Kroschwald S., Datenschutz und -souveränität für Verbraucher:innen im künstlich-intelligenten Fahrzeug, In: Boden, A., Jakobi, T., Stevens, G., Bala, C. Hgg., Verbraucherdatenschutz – Technik und Regulation zur Unterstützung des Individuums. Schriften der Verbraucherinformatik Band 1, 2021. DOI: 10.18418/978-3-96043-095-7_03

Datenschutz und -souveränität für Verbraucher:innen im künstlich-intelligenten Fahrzeug

Steffen Kroschwald
Hochschule Pforzheim, Zentrum für Verbraucherforschung und nachhaltigen Konsum (vunk)
steffen.kroschwald@hs-pforzheim.de

Abstract. Künstliche Intelligenz im autonomen Fahrzeug verarbeitet enorme Mengen an Daten. Beim Betrieb eines solchen Fahrzeugs basiert jede Bewegung auf einer datenbasierten, automatisierten und adaptiven Entscheidungsfindung. Aber auch, um Regeln zur Erkennung und Entscheidung in komplexen Situationen wie den hochindividuellen Verkehrsszenarien entwickeln zu können (KI-Training), sind bereits beachtliche Datenmengen von Fahrzeugen im Realverkehr erforderlich – zum Beispiel Videosequenzen aus Kamerafahrten. Für das Training Künstlicher Intelligenz ist es aus Sicht der Fahrzeugentwicklung attraktiv, auf den Datenschatz zuzugreifen, den die Gesamtheit der Fahrzeuge im realen Anwendungskontext erzeugen kann. Als Nutzer:innen und Insassen sind Verbraucher:innen so Teil einer groß angelegten Testdatenerhebung durch Fahrzeughersteller und Anbieter. Das wirft Datenschutzfragen auf. Ziel des vorliegenden Beitrags ist es herauszuarbeiten, inwiefern sich hierdurch Implikationen für die Rechte und Freiheiten von Verbraucher:innen ergeben und welche Mechanismen das geltende Recht sowie aktuelle legislative Entwicklungen bereithalten, den „Datenhunger“ der KI mit den Interessen an Datensouveränität und informationeller Selbstbestimmung in Einklang und Ausgleich zu bringen. Im Fokus steht dabei insbesondere, wie Anforderungen schon im Produktdesign „mitgedacht“ werden und damit für Verbraucher:innen rechts- und vertrauensfördernd wirken können.

Künstlich-intelligente, autonome Fahrzeuge

Fahrzeuge verfügen seit Jahrzehnten über Technologie zur Datenverarbeitung, mit dem Ziel, ihren Betrieb sicherer, komfortabler oder leichter zu machen. Um beispielsweise Informationen zum Zustand von Bauteilen, zum Fahrzeuginnenraum sowie zur Umgebung zu erfassen, werden mittlerweile unzählige Sensoren verbaut. Die erfassten Daten werden bislang in zentralen oder dezentralen „Electronic Control Units" (ECU) nach programmierten Algorithmen verarbeitet (*Krauß* et al. 2017, 10 f.). Diese Steuereinheiten greifen die Daten aus Sensoren ab, verarbeiten sie und senden, verkürzt gesagt, nach dem „EVA-Prinzip" in der Folge der Verarbeitung Befehle zur Ausführung an Aktoren in Fahrzeugkomponenten (*Krauß* 2019, 228). Dass dabei auch Daten in Fahrzeugen gespeichert werden, die etwa in Werkstätten ausgelesen und genutzt werden können – unter anderem, um die Produkte weiter zu verbessern – wird niemanden überraschen.[1] Darüber hinaus werden Neufahrzeuge schon seit einigen Jahren über Online- oder andere Datenanbindungen mit Backendservern, anderen Fahrzeugen oder Verkehrsinfrastruktur verbunden, mit denen sie im Betrieb Daten austauschen: zunächst zur Ermöglichung von Fahrzeug-, Mobilitäts- und Kommunikationsdiensten im Fahrzeug, etwa um echtzeitaktuelle Informationen und Inhalte wie Wetter und Verkehrslage für ihre Dienste und Funktionen zu erhalten. Aber auch, um sich aus der Ferne diagnostizieren, updaten oder steuern zu lassen (vgl. *CNIL*, S. 23 f.). Schließlich, um selbst, etwa als Teil einer Schwarminfrastruktur (*Roßnagel* 2019, S. 20 f.) oder zum Zwecke der Datensammlung im Rahmen datenbasierter Geschäftsmodelle von Herstellern und Dritten (*Hornung* 2019, S. 109 ff.) Daten bereitzustellen.

Aktuelle technische Entwicklungen heben solche Funktionen auf eine gänzlich neue Stufe. Komplexe Assistenzsysteme, z. B. (Sprach-)Assistenten (*Krämer* et al. 2019; *Knote* et al. 2020, S. 118 ff.), ermöglichen eine natürlichsprachliche Interaktion mit Fahrzeug- und Informationssystemen. Moderne Systeme identifizieren darüber hinaus Regelmäßigkeiten, interpretieren Gewohnheiten und leiten daraus Vorhersagen (Prädiktionen) ab; zum Beispiel, um Routen nach Fahrgewohnheiten oder Tagesabläufen vorzuplanen oder den Fahrmodus der Stimmung des Fahrers entsprechend einzustellen („Social Robots", *Craglia* et al. 2018, S. 23). Fahrerüberwachungssysteme erkennen Müdigkeit oder gar Emotionszustände anhand unzähliger Faktoren in unterschiedlichen Situationen und führen das Fahrzeug, wie beispielsweise jüngst durch Art. 6 Abs. 1 lit. a-d der Typengenehmigungs-Verordnung, VO/2019/2144, für Neufahrzeuge

---

1 Vgl. dazu beispielsweise den bei vielen Betriebsanleitungen von Fahrzeugherstellern zugrundegelegten und zwischen dem *Verband der Automobilindustrie und der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder* entwickelten „VDA Mustertext zur Datenverarbeitung im Fahrzeug", Berlin 2018, S. 3, https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_vda_mustertext.pdf, abgerufen am 25.01.2021.

vorgeschrieben, gegebenenfalls in einen sicheren Fahrmodus zurück (*Lüdemann/Knollmann* 2020, S. 403). Hochautomatisierte Fahrzeuge reagieren zunehmend selbstständig in Echtzeit auch auf komplexe, hochindividuelle Verkehrssituationen und interagieren dabei situativ mit dem Umfeld und der Verkehrsinfrastruktur autonom (*Ethikkommission automatisiertes und vernetztes Fahren* 2017, S. 6). Dies geschieht entweder noch menschlich überwacht oder aber zukünftig in bestimmten Anwendungsfällen oder gar dauerhaft ohne menschliche Eingriffsbereitschaft (*VDA* 2015, S. 15).

Derartige Systeme verfügen über „Künstliche Intelligenz“: Ihnen ist gemein, dass sie gesammelte Daten selbstständig interpretieren, daraus Schlussfolgerungen ziehen können sowie infolgedessen auch in komplexen (und lebensindividuellen) Situationen über ein Handeln zur Erreichung eines Ziels entscheiden (*Hochrangige Expertengruppe für Künstliche Intelligenz* 2018, S. 237). Künstlich-intelligente Systeme folgen nicht mehr nur einem programmierten „Wenn-Dann-Algorithmus“, sondern Regeln, die sie sich entweder im Vorfeld oder durch Analyse ihrer eigenen Entscheidungen und entsprechender Anpassung ihres Verhaltens durch „maschinelles Lernen“ aneignen. Dabei werden die neuartigen Fahrzeugsysteme weniger programmiert als vielmehr trainiert (*Craglia* et al. 2018, S. 20). Anders als bei der klassischen Programmierung entsteht Künstliche Intelligenz regelmäßig nicht durch die bloße Eingabe von Regeln, die auf Daten anzuwenden sind, aus denen das System sodann Ergebnisse erzeugt. Die Künstliche Intelligenz „lernt“ vielmehr – ähnlich wie Menschen – durch Erfassen vieler unterschiedlicher Situationen durch „zusehen“, also Eingabe oder Erfassen, oder „erleben“, also durch Analyse eigener Handlungen und ihrer Ergebnisse und entsprechende Anpassung (zum Lebenszyklus von KI-Systemen: *Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder* 2019, S. 2).

Um Regeln zur Erkennung und Entscheidung in derart komplexen Situationen wie den hochindividuellen Verkehrsszenarien entwickeln zu können, sind für Künstliche Intelligenz im autonomen Fahrzeug enorme Mengen an Test- und Realdaten – zum Beispiel Videosequenzen aus Kamerafahrten mit Fahrzeugen im Realverkehr – erforderlich. Sowohl in der Lern- als auch in der Betriebsphase werden durch und für Künstliche Intelligenz dabei auch personenbezogene Daten in erheblichem Umfang aus zahllosen Quellen und in verschiedenen Kontexten durch unterschiedliche Stellen in vielerlei Hinsicht verarbeitet. Ermöglicht wird diese Entwicklung durch die enorme Steigerung der Rechenleistung und den damit einhergehenden Preisverfall für Recheneinheiten, unter anderem auch durch die systemische Bündelung von Systemeinheiten auf Zentralrechnern und Plattformen in den Fahrzeugen. Ferner durch die Vernetzung der Fahrzeuge und neue Computing-Technologien und schließlich durch wirtschaftliche Anreize aufgrund von Disruptionen in den Geschäftsmodellen der Automobilhersteller und Mobilitätsanbieter sowie nicht zuletzt aufgrund von externen Faktoren wie dem Klimawandel und der damit dringend erforderlichen Verkehrswende, welche die

Entwicklung digitaler und autonomer Fahrzeugsysteme auch auf die politische Agenda gesetzt haben.

Die Zunahme der Verarbeitung von Daten wirft Datenschutzfragen auf. Ziel dieses Beitrags ist es herauszuarbeiten, welche Prinzipien und Grundbedingungen des Datenschutzes durch „KI im Fahrzeug“ berührt werden, inwiefern sich hierdurch Implikationen für die Rechte und Freiheiten für Verbraucher:innen und Nutzer:innen ergeben und welche Mechanismen das geltende Recht sowie aktuelle legislative Entwicklungen hierauf bereits bereithalten sowie, wo noch Maßnahmen- und Steuerungsbedarf besteht. Eine konkrete datenschutzrechtliche Bewertung, insbesondere zur Zulässigkeit der Verarbeitung, wird an den Verarbeitungstätigkeiten im Einzelfall vorzunehmen sein. Für eine datenschutzrechtliche Einordnung des Einsatzes der Künstlichen Intelligenz als Technologie im Fahrzeug an sich und ihrer Folgen ist eine abstraktere Betrachtungsebene zu wählen: Die Technologie wird sich – unabhängig von den im jeweiligen Einzelfall verarbeiteten Datenattributen der Fahrzeuge oder den konkreten Datenempfängern im Mobilitätskontext, Orten der Verarbeitung und technischen Verarbeitungseinrichtungen – im Zweifel an übergeordneten Vorgaben messen lassen müssen. Zu diesen gehören freilich in erster Linie Normen mit Verfassungsrang (*Roßnagel* 1993) wie etwa das Grundrecht auf Schutz personenbezogener Daten nach Art. 8 GrCh. Übergreifenden Charakter im Rahmen des Anwendungsbereichs der DSGVO haben aber auch die als Rahmenanforderungen verpflichtend zu verwirklichenden Datenschutzprinzipien des Art. 5 DSGVO (*Schantz* 2020, Rn. 2).

Datensparsamkeit und KI – ein Widerspruch?

Der Datenhunger der KI

Künstlich-Intelligente Fahrzeuge sind wahre „Datensauger“. Bereits um künstlich-intelligente Fahrzeugsysteme anzulernen, müssen sie beispielsweise mit Informationen (Trainingsdaten) zu echten Fahr- und Verkehrssituationen gespeist werden. Aus diesen leitet die Künstliche Intelligenz im Prozess des Maschinellen Lernens Regeln für Szenarien ab, denen sie im späteren realen Betrieb begegnen kann (*Wachenfeld/Winner* 2015, S. 469 f.). Dieser Lernprozess erfolgt entweder durch „überwachtes Lernen“, bei dem das System so lange mit Trainingsdaten versorgt wird, bis es das erwartete Ergebnis liefert. Oder das System lernt durch menschliche Bewertung der vom System gelieferten Ergebnisse in richtig oder falsch (bestärkendes Lernen). Besonderes Augenmerk verdient ferner die Lernmethode des „unüberwachten Lernens“: Dort lernt das System scheinbar von selbst, oder indem es Muster erkennt und Korrelationen bildet (*Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)*,

2019, S. 4). KI-Systeme für den autonomen Fahrzeugbetrieb werden beispielsweise trainiert, indem sie Bild- und Videosequenzen mit darin enthaltenen Objekten (wie Verkehrszeichen, anderen Fahrzeugen, Hindernissen etc.) oder auch Lebewesen (Menschen oder Tiere auf der Fahrbahn, am Fahrbahnrand etc.) sowie ihren entsprechenden Zuständen und Aktionen im Rahmen der Entwicklung ausgesetzt werden. Eine weitere Trainingsmöglichkeit für KI-Systeme besteht darin, dass sie sich im Realbetrieb solchen Situationen adaptiv anpassen (*Wachenfeld/Winner* 2015, S. 476).

Das Anlernen Künstlicher Intelligenz unterliegt einem Skaleneffekt: Die Verlässlichkeit des Lernergebnisses, mithin der Lernerfolg, hängt in der Regel von der zugrundeliegenden Datenmenge einerseits und der Diversität der bereitgestellten Daten andererseits ab. Autonome Fahrzeuge benötigen beispielsweise – anders als menschliche Fahrschüler – Trainingsdaten und -situationen aus Millionen von Fahrkilometern, um Regeln auch für potenziell komplexe, diffuse, individuelle und entsprechend seltene Verkehrssituationen und -anomalien zu entwickeln (*Craglia* et al. 2018, S. 103). Hierzu gehören im Falle autonomer Fahrzeuge ganz wesentlich auch Bild- und Videodaten. Sie dienen der Erkennung des Verkehrsumfelds, von Personen und Verkehrszeichen. Allein schon, um Personen und Objekte unterscheiden zu können, sie als Fußgänger oder Radfahrer zu identifizieren, aber auch, um deren potenzielles Verhalten im Verkehr zu erlernen, müssen künstlich-intelligente Systeme für autonome Fahrzeuge in der Anlernphase Bild- und Videodaten analysieren (*Lutz* 2020, S. 450), die im Rahmen von Testfahrten im Vorfeld oder auch mit den betreffenden Systemen selbst durch Kamerasysteme aufgezeichnet werden. Zur Unterscheidung von Personen sowie auch zur Identifikation von Bewegungen zwecks Ableitung von potenziellem Verhalten müssen Systeme Personen als solche nicht nur erkennen, sondern auch förmlich „in ihren Gesichtern lesen können." Beispielsweise, um aus (emotionalen) Reaktionen eines Passanten zu erkennen, ob dieser neugierig nach einem herannahenden Bus Ausschau hält oder gedankenversunken droht, die Straße zu betreten, um Gesten von Fahrradfahrern richtig zu deuten oder die Vorfahrtgewährung durch einen Autofahrer korrekt zu interpretieren (*Färber* 2015, S. 130 ff.). Nicht selten werden dabei Bilder in derart hoher Auflösung erzeugt und für den Zweck des Trainings verarbeitet, dass sich darauf körperliche und ggf. auch biometrische (*Europäischer Datenschutzausschuss* 2020b, Rn. 87) Merkmale erkennen und dadurch Menschen unterscheiden lassen (*Consultative Committee of the Convention 108* 2021, S. 3 ff.). Eine Identifizierbarkeit abgebildeter natürlicher Personen und damit das Vorliegen personenbezogener Daten wird sich regelmäßig nicht vollständig ausschließen lassen (*Lutz* 2020, S. 451).

Entgegenstehende Datenschutzprinzipien?

Im Sinne des Prinzips der Datenminimierung müssen diese personenbezogenen Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Art. 5 Abs. 1 lit. c DSGVO). Im Rahmen der autonomen Fahrzeugtechnologie ist das Prinzip der Datenminimierung bereits bei der Datenerhebung von Trainingsdaten virulent. Zunächst wird nicht jedes Trainingsdatum für den Zweck der Verarbeitung erheblich sein. So können beispielsweise akustische Sensoren an einem Testfahrzeug Umfeldgeräusche aufzeichnen, um Regeln zu Verkehrssituationen mit akustischen Ereignissen zu erlernen. Wenn die Aufzeichnung allerdings permanent, zum Beispiel auch bei abgestellten Fahrzeugen oder bei Testfahrten erfolgt, die keinen Zusammenhang mit dieser akustischen Information haben, Daten also erhoben werden, ohne einem konkreten Trainingszweck zu dienen, könnte es in diesem Beispiel bereits an der kausalen Zweckförderung (*Wolff* 2020, Rn. 48) durch die akustischen Daten fehlen. Die so erhobenen Daten wären für die Zwecke des Trainings der KI *nicht erheblich*.

Auch müsste die Verarbeitung auf das notwendige Maß beschränkt sein. Werden beispielsweise im Rahmen von Testfahrten Umfelddaten ohne Beschränkung erfasst, bei Kamerafahrten beispielsweise unter Anwendung von Rundumkameras, wird der Verantwortliche begründen (und im Sinne der Accountability nachweisen) können müssen, weshalb die Totalerfassung für den beabsichtigten Zweck auch *erforderlich* ist (*Europäischer Datenschutzausschuss* 2020b, Rn. 24 ff.). Zweifel an der Erforderlichkeit kämen beispielsweise auf, wenn mithilfe der betreffenden Entwicklungsfahrt nur eine Funktion für das Erkennen von Verkehrszeichen trainiert werden soll, bei der es auf eine Erfassung des rückwärtigen Verkehrs nicht ankommt. Die erfassten Daten wären in diesem Beispiel wohl nicht auf das notwendige Maß (hier z. B. Bilderfassung in Fahrtrichtung) beschränkt.

Schließlich müssten die Daten dem Zweck *angemessen* sein. So wird es beispielsweise Fälle geben, in denen für das Erlernen von Funktionen im Rahmen der Testdaten auch der Standort des Fahrzeugs erforderlich ist und Standortdaten für diesen Zweck in Testfahrzeugen erfasst werden. Nicht immer wird die Erhebung dieser Daten dem Zweck angemessen und damit verhältnismäßig sein (*Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen* 2018, S. 65). Werden solche Testfahrzeuge beispielsweise auch Mitarbeitern für private Fahrten überlassen, kann eine Angemessenheitsprüfung dazu führen, dass bei Fahrten zu ausgewiesenen Privatzeiten zum Schutz der betroffenen Mitarbeiter und ihrer Familien unter anderem diese Standorterfassung zu deaktivieren wäre.

Im Sinne adaptiver Lernverfahren ist es für das Training Künstlicher Intelligenz darüber hinaus aus Sicht der Fahrzeugentwicklung attraktiv, auf den Datenschatz zuzugreifen, den die Gesamtheit der Fahrzeuge nicht nur im Entwicklungsumfeld, sondern im realen Anwendungskontext erzeugen kann. So sind Fahrzeuge, die

bereits an Kunden ausgeliefert und von diesen betrieben werden, durch verbaute Sensoren und Kameras ähnlich wie Testfahrzeuge in der Lage, das reale Verkehrsgeschehen zu erfassen und so Teil einer groß angelegten Testdatenerhebung zu werden. Eine besondere Ausprägung stellen sogenannte „Shadow-Mode-Funktionen“ dar: Diese Funktionen „loggen“ in Kundenfahrzeugen Daten, mit denen sie „im Schatten“ eine zukünftige Realfunktion simulieren. Auf diese Weise lässt sich das mögliche Verhalten dieser Funktion in einem Realbetrieb prüfen und validieren (vgl. *Tesla* 2018). Auf Fragen der Zulässigkeit solcher Verarbeitungen und der Transparenz ebenso wie des Datenzugangs wird noch einzugehen sein. Mit Blick auf die Datenminimierung wäre hier die Erforderlichkeit einer solch umfassenden, massenhaften und teilweise auch permanenten Datenerhebung, beispielsweise Videoaufzeichnung, zu hinterfragen – dies vergleichbar mit der Debatte zur permanenten und anlasslosen Videoüberwachung aus Fahrzeugen (DashCams) (*Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)* 2019b, S. 2). Nicht nur die Dauer der Aufzeichnung, auch die undifferenziert granulare Datenerfassung kann dabei mit dem Prinzip der Datenminimierung kollidieren. So genügt es für viele Trainingsszenarien aggregierte Daten, in Umfang und Detailtiefe reduzierte oder verfälschte, teilweise sogar anonymisierte Daten einzusetzen (*Niemann/Kevekordes* 2020, 21; a.A. *Lutz* 2020, 452).

Speichern ohne Ende?

… für die KI-Entwicklung?

Bereits im Sinne der Datenminimierung, aber auch aufgrund des Prinzips der der Speicherbegrenzung nach Art. 5 Abs. 1 lit. e DSGVO wäre zu prüfen, welche der einmal erhobenen Trainingsdaten in welcher Form, an welchem Ort und für welchen Zeitraum gespeichert sind und weiterverarbeitet werden.

Einige Trainingsszenarien Künstlicher Intelligenz etwa kommen mit einer rein lokalen Verarbeitung im Fahrzeug oder direkt in dem betreffenden Steuergerät aus (*Europäischer Datenschutzausschuss* 2020a, Rn. 70; *Ethik-Kommission automatisiertes und vernetztes Fahren der Bundesregierung* 2017, S. 23). Eine Übermittlung an zentrale Server ist dabei zunächst nicht erforderlich: Beispielsweise kann die Erfassung von Fahrzielen und daraus die Ableitung eines Fahrprofils zur Erstellung eines Routenprädiktionsmodells regelmäßig im Fahrzeug selbst erfolgen. Auch das Anlernen von Sprachsteuerungen auf einen spezifischen Nutzer hin oder das bloße Erkennen von Merkmalen (zum Beispiel bestimmter Straßenzustände) muss nicht zwingend immer zu einer Speicherung von Rohdaten auf zentralen Servern führen. Selbst wenn Daten als Trainingsgrundlage oder als Datenbasis für schwarm-intelligente Funktionen (wie

etwa das Anlernen von Verkehrsmodellen für Verkehrssteuerungs-KI) dienen, wäre im Einzelfall fraglich, ob hierzu auf zentralen Servern Daten in Rohform vorliegen müssen.

Außerdem ist mit Blick auf die Prinzipien der Datenminimierung sowie der Speicherbegrenzung im Einzelfall zu prüfen, ob nach Erfassung und Abschluss der Datenanalyse die Rohdaten, zum Beispiel Videodaten, Tonaufnahmen oder technische Informationen in Verbindung mit Fahrzeugidentifikationsdaten in dieser Form gespeichert werden müssen: Viele Trainings- und Prädiktionsmodelle arbeiten beispielsweise mit aggregierten statistischen Informationen (*Europäischer Datenschutzausschuss* 2020a Rn. 76). Andere benötigen Rohinformationen, die sie aber unmittelbar analysieren (*Europäischer Datenschutzausschuss* 2020b Rn. 29). In vielen Fällen, in denen Analysen auf zentralen Servern erfolgen, werden zwar für die Übertragung von Daten noch Identifikatoren und Metainformationen (z. B. IP-Adressen, Fahrzeugidentifikationsnummern etc.) benötigt; diese sind dann aber nicht für den eigentlichen Anlernvorgang erforderlich. In solchen Fällen wären erhobene Trainings-Rohdaten sowie zugeordnete Daten zu Orten oder zu konkreten Fahrzeugen unter Umständen frühzeitig, in manchen Fällen auch ad hoc, zu aggregieren, zu pseudonymisieren oder gar unmittelbar nach der Analyse wieder zu löschen.

Für Fälle, in denen KI-Entwicklung im Rahmen wissenschaftlicher Forschung oder für statistische Zwecke erfolgt, kann die Speicherung über die für den Primärzweck erforderliche Dauer hinaus verlängert werden; eine unbegrenzte Vorratsdatenspeicherung legitimiert gleichwohl auch diese Ausnahme in Art. 5 Abs. 1 lit. e 2. Halbsatz DSGVO nicht, sodass auch in solchen Fällen entsprechende Maßnahmen der Anonymisierung und Pseudonymisierung berücksichtigt werden müssen (*Roßnagel* 2019b, S. 162).

… für Nachweis- und Ermittlungsfälle?

Nicht nur zum Zwecke der Entwicklung wecken Daten aus künstlich-intelligenten Fahrzeugen Begehrlichkeiten. Wird KI in sicherheitsrelevanten Produkten wie Fahrzeugen verbaut, ergeben sich für Hersteller wie für Kunden Sicherheits- und Haftungsfragen, für Behörden möglicherweise Ermittlungsinteressen. Entscheiden autonome Fahrzeuge eigenständig und weder menschlich gesteuert noch durch Menschen permanent eingriffsfähig überwacht auf Basis maschinell erlernter Regeln über Lenk-, Beschleunigungs- und Bremsbewegungen, die für Insassen und anderen Verkehrsteilnehmer Leben oder Tod bedeuten können, stellt sich die Frage, wer für Handeln oder Unterlassen dieser Systeme und in der Folge für Schäden an Rechtsgütern verantwortlich ist. Rechtsfolgen, die bislang insbesondere den Fahrzeugführern auferlegt waren, müssen neu allokiert werden. Entscheidungen der Systeme sind überdies aufgrund der Opazität nicht immer nachvollziehbar. Diese macht Systeme überdies anfällig für unentdeckte

Manipulation. Die Neuverteilung der Verantwortung auf Mehrere und die damit verbundene Komplexitätssteigerung in Verbindung mit einer erschwerten Nachvollziehbarkeit kann sich nachteilig auf die Rechtsdurchsetzung durch den Geschädigten auswirken (*Steege*, NVZ 2021, 6 f.).

Die Regulierung der Fahrzeugautomatisierung fokussiert deshalb stark die Nachweisführung des Handelns von Mensch und Maschine sowie ihrer Interaktion. Es werden, wie etwa mit § 63a StVG, Speicher gesetzlich vorgeschrieben, welche die Übergabe der Steuerung zwischen Mensch und Fahrzeug dokumentieren (*Brockmeyer* 2018, S. 258). Ferner solche, die im Falle bestimmter Situationen, wie bei Unfällen, Daten zum System- und Fahrzeugverhalten aufzeichnen, wie etwa der sogenannte Event Data Recorder, der beispielsweise im neuen § 1g StVG vorgeschrieben ist (*Lüdemann/Knollmann* 2020, S. 403; *Vásquez* 2021, S. 154 f.). Überdies sollen Akteure wie z. B. Hersteller in der Vor- oder Nachmarktkontrolle mit konkreten Nachweispflichten wie etwa in Bezug auf die Fahrzeug- und IT-Sicherheit bedacht werden, denen sie effektiv nur mit der Erhebung und Speicherung von Daten nachkommen können.[2] Zuletzt werden Fahrzeughersteller auch aus Eigeninteresse Daten ihrer Produktbeobachtung speichern, um sich zum Zwecke der Nachweisführung im Falle von Ansprüchen, beispielsweise aus dem Produkthaftungsrecht, absichern zu können (*Steege* 2021, 6 ff.).

Mit den Vorgaben gehen vielfältige Anforderungen zur Speicherung von regemäßig personenbezogenen Daten einher. Sie unterscheiden sich in Bezug auf

- die Qualität der Anforderung (z. B. Pflicht zum Verbau oder Betrieb von Speichern, Pflicht zur Speicherung, Pflicht zur Nachweisführung, Nachweisinteressen, die zur Speicherung führen, etc.),
- die Qualität zugrundeliegender Vorschriften (z. B. internationale und nationale Zulassungsvorschriften, Vorschriften zur Nachmarktkontrolle, Strafvorschriften, zivilrechtliche Haftungsregelungen, untergesetzliches Technikrecht, etc.),
- den Adressaten der Regelung (z. B. Hersteller, Halter, Fahrer, Nutzer etc.),
- den Anlass der Datenerhebung und den Anlass der Speicherung (permanent, anlassbezogen bei Interaktion zwischen Mensch und Maschine, anlassbezogen bei externen Ereignissen wie Unfällen oder Cyberattacken),
- die Art und den Ort der Speicherung (in Fahrzeugsystemen, in externen Speichermedien, auf zentralen Backends oder in staatlichen Datenbanken, in Herstellersystemen etc.),

---

2 Vgl. die UNECE-Zulassungsrichtlinie für das IT-Sicherheitsmanagement in Fahrzeugen, *UNECE*, Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system vom 25.06.2020, ECE/TRANS/WP.29/2020/79.

- die Art der Persistierung und Dauer der Speicherung (z. B. nur temporär, mit Ringspeichern, über festgelegte Zeiträume, dauerhaft, etc.)
- und schließlich die Zugriffsberechtigten und Nutzungszwecke (z. B. staatliche Stellen für Ermittlungs- und Verfahrenszwecke, Hersteller für Produktbeobachtungs- und Dokumentationszwecke, Kunden und Nutzer für Nachweiszwecke, etc.).

Diesen Speicherlösungen ist gemein, dass, sofern personenbezogene Daten im Anwendungsbereich der Datenschutzgrundverordnung verarbeitet werden, die Vorgaben des Art. 5 DSGVO, insbesondere der Rechtmäßigkeit und Speicherbegrenzung zu beachten sind. Neben der Ermittlung der Adressaten von Speicheranforderungen und auch der Verantwortlichen für die Verarbeitung muss im Einzelfall geprüft werden, ob die Speicherung für die Erfüllung einer rechtlichen Verpflichtung im Sinne des Art. 6 Abs. 1 lit. c DSGVO, der der Verantwortliche unterliegt, erforderlich ist. Eine rechtliche Verpflichtung, die zur Verarbeitung ermächtigt, wird regelmäßig auch Näheres zur Verarbeitung und der Dauer der Speicherung bestimmen müssen. So verpflichtet der neue § 1g Abs. 1 StVG den Halter dazu, gesetzlich bestimmte Daten zu speichern, legt in seinem Absatz 2 aber gleichzeitig dem Fahrzeughersteller Pflichten auf, die Speicher im Sinne des Privacy by Design so zu gestalten, dass die Speicherung dem Halter vorgabegemäß möglich ist (*Vásquez* 2021, S. 154 f.)

Bei der Speicherung zur Nachweisführung, die demgegenüber beispielsweise zur Erfüllung einer gesetzlichen Pflicht nicht zwingend erforderlich wäre, wird eine Verarbeitung in der Regel nicht auf Basis des Art. 6 Abs. 1 lit. c DSGVO gestützt werden können. Soweit eine Speicherung im Interesse des Herstellers liegt oder aber aus eigenem Produktbeobachtungsinteresse des Herstellers erfolgt, wird sie allenfalls auf Basis überwiegender berechtigter Interessen legitimierbar sein. Die Umstände der Speicherung müssen dann im Sinne des Art. 5 Abs. 1 lit e. DSGVO hinsichtlich der Dauer entsprechend überprüft und begrenzt werden.

Transparenz trotz Opazität

Nach Art. 5 Abs. 1 lit. a DSGVO sind personenbezogene Daten in nachvollziehbarer Weise zu verarbeiten und die Verarbeitung der betroffenen Person gemäß Art. 12 Abs. 1 DSGVO in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu vermitteln. Transparenzfragen stellen sich zunächst in Bezug auf den Prozess des Anlernens Künstlicher Intelligenz, etwa bei der Erhebung von Videodaten. Hier steht der Verantwortliche zunächst einer Vielzahl möglicher betroffener Personen gegenüber. Diese sind möglicherweise aufzuklären über eine eventuell ebenso große Vielfalt potenzieller Verarbeitungsszenarien und einer Reihe potenzieller Datenempfänger.

Information „im Vorbeifahren“

Als besonders schwierig stellt sich dabei die angemessene Aufklärung betroffener Personen im Umfeld eines Fahrzeugs dar, das Trainingsdaten etwa durch Kameras oder weitere Sensoren erhebt. Einziger Kontaktpunkt des Verantwortlichen einer solchen Datenerhebung mit der betroffenen Person im Fahrzeugumfeld ist im Realverkehr häufig nur der Moment, an dem das Fahrzeug die betroffene Person passiert (oder bei stehenden Fahrzeugen umgekehrt) und entsprechende Daten erhoben werden.

In Bezug auf die Verarbeitung von Bild- und Videodaten sind die Herausforderungen dabei vergleichbar mit der Transparenz in Bezug auf die Videoüberwachung (*Europäischer Datenschutzausschuss* 2020b; *Konferenz der Datenschutzbeauftragten des Bundes und der Länder* 2018, S. 2), bei der Passanten in einem Moment, in dem sie nicht mit der Aufklärung über die Verarbeitung und gegebenenfalls auch nicht mit Verarbeitung selbst rechnen, über eine Videodatenverarbeitung informiert werden müssen. Es bleibt dabei ein kurzes Zeitfenster, in dem die nach Art. 12 ff. DSGVO erforderlichen Informationen bereitgestellt werden können, wobei weder auf die Präzision der Information an den Betroffenen einerseits noch auf die Verständlichkeit verzichtet werden kann. Bei mit der Erhebung von Daten fahrender Fahrzeuge zusammenhängenden Informationspflichten ist diese Herausforderung erheblich verschärft (*Konferenz der Datenschutzbeauftragten des Bundes und der Länder* 2020, S. 2). Für die Wahrnehmung der Information bleiben oftmals nur wenige Augenblicke. Selbst wenn beispielsweise Test- und Entwicklungsfahrzeuge – in Anlehnung an die Empfehlung zu Piktogrammen für die Videoüberwachung (*Europäischer Datenschutzausschuss* 2020b, Rn. 115) – über entsprechende auf allen Fahrzeugseiten angebrachte Kennzeichnungen verfügen, ist die Wahrscheinlichkeit einer Kenntnisnahme im öffentlichen Straßenverkehr davon abhängig, ob die betroffene Person das betreffende Fahrzeug bewusst wahrnimmt und die Informationen in diesem Moment verarbeiten kann.

Noch bedeutend schwieriger wird schließlich die Einhaltung des Transparenzprinzips sein, wenn die Datenerhebung nicht nur auf Test- und Entwicklungsfahrzeuge beschränkt ist, sondern – wie im Shadow Mode – auch mithilfe von Kundenfahrzeugen erfolgt. Eine gewisse Erleichterung könnte sich indes aus Art. 14 Abs. 5 lit. b DSGVO für Fälle ergeben, in denen Daten nicht bei der betroffenen Person erhoben werden, sondern beispielsweise bestehende KI-Trainingsdatensätze – insbesondere zu wissenschaftlichen Forschungszwecken und statischen Zwecken (*Roßnagel* 2019b, S. 169) – erneut oder zu anderen Zwecken verarbeitet werden und die Information der Betroffenen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde (*Niemann/Kevekordes* 2020, S. 181).

Undurchschaubare Intelligenz

Die Transparenzanforderung des Art. 5 Abs. 1 lit. a DSGVO ist nicht nur in Bezug auf die Information betroffener Personen beim Anlernen Künstlicher Intelligenz, sondern auch bei ihrem (späteren) Betrieb von Bedeutung. Dabei führt insbesondere die Anforderung der Verarbeitung „auf nachvollziehbare Weise“ zu Herausforderungen. Es gehört zu den Merkmalen Künstlicher Intelligenz, dass zwar Dateneingaben in oder Erhebungen durch Künstliche Intelligenz bekannt sind oder zurückverfolgt werden können und auch das Ergebnis der Verarbeitung, zumindest aus dem darauffolgenden Handeln des Systems, abgeleitet werden kann. Insbesondere bei der Verarbeitung durch multiple Ebenen in Neuronale Netzen (*Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder* 2019a, S. 5 f.) sind die eigentlichen Verarbeitungswege, die zu einer Entscheidung durch das System führen, häufig nicht nachvollziehbar; die KI stellt sich als eine Art „Black Box“ dar (*Craglia* et al., 2018, S. 14; *Hochrangige Expertengruppe für Künstliche Intelligenz* 2019, S. 6). Diese „Opazität“ (*Europäische Kommission* 2020a, S.14) Künstlicher Intelligenz erschwert zunächst die Umsetzung von Informations- und Auskunftspflichten des für die Verarbeitung Verantwortlichen (*Europäische Kommission*, 2018, S. 17).

Besondere Anforderungen wären an autonome Fahrzeuge zu stellen, deren Künstliche Intelligenz Entscheidungen trifft, denen die betroffene Person unterworfen wird. Vorstellbar wären die in der ethischen Diskussion dominierenden Dilemmaentscheidungen (*Ethikkommission automatisiertes und vernetztes Fahren* 2017, S. 17). Denkbar wäre ferner beispielsweise, dass autonome Fahrzeuge aufgrund der Entscheidung Künstlicher Intelligenz die zulässige Geschwindigkeit übertreten. Möglich sind auch Alltagsentscheidungen wie der Fall, dass das mit dem heimischen Kühlschrank gekoppelte Fahrzeug einen von ihm gewählten Supermarkt anfährt, um dort durch das System vorbestellte Ware abzuholen. Betroffene Personen haben nach Art. 22 Abs. 1 DSGVO das Recht, einer solchen Entscheidung nicht unterworfen zu werden, wenn diese ihr gegenüber rechtliche Wirkung hat oder sie in ähnlicher Weise erheblich beeinträchtigt, es sei denn, eine der Ausnahmen des Art. 22 Abs. 2 DSGVO greift. Zwar läge im Fall des Supermarkts möglicherweise ein im Sinne des Art. 22 Abs. 1 lit. a DSGVO zu erfüllender Vertrag für einen entsprechenden Online-Dienst, den der Nutzer abgeschlossen hat, zugrunde. Auch könnten entsprechende Rechtsvorschriften nach lit. b oder eine Einwilligung nach lit. c die Entscheidung ermöglichen. Jedenfalls aber müssten nach Art. 22 Abs. 3 DSGVO für Fälle des Art 22 Abs. 2 lit. a und c vom Verantwortlichen angemessene Maßnahmen zur Wahrung von Rechten, Freiheiten und berechtigten Interessen getroffen werden. Es müssten Möglichkeiten bereitstehen, dass eine Person seitens des Verantwortlichen in die Verarbeitung eingreift (*Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder* 2019a, S. 14) sowie dass die betroffene Person den eigenen Standpunkt darlegen und die Entscheidung

gegebenenfalls anfechten kann (*Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder* 2019c, S. 3). Ferner wären nach Art. 22 Abs. 4 DSGVO Entscheidungen auf Basis besonderer Kategorien betroffener Personen nochmals eingeschränkt.

Die Umsetzung künstlich-intelligenter Systeme in autonomen Fahrzeugen, die automatisierte Entscheidungen im Sinne des Art. 22 DSGVO treffen, ist vor diesem Hintergrund schon deshalb komplex, weil die erforderliche Transparenz nach Art. 13 Abs. 2 lit. f DSGVO und Art. 14 Abs. 2 lit. g DSGVO über die involvierte Logik nicht immer herstellbar sein wird.

Alles für gute Zwecke? – KI und Zweckbindung

Verwertungsinteressen und -risiken

Insbesondere die Fahrzeugentwicklung ist, speziell zum Anlernen Künstlicher Intelligenz für Fahrzeuge, auf große Umfänge von Fahrzeug- und Umfelddaten angewiesen. Dass Daten dabei nicht für jeden Entwicklungszweck erneut erhoben werden, sondern auf zentralen Datenseen für die mögliche Mehrfachbenutzung – auch durch mehrere Parteien – vorgehalten werden, folgt ökonomisch-technischen Erwägungen wie etwa Skaleneffekten (*Craglia* et al., 2018, S. 103 f.). Solche Effekte lassen sich auch durch die Verbindung verschiedener Datenquellen sowie Verknüpfung von Daten, etwa im Rahmen von Big-Data-Analysen, herbeiführen. Diesen Vorgängen ist gemein, dass Daten aus ihrem ursprünglichen Verwendungszusammenhang herausgelöst und in einen neuen Nutzungskontext überführt, also zu neuen Zwecken weiterverarbeitet werden. Das Prinzip der Zweckbindung steht einer datengetriebenen Technologie wie der Künstlichen Intelligenz damit zunächst einmal ähnlich diametral gegenüber wie das der Datenminimierung (*Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder* 2019c, S. 3).

Durch die Anbindung von Online-Fahrzeugen an zentrale Hersteller-Backends und das Angebot von Online-Diensten werden in unzähligen Fahrzeugen generierte Fahrzeug- und Umfelddaten aus der Realnutzung der Fahrzeuge an diese Hersteller-Backends übertragen. Sie werden dort gegebenenfalls für den Primärzweck der Erbringung eines (vertraglich zugesicherten) Dienstes verarbeitet, sind aber gleichzeitig mit Blick auf eine Folgenutzung als Trainingsdaten für künstlich-intelligente Systeme autonomer Fahrzeuge höchst attraktiv. Als solche liegt auch der Reiz der ökonomischen Verwertung solcher Trainingsdaten als Geschäftsmodell etwa von Herstellern, zum Beispiel gegenüber weiteren KI-Entwicklern, auf der Hand (*Hornung* 2019, S. 109 ff.).

Schon aufgrund der Vielfältigkeit der Daten, der zahlreichen Schnittstellen und Verknüpfungsmöglichkeiten in „Fahrzeug-Backends“ werden Risiken mit Blick

auf eine Zweckänderung von Daten deutlich: Wo künstlich-intelligente Fahrzeugsysteme Fahrzeug- und Umfelddaten, Standort-, Bewegungs- und Zeitdaten, akustische und optische Daten, Daten aus dem Fahrzeuginnenraum, darunter etwa auch zu Emotionen des Fahrers aufgrund einer Stimmanalyse, mit Daten aus verknüpften Geräten wie Kontaktdaten aus Smartphones, Daten anderer Verkehrsteilnehmer und -systemen und weiteren Daten aus Systemen des Unternehmens wie etwa aus Kundendatensätzen der Hersteller oder – in der Rolle des fahrzeugnutzenden Mitarbeiters – der Personalakte zusammenführen können, bedient dies allgemeine Befürchtungen vor einer Totalüberwachung (*Ethik-Kommission automatisiertes und vernetztes Fahren* 2017, S. 12 Ziff. 13).

Zweckbindungs- und -kompatibilitätsgebot

Art. 5 Abs. 1 lit. b DSGVO gebietet die Festlegung auf einen Verarbeitungszweck schon bei der Datenerhebung. Die Weiterverarbeitung muss sodann nach einer mit diesem Erhebungszweck zu vereinbarenden Weise erfolgen. Jede Zweckänderung muss entsprechend einer Prüfung auf die Vereinbarkeit der Zwecke unterzogen werden. Beruht die beabsichtige Sekundärverarbeitung nicht auf der Einwilligung der betroffenen Person oder einer entsprechenden Rechtsvorschrift, ist für die Prüfung dieser „Zweckkompatibilität“ unter anderem die Verbindung zwischen dem Primär- und dem Sekundärzweck zu untersuchen. Dazu sind auch der Kontext der Datenerhebung und die „vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen“ (Ewg. 50 Satz 6 DSGVO) zu erforschen.

Werden Trainingsdaten gezielt für das Anlernen künstlich-intelligenter Systeme erhoben, können sich Erhebungs- und Weiterverarbeitungszweck zwar häufig decken, problematisch ist dabei aber die Festlegung hinreichend bestimmter Zwecke (*Artikel 29 Datenschutzgruppe* 2013, S. 15). Je nach Erhebungsszenario werden Daten beispielsweise im Rahmen von Entwicklungsfahrten erhoben und sollen dann für eine Vielzahl möglicher Entwicklungsprojekte im Rahmen des autonomen Fahrens verwendet werden. Verantwortliche stehen dabei vor der praktischen Herausforderung, Erhebungszwecke möglichst eindeutig zu bestimmen, ohne die Bandbreite der Nutzungsmöglichkeiten dabei zu sehr einzuschränken (*Schantz* 2020, Rn. 15). Gleichwohl: Wird im Falle einer solchen Entwicklungstätigkeit der Zweck der Erhebung von Trainingsdaten eng bestimmt, ist damit die Weiternutzung nicht automatisch verwehrt. Die Kompatibilitätsprüfung im Sinne des Art. 6 Abs. 4 DSGVO für die Weiternutzung zu anderen (vergleichbaren und in einer engen Verbindung stehenden) Entwicklungszwecken des Verantwortlichen wird in solchen Fällen nicht selten positiv ausfallen.

Jedoch könnte das Angebot solcher Trainingsdaten an Dritte im Rahmen einer ökonomischen Verwertung anders zu bewerten sein (*Artikel 29 Datenschutzgruppe*

2013, S. 129). Werden entsprechende Daten beispielsweise im Zusammenhang mit einem Beschäftigungsverhältnis zum Beispiel aus Dienstfahrzeugen erhoben, wird die betroffene Person regelmäßig erwarten dürfen, dass in Bezug zu ihr verarbeitete Daten nicht an Dritte verkauft werden (*Frenzel* 2021, Rn. 49, der zum Beispiel das Bestehen eines langjährigen Vertrauensverhältnis als Ausschlussgrund einer solchen Weitergabe nennt).

Entstehen personenbezogene Daten aus der Nutzung von Diensten durch (Fahrzeug-)Nutzer, ist der Primärzweck regelmäßig nicht die Generierung von Trainingsdaten, sondern die Bereitstellung und der Betrieb des Dienstes. Eine Weiternutzung dieser Daten zum Zweck des KI-Trainings stellt insofern eine Zweckänderung dar. Ob der neue Zweck mit dem ursprünglichen Erhebungszweck – der Bereitstellung und dem Betrieb von Diensten – vereinbar ist, ist ebenfalls nach Art. 6 Abs. 4 DSGVO zu bewerten. Neben der Verbindung zwischen den Zwecken und dem Verhältnis zwischen betroffener Person und dem Verantwortlichen sind auch die Art der personenbezogenen Daten, mögliche Folgen der Weiterverarbeitung und das Vorhandensein geeigneter Garantien, darunter die Verschlüsselung und Pseudonymisierung zu berücksichtigen.

Datenschutzfreundliche Maßnahmen wie die frühzeitige Aggregation von Daten, idealerweise noch im Fahrzeug selbst, das Entfernen von Identifikationsmerkmalen wie der Fahrzeugidentifikationsnummer aus dem Rohdatensatz, ebenso wie der Ausschluss von Standort- und Bewegungsdaten aus der Sekundärnutzung können hier beispielsweise positiv in die Bewertung der Zweckkompatibilität einfließen (*Artikel 29 Datenschutzgruppe* 2013 S. 27, unter anderem auch m. V. a. den Einsatz von „privacy enhancing technologies“). Mit Blick auf die Verbindung der Zwecke, das Verhältnis zum Verantwortlichen und auch möglichen Folgen der Verarbeitung könnte auch eine Rolle spielen, ob Nutzer durch die Weiterverarbeitung zumindest mittelbar profitieren. Beispielsweise, indem sie auf Schwarminformationen zur Verkehrs- und Straßenlage, die auch aus Daten im Rahmen ihrer eigenen Dienstnutzung generiert wurden, selbst zugreifen können (*Artikel 29 Datenschutzgruppe* 2013, S. 23 und 25 für weitere Beispiele, wie „positive“ Auswirkungen auf die betroffene Person als Argument für die Vereinbarkeit einfließen können, vgl. dort auch Annex 4 die Beispiel 6 und 11). Auch werden Nutzer, die von Herstellern als Testnutzer angeworben werden und hierfür Dienste oder Testfahrzeuge frühzeitig nutzen dürfen, wohl regelmäßig vernünftigerweise erwarten müssen, dass sie aufgrund der spezifischen Beziehung zum Hersteller mit der Nutzung auch zur Trainingsdatenbasis des Herstellers beitragen (zur „implizierten Zweckänderung“ im Verhältnis zwischen betroffener Person und Verantwortlichen, *Artikel 29 Datenschutzgruppe* 2013, S. 23).

Die ökonomische Verwertung gegenüber Dritten könnte demgegenüber nicht hinreichend mit dem Erhebungszweck vereinbar sein: Zum einen da sich durch die Bereitstellung an Dritte Risiken der Verarbeitung mit möglichen negativen Folgen auf die betroffene Person ergeben können. Zum anderen ist fraglich, ob betroffene

Personen, die ein Fahrzeug oder einen Dienst erworben haben, damit rechnen müssen, dass die hierbei erhobenen Daten an Dritte „verkauft“ werden (u. a. auch zur Streubreite der Datenbereitstellung an Dritte, *Artikel 29 Datenschutzgruppe* 2013, S. 26).

Zuletzt könnte auch eine Verknüpfung von Daten aus der Fahrzeugnutzung mit weiteren Datenquellen, beispielsweise Kundendatenbanken der Hersteller, regelmäßig nicht mit dem Erhebungszweck vereinbar sein: Die Erhebung derartiger Daten erfolgt meist in der Kundenwahrnehmung in jeweils völlig unterschiedlichen Kontexten – beispielsweise dem Fahrzeug- oder Dienstekauf bei einem Händler oder online einerseits und dem Produktbetrieb während der Fahrt andererseits. Es ist wohl kaum anzunehmen, dass eine derartige Verkettung dieser beiden Welten und ihrer Daten in der vernünftigen Erwartung des Kunden liegt. Entsprechend sieht beispielsweise das „Standarddatenschutzmodell“ das Gewährleistungsziel der „Nichtverkettung“ berührt, wenn „zusammenzuführende Daten für unterschiedliche Zwecke erhoben wurden (B.1.2 Zweckbindung)“ (*AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder* 2020, S. 27, Ziele C.1.5 i. V. m. B 1.2; vgl. auch *Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder* 2018b S. 18).

Forschungsprivilegien

Art. 5 Abs. 1 lit. b DSGVO sieht schließlich eine Erleichterung der Anforderungen an die Zweckänderung für die Weiterverarbeitung unter anderem für wissenschaftliche Forschungszwecke oder für statistische Zwecke vor. Eine zweckändernde Weiterverarbeitung zu diesen Zwecken gilt gemäß Art. 89 Abs. 1 DSGVO nicht als unvereinbar mit den ursprünglichen Zwecken. Soweit im Rahmen der Verarbeitung personenbezogener Daten beim Anlernen (und auch beim Betrieb) künstlich-intelligenter Systeme für autonome Fahrzeuge Forschungszwecke im Sinne des Art. 89 DSGVO vorliegen, dürfte der Verantwortliche insofern regelmäßig auch die Vereinbarkeit einer zweckändernden Verarbeitung annehmen (*Roßnagel* 2019, S. 162). Allerdings unterliegt eine solche „privilegierte“ Verarbeitung den Anforderungen des Art. 89 Abs. 1 DSGVO – konkret „geeigneten Garantien für die Rechte und Freiheiten“ im Sinne „technischer und organisatorischer Maßnahmen“. Die Vereinbarkeit dürfte im Ergebnis grundsätzlich (nur) dann ohne Weiteres anzunehmen sein, wenn die Daten nachweislich anonymisiert oder hinreichend pseudonymisiert sind (Art. 89 Abs. 1 Satz 3 und 4; Ewg. 156 Satz 3 DSGVO; siehe auch *Roßnagel* 2019, 162).

Datenrichtigkeit als Schutz vor Bias-Risiken

Die Datenrichtigkeit im Sinne des Art. 5 Abs. 1 lit. d DSGVO nimmt im Zusammenhang mit Künstlicher Intelligenz eine besondere Rolle ein. Wenn

Entscheidungsprozesse aufgrund der Opazität der KI schwer nachvollziehbar sind, dient die Gewährleistung der Richtigkeit der verarbeiteten Informationen als eine Art „vorgelagerter Schutz“. Bereits die für das Anlernen der KI zugrundeliegenden Trainingsdaten können die interne Regelbildung maßgeblich beeinflussen. Auch die im KI-Betrieb eingegebenen oder erfassten Daten sind maßgeblich für mögliche, wie dargelegt nicht immer nachvollziehbare Entscheidungen der Künstlichen Intelligenz. Sind derartige Daten unrichtig, können sich gefährliche, potenziell diskriminierende „Bias“-Effekte einstellen, (*Craglia* et al. 2018, S. 13; *Europäische Kommission* 2019, S. 2; *Europäische Kommission* 2020c, S. 11 f.; *Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder* 2019c, S. 2), die im Betrieb durch ein selbstständiges unüberwachtes Weiterlernen noch verstärkt werden können (*Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder* 2019a, S. 4). Vorstellbare Risiken und konkret auch Diskriminierungen im Rahmen autonomer Fahrzeuge sind dabei vielfältig. So könnten Fahrzeuge beispielsweise – aufgrund falsch angeeigneter Regeln – fehlerhafte Annahmen über Fahrsicherheitsbedürfnisse von Insassen treffen. Sie könnten Fahrtrouten auf Basis solcher „Biases“ auswählen, die für den Einzelnen nachteilhaft sind. Vorstellbar wären aber auch insbesondere Diskriminierungen im Zusammenhang mit dem Angebot von Zusatzdiensten. Falsche oder unvollständige Informationen könnten beispielsweise bei der Auswahl oder der Preisgestaltung solcher Zusatzdienste zu ungerechtfertigten Differenzierungen führen und bestimmte Personen oder Personengruppen benachteiligen.

Verantwortlichkeit und Rechenschaftspflicht

Sowohl bei der Verarbeitung von Trainingsdaten als auch beim Betrieb Künstlicher Intelligenz in autonomen Fahrzeugen ist es nicht unüblich, dass unterschiedliche Verantwortliche – allein oder gemeinsam mit anderen – über die Zwecke und Mittel der jeweiligen Verarbeitung entscheiden (*Kroschwald* 2015, S. 91 f.). Der Betrieb eines autonomen Fahrzeugs ist zukünftig vielleicht regelmäßig Teil einer digital gesteuerten Mobilitätskette mit zahlreichen Akteuren (*Vásquez/Kroschwald* 2020, S. 217 f.; *Ethikkommission automatisiertes und vernetztes Fahren* 2017, S. 27 f.). Die Zuordnung datenschutzrechtlicher Verantwortung wird dadurch komplexer.

Darüber hinaus werden möglicherweise wesentliche Weichen für die spätere Verarbeitung bereits im Entwicklungsprozess oder entlang der Wertschöpfungskette gestellt – etwa beim Anlernen Künstlicher Intelligenz. Die hierbei handelnden Akteure sind aber nicht zwingend stets als Verantwortliche im Sinne des Datenschutzrechts zu qualifizieren, wenn es um die Verarbeitung im (späteren) Produktbetrieb geht. Insbesondere Fahrzeughersteller oder Entwickler Künstlicher Intelligenz, die in ihrer Rolle und mit ihrem technischen Verständnis den Produktdatenschutz maßgeblich gestalten können, sind an wesentliche

Anforderungen, etwa des Art. 25 DSGVO nur gebunden, sofern sie Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO sind (*Vásquez/Kroschwald*, 2020, S. 219; kritisch auch *Richter* 2012, S. 576; *Bieker/Hansen* 2017, S. 165; *Roßnagel/Nebel/Richter* 2015, S. 455; *Jandt* 2017, S. 562; *Baumgartner/Gausling* 2017, S. 308). Entlang der Lieferkette des künstlich-intelligenten Mobilitätsökosystems werden Hersteller, anders als im Produktkonformitäts- und -sicherheitsrecht (*Europäische Kommission* 2020b, S. 8; *Europäische Kommission 2020c*, S. 22; *Ethikkommission automatisiertes und vernetztes Fahren* 2017, S. 27 f.), durch das Datenschutzrecht selbst insofern nicht verpflichtet. Gemäß Ewg. 78 DSGVO sollen Hersteller, sofern sie nicht selbst Verantwortliche sind, nur zum Datenschutz durch Technikgestaltung und zu datenschutzfreundlichen Voreinstellungen „ermutigt" werden. Solches führt insbesondere in asymmetrischen Machtverhältnissen zwischen Parteien zu (rechtsökonomisch) ungünstigen Anreizbedingungen (*Vásquez/Kroschwald* 2020, S. 218 – 220). Für das Vertrauen in den Datenschutz künstlich-intelligenter, autonomer Fahrzeugsysteme sind diese Asymmetrien hinderlich.

Positiv zu bewerten ist insofern der Regelungsansatz des im Rahmen des „Gesetzes zum autonomen Fahren" neu in das Straßenverkehrsgesetz eingefügten § 1g StVG. Dieser verpflichtet Halter – das können neben privaten Fahrzeughaltern freilich auch Anbieter von (teil-)autonomen Carsharing-Fahrzeugen und Fahrzeugvermieter ebenso sein – in Absatz 1, bestimmte Daten beim Betrieb eines Kraftfahrzeugs (Abs. 1 Satz 1) anlassbasiert (Abs. 2) zu speichern und diese erforderlichenfalls an Behörden zu übermitteln (Abs. 1 Satz 2). Gleichzeitig verpflichtet § 1g Abs. 3 StVG die „Hersteller eines Kraftfahrzeugs" dazu, das „Fahrzeug so auszustatten, dass die Speicherung der Daten gemäß Absatz 1 und 2 dem Halter tatsächlich möglich ist." Der Hersteller wird ferner verpflichtet, „den Halter präzise, klar und in leichter Sprache über die Einstellungsmöglichkeiten zur Privatsphäre und zur Verarbeitung der Daten, die beim Betrieb des Kraftfahrzeugs in der autonomen Fahrfunktion verarbeitet werden, zu informieren" und sicherzustellen, dass die diesbezügliche Software des Kraftfahrzeugs „Wahlmöglichkeiten zur Art und Weise der Speicherung und der Übermittlung der in der autonomen Fahrfunktion verarbeiteten Daten [vorsieht] und dem Halter entsprechende Einstellungen" ermöglicht. Der mit § 1g StVG verbundene Ansatz, explizit auch dem Hersteller vorgenannte Pflichten im Sinne eines „Privacy by Design" in Anlehnung an Art. 25 DSGVO aufzuerlegen, gleichzeitig aber ihm nicht die Pflicht (und damit auch nicht ohne Weiteres das Recht) zur Erhebung und Speicherung dieser Daten zuzuordnen, sondern dieses beim Halter als Verantwortlichen zu belassen, ist innovativ (*Vásquez* 2021, S. 149 ff.). Die Regelung vermeidet eine weitere Datenhoheit bei Herstellern. Sie verpflichtet diese Hersteller aber angesichts ihres technologischen Wissens- und Gestaltungsvorsprungs, dem Halter die Mittel und Wege an die Hand zu geben, seiner straßenverkehrs- und auch datenschutzrechtlichen Verantwortung (ggf. auch

Dritten Fahrzeugnutzern und -insassen gegenüber) nachkommen zu können (*Vásquez* 2021, S. 154 f.).

Gestaltungsansätze und Ausblick

Aufgabe der verbraucher- und nutzerrechtsorientierten Technikgestaltung ist es, positive Gestaltungsansätze für künstlich-intelligente Fahrzeugsysteme zu finden. Die in diesem Beitrag nur angerissenen rechtlichen Rahmenbedingungen müssen in technische und geschäftsmodellbezogene, produkt- und prozessorientierte Umsetzungswege überführt und möglichst schon im Design mitgedacht werden. Dabei sind – so auch im Sinne der Privacy by Design – widerstreitende Interessen und auch Grundrechte zu berücksichtigen und zum Ausgleich zu bringen (*Roßnagel* 2019, S. 17 ff.). Datenschutzfreundliche Gestaltung soll damit zu einem Mehr an Rechtssicherheit führen, aber auch vertrauensfördernd und attraktivitätssteigernd wirken. Mit einzelnen Gestaltungsansätzen befasst sich ein Beitrag an anderer Stelle vertiefend (*Kroschwald* 2021, S. 526 ff.); sie sollen hier nur überblickartig genannt werden.

Die Gestaltung Künstlicher Intelligenz sollte dabei vom in der Europäischen (*Europäische Kommission* 2018, S. 14) und nationalen KI-Strategie (*Bundesregierung* 2020, S. 3) formulierten Ansatz der „human-centric AI“ ausgehen. Sie stellt „menschliche Werte […] in den Mittelpunkt der Entwicklung, Einführung, Nutzung und Überwachung der KI-Systeme“, wodurch „die Achtung der Grundrechte gewährleistet werden“ soll (*Hochrangige Expertengruppe für Künstliche Intelligenz* 2020, S. 48 Rn. 153). Aufsichts- und Einwirkungsmöglichkeiten wie die Prinzipien des „Human Agency and Oversight“, des „Human in the Loop“ sowie des „Human in Command“ eignen sich als Gestaltungskriterien zur Umsetzung der datenschutzrechtlichen Selbstbestimmung von Verbraucher:innen und Nutzer:innen in der Interaktion mit Künstlicher Intelligenz (*Hochrangige Expertengruppe für Künstliche Intelligenz* 2020, S. 48 Rn. 65; *Kroschwald* 2021, S. 527).

Ein professionelles Data Mapping und Data Management erlaubt die Planung von Datenbedarfen und deren Nutzung unter möglichst geringen Einwirkungen auf Rechte und Interessen von betroffenen Personen. Daten können so ein „Datenleben lang“ organisiert, über die Datenwege hinweg verwaltet, wo möglich pseudonymisiert oder anonymisiert, im Hinblick auf Zugriffs- und Verarbeitungsrechte verwaltet und, wenn erforderlich, der Löschung zugeführt werden. Moderne Anonymisierungsverfahren ermöglichen die Nutzung selbst von Videodaten, auf denen möglicherweise erfasste Personen unkenntlich gemacht werden, ohne den Nutzen des Materials für KI-Trainingszwecke zu schmälern (*Ethikkommission automatisiertes und vernetztes Fahren* 2017, S. 25; *Kroschwald* 2021, S. 527).

Herausfordernd bleibt die Herstellung von Transparenz im Nutzungskontext. Sie darf den Betroffenen nicht überlasten, in Gefahrensituationen nicht ablenken und muss Basis für selbstbestimmte Entscheidungen sein. Wo KI-Entscheidungen nicht vorherbestimmbar oder beschreibbar sind, können Beschreibungen über Technologien und dahinterstehende Geschäftsmodelle dennoch Transparenz für betroffene Personen herstellen (*Kroschwald* 2021, S. 527 f.).

Mögliche datenschutzfreundliche Innovationsanreize könnten sich auch aus den neuen, ab 2022 geltenden verbraucherschützenden Vorschriften im zivilrechtlichen Schuldrecht zu digitalen Produkten ergeben. Indem Verbraucher – selbst bei scheinbar kostenfreien Produkten und Diensten, die sie aber förmlich mit ihren personenbezogenen Daten „bezahlen", Gewährleistungsrechte möglicherweise auch für die Nichteinhaltung von „Privacy by Design"-Anforderungen geltend machen können, könnte ein datenschutzfreundlicher Selbststeuerungsmechanismus bei Unternehmern in Gang gesetzt werden (*Kroschwald/Polenz* 2021, § 6).

Die systematische Sicherstellung der Datensicherheit und des Privacy by Design – auch als Managementaufgabe – wird von Gesetzgebern erst langsam eingefordert (*Vásquez* 2021, S. 155 ff.). Aufseiten der Regulierung sind risikobasierte Ansätze, wie sie letztlich bereits durch die DSGVO gefordert werden, wie etwa auch die Pflicht zur Durchführung von Folgenabschätzungen sinnvoll, wenn sie Innovation nicht in Bürokratie ersticken. Vielversprechend scheint hierbei der Ansatz von „Regulatory Sandbox-Enviroments" (*Craglia* et al. 2018, S. 64) oder „Reallaboren" (*Bundesregierung* 2020, S. 3) zu sein. Es handelt sich dabei um geschützte Experimentierräume für den Einsatz Künstlicher Intelligenz. In solchen kann – auch für den Sektor Mobilität und Verkehr – laborähnlich das Zusammenwirken von Recht und Technik im kleinen Raum erprobt werden.

Literatur

AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2020), Das Standard-Datenschutzmodell, Version 2.0b vom 01.04.2020, Berlin 2020.

Artikel 29 Datenschutzgruppe (2013), Opinion 03/2013 on purpose limitation, WP 203, Brüssel 2013.

Balzer, T./Nugel, M. (2014), Minikameras im Straßenverkehr – Datenschutzrechtliche Grenzen und zivilprozessuale Verwertbarkeit der Videoaufnahmen, NJW 2014, S. 1622-1627.

Baumgartner, U./Gausling, T. (2017), Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen – Was Unternehmen jetzt nach der DS-GVO beachten müssen, ZD 2017, S. 308-313.

Bieker, F./Hansen, M. (2017), Datenschutz „by Design" und „by Default" nach der neuen europäischen Datenschutz-Grundverordnung, RDV 2017, S. 165-170.

Brockmeyer, H. (2018), Treuhänder für Mobilitätsdaten – Zukunftsmodell für hoch- und vollautomatisierte Fahrzeuge? Erwägungen zur ausstehenden Regulierung des Speicherorts für die Daten nach § 63a Abs. 1 StVG, ZD 2018, S. 258-263.

Bundesregierung 2020, Strategie Künstliche Intelligenz der Bundesregierung, Fortschreibung 2020, Stand: Dezember 2020, Berlin 2020.

Consultative Committee of the Convention 108, Guidelines on Facial Recognition, Brüssel 2021

Craglia, M. et al (2018): Artificial Intelligence – A European Perspective, Joint Research Centre der EU-Kommission, Luxemburg 2018.
Ethikkommission automatisiertes und vernetztes Fahren (2017), Bericht im Auftrag der Bundesregierung, Juni 2017, Berlin 2017
Europäischer Datenschutzausschuss (2020a), Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications vom 28.01.2020, Version 1.0, Brüssel 2020.
Europäischer Datenschutzausschuss (2020b), Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Version 2.0 vom 29.01.2020, Brüssel 2020.
Europäische Kommission (2018), Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Künstliche Intelligenz für Europa, COM (2018) 237, Brüssel 2018.
Europäische Kommission (2018), Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Künstliche Intelligenz für Europa, COM (2018) 237
Europäische Kommission (2019), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Building Trust in Human-Centric Artificial Intelligence, COM (2019) 168, Brüssel 2019
Europäische Kommission (2020a): Europäische Kommission, White Paper on Artificial Intelligence – A European approach to Excellence and Trust, COM (2020) 65, Brüssel 2020.
Europäische Kommission (2020b), Bericht der Kommission an das Europäische Parlament, den Rat und den Europäischen Wirtschafts- und Sozialausschuss, Bericht über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung, COM (2020) 64, Brüssel 2020.
Europäische Kommission (2020c), White Paper on Artificial Intelligence – A European approach to Excellence and Trust, COM (2020) 65, Brüssel 2020.
Färber, B. (2015), Kommunikationsprobleme zwischen autonomen Fahrzeugen und menschlichen Fahrern?, in: Maurer/Gerdes/Lenz/Winner (Hrsg.), Autonomes Fahren – Technische, rechtliche und gesellschaftliche Aspekte, Wiesbaden 2015, S. 127-146..
Frenzel, S. (2021), Kriterien der Prüfung der Vereinbarkeit, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, Art. 6 Rn. 49, 3. Auflage, München 2021.
Hochrangige Expertengruppe für Künstliche Intelligenz (2019), Eine Definition der KI: Wichtigste Fähigkeiten und Wissenschaftsgebiete, Brüssel 2019
Hochrangige Expertengruppe für Künstliche Intelligenz (2020), Hochrangige Expertengruppe für Künstliche Intelligenz, Ethik-Leitlinien für eine vertrauenswürdige KI, Brüssel 2020.
CNIL (2017), Compliance Package Connected Vehicles and Personal Data, Scenario No. 2, Paris 2017.
Hornung, G. (2019), Ökonomische Verwertung und informationelle Selbstbestimmung in: Roßnagel/Hornung (Hrsg.), Grundrechtsschutz im Smart Car, Wiesbaden 2019, S. 109-126.
Jandt, S. (2017), Datenschutz durch Technik in der DS-GVO, Präventive und repressive Vorgaben zur Gewährleistung der Sicherheit der Verarbeitung, DuD 2017, S. 562-566.
Krämer, N.. et al. (2019), KI-basierte Sprachassistenten im Alltag – Forschungsbedarf aus informatischer, psychologischer, ethischer und rechtlicher Sicht, Duisburg, 2019.
Knote, R. et al. (20220), Rechtsverträgliche und qualitätszentrierte Gestaltung für „KI made in Germany“ – Ein interdisziplinärer Ansatz am Beispiel smarter persönlicher Assistenten, Informatik Spektrum 2020, 118-128.
Krauß, C. et.al, (2017), Anforderungsanalyse für Selbstdatenschutz im vernetzten Fahrzeug, Darmstadt 2017, https://sedafa-projekt.de/media/D1_final.pdf.

Krauß, C. (2019), Selbstdatenschutz im vernetzten Fahrzeug und dessen technische Umsetzung, in: Roßnagel/Hornung (Hrsg.), Grundrechtsschutz im Smart Car, Wiesbaden 2019, S. 227-244.
Kroschwald, Informationelle Selbstbestimmung auch auf der Straße, in: Schartner/Lemke-Rust/Ullmann (Hrsg.), DACH Security 2015 – Bestandsaufnahme, Konzepte, Anwendungen, Perspektiven, Frechen 2015, S. 86-97.
Kroschwald, S. (2021), Künstliche Intelligenz im autonomen Auto, DuD 2021, S. 522-528.
Kroschwald, S./Polenz, S. (2021), § 6 Digitale Produkte und Datenschutz, in: Brönneke/Föhlisch/Tonner (Hrsg.), Das neue Schuldrecht – Digitale Produkte, Kaufrecht, Vertragsrecht, § 6, Baden-Baden 2021.
Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2018), Kurzpapier Nr. 15 – Videoüberwachung nach der Datenschutz-Grundverordnung vom 17.12.2018, Berlin 2018.
Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (2018b), Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, Stand März 2018, Berlin 2018.
Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (2019a), Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen 2019, Berlin 2019.
Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) (2019b), Positionspapier zur Unzulässigkeit von Videoüberwachung aus Fahrzeugen (DashCams) vom 28.01.2019, Berlin 2019.
Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, (2019c), Entschließung am 03.04.2019: Hambacher Erklärung zur Künstlichen Intelligenz, Berlin 2019.
Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (2018), 24. Datenschutz- und Informationsfreiheitsbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen 2018, Düsseldorf 2018.
Lüdemann, V./Knollmann, D. (2020), Überwachung von Fahrzeug und Fahrer – Die neuen EU-Vorgaben für Unfalldatenspeicher und Fahrerüberwachungssysteme, ZD 2020, S. 403-409.
Lutz, L. (2020), Datenschutzrechtliche Herausforderungen auf dem Weg zum automatisierten Fahren – Verarbeitung von Daten aus dem öffentlichen Verkehrsraum zur Algorithmenentwicklung, ZD 2020, S. 450-454.
Niemann, F./Kevekordes, J. (2020), Machine Learning und Datenschutz, Teil 1, CR 2020, S. 17-25.
Roßnagel, A. (1993), Rechtswissenschaftliche Technikfolgenforschung: Umrisse einer Forschungsdisziplin, Baden-Baden 1993.
Roßnagel, A./Nebel, M./Richter, P. (2015), Was bleibt vom Europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO, ZD 2015, S. 455-460.
Roßnagel, A. (2019a), Grundrechtsverwirklichung im vernetzten und automatisierten Straßenverkehr, in: Roßnagel/Hornung (Hrsg.), Grundrechtsschutz im Smart Car, Wiesbaden 2019, S. 17-42.
Roßnagel, A. (2019b), Datenschutz in der Forschung – Die neuen Datenschutzregelungen in der Forschungspraxis von Hochschulen, ZD 2019, S. 157-164.
Steege, H. (2021), Auswirkungen von künstlicher Intelligenz auf die Produzentenhaftung in Verkehr und Mobilität – Zum Thema des Plenarvortrags auf dem 59. Deutschen Verkehrsgerichtstag NVZ 2021, 6-13.
Schantz, P. (2020), Bedeutung der Grundsätze, in: Wolff/Brink (Hrsg.), Beck OK Datenschutzrecht, Art. 5 DSGVO Rn. 2, München 2020.
Tesla (2019), Introducing Software Version 9.0, Blogbeitrag vom 05.08.2018, https://www.tesla.com/de_DE/blog/introducing-software-version-9, abgerufen am 30.01.2021.

Vásquez, S./Kroschwald, S. (2020), Produktdatenschutz: Verantwortung zwischen Herstellern und Anbietern – Data-driven vehicles: Privacy by Design aus dem Blickwinkel der Principal-Agent-Theorie, MMR 20200, 217-221.

Vásquez, S. (2021), Privacy by Design: eine gemeinsame Herausforderung von IT, Ingenieuren, und Managern zur effektiven Umsetzung des Datenschutzrechts – ein Anwendungsfall am Beispiel des autonomen Fahrzeugs, in: Taeger (Hrsg.), Im Fokus der Rechtsentwicklung - die Digitalisierung der Welt, Tagungsband Herbstakademie 2021, Oldenburg 2021, S.149-159.

VDA (2015), Automatisierung von Fahrerassistenzsystemen zum automatisierten Fahren, Berlin 2015.

Wachenfeld, W. / Winner, W. (2015): Lernen autonome Fahrzeuge?, in: Maurer / Gerdes / Lenz / Winner (Hrsg.), Autonomes Fahren – Technische, rechtliche und gesellschaftliche Aspekte, Wiesbaden 2015, S. 465-488.

Wolff, H. (2020), Syst. A Prinzipien des Datenschutzrechts Rn. 48, in: Wolff/Brink (Hrsg.), Beck OK Datenschutzrecht, München 2020.