

Saarbrücken, 30.04.2021

Deutscher Bundestag
Ausschuss für Verkehr
und digitale Infrastruktur
Ausschussdrucksache

19(15)489-E

Stellungnahme zur 111. Sitzung -
Öffentl. Anhörung am 03.05.2021

Stefan Hessel

Algoright e.V.

Rechtsanwalt bei reuschlaw Legal Consultants

stefan.hessel@algoright.de

Stellungnahme als Sachverständiger zum Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren*

Vorbemerkung:

Zunächst möchte ich mich für die Gelegenheit eine Stellungnahme zum „Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren“ abzugeben bedanken. Ich bin Erster Vorsitzender des gemeinnützigen Vereins Algoright e.V., der sich mit einer interdisziplinären Perspektive mit aktuellen Herausforderungen beim Einsatz neuer Technologien und den daraus folgenden Auswirkungen auf die Gesellschaft beschäftigt. Darüber hinaus befasse ich mich als Rechtsanwalt bei der Kanzlei reuschlaw Legal Consultants und als Autor wissenschaftlicher Fachpublikationen regelmäßig mit rechtlichen Fragestellungen in den Bereichen Cybersicherheit und Datenschutz.

Meine Stellungnahme gliedert sich in drei Teile. Im ersten Teil skizziere ich das technologische Konzept des autonomen Fahrens. Im zweiten Teil stelle ich die mit der Technologie einhergehenden Risiken und Herausforderungen mit Bezug auf Cybersicherheit, Datenschutz und ethische Aspekte dar, bevor ich in Teil 3 erläutere, ob und inwieweit der Gesetzentwurf diesen Risiken und Herausforderungen ausreichend Rechnung trägt.

I. Das technologische Konzept des autonomen Fahrens

Gegenstand des automatisierten und autonomen Fahrens ist die Ersetzung der menschlichen Steuerung des Fahrzeugs durch eine maschinelle Steuerung. Zur Beschreibung von Art und Umfang der vom Menschen auf die Maschine übertragenen Fahrfunktionen existieren verschiedene Stufenmodelle, die

* Die Stellungnahme gibt lediglich meine persönliche Auffassung wieder. Ich danke Dipl.-Jur. Karin Potel, Rechtsreferendarin und Wissenschaftliche Mitarbeiterin bei reuschlaw Legal Consultants, sowie den Algoright-Experten Kevin Baum, Moritz Schillo und Jonas Wahl für ihre Unterstützung bei der Erstellung dieser Stellungnahme.

ausgehend von einer menschlichen Steuerung des Fahrzeugs einen zunehmenden Automatisierungsgrad durch steigende Stufen beschreiben. Die Modelle der Bundesanstalt für das Straßenwesen (BASt) und der National Highway Traffic Safety Administration (NHTSA) differenzieren hierbei zwischen vier Stufen.¹ Der Verband der Automobilindustrie e.V. (VDA) und die Society of Automotive Engineers (SAE) sehen fünf Stufen vor.² Der wesentliche Unterschied zwischen den vier- und fünfstufigen Modellen besteht darin, dass die fünfstufigen Modelle nach dem voll automatisierten Fahren (Stufe vier) noch ein fahrerloses autonomes Fahren vorsehen. Der Gesetzentwurf umfasst im Wesentlichen Fahrzeuge der Stufen vier und fünf.

Um das Ziel einer Übertragung von Aufgaben, die zuvor einem menschlichen Fahrer oblagen, auf das Fahrzeug zu erreichen, ist notwendig die Umgebung und entstehende Situationen durch eine maschinelle Wahrnehmung des Fahrzeugs zu erfassen, zu bewerten und die notwendigen Reaktionen auszulösen. Entscheidend für den Erfolg des autonomen Fahrens ist dabei, dass die maschinelle Wahrnehmung mit der menschlichen Wahrnehmung vergleichbar, das heißt mindestens genauso effizient und zuverlässig ist. Im Idealfall ist die maschinelle Wahrnehmung sogar deutlich besser als die menschliche.

Bei der Realisierung einer maschinellen Wahrnehmung wird auf Sensoren zurückgegriffen, welche unter anderem auf Kameratechnik, Radar oder Lidar (Light Detection and Ranging) beruhen.³ Die verschiedenen Sensoren bieten dabei ein breites Wahrnehmungsspektrum. Die Kameratechnik weist eine hohe Kontrastierung auf und bietet daher die Möglichkeit Unterschiede in der Textur der einzelnen Objekte erkennen zu können.⁴ Beim Einsatz der Kameratechnik gestaltet sich jedoch die Bestimmung der Entfernung von Objekten je weiter das Fahrzeug davon entfernt ist als schwierig.⁵ Im Gegensatz zur Kameratechnik ermöglichen Radar- oder Lidarsensoren eine exakte Berechnung der Entfernung zum Objekt.⁶ Mit der Hilfe von Radarsensoren ist jedoch die Erfassung der Außenabmessungen von Objekten nur eingeschränkt möglich und eine Erfassung der Textur von Objekten ausgeschlossen.⁷ Als praxistauglich erscheint daher lediglich eine Kombination der verschiedenen Sensoren (sog. Sensordatenfusion) die eine umfassende Erfassung des Fahrzeugumfeldes gewährleistet.⁸ Nur auf diese

¹ Gasser et al., Berichte der Bundesanstalt für Straßenwesen, Heft F 83, 2012; NHTSA (National Highway Traffic Safety Administration), Preliminary Statement of Policy Concerning Automated Vehicles, 2013, https://www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf (zuletzt abgerufen am 30.04.2021).

² SAE (Society of Automotive Engineers), Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, v. 15.06.2018, https://www.sae.org/standards/content/j3016_201806/ (zuletzt abgerufen am 30.04.2021); VDA (Verband der Automobilindustrie e.V.), Automatisierung – Von Fahrerassistenzsystemen zum automatisierten Fahren, v. 03.09.2015, <https://www.vda.de/de/services/Publikationen/automatisierung.html> (zuletzt abgerufen am 30.04.2021).

³ Dietmayer, in: M. Maurer et al. (Hrsg.), Autonomes Fahren, S. 422.

⁴ Dietmayer, in: M. Maurer et al. (Hrsg.), Autonomes Fahren, S. 422.

⁵ Dietmayer, in: M. Maurer et al. (Hrsg.), Autonomes Fahren, S. 422.

⁶ Dietmayer, in: M. Maurer et al. (Hrsg.), Autonomes Fahren, S. 422.

⁷ Dietmayer, in: M. Maurer et al. (Hrsg.), Autonomes Fahren, S. 422.

⁸ Kernhof, in: T. Tille (Hrsg.), Automobil-Sensorik 2, S. 29.

Weise ist eine effektive Algorithmen basierte Analyse der vorliegenden Situation sowie der Abschätzung und Auswahl eines angemessenen Fahrzeugverhaltens möglich.



Abbildung 1: Übersicht über die maschinelle Wahrnehmung der Fahrzeugumgebung: Neben Sensoren wie Kamera, Lidar und Radar spielen auch die Standortbestimmung und im Fahrzeug gespeicherte Daten, wie zum Beispiel Karten, eine Rolle.

Quelle: Hessel/Leffer/Potel, See No EVIL – Angriffe auf Autonome Fahrzeuge und deren Strafbarkeit, InTeR 2020, 208 (210).

II. Risiken und Herausforderungen

1. Cyberangriffe auf Fahrzeuge

Die maschinelle und die menschliche Wahrnehmung der Umgebung sind nicht deckungsgleich. Diese Differenz bietet verschiedene Angriffs- und Eingriffsmöglichkeiten für Dritte. So sind Angriffe auf die maschinelle Wahrnehmung möglich, die bei menschlicher Wahrnehmung nicht denkbar wären.⁹ Dies ist jedoch von der konkret vorgefundenen Situation abhängig. In anderen Fällen kann die maschinelle Wahrnehmung die menschliche übertreffen.¹⁰ Infrarotkameras sind beispielsweise im Zusammenhang mit der Umgebungserkennung in der Lage selbst bei Dunkelheit Objekte gezielt wahrzunehmen. Diese Fähigkeit entzieht sich jedoch der menschlichen Wahrnehmungsfähigkeit.¹¹ Diese Unterschiede können durch Angreifer gezielt zur Täuschung des Fahrzeuges ausgenutzt werden, dabei kann es zu erheblichen Beeinträchtigungen des Straßenverkehrs und zu Schädigungen anderer Verkehrsteilnehmer kommen.

Erschwerend dazu kommt, dass durch Angreifer ermittelte Täuschungsmethoden bei einer unbestimmten Anzahl von Fahrzeugen zum Einsatz kommen können, da sie aufgrund mangelnder

⁹ Hessel/Leffer/Potel, See No EVIL – Angriffe auf Autonome Fahrzeuge und deren Strafbarkeit, InTeR 2020, 208 (210).

¹⁰ Hessel/Leffer/Potel, See No EVIL – Angriffe auf Autonome Fahrzeuge und deren Strafbarkeit, InTeR 2020, 208 (210).

¹¹ Hessel/Leffer/Potel, See No EVIL – Angriffe auf Autonome Fahrzeuge und deren Strafbarkeit, InTeR 2020, 208 (210).

Individualität der maschinellen Wahrnehmung ohne Anpassungen übertragen werden können.¹² Dies stellt einen entscheidenden Nachteil im Vergleich zur menschlichen Wahrnehmung dar. Während demnach die Täuschung der menschlichen Wahrnehmung stets ortgebunden zu erfolgen hat, kann eine Täuschung der maschinellen Wahrnehmung an beliebig vielen Orten gleichzeitig und bei einer Vielzahl von Fahrzeugen vorgenommen werden. Bei den skizzierten Angriffsmöglichkeiten handelt es sich keineswegs um ein Gedankenexperiment. Beispiele aus der Praxis belegen die tatsächlich gegebenen Schwachstellen und verdeutlichen das hohe Risiko- und Missbrauchspotential.

Angriffe auf autonome Fahrzeuge können trivialer Natur sein. So gelang es dem US-Verbrauchermagazin „Consumer Reports“ bei einem Fahrzeug des Herstellers Tesla – ausgestattet mit einem Fahrassistenten – auf einer Teststrecke das System, ohne einen Fahrer, zu verwenden.¹³ Die Sicherheitsfunktion des Fahrzeuges, die durch das Anlegen des Sicherheitsgurtes durch den Fahrer auf dem Fahrersitz gewährleistet werden sollte, konnte durch vorheriges Schließen des Gurtes ohne Fahrer umgangen werden, so dass ein Verlassen des Fahrersitzes bei Reduktion der Geschwindigkeit ermöglicht wurde.¹⁴ Durch eine am Lenkrad befestigte Kette konnte das Gewicht der Hände am Lenkrad simuliert werden.¹⁵ Die Fahrt wurde so ohne Fahrer nur durch das Assistenzsystem fortgesetzt. Da das Fahrzeug nicht wahrnehmen konnte, dass der Fahrer den Fahrersitz verlassen hatte, wurde auch keine Warnung durch das System abgegeben.¹⁶ Neben den allgemeinen Gefahren, die dadurch für den Straßenverkehr entstehen könnten, besteht in diesem Zusammenhang auch ein Risiko für Angriffe mit terroristischem Hintergrund. Bereits in der Vergangenheit wurden Fahrzeuge zu Terroranschlägen verwendet, so zum Beispiel bei den Anschlägen in Berlin¹⁷ und Nizza¹⁸.

Weitere Beispiele der Täuschung der maschinellen Wahrnehmung zeigen sich im Zusammenhang mit Verkehrszeichen. Beispielfähig können das Ausnutzen von Adversarial Learning sowie die Manipulation durch Projektion genannt werden.

¹² Hessel/Leffer/Potel, See No EVIL – Angriffe auf Autonome Fahrzeuge und deren Strafbarkeit, InTeR 2020, 208 (210).

¹³ Spiegel, Fahrt ohne Fahrer – US-Verbraucherschützer hebeln Teslas Autopilot aus, Meldung vom 23.04.2021, 15.25 Uhr, abrufbar unter: <https://www.spiegel.de/auto/autopilot-von-tesla-us-verbraucherschuetzer-hebeln-fahrassistent-aus-a-4e544b2c-f9cc-4d5e-8e62-66c2325fe66f> (zuletzt abgerufen am 23.04.2021).

¹⁴ Spiegel, Fahrt ohne Fahrer – US-Verbraucherschützer hebeln Teslas Autopilot aus, Meldung vom 23.04.2021, 15.25 Uhr, abrufbar unter: <https://www.spiegel.de/auto/autopilot-von-tesla-us-verbraucherschuetzer-hebeln-fahrassistent-aus-a-4e544b2c-f9cc-4d5e-8e62-66c2325fe66f> (zuletzt abgerufen am 23.04.2021).

¹⁵ Spiegel, Fahrt ohne Fahrer – US-Verbraucherschützer hebeln Teslas Autopilot aus, Meldung vom 23.04.2021, 15.25 Uhr, abrufbar unter: <https://www.spiegel.de/auto/autopilot-von-tesla-us-verbraucherschuetzer-hebeln-fahrassistent-aus-a-4e544b2c-f9cc-4d5e-8e62-66c2325fe66f> (zuletzt abgerufen am 23.04.2021).

¹⁶ Spiegel, Fahrt ohne Fahrer – US-Verbraucherschützer hebeln Teslas Autopilot aus, Meldung vom 23.04.2021, 15.25 Uhr, abrufbar unter: <https://www.spiegel.de/auto/autopilot-von-tesla-us-verbraucherschuetzer-hebeln-fahrassistent-aus-a-4e544b2c-f9cc-4d5e-8e62-66c2325fe66f> (zuletzt abgerufen am 23.04.2021).

¹⁷ Süddeutsche Zeitung, Anschlag auf Berliner Weihnachtsmarkt, https://www.sueddeutsche.de/thema/Anschlag_auf_Berliner_Weihnachtsmarkt (zuletzt abgerufen am 30.04.2021).

¹⁸ Zeit.de, Anschlag in Nizza: Attentat mit einem LKW <https://www.zeit.de/gesellschaft/zeitgeschehen/2016-07/anschlag-nizza-lastwagen-terror-francois-hollande> (zuletzt abgerufen am 30.04.2021).

Moderne Fahrzeuge bedienen sich bei der Erkennung von Objekten der Klassifikation.¹⁹ Zur Herausbildung der Klassifikationen werden häufig maschinelle Lernverfahren eingesetzt.²⁰ Diese Vorgehensweise bietet jedoch auch Schwachstellen, die durch Angreifer ausgenutzt werden können. Bei Adversarial-Learning-Angriffen modifiziert der Angreifer die Muster eines Objektes so, dass dadurch die Wahrscheinlichkeit einer korrekten Erkennung und Einordnung durch das Fahrzeug herabgesetzt oder unmöglich gemacht wird.²¹ Die Besonderheit dieser Angriffsmethode besteht darin, dass die Manipulation nicht zu einer Täuschung der menschlichen Wahrnehmung führt.²² Manipulationen, wie das Kleben einer Folie auf ein Verkehrszeichen, durch die das Fahrzeug nicht mehr in der Lage ist dieses korrekt abzulesen sind bereits durch wissenschaftliche Untersuchungen belegt.²³

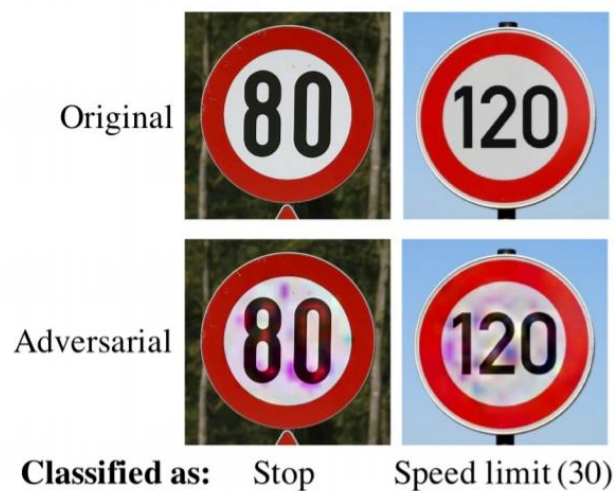


Abbildung 2: Beispiel für einen Adversarial-Learning-Angriff: Die manipulierten Verkehrszeichen (unten) werden einmal als Stoppschild und einmal als Tempo-30-Schild erkannt. Quelle: Sitawarin et al., DARTS: Deceiving Autonomous Cars with Toxic Signs, v. 31.05.2018, <https://arxiv.org/pdf/1802.06430.pdf> (zuletzt abgerufen am 30.04.2021), S. 2.

Daneben besteht auch die Möglichkeit einer Manipulation durch die Projektion von vermeintlichen Verkehrszeichen auf Oberflächen, die im Wahrnehmungsbereich des Fahrzeuges liegen. Derartige Projektionen können zwar durch das menschliche Auge als solche entlarvt werden, bei der maschinellen Wahrnehmung ist dies jedoch nicht immer der Fall. Ein Beispiel hierfür sind wissenschaftliche Untersuchungen bei Assistenzsystemen, welche in der Lage sind Verkehrszeichen zu erkennen und den Fahrer auf zulässige Höchstgeschwindigkeiten hinzuweisen.²⁴

¹⁹ Dietmayer, in: M. Maurer et al. (Hrsg.), Autonomes Fahren, S. 423.

²⁰ Dietmayer, in: M. Maurer et al. (Hrsg.), Autonomes Fahren, S. 423.

²¹ Lim/Taeihagh, Sustainability 11/2019, S. 1, 13.

²² Papernot et al., in: IEEE, European Symposium on Security and Privacy (EuroS&P), 2016, S. 372, 387.

²³ Sitawarin et al., DARTS: Deceiving Autonomous Cars with Toxic Signs, v. 31.05.2018, <https://arxiv.org/abs/1802.06430> (zuletzt abgerufen am 30.04.2021).

²⁴ Nassi et al., MobilBye: Attacking ADAS with Camera Spoofing, v. 24.6.2019, <https://arxiv.org/abs/1906.09765> (zuletzt abgerufen am 30.04.2021).

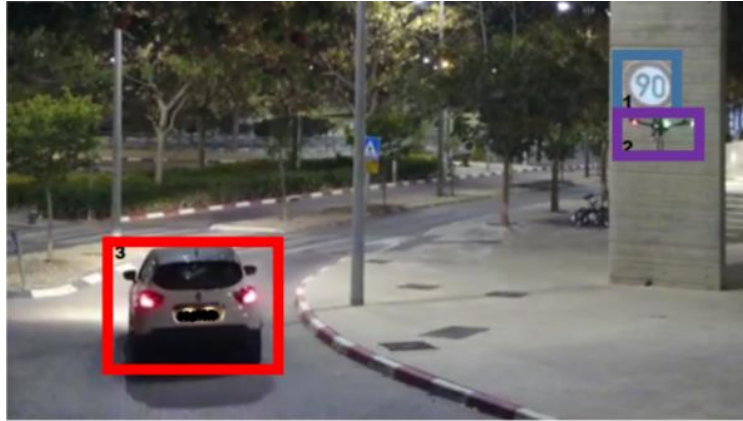


Abbildung 3: Beispiel für einen Angriff mit Hilfe einer Projektion: Eine Drohne (2) projiziert ein Verkehrszeichen (1) an eine Hauswand. Das vorbeifahrende Auto (3) erkennt dieses Zeichen als echt und gibt eine Warnung an den Fahrer aus. Quelle: Nassi et al., MobilBye: Attacking ADAS with Camera Spoofing, v. 24.6.2019, <https://arxiv.org/pdf/1906.09765.pdf> (zuletzt abgerufen am 30.04.2021).

Durch die zunehmende Übertragung der menschlichen Fahrzeugsteuerung auf eine maschinelle entstehen somit neue Angriffsvektoren, die es durch technische Gegenmaßnahmen und entsprechende gesetzliche Vorgaben zu verhindern gilt. Auch auf US-amerikanischer Ebene gibt es bereits Bestrebungen autonome Fahrzeuge mit Technologien zur Verhinderung von Terroranschlägen auszustatten.²⁵

2. Datenschutz

Beim autonomen Fahren werden umfangreich Daten verarbeitet. Hierbei kann es sich nicht nur um Sachdaten, sondern auch um Daten der Fahrzeuginsassen, aber auch von Personen aus dem Umfeld des Fahrzeuges handeln. Es besteht somit ein Risiko, dass die Privatsphäre des Halters oder Fahrers, aber auch die eines unbeteiligten Dritten beeinträchtigt wird. Bei der effektiven Umsetzung des Konzeptes des autonomen Fahrzeuges ist die Verarbeitung von Daten jedoch unverzichtbar. Es gilt daher einen angemessenen Ausgleich zwischen der notwendigen Datenverarbeitung, und dem Recht auf Privatsphäre zu finden. Die Datenverarbeitung sollte den Grundsätzen der Datensparsamkeit und Datenvermeidung folgend daher stets auf das zur Erreichung des mit der Datenverarbeitung verfolgten Zwecks erforderliche Maß beschränkt sein. Hilfreich können außerdem datenschutzfreundliche Voreinstellungen sein, die bereits bei Auslieferung hinterlegt werden und die Datenverarbeitung auf ein zum Betrieb erforderliche Mindestmaß beschränken, sofern der Nutzer nicht bei der Aktivierung weitergehender Funktionen abweichende Einstellungen vornimmt.²⁶

²⁵ The Guardian, Self-driving cars must have technology to prevent use in terror, lawmakers say, <https://www.theguardian.com/technology/2017/sep/06/self-driving-cars-terrorism-cybersecurity-technology> (zuletzt abgerufen am 30.04.2021).

²⁶ Ethik-Kommission automatisiertes und vernetztes Fahren, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile (zuletzt abgerufen am 30.04.2021), S. 25.

Die erhobenen Daten erlauben teils umfassende Rückschlüsse auf die beteiligten natürlichen Personen, denn sie können Daten über Tagesrhythmus, Bewegungsprofile, Körpergröße (z.B. durch Ermittlung anhand der Sitzeinstellungen), Anzahl an Mitfahrern (z.B. aufgrund der Anzahl der geschlossenen Gurte), Telefonlisten sowie Musikgeschmack des Fahrers sowie anderer Insassen enthalten.²⁷ Daher sind sie als personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO zu qualifizieren.²⁸

Die Anwendbarkeit der DSGVO sorgt für einen weitreichenden Schutz der personenbezogenen Daten und stellt Datenverarbeitungen unter ein Verbot mit Erlaubnisvorbehalt. Ohne taugliche Rechtsgrundlage (Art. 6 Abs. 1 Buchst. a bis Buchst. f DSGVO) ist eine Verarbeitung personenbezogener Daten daher unzulässig. Bisher unzureichend beantwortet ist jedoch wer als Verantwortlicher (Art. 4 Nr. 7 DSGVO) über die Zwecke und Mittel der Datenverarbeitung beim Autonomen Fahren entscheidet. Dies ist aber von entscheidender Bedeutung, da mit der datenschutzrechtlichen Verantwortlichkeit die Pflicht zur Umsetzung der datenschutzrechtlichen Vorgaben folgt. Als problematisch ist in diesem Zusammenhang insbesondere Übertragung der datenschutzrechtlichen Verantwortlichkeit auf Privatpersonen zu sehen, da diese regelmäßig nicht in der Lage sein dürften die Vorgaben der DSGVO, die trotz der Haushaltsausnahme im Bereich des Autonomen Fahrens weite Anwendung finden dürften, umzusetzen. Neben den notwendigen Einflussmöglichkeiten auf die technischen Abläufe der Datenverarbeitung ist hierbei auch die Privatsphäre der Verantwortlichen selbst zu beachten. Nach Art 13 Abs. 1 Buchst. a DSGVO muss der Verantwortliche in seinen Datenschutzinformationen beispielsweise seinen Namen und seine Kontaktdaten angeben. Dies ist im öffentlichen Straßenverkehr abzulehnen und würde, insbesondere für Menschen die Diskriminierung ausgesetzt sind, zusätzliche Risiken schaffen. Eine datenschutzrechtliche Verantwortlichkeit des privaten Fahrzeughalters führt auch zu einer Zersplitterung der Steuerungsmöglichkeiten durch die Datenschutzaufsichtsbehörden. Ein Beispiel hierfür ist das Einschreiten der Berliner Datenschutzaufsicht gegen einen Tesla-Besitzer wegen der Aktivierung des Wächter-Modus (Sentry Mode), der das Fahrzeug durch Videoüberwachung u.a. vor Vandalismus schützen soll, im öffentlichen Verkehrsraum.²⁹

Unabhängig von der datenschutzrechtlichen Verantwortlichkeit ist anzumerken, dass einige Verpflichtungen der DSGVO mit dem autonomen Fahren grundsätzlich inkompatibel scheinen. Ein Beispiel hierfür ist die Gewährleistung der Informationspflichten bei der Erhebung von personenbezogenen Daten von Passanten im Umfeld von Autonomen Fahrzeugen. In der Regel werden

²⁷ Landesbeauftragte für den Datenschutz Niedersachsen, 10 Fragen und Antworten zum Thema Datenschutz im Kfz, https://lfd.niedersachsen.de/startseite/themen/weitere_themen_von_a_z/kfz/kfz-und-datenschutz-148981.html (zuletzt abgerufen am 30.04.2021).

²⁸ Steege, Künstliche Intelligenz und Mobilität, SVR 2021 1 (5).

²⁹ Teslamag.de, Bericht: Tesla-Besitzer wegen Wächter-Modus von Berliner Datenschutz-Behörde verwarnt, <https://teslamag.de/news/bericht-tesla-besitzer-waechter-modus-berliner-datenschutz-behoerde-verwarnt-34714/amp> (zuletzt abgerufen am 30.04.2021).

persönliche Merkmale dieser zwar unmittelbar nach der Erfassung anonymisiert, dennoch liegt jedoch eine Datenverarbeitung vor. Den Betroffenen in dieser Konstellation jedoch sämtliche Pflichtinformationen des Art. 13 DSGVO mitzuteilen bzw. zur Verfügung zu stellen, erscheint kaum sinnvoll umsetzbar und mit Blick auf die geringe Beeinträchtigung der Privatsphäre, die bei einer unmittelbaren Anonymisierung gewährleistet werden kann, auch nicht notwendig. Sinnvoller erscheint hier beispielsweise ein Nachweis der Tauglichkeit des Anonymisierungsverfahrens, beispielsweise über eine Zertifizierung.

3. Ethische und gesellschaftliche Aspekte

Aus ethischer Sicht steht das autonome Fahren diversen Herausforderungen gegenüber. Bereits im Jahr 2016 hat das BMVI daher eine Ethik-Kommission mit der Bewertung des autonomen Fahrens und der Entwicklung von Leitlinien beauftragt. Der Einsatz von autonomen Fahrzeugen folgt grundsätzlich dem Nützlichkeitsgedanken sowie den Grundsätzen der Privatautonomie.³⁰ Der Schutz von Menschen genießt dabei Vorrang vor dem Nützlichkeitsgedanken.³¹ Die in diesem Zusammenhang vorgebrachte Argumentation ist aber in sich nicht ganz schlüssig, denn die Automatisierung wird auf der anderen Seite als Faktor der Schadensreduzierung verstanden.³² Ziel der technischen Umsetzung soll darüber hinaus die Vermeidung von „Dilemma-Situationen“ sein, das heißt Situationen, in denen das Fahrzeugsystem zwischen zwei nicht abwägungsfähigen Übeln entscheiden muss.³³ Höchste Priorität bei technisch unvermeidbaren Ereignissen muss im Rahmen einer Güterabwägung dem Schutz des menschlichen Lebens zukommen.³⁴ Sachschäden sind insoweit Personenschäden stets vorzuziehen. Vor besonderen ethischen Problemen stehen Betroffene und Fahrzeugsysteme, soweit es um die Abwägung Leben gegen Leben geht. Bei unausweichlichen Unfallsituationen ist jede Qualifizierung nach persönlichen Merkmalen (Alter, Geschlecht, körperliche oder geistige Konstitution) strikt untersagt.³⁵ Dagegen wird aber eine allgemeine Programmierung, die eine Minderung der Anzahl von

³⁰ Ethik-Kommission automatisiertes und vernetztes Fahren, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile (zuletzt abgerufen am 30.04.2021), S. 10.

³¹ Ethik-Kommission automatisiertes und vernetztes Fahren, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile (zuletzt abgerufen am 30.04.2021), S. 10.

³² Vgl. dazu Regel Nr. 5: Ethik-Kommission automatisiertes und vernetztes Fahren, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile (zuletzt abgerufen am 30.04.2021), S. 10.

³³ Regel Nr. 5: Ethik-Kommission automatisiertes und vernetztes Fahren, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile (zuletzt abgerufen am 30.04.2021), S. 10.

³⁴ Regel Nr. 7: Ethik-Kommission automatisiertes und vernetztes Fahren, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile (zuletzt abgerufen am 30.04.2021), S. 11.

³⁵ Ethik-Kommission automatisiertes und vernetztes Fahren, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile (zuletzt abgerufen am 30.04.2021), S. 11.

Personenschäden vorsieht als vertretbar erachtet.³⁶ Während demnach ein Leben nicht gegen ein anderes abgewogen werden darf, soll jedenfalls das fragliche Programmierungsziel einer möglichst geringen Opferzahl im Falle eines unausweichlichen Unfalles zulässig sein. Eingesetzte Algorithmen bergen jedoch die Gefahr der Diskriminierung.³⁷ Komplexe oder intuitive Unfallfolgenabschätzungen sind außerdem nicht so gesetzlich abbildbar, dass sie die Entscheidung eines sittlich urteilsfähigen, verantwortlichen Fahrzeugführers ersetzen oder vorwegnehmen können.³⁸ Hierbei ist freilich zu berücksichtigen, dass auch der Mensch in Extremsituationen an seine Grenzen stößt und es ihm oftmals innerhalb kürzester Entscheidungsspielräume nicht gelingt rationale oder vorhersehbare Entscheidungen zu treffen. Während der Tod eines Menschen in diesen Fällen den Notstandsregelungen unterfällt, kann dies nicht für autonome Fahrzeuge gelten, die innerhalb kürzester Zeit eine Vielzahl von Handlungsmöglichkeiten durchspielen und bewerten können. An die Grenzen des ethisch-vertretbaren gelangt man schnell unter dem Aspekt, dass es sich bei den Systementscheidungen in jedem Fall um Fremdentcheidungen handelt, die zwar ethisch-korrekten Entscheidungsmustern folgen können und damit dem Grundkonsens entsprechen, im Einzelfall aber nicht durch den nachvollziehbaren Selbsterhaltungstrieb des Fahrers gedeckt werden.³⁹ Dies stellt eine höchst brisante Problematik dar. Die eigene Aufopferung aus Gründen der Solidarität kann dem Einzelnen nicht auferlegt werden.⁴⁰ Die Tötung einer Person muss daher ausnahmslos dem Unrecht zugeordnet werden.⁴¹ Ins Wanken kann diese Annahme nur bei drohender Gefahr für eine Vielzahl von Personen kommen, was jedoch – auch vor dem Hintergrund der Bundesverfassungsgerichtsentscheidung zum Luftsicherheitsgesetz (BVerfG, Urteil vom 15. Februar 2006, Az. 1 BvR 357/05) – kritisch zu betrachten ist.

Problematisch ist darüber hinaus, dass eine Verlagerung der Verantwortung durch den Einsatz autonomer Fahrzeuge stattfindet, sodass die bisher dem Fahrer zukommende Verantwortung den Herstellern und Betreibern zugeordnet wird und damit fernab des eigentlichen Unfallgeschehens

³⁶ Ethik-Kommission automatisiertes und vernetztes Fahren, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile (zuletzt abgerufen am 30.04.2021), S. 11.

³⁷ Steege, Künstliche Intelligenz und Mobilität, SVR 2021, 1 (5).

³⁸ Ethik-Kommission automatisiertes und vernetztes Fahren, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile (zuletzt abgerufen am 30.04.2021), S. 11.

³⁹ Beispielhaft dazu nennt die Ethik-Kommission am Fahrbandrand spielende Kinder, während ein menschlicher Fahrer die Wahl selbst zwischen seinem eigenen Leben und dem Leben der Kinder treffen könnte, ist ein Programmierer gezwungen diese Konstellationen anhand des Grundkonsens vorab zu entscheiden, Ethik-Kommission automatisiertes und vernetztes Fahren, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile (zuletzt abgerufen am 30.04.2021), S. 16.

⁴⁰ Ethik-Kommission automatisiertes und vernetztes Fahren, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile (zuletzt abgerufen am 30.04.2021), S. 18.

⁴¹ Ethik-Kommission automatisiertes und vernetztes Fahren, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile (zuletzt abgerufen am 30.04.2021), S. 18.

stattfindet.⁴² Auch infrastrukturelle, politische sowie rechtliche Entscheidungsinstanzen können Einfluss auf die potentiellen Entscheidungen ausüben.⁴³ Ein besonderes Herstellerinteresse lässt sich auf produkthaftungsrechtliche Aspekte, die mit dem Einsatz der autonomen Fahrzeuge einhergehen begründen. Im Sinne einer effektiven Missbrauchsverhinderung müssen Leitlinien und Anforderungen an die Programmierung durch eine unabhängige öffentliche Stelle gesetzt werden und anschließend eine umfassende Aufklärung der Öffentlichkeit stattfinden.⁴⁴ Aus Gründen der allgemeinen Akzeptanz, ist es neben den bereits im Zusammenhang mit den Angriffsmöglichkeiten beschriebenen Risiken erforderlich, dass geeignete Maßnahmen zum Schutz gegen Cyberangriffe zu etablieren. Transparenz und Nachvollziehbarkeit der Entscheidungsprozesse sind ebenfalls erforderlich. Die Erheblichkeit der zugrunde gelegten Daten und Bewertungsmaßstäbe muss klar definiert sein. Diese Faktoren spielen auch bei der Analyse fehlerhaften Verhaltens eine entscheidende Rolle, wenn es um die Frage geht, ob dieses auf Programmierungs- oder Hardwarefehler zurückzuführen ist. Erheblich ist in diesem Zusammenhang die Verlässlichkeit der in die Auswertung einfließenden Daten, die insbesondere durch äußere Umstände – wie z.B. wetterbedingte Beeinträchtigungen – getrübt sein können.

Daneben muss auch die Übergabe der Fahrzeugkontrolle durch das System an den Fahrer betrachtet werden. Diese muss störungs- und risikofrei erfolgen, was insbesondere erfordert, dass dem Fahrer genügend Zeit bleibt sich durch eine Analyse der akuten Verkehrssituation auf die Übernahme einzustellen. Ein Ad-Hoc-Eingreifen erscheint daher undurchführbar und risikobehaftet. Im Vorfeld muss die Verteilung der Verantwortung sowie die Übernahme der Aufgaben eindeutig festgelegt sein.

Natürlich können Funktionsstörungen bei autonomen Fahrzeugen nicht vollständig ausgeschlossen werden, die damit einhergehenden Risiken können nicht unberücksichtigt bleiben. Dennoch überwiegen bei einer Gesamtschau der Vor- und Nachteile des autonomen Fahrens die Vorteile, die sich insbesondere in einer erheblichen Steigerung der Mobilität für eine Vielzahl von Personen, einer insgesamt erhöhten Sicherheit des allgemeinen Straßenverkehrs sowie einem möglichen Zeitgewinn durch Verzicht auf den Fahrer widerspiegeln.⁴⁵

⁴² Ethik-Kommission automatisiertes und vernetztes Fahren, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile (zuletzt abgerufen am 30.04.2021), S. 11.

⁴³ Ethik-Kommission automatisiertes und vernetztes Fahren, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile (zuletzt abgerufen am 30.04.2021), S. 11.

⁴⁴ Ethik-Kommission automatisiertes und vernetztes Fahren, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile (zuletzt abgerufen am 30.04.2021), S. 12.

⁴⁵ Ethik-Kommission automatisiertes und vernetztes Fahren, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile (zuletzt abgerufen am 30.04.2021), S. 15.

Das autonome Fahren kann auch einen wesentlichen Beitrag zur Verkehrswende leisten. Dabei spielen jedoch verschiedene Faktoren der Einsetzung autonomer Fahrzeuge eine entscheidende Rolle. Zum einen kommt der Aspekt der Verkehrssicherheit zum Tragen, da der flächendeckende Einsatz autonomer Fahrzeuge eine Steigerung der Sicherheit des Straßenverkehrs verspricht. Ziel ist dabei die Abkehr von unterstützenden Funktionen wie beim assistierten Fahren hin zum Einsatz fahrerloser autonomer Fahrzeuge. Dies soll Bürgern, die aufgrund von körperlichen Einschränkungen oder fehlender Fahrerlaubnis bisher dem Straßenverkehr fernblieben, neue Mobilitätschancen eröffnen. Neben fortbestehendem Individualverkehr sind auch Shared-Modelle denkbar. Darüber hinaus versprechen derartige Modelle auch positive Umweltauswirkungen sowie eine Anbindung strukturschwacher und ländlicher Regionen.⁴⁶ Zur Nutzung dieser Potentiale bedarf es jedoch einer genauen Betrachtung der Einsatzszenarien, entsprechender Anreize und infrastruktureller Rahmenbedingungen. Das bloße Vorhandensein einer Technologie führt noch nicht zu ihrem sinnvollen und gesellschaftlich wünschenswerten Einsatz.

III. Der Gesetzentwurf im Einzelnen

Mit Blick auf die aufgezeigten Risiken, Herausforderungen und rechtlichen Unklarheiten bei der Entwicklung und dem Einsatz autonomer Fahrzeuge ist eine gesetzliche Regelung ausdrücklich zu begrüßen. Der vorliegende Gesetzentwurf kann diesbezüglich jedoch lediglich als Regelung verstanden werden, die einen Testbetrieb autonomer Fahrzeuge erlaubt und damit die wissenschaftliche Basis für die Bewertung der Technologie verbessert. Geht man jedoch davon aus, dass die Regelung über den Testbetrieb hinaus – insbesondere für den Einsatz von autonomen Fahrzeugen durch Privatpersonen – gelten soll, erweist sie sich, wie die folgenden Ausführungen verdeutlichen, in weiten Teilen als nicht ausreichend. Die insoweit offen bleibenden Fragen müssen beantwortet und einer Regelung auf europäischer Ebene zugeführt werden.

1. § 1e StVG

§ 1e StVG regelt die Zulässigkeitsvoraussetzung für den Betrieb eines autonomen Fahrzeuges. Der Betrieb eines autonomen Fahrzeuges ist nach § 1e Abs. 1 Nr. 1 StVG zulässig, soweit die Voraussetzungen des § 1e Abs. 2 StVG vorliegen. Kraftfahrzeuge müssen in der Lage sein die Fahraufgabe innerhalb des jeweiligen festgelegten Betriebsbereichs selbständig zu bewältigen, ohne dass eine fahrzeugführende Person in die Steuerung eingreift oder die Fahrt des Kraftfahrzeugs permanent von der technischen Aufsicht überwacht wird. Die Voraussetzungen für den Betrieb eines autonomen Fahrzeuges nach § 1e Abs. 2 StVG müssen jedoch ins Verhältnis zu möglichen Risiken und Herausforderungen gesetzt werden. Zu diesen zählen die zuvor skizzierten Angriffsszenarien.

Für den Bereich der Cybersicherheit wurden hierzu bereits im März 2021 die durch das Weltforum für die Harmonisierung von Fahrzeugvorschriften (WP.29) als Arbeitsgruppe der Wirtschaftskommission

⁴⁶ Haupt, Auf dem Weg zum autonomen Fahren, NZV 2021, 172 (173).

der Vereinten Nationen für Europa (UNECE) erarbeiteten Regelungen verbindlich auf europäischer Ebene umgesetzt. Diese enthalten neben der Verpflichtung der Hersteller zur Einführung eines Managementsystems für Cybersicherheit in Fahrzeugen auch eines Rechtsrahmens für die Durchführung von Updates aus der Ferne (Over-the-Air-Updates) und gehen damit inhaltlich über die Anforderungen des Entwurfs hinaus.

Die Regelung des § 1e Abs. 2 Nr. 2 StVG wird darüber hinaus der Komplexität der aufgezeigten ethischen Herausforderungen beim autonomen Fahren nicht gerecht. Hier wäre eine deutlich klarere Regelung wünschenswert, welche die Vorgaben der Ethikkommission stärker berücksichtigt und an der tatsächlichen Leistungsfähigkeit der Technik ausgerichtet ist.

Liegen die technischen Voraussetzungen gemäß § 1e Abs. 2 StVG sowie die Selbsterklärung des Herstellers nach § 1f Abs. 3 Nr. 4 vor, erteilt das Kraftfahrt-Bundesamt auf Antrag des Herstellers gemäß § 1e Abs. 3 StVG eine Betriebserlaubnis für ein Kraftfahrzeug mit autonomer Fahrfunktion. Auf europäischer Ebene ist jedoch bereits eine deutliche Abkehr von dem Prinzip der Selbsterklärung des Herstellers erkennbar.⁴⁷ Die Komplexität der bestehenden Anforderungen sowie spezielle Kenntnisse, die zur Beurteilung und Einschätzung sowie zur Überprüf- und Nachweisbarkeit der Compliance der technischen Ausrüstung sprechen auch hier für eine Zertifizierung durch unabhängige Dritte.

2. § 1f StVG

Dem Halter wird nach § 1f StVG die Aufgabe übertragen die Verkehrssicherheit und die Umweltverträglichkeit des Fahrzeuges zu erhalten. In diesem Zusammenhang ist jedoch nicht ersichtlich, inwieweit die nach § 1f Nr. 1-Nr.3 StVG konkret übertragenen Aufgaben zur Erhaltung der Umweltverträglichkeit beitragen sollen. Insoweit besteht Konkretisierungsbedarf. § 1f Abs. 2 StVG regelt die Eingriffsmaßnahmen der Technischen Aufsicht. Unklar bleibt jedoch inwieweit eine Rückübertragung auf das Fahrzeug möglich ist und unter welchen Rahmenbedingungen diese Rückübertragung zu erfolgen hätte.

3. § 1g StVG

§ 1g StVG regelt die Datenverarbeitung der Nutzung von autonomen Fahrzeugen. Der Halter ist zur Speicherung der in § 1g Abs. 1 S. 1 Nr. 1-Nr. 13 StVG genannten Daten verpflichtet. Diese sind nach § 1g Abs. 1 S. 2 StVG auf Verlangen dem Kraftfahrt-Bundesamt und den zuständigen Landesbehörden zu übermitteln. § 1g StVG unterscheidet dabei zwischen Daten die beim Betreib zu speichern sind (Abs. 1) sowie Daten die einer anlassbezogenen Speicherung (Abs. 2) unterliegen. Vor dem Hintergrund dieser Vorschrift ist der Halter als datenschutzrechtlicher Verantwortlicher anzusehen. Dies erscheint

⁴⁷ So zum Beispiel in der Marktüberwachungsverordnung, dem Cybersecurity Act sowie der IT-Sicherheitsverordnung.

jedoch wenig überzeugend. So hat der Halter, insbesondere wenn es sich um eine Privatperson handelt, kaum Einflussmöglichkeiten auf die technische Ausgestaltung des Fahrzeugs und dürfte zugleich mit der Einhaltung der datenschutzrechtlichen Vorgaben überfordert sein.

Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Die Entscheidung über Zwecke und Mittel der Verarbeitung muss bereits aus Gründen der Gewährleistung der Funktionsfähigkeit des Fahrzeuges als auch aus Gründen der Praktikabilität beim Hersteller liegen. So erscheint der Halter nicht als tauglicher Adressat im Sinne der Norm, welche insoweit Anpassungsbedarf aufweist. Sinnvoller erscheint es daher die Verantwortlichkeit dem Hersteller zuzuordnen und damit auf eine einheitliche Gewährleistung durch diesen hinzuwirken oder die Konzepte der DSGVO für den Bereich des autonomen Fahrens grundsätzlich zu überarbeiten. Hier bei ist auch zu berücksichtigen, dass der Hersteller einen nicht unerheblichen Teil der Daten benötigen dürfte, um seinen Anforderungen an ein Cybersecurity Managementsystem nach den Vorgaben der UNECE WP.29 nachzukommen. Darüber hinaus enthält die Vorschrift keine Regelung dazu, wie mit Daten unbeteiligter Dritter zu verfahren ist.

4. § 11 StVG

Gemäß § 11 StVG wird das Bundesministerium für Verkehr und digitale Infrastruktur beauftragt die Anwendung der Regelungen des Gesetzes insbesondere im Hinblick auf die Auswirkungen auf die Entwicklung des autonomen Fahrens, die Vereinbarkeit mit Datenschutzvorschriften sowie die aufgrund von Erprobungsgenehmigungen im Sinne des § 1i Abs. 2 StVG gewonnenen Erkenntnisse auf wissenschaftlicher Grundlage in nicht personenbezogener Form zu evaluieren und den Deutschen Bundestag über die Ergebnisse der Evaluierung zu unterrichten. Sofern erforderlich, soll das Bundesministerium für Verkehr und digitale Infrastruktur die Evaluierung zu einem von ihm festzulegenden Zeitpunkt bis zum Jahr 2030 erneut durchführen. Eine Evaluierung des Gesetzes und der gesetzlichen Vorgaben zum autonomen Fahren ist zu begrüßen. Es ist jedoch fraglich, ob der angegebene Umfang ausreichend ist und daher genügend Aufschluss über die Entwicklungen bieten kann. Auch ist zu bemängeln, dass eine Evaluierung ohne ein Gesamtkonzept wenig sinnvoll erscheint.