*e* Abs. 1 E-SVG explizit auf: 1. das UN-Reglement Nr. 155 über einheitliche Vorschriften für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit verwiesen und 2. das Cybersicherheits-Managementsystems, dass in der EU ab Mitte 2022 für neue Typengenehmigungen erfüllt sein muss, S. 34.

47 SVG-Botschaft, S. 65.

48 SVG-Botschaft, S. 41.

49 Bemerkung: Im Vernehmlassungsverfahren ist der Entwurf der Verordnung zum *rev*DSG auf starke Kritik gestoßen, formell und materiell. Exemplarisch dazu: https://www.datenschutz-forum.ch/wp-content/uploads/2021/10/21_Vernehmlassung_VDSG_def.pdf

mission die Schweiz weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau anerkennt und die grenzüberschreitende Datenübermittlung auch künftig ohne weitere Hürden möglich bleibt.[50] Dabei werden neue Instrumente der DSGVO wie *Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen* (Art. 7 *rev*DSG) sowie die *Datenschutz-Folgeabschätzung* (Art. 22 *rev*DSG) übernommen.

Die Datenverarbeitung durch Private unterscheidet sich auch im *rev*DSG grundsätzlich von derjenigen in der DSGVO, indem weiterhin für die Verarbeitung von Personendaten kein Rechtfertigungszwang gilt, sondern diese unter Einhaltung der datenschutzrechtlichen Grundsätze i.d.R. erlaubt ist (Art. 6 *rev*DSG). Die Schweiz knüpft wie die EU an das Auswirkungsprinzip an (Art. 3 Abs. 1 *rev*DSG);[51] Fahrzeughersteller im Ausland, deren Datenverarbeitungen sich auf die Schweiz auswirken, sollten deshalb genau prüfen, welche Schweizer Datenschutznormen für sie im Einzelfall anwendbar sind.

Beim hochautomatisierten Fahren benötigen die eingesetzten KI-Technologien, wie im technischen Teil dargestellt, den Zugriff auf große Datenmengen. Deshalb stellt sich die Frage, wer die Verantwortung für die Einhaltung des Datenschutzes trägt. Nach geltendem Recht trägt der Fahrzeughalter als Inhaber der Datensammlung die Verantwortung (Art. 3 Bst. i DSG). Im *rev*DSG (Art. 5 Bst. j) ist der Verantwortliche – wie bisher der Inhaber der Datensammlung – derjenige, der über den Zweck und die Mittel (z.B. materielle oder automatisierte Bearbeitung, verwendete Software) der Verarbeitung entscheidet.[52] Neu kann der Verantwortliche „alleine oder zusammen mit anderen" darüber entscheiden (gemeinsame Verantwortung). Damit die Fahrzeughalter ihre datenschutzrechtliche Verantwortung übernehmen können, bräuchten sie das Wissen über die Datenflüsse und Auswahl- sowie Einflussmöglichkeiten darüber. Bei Haltern von HAFs ist davon auszugehen, dass diese nicht mehr alleine über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheiden können. Somit müsste eine gemeinsame Verantwortung mit den Fahrzeugherstellern und Dienstleistern geprüft werden, sofern diese nicht bereits in der Teilrevision des SVG festgelegt worden ist.

Bereits heute erfassen und verarbeiten die Fahrzeughersteller und Dienstleister (grenzüberschreitend) eine Vielzahl personenbezogener Daten aus den Fahrzeugen mittels Mobilfunkverbindung oder lassen sich diese über Servicewerkstätten übermitteln.[53] Personenbezogene Auswertungen aus Fahrzeugen bergen das Risiko, dass sie zu Rückschlüssen auf Persönlichkeitsmerkmale und Krankheiten der Fahrzeuginsassen und v.a. der Fahrzeugführer führen.[54] Mit der zunehmenden Datenmenge und deren Verknüpfungsmöglichkeiten laufen deshalb Fahrzeughersteller und Dienstleister als Auftrags- oder Unterauftragsbearbeiter nach Art. 10*a* DSG (Art. 9 *rev*DSG) oder als gemeinsam Verantwortliche zunehmend Gefahr, dass sie Grundsätze des Datenschutzes wie das Verhältnismäßigkeitsprinzip und das Transparenzgebot (Art. 4 Abs. 2 und 4 DSG; Art. 6 Abs. 3 *rev*DSG) verletzen und *Profiling* betreiben. Das Profiling wird als Begriff im *rev*DSG neu unterteilt in „*Profiling*" (Art. 5 Bst. f) und „*Profiling mit hohem Risiko*" (Art. 5 Bst. g). Letzteres soll vorliegen, wenn personenbezogene Daten automatisiert verarbeitet werden und eine Verknüpfung von Daten die Beurteilung wesentlicher Aspekte der Persönlichkeit erlaubt, die ein hohes Risiko für die Persönlichkeit oder die Grundrechte einer natürlichen Person mit sich bringen. Beim Profiling mit hohem Risiko wird nicht nur der Prozess beschrieben, sondern auch das *Ergebnis der Datenbearbeitung*. Damit hat das Parlament eine Differenz zur DSGVO geschaffen, welche diesen Begriff nicht kennt.

---

und http://www.vud.ch/view/data/2124/Veranstaltungen%20Archiv/210913%20VUD%20E-VDSG%20Kommentierung%20und%20Anpassungsvorschläge.pdf. Ursprünglich sollte das *rev*DSG auf den 1. Januar 2022 in Kraft treten, s.a. SVG-Botschaft, S. 65.

50 Der Angemessenheitsbeschluss der EU-Kommission nach Artikel 97 der Verordnung (EU) 2016/679 steht noch aus, vgl. Bundesamt für Justiz: https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html.

51 Rechtsprechung zum Auswirkungsprinzip, s. Urteil Google Street View, BGE 138 II 346 E. 8.

52 BBl **2017** 7023.

53 ADAC-Bericht (oben 1.), S. 4.

54 Vgl. 2.1.3.

5. Fazit und Ausblick

Die vorstehende Betrachtung hat aufgezeigt, dass ein sicherer Betrieb von HAF nicht ohne die Verarbeitung personenbezogener Daten auskommt und zahlreiche Sensordaten anfallen. Die einschlägigen rechtlichen Bestimmungen in der Europäischen Union, Deutschland und der Schweiz sind im Hinblick auf die datenschutzrechtlichen Herausforderungen des hochautomatisierten Fahrens jedoch entwicklungsbedürftig. Insoweit hat sich gezeigt, dass insbesondere die Bestimmung der Verantwortlichkeit *de lege lata* noch nicht überzeugend gelöst ist, und auch die im europäischen Recht erforderliche datenschutzrechtliche Rechtfertigung teilweise ungeklärt ist.