Rechtsgutachten KoTAM

Dr. Dr. Hans Steege / Prof. Dr. Daniela Winkler

Inhalt

A. Frage 1: Beurteilung der Aktivitäten zum Thema Daten, Datenschutz und -sicherheit in ausgewählten Projekten bzw. Testfeldern aus rechtlicher Perspektive

I. Einleitung

Im Rahmen der ersten Frage werden Aktivitäten zum Thema Daten, Datenschutz und Datensicherheit in ausgewählten Projekten bzw. Testfeldern aus rechtlicher Perspektive untersucht. Zu diesem Zweck wird die Datenauswertung des Auftraggebers zu Grunde gelegt. Im Mittelpunkt steht die Frage, inwieweit die dort genannten Tätigkeiten datenschutzrechtlich relevant sind.

Die weitere Frage, ob die Maßnahmen Vorgaben des Datenschutzes ausreichend beachten, kann im Rahmen dieses Gutachtens aufgrund der vorhandenen knappen Informationen, die sich aus der vorliegenden Excel-Tabelle ergeben, sowie der Tiefe der hierzu notwendigen Ausführungen in dem vorliegenden Rahmen jedoch nicht umfänglich geprüft werden. Insbesondere die Hinweise auf die Speicherdauer bzw. Maßnahmen zur Einhaltung der DSGVO sind zu knapp gehalten, um an dieser Stelle eine abschließende Analyse durchzuführen.

II. Potentiell datenschutzrelevante Tätigkeiten

Im folgenden werden die vom Auftraggeber benannten, in Interviewanfragen gemeldeten Tätigkeiten in ausgewählten Projekten bzw. Testfeldern auf ihre Datenschutzrelevanz überprüft. Die Datenschutzrelevanz ergibt sich aus der Anwendbarkeit der europäischen Datenschutzgrundverordnung (DSGVO). Gemäß Art. 2 I DSGVO ist der sachliche Anwendungsbereich der Verordnung eröffnet „für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten, die in einem Datensystem gespeichert sind oder gespeichert werden sollen“.

Der sachliche Anwendungsbereich der DSGVO ist daher erst eröffnet, wenn es um die Verarbeitung *personenbezogener Daten* geht. *Personenbezogene Daten* sind entsprechend der Legaldefinition in Art. 4 Nr. 1 DSGVO „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dabei kann es sich um direkte Informationen handeln, wie beispielsweise den Namen, die Adresse, die Telefonnummer oder die E-Mail-Adresse einer Person. Es können aber auch indirekte Informationen sein, die in Verbindung mit anderen Daten verwendet werden können, um eine Person zu identifizieren, wie beispielsweise Geburtsdatum, Geschlecht, Beruf oder IP-Adresse. Wichtig ist zu beachten, dass eine Person nicht identifiziert, sondern lediglich identifizierbar sein muss. Dies ist entsprechend Art. 4 Nr. 1 2. Hs. DSGVO der Fall, wenn die natürliche Person „direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu

einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“. Liegen also bspw. Kameraaufnahmen einer Person vor, genügt die Möglichkeit, diese Bilder mithilfe eines Gesichtserkennungsprogramms einer Person zuzuordnen, grundsätzlich dazu, von ihrer Identifizierbarkeit auszugehen.[1] Dies gilt auch für mit einem Foto verbundene GPS-Daten, die mit den Bilddaten gespeichert werden und eine genaue Lokalisierung ermöglichen.[2] Um festzustellen, ob eine *natürliche Person identifizierbar* ist, sind alle Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren.[3] Im einzelnen ist dann abzuwägen, die vorhanden Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden. Dabei sind alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, heranzuziehen, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.[4]

Erforderlich ist schließlich die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten. Der Begriff der *Automatisierung* ist weit zu verstehen und umfasst alle Verfahren, bei denen ein Datenverarbeitungsvorgang anhand eines vorgegebenen Programms ohne weiteres menschliches Zutun selbsttätig erledigt wird.[5] Eine Digitalisierung der verarbeiteten Daten ist hinreichende, aber nicht notwendige Bedingung der Automatisierung.[6] Die Verarbeitung von Daten durch automatisierte oder autonome Fahrzeuge ist unzweifelhaft als automatisierte Datenverarbeitung zu verstehen.

Verarbeitung personenbezogener Daten ist gemäß Art. 4 Nr. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten. Exemplarisch werden das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung genannt. Ohne explizit aufgeführt zu werden, fällt auch die Anonymisierung unter die Verarbeitungsformen. Darunter ist ein Vorgang zu verstehen, der darauf gerichtet ist, dass personenbezogene Daten ihren Personenbezug verlieren.[7] Anonymisierte Daten sind dementsprechend nicht mehr personenbezogen; der Vorgang der Anonymisierung muss sich jedoch an den Maßstäben der DSGVO messen lassen.

[1] So EuGH, NJW 2015, 463 Rn. 22.
[2] BeckOK-Datenschutzrecht/*Schild*, Art. 4 DSGVO Rn. 14.
[3] BeckOK-Datenschutzrecht/*Schild*, Art. 4 DSGVO Rn. 15.
[4] BeckOK-Datenschutzrecht/*Schild*, Art. 4 DSGVO Rn. 15, 18.
[5] BeckOK-Datenschutzrecht/*Bäcker*, Art. 2 DSGVO Rn. 2.
[6] BeckOK-Datenschutzrecht/*Bäcker*, Art. 2 DSGVO Rn. 2.
[7] Kühling/Buchner/*Herbst*, DS-GVO/BDSG, 4. Aufl. 2024, Art. 2 DS-GVO Rn. 37b.

Problematisch bleibt daher regelmäßig die Frage, ob die erhobenen Daten personenbezogen sind, was im Einzelnen erörtert wird.

1. Fahrzeugtrajektoren

Der Auswertung der Interviewanfragen entsprechend finden sich in den ausgewählten Projekten bzw. Testfeldern Daten von *Fahrzeugtrajektoren*. Dies sind Pfade oder Bewegungsmuster der Fahrzeuge auf der Straße, wobei verschiedene Aspekte wie Position, Geschwindigkeit, Richtung, Beschleunigung und Verzögerung oder andere Parameter, die das Verhalten eines Fahrzeugs auf der Straße charakterisieren, berücksichtigt werden. Durch entsprechende Daten können Prozesse der Verkehrsplanung und -modellierung unterstützt werden. Sie können das Verhalten von Fahrzeugen auf bestimmten Straßenabschnitten oder in speziellen Verkehrsszenarien prognostizieren und auf diesem Weg Verkehrssysteme effizienter gestalten und die Verkehrsbelastung verringern. Bei der Entwicklung autonomer Fahzeuge werden Fahrzeugtrajektoren verwendet, um das Fahrverhalten der Fahrzeuge zu modellieren und zu optimieren. Durch die Analyse von Fahrzeugtrajektoren können autonome Fahrzeuge lernen, wie sie sich sicher und effizient im Straßenverkehr bewegen können. In Testfeldern dienen sie dazu, das Verkehrsverhalten der beteiligten Fahrzeuge nachzuverfolgen und zu untersuchen.

Entsprechend der Eigeneinschätzung der Befragten stellen Fahrzeugtrajektoren keine personenbezogenen Daten dar. Dem ist grundsätzlich zuzustimmen, da Fahrzeugtrajektoren in erster Linie mathematische Modelle oder Simulationen darstellen, die das Verhalten von Fahrzeugen auf der Straße vorhersagen. Sie basieren auf allgemeinen Verkehrsdaten wie Geschwindigkeit, Richtung und Verkehrsdichte. Diese Daten sind in der Regel anonymisiert und enthalten keine Informationen über einzelne Fahrer oder Fahrzeuge. Etwas anderes könnte allerdings gelten, soweit die Daten mit einzelnen Fahrern in Verbindung gebracht werden können. Während einer Testfahrt können auch die Trajektorien ausgewertet werden. Hierbei kann die Betrachtung isoliert oder anonymisiert erfolgen. Es kann auch eine Mischung mit anderen Datensätzen vorgenommen werden oder die Trajektorie eines bestimmten Fahrzeugs untersucht werden. In diesen Fällen stellen auch Trajektoren personenbezogene Daten des Fahrers da, da dieser bekannt ist. Um hinreichenden Datenschutz sicherzustellen, ist in darauf zu achten, dass eine solche Verbindung nicht hergestellt werden kann.

2. Prozessdaten in Anlagen (bspw. LSA)

Die Auswertung der Interviewanfragen verweist auch auf (LSA-)Prozessdaten in Anlagen. Prozessdaten in Anlagen beziehen sich auf Informationen, die während des Betriebs einer Anlage erfasst werden. Diese Daten geben Einblick in den Zustand, die Leistung und die Prozesse innerhalb der Anlage. LSA-Prozessdaten, auf die vorliegend bei den

Interviewanfragen gesondert verwiesen wurde, verarbeiten Informationen von Lichtsteuerungsanlagen.

Entsprechend der Eigeneinschätzung der Befragten stellen (LSA-)Prozessdaten keine personenbezogenen Daten dar. Dem ist zuzustimmen, soweit es sich um ausschließlich anlagenbezogene Daten handelt. Diese sind als sog. Sachdaten einzustufen.[8] Insbesondere LSA-Prozessdaten sind neutral und können keine personenbezogene Daten enthalten.

3. GPS-Daten der Fahrzeugflotte

Entsprechend der Auswertung der Interviewanfragen werden auch GPS-Daten der Fahrzeugflotte erhoben. Diese beziehen sich auf die Positionsdaten, die von den GPS-Empfängern in den Fahrzeugen einer Flotte erfasst werden, welche Auskunft über den genauen Standort der Fahrzeuge zu bestimmten Zeitpunkten geben. Die in Echtzeit erfassten GPS-Daten können geographische Koordinaten der Fahrzeuge, ihre Geschwindigkeit, die Fahrtrichtung, den Zeitpunkt der Erfassung oder auch den Kraftstoffverbrauch und den Kilometerstand enthalten und hierdurch zu dienen, die Fahrzeugflotte zu überwachen, Fahrzeugpositionen zu verfolgen oder die Fahrzeugleistung zu analysieren.

Entsprechend der Eigeneinschätzung der Befragten stellen die GPS-Daten der Fahrzeugflotte keine personenbezogenen Daten dar. Diese Bewertung bezieht sich vermutlich darauf, dass derartige Informationen zunächst an dem Fahrzeug anknüpfen. Sie können jedoch auch verwendet werden, um Bewegungen und Aktivitäten einer Person (des Fahrzeugführers oder eines Mitfahrers) nachzuverfolgen, sofern diese Daten miteinander kombiniert werden. In diesen Fällen sind auch GPS-Daten personenbezogen.[9] Hieraus können dann weitere Informationen abgeleitet werden, etwa spezifische Orten, an denen sich eine Person regelmäßig aufhält.

4. Informationen über TF-Nutzer

Über Testfeldnutzer, d.h. Fahrer und sonstige Insassen der im Testfeld genutzten automatisierten und autonomen Fahrzeuge, werden verschiedene Informationen erhoben. Dies sind zum einen Informationen, die über Nutzerfragebögen erfragt werden. Nutzerfragebögen werden in der Auswertung zwar nicht bei den erhobenen, jedoch bei den dauerhaft gespeicherten Daten genannt. Nutzerfragebögen dienen vorliegend dazu, Informationen von Nutzern etwa über ihre Fahrgewohnheiten oder ihre Wahrnehmung des Fahrzeugverhaltens zu erlangen, um die gewonnenen Erkenntnisse besser einordnen zu können.

[8] Hierzu BeckOK-Datenschutzrecht/*Schild*, Art. 4 DSGVO Rn. 22.
[9] Vgl. BeckOK-Datenschutzrecht/*Schild*, Art. 4 DSGVO Rn. 21.

Nutzerfragebögen enthalten immer dann personenbezogene Informationen, wenn sie einem konkreten Nutzer (etwa durch Angabe des Namens und weiterer personenbezogener Informationen, wie Geburtsdatum etc) zugeordnet werden können. Um dies zu verhindern, ist zu empfehlen, dass solche Fragebögen anonymisiert gestaltet sind.

Daneben können während des Fahrtvorgangs Daten über die Insassen erhoben werden, um die Sicherheit und das Fahrerlebnis zu verbessern. So können autonome Fahrzeuge Informationen über Sitzposition, Sitzhöhe, Neigung und andere Einstellungen des Fahrers erfassen. Sie können weiterhin Sensoren verwenden, um biometrische Daten wie Herzfrequenz, Atemfrequenz oder Stressniveau des Fahrers zu erfassen. Durch Innenraumkameras kann die Blickrichtung des Fahrers verfolgt werden, um bei Ablenkung oder Müdigkeit entsprechende Maßnahmen zu ergreifen. Hierin liegen höchstpersönliche Informationen, die datenschutzrechtlich relevant werden, soweit sie einer konkreten Person zugeordnet werden können.

5. Reisezeiten

Erhoben werden auch Daten zu Reisezeiten. Reisezeiten beziehen sich auf die Dauer, die benötigt wird, um von einem Ort zum anderen zu reisen.

Entsprechend der Eigeneinschätzung der Befragten stellen die Daten zu Reisezeiten keine personenbezogenen Daten dar. Reisezeiten stellen an sich keine personenbezogenen Daten dar, da sie keine Informationen enthalten, die eine Identifizierung einer bestimmten Person ermöglichen. Reisezeiten sind in der Regel allgemeine Informationen über die Dauer einer Reise zwischen zwei Orten. Jedoch kann es sein, dass bei der Verwendung bestimmter Dienste oder Anwendungen personenbezogene Daten im Zusammenhang mit Reisezeiten erfasst werden. Zum Beispiel könnten Standortdaten verwendet werden, um die geschätzte Reisezeit für eine bestimmte Person zu berechnen.

6. Zählschleifen

Die Auswertung der Interviewanfragen verweist auch auf die Datenerhebung durch Zählschleifen. Zählschleifen – also elektronische Vorrichtungen, die geeignet sind den Durchgang von Personen oder Objekten zu zählen – können eingesetzt werden, um den Verkehr (etwa an Ampeln und Mautstellen) zu überwachen,

Entsprechend der Eigeneinschätzung der Befragten stellen die aus Zählschleifen gewonnen Daten keine personenbezogenen Daten. Dem ist zuzustimmen, da Zählschleifen hauptsächlich

dazu dienen, den Durchgang von Personen oder Objekten zu zählen, ohne individuelle Informationen zu erfassen. Die Schleifen registrieren lediglich das Vorhandensein oder die Bewegung von etwas über die Schleife hinweg, ohne spezifische Identifizierungsinformationen zu erfassen. Es handelt sich daher um sog. Sachdaten.[10]

Eine andere Bewertung wäre lediglich angezeigt, wenn durch zusätzliche Technologien (wie etwa Videoüberwachung oder Gesichtserkennung) weitere Informationen erfasst werden, die eine Individualisierung ermöglichen.

7. Verkehrsrelevante Daten (Baustellen, Wetter, Verkehr)

Erhoben werden auch verkehrsrelevante Daten, die sich auf Informationen über den Verkehr beziehen. Diese Daten können verschiedene Aspekte des Verkehrs umfassen, wie etwa die Anzahl der Fahrzeuge, deren Geschwindigkeit, die Verkehrsflussmuster, die Verkehrsdichte oder Anzahl und Art von Verkehrsunfällen. Verkehrsdaten werden zu dem Zweck gesammelt, den Verkehr zu analysieren, Verkehrsströme zu überwachen, Verkehrsprognosen zu erstellen und Verkehrsmanagementmaßnahmen zu planen.

Entsprechend der Eigeneinschätzung der Befragten stellen Verkehrsdaten keine personenbezogenen Daten dar. Dem ist zuzustimmen, da Verkehrsdaten aggregierte und anonymisierte Informationen sind, die keine individuellen personenbezogenen Daten enthalten.

8. V2X-Nachrichten

Hinsichtlich der V2X-Nachrichten sowie der spezielleren Probe Vehicle Data (PVD), einem Anwendungsfall der V2X-Kommunikation, wird auf die ausführliche Darstellung zu Frage 2 verwiesen.

9. Kamerabilder

Erhoben werden auch Kamerabilder von automatisierten und autonomen Fahrzeugen. Neben Sensoren wie Lidar und Radar sind derartige Fahrzeuge auch auf Kamerabilder angewiesen, um sich ein umfassendes Bild von der Umgebung zu machen. Derartige Bilder dienen dazu, die Umgebung des Fahrzeugs zu erfassen und Informationen über Straßenverhältnisse, Verkehrsteilnehmer und Hindernisse zu liefern. Die Kamerabilder werden von den Sensoren des autonomen Fahrzeugs verarbeitet, um eine genaue Wahrnehmung der Umgebung zu ermöglichen und Entscheidungen über das Fahrverhalten zu treffen.

[10] Hierzu BeckOK-Datenschutzrecht/*Schild*, Art. 4 DSGVO Rn. 22.

Entsprechend der Eigeneinschätzung der Befragten stellen Kamerabilder personenbezogenen Daten dar. Über solche Kamerabilder können in bis zu 360°-Reichweite bspw. Personen aufgenommen werden. Die verfügbare Auflösung ermöglicht es, andere Verkehrsteilnehmende zu erkennen.[11] Diese Personen können etwa über Gesichtserkennungsprogramme identifiziert werden. Aufgenommen werden desweiteren Kennzeichen, die wiederum durch eine Halterabfrage mit Informationen über den Halter verbunden werden können und diesen bzw. ggf. auch den Fahrer mittelbar identifizierbar machen.[12] Mithilfe weiterer Informationen lassen sich solche Bilder mit Informationen über Zeitpunkt und Standort der Aufnahme verknüpfen. Daher ist der Eigeneinschätzung der Befragten zuzustimmen, dass Kamerabilder einen Personenbezug aufweisen. Es ist feststellbar, dass autonome Fahrzeuge zu einem System mit Rundumvideoüberwachung der Umgebung werden und damit weitreichende Datenschutzinteressen der das Fahrzeug umgebenden Personen tangieren.[13]

Eine Ausnahme ist für Wärmebildkameras festzustellen, welche durch Nutzung von Infrarotstrahlung Wärmestrahlung erfassen und in ein sichtbares Bild umwandeln können. Sie werden in autonomen Fahrzeugen eingesetzt, um die Umgebung zu erfassen und potenzielle Hindernisse oder Gefahren zu erkennen. Durch die Erfassung der Wärmesignaturen von Objekten können Wärmebildkameras beispielsweise helfen, Fußgänger, Tiere oder andere Fahrzeuge auch bei schlechten Sichtverhältnissen zu erkennen. In dem vorliegenden Kontext, der Erfassung von Personen und Objekten im Straßenverkehr, ist eine Identifizierbarkeit nahezu gänzlich ausgeschlossen.

Kamerabilder werden in der Auswertung weder bei den permanent noch den zeitweilig gespeicherten Aufnahmen angegeben.

Daneben können auch weitere *Rohdaten* von den verschiedenen Fahrzeugsensoren erfasst werden. Neben (Wärmebild-)Kameraaufzeichnungen kommen insbesondere Lidar- und Radaraufnahmen in Betracht. Zur Nutzung entsprechender Sensoren gibt es keine Informationen in den bereitgestellten Unterlagen. Hier findet sich lediglich der allgemeine Hinweis auf die Verwendung von Rohdaten. Allgemein lässt sich feststellen, dass Radarsensoren für den Fern- und Nahbereich zur Erfassung der Umgebungsbeschaffenheit dient, während Lidar mittels Lasertechnik die exakte Entfernung von Punkten innerhalb der Umgebung bestimmen kann. Bei letzterer erlaubt es die bisherige Auflösung noch nicht, Gesichter oder Kfz-Kennzeichen zu erkennen.[14]

[11] *Wagner*, Smart Mobility – Rechtliche Aspekte, FZI Forschungszentrum Informatik, S. 11.
[12] BeckOK-Datenschutzrecht/*Schild*, Art. 4 DSGVO Rn. 21; *Werner/Wagner/Pieper*, RDV 2020, 111 (112); vgl. auch OVG Münster NVwZ 2018, 742.
[13] *Wagner*, Smart Mobility – Rechtliche Aspekte, FZI Forschungszentrum Informatik, S. 11.
[14] *Wisselmann*, Technische Fahrzeugentwicklung – Hochautomatisiertes Fahren ab 2020?, in Rechtliche Aspekte automatisierter Fahrzeuge, 2015, S. 11 ff.; *Wagner*, Smart Mobility – Rechtliche Aspekte, FZI Forschungszentrum Informatik, S. 11.

10. Perception

Entsprechend der Auswertung der Interviewanfragen werden auch Perceptionsdaten gesammelt. *Perception* bezieht sich auf den Prozess der Verarbeitung der Rohdaten, um ein Verständnis der Umgebung des autonomen Fahrzeugs zu erlangen; es handelt sich also um einen Prozess der Umgebungswahrnehmung. Dieser Prozess umfasst die Anwendung von Algorithmen und KI-Techniken, um Objekte, Hindernisse, Straßenmarkierungen, Verkehrszeichen und andere relevante Informationen zu erkennen und zu interpretieren. Die *Perception* ermöglicht dem Fahrzeug, seine Umgebung zu verstehen und Entscheidungen zu treffen, um sicher zu navigieren und mit anderen Verkehrsteilnehmern zu interagieren.

Entsprechend der Eigeneinschätzung der Befragten können diese Daten allgemein personenbezogen sein. Im Speziellen wird dies für Handover-Prozesse herausgehoben. Ein Handover beim autonomen Fahren bezieht sich auf den Übergang der Fahrzeugkontrolle von einem autonomen System zum menschlichen Fahrer oder umgekehrt. Dies kann auf verschiedene Weisen stattfinden, abhängig von den Fähigkeiten des autonomen Systems und den Anforderungen der jeweiligen Situation. Es kann eine visuelle oder akustische Benachrichtigung erfolgen, die den Fahrer auffordert, die Kontrolle zu übernehmen. Dieser Übergang kann in bestimmten Situationen erforderlich sein, beispielsweise wenn das autonome System nicht in der Lage ist, eine bestimmte Fahraufgabe zu bewältigen oder wenn es zu unvorhergesehenen Ereignissen kommt. Insbesondere während dieses Vorgangs können Daten über den Fahrer erfasst und ausgetauscht werden, wie etwa biometrische Daten zur Identifizierung des Fahrers oder Daten zur Überwachung des Fahrerzustands, etwa um sicherzustellen, dass der Fahrer in der Lage ist, die Kontrolle über das Fahrzeug zu übernehmen. Bereits die Speicherung von GPS-Positionen und Zeitangaben im Moment des Wechsels der Fahrzeugsteuerung kann zur Identifikation anhand des konkreten Aufenthaltsortes führen.[15] Da sich diese Daten dem Fahrzeugführer zuordnen lassen, sind sie daher als personenbezogen zu bewerten.

Als datenschutzrelevant werden auch Trackingprozesse bewertet. Hierbei handelt es sich um einen spezifischen Teil des Perceptionprozesses, der sich auf die Verfolgung von Objekten konzentriert. Dies geschieht durch die kontinuierliche Aktualisierung der Position, Geschwindigkeit und möglicherweise anderer Eigenschaften von Objekten im Raum. Hierdurch kann die Bewegung von Fahrzeugen, Fußgänger oder anderen Hindernissen verfolgt werden, um mögliche Kollisionen zu vermeiden. Sofern hierdurch etwa Personen erfasst werden, die sich in der Umgebung befinden, ist der Personenbezug gegeben.

[15] *Werner/Wagner/Pieper*, RDV 2020, 111 (112).

III. Rechtmäßigkeit der Verarbeitung personenbezogener Daten

Mangels detaillierterer Informationen zum Umgang mit den erhobenen personenbezogenen Daten werden im Folgenden allgemeinere Erwägungen zu den Rechtmäßigkeitsanforderungen niedergelegt.

1. Einwilligung gemäß Art. 6 Abs. 1 UAbs. 1 lit. a) DSGVO

Die Erlaubnis zur Verarbeitung personenbezogener Daten besteht einerseits, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat (Art. 6 Abs. 1 UAbs. 1 lit. a) DSGVO). Hieran ist bei sämtlichen Daten zu denken, welche die Testfeld-Teilnehmer betreffen. Diese können grundsätzlich in die Erhebung ihrer Daten zum Zwecke der Erforschung und Fortentwicklung des automatisierten und autonomen Fahrens einwilligen. Im Einzelnen betrifft dies Informationen über Testfeldnutzer, die in Nutzerfragebögen erfragt oder im Rahmen des Fahrtvorgangs, insbesondere bei Handover-Prozessen, erfasst werden. Daneben kann dies Fahrzeugtrajektoren, LSA-Prozessdaten, GPS-Daten oder Daten zu Reisezeiten betreffen, sowie diese – entsprechend der obigen Überlegungen – im Einzelfall personenbezogen sind.

Allerdings ist zu beachten, dass die innenraumbezogenen Daten von den jeweiligen Fahrinsassen jeweils vor Fahrtantritt erteilt werden muss, was sich als wenig praktikabel erweist.[16] Zudem kann die Einwilligung gemäß Art. 7 Abs. 3 S. 1 DSGVO jederzeit widerrufen werden. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung zwar nicht berührt. In diesem Moment dürfen die erlangten Daten jedoch nicht weiter verwertet werden, was im Falle der Testfeldforschung sehr problematisch wäre.

Ausgeschlossen ist eine Einwilligungslösung zudem bei allen personenbezogenen Daten von Drittbetroffenen. Dies geschieht insbesondere durch Kamerabilder sowie sonstige Rohdatenerfassung in Zusammenschau mit daraus abgeleiteten Perceptions. Wie bereits oben erläutert, ermöglichen autonome Fahrzeuge eine dauerhafte und umfassende Beobachtung des Umgebungsraums.

2. „Wahrnehmung einer Aufgabe im öffentlichen Interesse“ gemäß Art. 6 Abs. 1 UAbs. 1 lit. e) DSGVO

[16] *Wagner*, Smart Mobility – Rechtliche Aspekte, FZI Forschungszentrum Informatik, S. 24.

Weiterhin könnte eine Rechtfertigung nach Art. 6 Abs. 1 UAbs. 1 lit. e) DSGVO in Betracht kommen, wonach eine Datenverarbeitung auch ohne Einwilligung möglich ist, wenn diese der „Wahrnehmung einer Aufgabe im öffentlichen Interesse“ dient. Die Fort- und Weiterentwicklung des automatisierten und autonomen Fahrens liegt im weitesten Sinne im öffentlichen Interesse, da hierdurch einerseits die Verkehrssicherheit mittel- bis langfristig erhöht und eine weitreichende Teilhabe aller Bevölkerungsgruppen (auch körperlich beeinträchtigter oder älterer Personen) an individuellen Fortbewegungsmöglichkeiten sichergestellt werden wird. Der EuGH hat explizit festgestellt, dass „die Verbesserung der Straßenverkehrssicherheit ein von der Union anerkanntes Ziel im allgemeinen Interesse“ ist und die Mitgliedstaaten daher berechtigt sind, „ die Straßenverkehrssicherheit als „Aufgabe …, die im öffentlichen Interesse liegt“, im Sinne von Art. 6 Abs. 1 Buchst. e der DSGVO einzustufen“.[17] Dies muss zugleich Prozesse der Weiterentwicklung der Sicherheit des Straßenverkehrs durch Formen automatisierter und autonomer Fahrprozesse von der bloßen Anwendung derartiger Mobilitätsformen unterscheiden. Welche Anforderungen an die Erhöhung der Straßenverkehrssicherheit zu stellen sind, ist damit noch nicht im Detail beantwortet.

3. „Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten“ gemäß Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO

Nach Art. 6 Abs. 1 lit. f) DSGVO ist eine Datenverarbeitung schließlich auch dann zulässig, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Da vorliegend die Datenverarbeitung in Testfeldern betroffen ist, könnten die berechtigten Interessen auf der zugrunde liegenden Forschungstätigkeit fußen. Forschungstätigkeit wird insgesamt durch die DSGVO privilegiert, was in verschiedenen Vorschriften zum Ausdruck kommt. So sind einerseits die Rechte der betroffenen Personen nach Art. 15, 16, 18, 21 DSGVO beschränkt, soweit dies die Verwirklichung des Forschungszwecks unmöglich macht oder ernsthaft beeinträchtigt und die Beschränkung für die Erfüllung der Forschungszwecke notwendig ist (Art. 89 Abs. 2 DSGVO i.S.m. § 27 Abs. 2 BDSG).

Bereits aus diesen Sondervorschriften lässt sich ableiten, dass der Datenerhebung zu Forschungszwecken eine besondere Privilegierung zugesprochen wird. Forschungstätigkeit zählt zugleich zu den in Art. 179 AEUV ausdrücklich erwähnten Zielen der Union. Im konkreten Fall wird diese Zielrichtung durch ein allgemeines Interesse der Allgemeinheit an verkehrssichernder Technik.[18]

[17] EuGH, Urt. vom 22.06.2021 – C-439/19, BeckRS 2021, 15289, Rn. 108.
[18] Hierzu Oppermann/Stender-Vorwachs (Hrsg.), Autonomes Fahren: Rechtsprobleme, Rechtsfolgen, technische Grundlagen, 2. Auflage 2020.

Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO privilegiert die Verarbeitung von personenbezogenen Forschungsdaten allerdings nur unter der Voraussetzung, dass die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Daher ist zunächst zu untersuchen, ob es ein gleich geeignetes, milderes Mittel gibt – konkret, ob der Einsatz datenschutzfreundlicher Technik technisch möglich und wirtschaftlich zumutbar ist. Zudem sind die verfolgten Forschungsinteressen gegen die Interessen der betroffenen Personen abzuwägen. Konkret ist hierbei die Eingriffsintensität zu untersuchen, die sich aus der zeitlich-räumlichen Ausdehnung, der Anzahl der betroffenen Personen, der Speicherdauer und den Zugriffsmöglichkeiten ergeben. Eine besondere Eingriffstiefe kann sich etwa auch daraus ergeben, dass durch die Datenverarbeitung Bewegungsprofile erstellt werden können. Vorliegend fehlt es leider an den notwendigen Informationen, um die getroffenen Maßnahmen auf die Einhaltung dieser Maßgaben überprüfen zu können.

IV. Pflichten beim Umgang mit personenbezogenen Daten

Beim Umgang mit personenbezogenen Daten sind spezifische Pflichten einzuhalten, von denen die wichtigsten im Folgenden kurz benannt werden:

- Gemäß Art. 13 DSGVO entsteht bei der Erhebung personenbezogener Daten eine Informationspflicht. Danach hat der Verantwortliche der betroffenen Person zum Zeitpunkt der Datenerhebung die in Art. 13 DSGVO näher aufgeführten Informationen zu übermitteln, insbesondere die Identität und die Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten, die Zwecke der Verarbeitung und ggf. die berechtigten Interessen, die Empfänger der Daten sowie die Übermittlungsabsicht in Drittstaaten. Dieser Informationspflicht kann in der Praxis durch eine Datenschutzerklärung (mit Blick auf den Fahrer) oder ein Kameraschild (mit Blick auf sonstige Verkehrsteilnehmer) erfolgen.

- Gemäß Art. 15 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Sofern dies der Fall ist, hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf weiterführende Informationen, die in Art. 15 Abs. 1 DSGVO im Weiteren ausdifferenziert werden.

- Aus Art. 16 DSGVO resultiert das Recht der betroffenen Person, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten und ggf. die Vervollständigung unvollständiger personenbezogener Daten zu verlangen.

- Nach Art. 18 DSGVO hat eine betroffene Person das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn die im weiteren in der Norm ausdifferenzierten Voraussetzungen gegeben sind.

- Die betroffene Person hat schließlich nach Art. 21 DSGVO das Recht, auf persönlichen Gründen gegen die Verarbeitung sie betreffender personenbezogener Daten Widerspruch einzulegen.

Hier sind einzelne Informationen in den Interviewanfragen enthalten. Diese sind jedoch nicht hinreichend, um abschließend beurteilen zu können, ob alle datenschutzrechtlichen Pflichten eingehalten wurden. Zur Beantwortung dieser Frage bedurfte es gegebenenfalls einer weiteren detaillierten Untersuchung auf der Grundlage eines größeren Datenpakets.

V. Ergebnis

Die Beurteilung ausgewählter Aktivitäten zum Thema Daten, Datenschutz und -sicherheit kulminiert insbesondere in der Frage, ob die erhobenen Daten einen Personenbezug aufweisen, da sie andernfalls nicht dem Anwendungsbereich der DSGVO unterfallen. Diese Frage ist im Hinblick auf die einzelnen Maßnahmen detailliert zu prüfen. Eine abschließende Entscheidung ist tlw. aufgrund der knappen Informationslage nicht möglich.

Genauerer Untersuchung bedarf des Weiteren die Frage, wann eine Verarbeitung personenbezogener Daten zulässig ist. Im Hinblick auf den Betrieb von Testfeldern für automatisiertes und autonomes Fahren ist insbesondere an die Privilegierung wissenschaftlicher Tätigkeiten zu denken.

Unabhängig hiervon sind immer die von der DSGVO formulierten Pflichten zum Umgang mit personenbezogenen Daten zu beachten.

B. Frage 2: Beurteilung des Themas Datensicherheit (Security) bei Autonomer Mobilität aus rechtlicher Perspektive

I. Umfang des Gutachtens – Frage 2

Gewünscht ist die Beurteilung des Themas Datensicherheit (Security) sowie Datenschutz für Betreiber von Testfeldern zur Erprobung autonomer, teleoperierter und vernetzter Mobilität aus rechtlicher Perspektive. Dies umfasst die Beurteilung der Rechtslage bzgl. der Sicherung von Daten, die bei der Benutzung von Testfeldern zur Erprobung autonomer Mobilität gegen verschiedene Angriffe von außen bestehen. Aufgrund des sehr weit gefassten Rahmens ist eine Beurteilung von sämtlichen Rechtsfragen und Rechtsgebieten im Detail nicht möglich, sodass unter Umstände eine Nachbeauftragung erforderlich ist, um strittige Aspekte einer Klärung zuzuführen.

II. Einleitung

Der Schutz von Daten nimmt bei zunehmender Automatisierung und Vernetzung von Fahrzeugen mit anderen Fahrzeugen sowie der Infrastruktur einen hohen Stellenwert ein. Aber auch beim Betrieb von Testfeldern zur Erforschung und Erprobung von automatisierten und autonomen Fahrfunktionen sowie weiterer Funktionen von Kraftfahrzeugen kommt dem Schutz der anfallenden Daten eine besondere Bedeutung zu. Dabei variieren die notwendigen Maßnahmen zum Schutz dieser Daten je nach Datenart. Neben dem Schutz von personenbezogenen Daten und dem Schutz von Geschäftsgeheimnissen nimmt der Bereich der IT-Sicherheit einen großen Bereich ein.[19] Denn nicht nur Kraftfahrzeuge können Ziel von Cyberangriffen sein, sondern auch Testfelder stellen ein potenzielles Ziel dar.

Es existiert kein spezielles Gesetz für Testfelder, in dem Anforderungen an diese hinsichtlich der Datensicherheit und des Datenschutzes normiert sind. Hinzu kommt, dass der Begriff „Testfeld“ kein feststehender Begriff ist. Vielmehr können Umfang sowie Dienstleistungen und Angebote je nach Testfeld variieren. Daher können je nach Ausgestaltung und Aktivitäten auf dem Testfeld unterschiedliche Gesetze einschlägig sein. Anknüpfungspunkt ist aufgrund einer Lex Testfeld immer der Lebenssachverhalt. Betreiber von Testfeldern können zudem personenidentisch mit dem Nutzer eines solchen Testfelds sein und selbstständig Fahrzeuge und Fahrfunktionen testen. Betreiber von Testfeldern können auch in unterschiedlichen Rollen betroffen sein. Die Vorschriften der AFGBV richten sich beispielsweise an denjenigen, der eine Erprobungsgenehmigung für autonome Fahrfunktionen beantragt. Zunächst sind Betreiber von Testfeldern nicht Normadressat. Dies ändert sich jedoch dann, wenn ein Testfeldbetreiber einen solchen Antrag auf Genehmigung stellt. Im Gutachten wird daher differenziert zwischen Gesetzen, die unmittelbar Anwendung finden, aber auch solchen, die mittelbar oder in besonderen Konstellationen relevant werden können.

Die Thematik ist besonders komplex, da es keine primäre Rechtsquelle zur Informationssicherheit und Cybersicherheit sowie dem Schutz von Daten gibt, die Aufschluss

[19] *Barlag*, ZD-Aktuell 2016, 05421; *Lüdemann*, ZD 2015, 247, 251.

über die zu treffenden, notwendigen Anforderungen und Maßnahmen gibt.[20] Vielmehr sind neben nationalem Bundesrecht auch EU-Recht sowie völkerrechtliche Verträge zu beachten. Dabei stellt sich zudem immer die Frage, ob eine Rechtsquelle im Verhältnis zu einer anderen vorgeht, also lex specialis ist. Auf den ersten Blick in Betracht kommende relevante Rechtsquellen im Kontext der IT-Sicherheit sind im nationalen Recht das BSI-Gesetz, die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz, das Produktsicherheitsgesetz, das Produkthaftungsgesetz, die deliktische Produzentenhaftung nach § 823 Abs. 1 BGB sowie im europäischen Recht der Cybersecurity Act, die NIS-Richtlinie, die Datenschutz-Grundverordnung, die Warenkauf-Richtlinie, die Digitale-Inhalte-Richtlinie, die EG-Produktsicherheitsrichtlinie und im völkerrechtlichen Kontext die UN Regulation on Cybersecurity und Cybersecurity Management Systems sowie die UN Regulation on Software Updates und Software Update Management Systems. Allein diese kurze, unvollständige Aufzählung verdeutlicht die Komplexität aufgrund der unterschiedlichen Rechtsquellen auf unterschiedlichen Ebenen. Hinzu kommt, dass die jeweiligen Rechtsquellen teilweise nur Schnittmengen sowie einzelne Regelungen zur IT-Sicherheit enthalten und ansonsten einen vollständig anderen Regelungs- und Anwendungsbereich haben.

Im Folgenden sollen rechtliche Anforderungen aufgezeigt werden, die zum Schutz von Daten gegen Angriffe von außen getroffen werden müssen.

III. Informationssicherheit und Cybersicherheit

Der Schutz von Daten ist auch im Rahmen der Informations- und Cybersicherheit von Bedeutung. Die Begriffe Informationssicherheit und Cybersicherheit werden oft im Zusammenhang mit Cyberangriffen benutzt.
Die Informationssicherheit zielt darauf ab, dass ein System, welches Daten verarbeitet, die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sowie Authentizität einhalten kann.[21] Eine Legaldefinition des Terms „IT-Sicherheit“ findet sich in § 2 Abs. 2 S. 4 BSIG.[22] Sicherheit in der Informationstechnik meint danach die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen in informationstechnischen Systemen, Komponenten oder Prozessen oder bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen.

Ist von Sicherheit in der Informationstechnik die Rede, so ist zu beachten, dass dies nicht mit der Produktsicherheit im Produkthaftungsrecht gleichzusetzen ist.[23]

Im Bereich der IT-Sicherheit nehmen nationale und internationale Normen und Standards eine entscheidende Stelle in der Praxis ein. In Betracht kommen hierbei etwa die von der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC) veröffentlichte ISO/IEC 27000-Reihe sowie der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI). Diese industrieseitigen Standards sind keine Rechtsquelle, sodass sie keine bindende Wirkung entfalten. Gleichwohl können sie

[20] Anders ist dies indem mit Blick auf das Datenschutzrecht. Innerhalb der EU ist dieses durch die DS-GVO seit 2018 vollharmonisiert.
[21] *Wagner*, Das neue Mobilitätsrecht, 2021, S. 185; *Rockstroh/Kunkel*, MMR 2017, 77, 78; *Bräutigam/Klindt*, NJW 2015, 1137, 1141.
[22] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. August 2009 (BGBl I. S. 1885).
[23] *Rockstroh/Kunkel*, MMR 2017, 77, 78.

unmittelbar Bedeutung erlangen, sofern ein Gesetz auf den Stand der Technik verweist oder direkt auf eine Norm verwiesen wird, die ihrerseits explizite Anforderungen enthält. Dies führt zu produkthaftungsrechtlichen Implikationen, da dadurch das zu erwartende Sicherheitsniveau determiniert wird.[24]

Im Folgenden soll auf verschiedene Bereiche der Informationssicherheit eingegangen werden.

1. Internationale Regelungen

Im Bereich des Straßenverkehrs sind insbesondere die UN-ECE-Regelungen maßgeblich, da das europäische EG-Typgenehmigungsrecht auf diese verweist. Für Automobilhersteller und weitere Adressaten dieser Regelungen bedeutet dies, dass sie im Rahmen des Typgenehmigungsprozesses nachweisen müssen, dass die Anforderungen aus den anwendbaren UN-ECE-Regelungen eingehalten werden.[25]

Im Kontext der Informationssicherheit sowie der Cybersicherheit sind bspw. Regelungen zu automatisierten Spurhaltesystemen, zur Cybersicherheit sowie zu Software-Updates relevant.

a. UN-ECE-Regelung *Nr. 157*

Die UN-ECE-Regelung Nr. 157 – Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich des automatischen Spurhalteassistenzsystems (ALKS)[26] [2021/389] ist am 22.1.2021 in Kraft getreten.[27] Es handelt sich bei der UN-ECE-Regelung Nr. 157 um die erste Vorschrift – auf internationaler Ebene – die die Genehmigung einer Level 3 SAE J3016 Fahrfunktion regelt.[28] Das ALKS steuert die Quer- und Längsbewegung des Fahrzeugs, ohne dass der Fahrzeugführer aktiv die Quer- oder Längsbewegung steuern oder Fahrbefehle geben muss. Der Einsatz dieser Spurhaltesysteme ist lediglich auf Autobahnen zulässig und nur bis 60 km/h erlaubt.[29] Zudem werden gem. Ziffer. 1.1. lediglich Fahrzeuge der Klasse M1 erfasst. Kann das automatisierte Spurhaltesystem durch Updates aktualisiert werden, so müssen Hersteller sowohl ein Cybersicherheitsmanagementsystem (CSMS) als auch ein Software-Update-Managementsystem (SUMS) einrichten.

Abschnitt 9 regelt die Cybersicherheit und Softwareaktualisierung. Nach Ziffer 9.1 darf die Wirksamkeit des Systems nicht durch Cyberangriffe, Cyberbedrohungen oder Schwachstellen beeinträchtigt werden. Die Wirksamkeit der getroffenen Sicherheitsmaßnahmen ist durch Einhaltung der UN-ECE-Regelung Nr. 155 nachzuweisen. Ziffer 9.2 fordert zudem bei möglichen Softwareaktualisierungen des Systems, dass die Wirksamkeit der Software-Updates und der jeweiligen Prozesse durch Einhaltung der UN-ECE-Regelung Nr. 156 nachzuweisen ist.

Diese Anforderungen treffen den Fahrzeughersteller, nicht aber etwa Betreiber von Testfeldern.

---

[24] Zu haftungsrechtlichen Implikationen von technischen Normen und Standards siehe *Rockstroh/Kunkel*, MMR 2017, 77, 81.
[25] *Steege*, NZV 2022, 257, 262
[26] ALKS steht für Automated Lane Keeping System.
[27] Eingehend zur UN-Regelung Nr. 157 *Will*, NZV 2020, 163 ff.
[28] *Malzhacker*, in: Chibanguza/Kuß/Steege, Künstliche Intelligenz, 2022, Kap. § 3 J. Rn. 13.
[29] *von Bodungen/Gatzke*, RDi 2022, 354, 362.

b. UN-ECE-Regelung Nr. 155

Die UN-ECE-Regelung Nr. 155 – Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems [2021/387] ist am 22.01.2021 in Kraft getreten.[30]

Der Anwendungsbereich der Regelung gilt gem. Ziffer 1.1 hinsichtlich der Cybersicherheit für die Fahrzeugklassen M und N. Daneben sind auch Kraftfahrzeuge der Klasse O erfasst, sofern diese mit mindestens einem elektronischen Steuergerät ausgerüstet sind. Ausgehend von Ziffer 1.2 gelten die Regelungen ebenfalls für die Fahrzeugklassen L6 und L7, die mit „Funktionen des autonomen Fahrens ab Autonomiestufe 3 ausgestattet sind". Wenngleich der Begriff autonomes Fahren verwendet wird, sind bereits Fahrzeuge des Level 3 erfasst, bei denen es sich um automatisierte Fahrzeuge handelt. In der Praxis sollten daher sowohl national anwendbare Rechtsvorschriften wie die §§ 1a ff. sowie 1d ff. StVG beachtet werden[31] als auch die Stufen des Standards SAE J3016.[32]

Nationale Vorschriften gehen der UN-ECE-Regelung Nr. 155 ausdrücklich nicht vor (Ziffer 1.3). Dies umfasst insbesondere Gesetze und Verordnungen, die den Zugang zum Fahrzeug, zu den Fahrzeugdaten sowie den Zugriff auf die Fahrzeugfunktionen und Ressourcen sowie Zugangsbedingungen betreffen. Somit findet die UN-ECE-Regelung Nr. 155 auch dann Anwendung, wenn anderslautende nationale Rechtsvorschriften existieren. Gleiches gilt gemäß Ziffer 1.3 im Hinblick auf nationale und regionale Rechtsvorschriften, die den Schutz der Privatsphäre sowie den Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten betreffen. Darüber hinaus findet die UN-ECE-Regelung Nr. 155 auch dann Anwendung, wenn nationale oder regionale Rechtsvorschriften die Entwicklung sowie die Installation und Systemintegration von physischen und digitalen Ersatzteilen und Bauteilen hinsichtlich der Cybersicherheit regeln.

Mit Blick auf den Zweck der Harmonisierung überzeugt dieser Vorrang der UN-ECE-Regelung Nr. 155.

Cybersicherheit meint i.S. der UN-ECE-Regelung Nr. 155 gem. Ziffer 2.2 einen Zustand, in dem Fahrzeuge und deren Funktionen vor Cyberbedrohungen für elektrische oder elektronische Bauteile geschützt sind. Cybersicherheitsmanagementsystem (CSMS) meint dabei einen systematischen, risikobasierten Ansatz zur Festlegung von organisatorischen Abläufen, Zuständigkeiten und Governance hinsichtlich des Umgangs mit Risiken im Zusammenhang mit Cyberbedrohungen für Fahrzeuge und beim Schutz von Fahrzeugen vor Cyberangriffen (Ziffer 2.3).

Die Einhaltung der Anforderungen aus der UN-ECE-Regelung Nr. 155 treffen den Automobilhersteller. Er muss die Einhaltung zudem nachweisen. Die Anforderungen sind außerdem zulassungsrelevant. Nach Ziffer 5.1 dürfen Genehmigungsbehörden die Typgenehmigung hinsichtlich der Cybersicherheit nur für solche Fahrzeugtypen erteilen, die

[30] Veröffentlicht am 9.3.2021 im Amtsblatt der Europäischen Union. Die rechtsverbindlichen Originaltexte sind: ECE/TRANS/WP.29/2020/79, ECE/TRANS/WP.29/2020/94 sowie ECE/TRANS/WP.29/2020/97.
[31] Umfassend zum nationalen Rechtsrahmen zum hoch- und vollautomatisierten sowie autonomen Fahren, *Steege*, PHi 5-6/2021, 210 ff.; *Steege*, PHi 1/2022, 18 ff.
[32] Zu den verschiedenen Stufenklassifikationen des automatisierten Fahrens und den rechtlichen Auswirkungen eingehend *Steege*, Automatisierte Rechtsanwendung und ihre Grenzen, 2023, S. 46 ff.

die Anforderungen der UN-ECE-Regelung Nr. 155 erfüllen. Die Anforderungen gelten folglich nicht für Betreiber von Testfeldern.

c. UN-ECE-Regelung Nr. 156

Am 22.01.2021 ist die UN-ECE-Regelung Nr. 156 – Einheitliche Bestimmungen für die Genehmigung von Kraftfahrzeugen hinsichtlich der Softwareaktualisierung und des Softwareaktualisierungsmanagementsystems [2021/388] in Kraft getreten.[33]

Der Anwendungsbereich der UN-ECE-Regelung Nr. 156 erfasst Fahrzeuge der Klassen M, N, O, R, S und T, sofern bei diesen Softwareaktualisierungen möglich sind. Was unter Softwareaktualisierung zu verstehen ist, wird in Ziffer 2.3 legaldefiniert. Danach handelt es sich dabei um „ein Paket, das für das Upgrade auf eine neue Version verwendet wird; dies schließt eine Änderung der Konfigurationsparameter ein".

Auch diese Anforderungen sind zulassungsrelevant. Den Antrag auf Genehmigung eines Fahrzeugtyps hinsichtlich der Verfahren zur Softwareaktualisierung muss der Fahrzeughersteller einreichen oder ein von ihm Bevollmächtigter (Ziffer 3.1).

Den Hersteller treffen dabei verschiedene Pflichten im Kontext der Sicherheit, die er nachweisen muss. So muss er das Verfahren aufzeigen, welches Einsatz findet, um Softwareaktualisierungen „nach vernünftigem Ermessen vor Manipulationen" zu schützen, Ziffer 7.1.3.1. Auch die Verfahren zur Aktualisierung der Software müssen ihrerseits hinreichend geschützt sein, Ziffer 7.1.3.2. Zudem müssen sowohl die Verfahren zur Überprüfung als auch zur Validierung der Funktionalität der Software und des Codes der im Fahrzeug verwendeten Software geeignet sein. Darüber hinaus treffen den Hersteller in Ziffer 7.1.4 weitergehende Anforderungen bei drahtlosen Softwareaktualisierungen, sog. Over-the-Air-Updates (OTA). So muss der Hersteller die Verfahren benennen, die Anwendung finden, damit die Durchführung von Softwareaktualisierungen keine Auswirkungen auf die Sicherheit hat, sofern sie während der Fahrt erfolgen. Schließlich muss bei bestimmten Aktualisierungen, etwa der Kalibrierung von Sensoren, sichergestellt sein, dass bspw. eine dafür qualifizierte Person anwesend ist oder das Verfahren kontrolliert wird, Ziffer 7.1.4.2.

Über diese Anforderungen hinaus finden sich zahlreiche weitere Anforderungen, etwa zu drahtlosen Aktualisierungen sowie hinsichtlich der Software.

Diese Anforderungen richten sich an den Automobilhersteller. Sie sind zu erfüllen, um einen Fahrzeugtyp zuzulassen.

2. Europäischer Rechtsrahmen

Ein einheitlicher europäischer Rechtsrahmen für die Implementierung und Etablierung eines einheitlichen Standards der IT-Sicherheit existiert trotz der großen Bedeutung der Materie nicht.[34] Anforderungen an die IT-Sicherheit finden sich in zahlreichen Gesetzen, sodass diese nicht einheitlich Anwendung finden und kein einheitliches Bild des IT-Sicherheitsrechts besteht.

[33] Veröffentlicht am 9.3.2021 im Amtsblatt der Europäischen Union, L 82/60. Der rechtsverbindliche Originaltext ist ECE/TRANS/WP.29/2020/80.
[34] *Bräutigam/Klindt*, NJW 2015, 1137, 1141.

a. *Cybersecurity Act*

Am 28.06.2021 ist der Rechtsakt zur Cybersicherheit, „CSA“, (VO (EU) 2019/881) in Kraft getreten. Die Verordnung verfolgt verschiedene Regelungsziele. Diese finden sich in Art. 1 CSA. In der Verordnung werden die Ziele, Aufgaben und organisatorischen Aspekte der ENISA (Agentur der Europäischen Union für Cybersicherheit) festgelegt, Art. 1 Abs. 1 lit. a CSA. Dadurch soll das Mandat der ENISA weiter gestärkt werden.[35] Zudem wird ein einheitlicher, vollharmonisierter Rahmen zur Festlegung europäischer Schemata für die Cybersicherheitszertifizierung geschaffen, mit dem Ziel, für IKT-Produkte, -Dienste und -Prozesse in der Union ein angemessenes Maß an Cybersicherheit zu gewährleisten. Dadurch soll eine Fragmentierung des Binnenmarktes hinsichtlich Zertifizierungsschemata innerhalb der Europäischen Union verhindert werden, Art. 1 Abs. 1 lit. b CSA. Die ausgegebenen Zertifikate sollen innerhalb der Europäischen Union anerkannt werden, was zu Vertrauen führen soll.[36]

b. *Datenschutzrecht*

Datenschutz ist in der Europäischen Union durch die Datenschutz-Grundverordnung vollharmonisiert.[37] Aufgrund der Relevanz dieser Anforderungen an die Betreiber von Testfeldern und Nutzer von Testfeldern werden die Anforderungen untenstehend in einem gesonderten Abschnitt zum Datenschutzrecht dargestellt.[38]

c. *Kritische Infrastrukturen i.S. der NIS-Richtlinie*

Für kritische Infrastrukturen existieren mit der Richtlinie zum Sicherheitsniveau von Netz- und Informationssystemen (NIS-Richtlinie)[39] eigenständige Regelungen innerhalb der Europäischen Union. Art. 1 Abs. 1 NIS-Richtlinie sieht vor, dass ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen innerhalb der Europäischen Union erreicht werden soll.

Besondere Anforderungen existieren für Betreiber wesentlicher Dienste. Diese sind in Art. Art. 4 Nr. 4 NIS-Richtlinie legaldefiniert. Danach handelt es sich bei ihnen um „eine öffentliche oder private Einrichtung einer in Anhang II genannten Art, die den Kriterien des Artikels 5 Absatz 2 entspricht“. Damit kommt es zunächst maßgeblich auf die in Anhang II genannten Einrichtungen an. Anhang II nennt als 2. Sektor den Verkehrssektor und zählt unter d) den Straßenverkehr auf. Davon umfasst sind einerseits Straßenverkehrsbehörden i.S. des Art. 2 Nr. 12 VO (EU) 2015/962 zur Bereitstellung von Echtzeit-Verkehrsinformationsdiensten innerhalb der Europäischen Union. Andererseits werden Betreiber intelligenter Verkehrssysteme i.S. des Art. 4 Nr. 1 RL 2010/40/EU erfasst, die einen Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern vorsehen. Die ITS-Richtlinie definiert in Art. 4 Nr. 1 intelligente Verkehrssysteme und meint damit Systeme, „bei denen Informations- und Kommunikationstechnologien im Straßenverkehr, einschließlich seiner Infrastrukturen, Fahrzeuge und Nutzer, sowie beim

[35] *Rath/Ekardt/Schiela*, MMR 2023, 83, 88.
[36] *Maseberg/Michael/Müller/Seidel*, in: Kipker, Cybersecurity, 2. Aufl. 2023, Kap. 5 Rn. 42.
[37] Verordnung (EU) 2016/679.
[38] Siehe untenstehend unter VIII. Datenschutzrecht – DS-GVO.
[39] Richtlinie (EU) 2016/1148.

Verkehrs- und Mobilitätsmanagement und für Schnittstellen zu anderen Verkehrsträgern eingesetzt werden“.

Art. 5 NIS-Richtlinie sieht die Ermittlung der Betreiber wesentlicher Dienste vor. Als Kriterien zur Ermittlung von Betreibern wesentlicher Dienste, auf die Art. 4 Nr. 4 NIS-Richtlinie referenziert, nennt Art. 5 Abs. 2 NIS-Richtlinie:
- Die Bereitstellung eines Dienstes, der für die Aufrechterhaltung kritischer gesellschaftlicher und / oder wirtschaftlicher Tätigkeiten unerlässlich ist (Art. 5 Abs. 2 lit. a NIS-Richtlinie),
- die Abhängigkeit der Bereitstellung des Dienstes von Netz- und Informationssystemen (Art. 5 Abs. 2 lit. b NIS-Richtlinie)
- und dass ein Sicherheitsvorfall eine erhebliche Störung bei der Bereitstellung des Dienstes bewirken würde (Art. 5 Abs. 2 lit. c NIS-Richtlinie).

Nur wenn diese abschließend aufgezählten Kriterien erfüllt sind, handelt es sich um einen Betreiber wesentlicher Dienste. Dies war im Rahmen der in Art. 5 Abs. 1 NIS-Richtlinie vorgesehenen Ermittlung durch die Mitgliedstaaten bis zum 9.11.2018 vorgesehen. Betreiber von Testfeldern müssen folglich diese drei Kriterien erfüllen, damit es sich bei ihnen um Betreiber wesentlicher Dienste i.S. des Art. 4 Nr. 4 NIS-Richtlinie handelt. Dabei dürfte es schon am Merkmal der kritischen, gesellschaftlichen und / oder wirtschaftlichen Tätigkeit scheitern, sodass davon auszugehen ist, dass es sich bei Betreibern von Testfeldern nicht um Betreiber von wesentlichen Diensten i.S. des Art. 4 Nr. 4 NIS-Richtlinie handelt. Werden jetzige Testfelder in Zukunft anders genutzt und sind Teil einer notwendigen, intelligenten Infrastruktur, auf die das automatisierte und autonome sowie vernetzte Fahren aufbaut, so kann eine Beurteilung anders ausfallen. Dies ist insbesondere dann der Fall, wenn die Infrastruktur (ehemaliges Testfeld) gesellschaftlich relevant ist, da davon der Straßenverkehr abhängt. Damit muss zuvor allerdings eine andere Nutzungsart der Testfelder einhergehen. Erwächst ein Testfeldbetreiber zum Bereitsteller von Infrastruktur für den Straßenverkehr und hängt dessen Sicherheit und Funktionieren maßgeblich davon ab, rücken neben der Frage, ob es sich dann um den Betreiber eines wesentlichen Dienstes handelt, weitere rechtliche Fragestellungen und mögliche Anforderungen in den Mittelpunkt. Insofern sollte vor der Änderung der Nutzung überprüft werden, welche rechtlichen Konsequenzen dies für den Betreiber einer solchen Infrastruktur hat. Virulent können bei Fehlern sowie Hackerangriffen insbesondere haftungsrechtliche Fragestellungen werden.

In Art. 14 NIS-Richtlinie finden sich Sicherheitsanforderungen, die Betreiber wesentlicher Dienste erfüllen müssen, und Anforderungen zur Meldung von Sicherheitsvorfällen.
So müssen gem. Art. 14 Abs. 1 S. 1 NIS-Richtlinie die jeweiligen Mitgliedstaaten sicherstellen, dass die Betreiber von wesentlichen Diensten geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die für ihre Dienste eingesetzt werden, zu bewältigen. Nach S. 2 müssen die getroffenen Maßnahmen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das im Hinblick auf das existierende Risiko angemessen ist.[40] Durch diesen Verweis auf den Stand der Technik wird die Rechtsprechung zu den jeweiligen Sicherheitsniveaus relevant. Zudem sollen die Mitgliedstaaten sicherstellen, dass Auswirkungen von Sicherheitsvorfällen so gering wie möglich sind, Art. 14 Abs. 2 NIS-Richtlinie. Kommt es zu einem Sicherheitsvorfall, so muss der Betreiber des wesentlichen Dienstes gem. Art. 14 Abs. 3 NIS-Richtlinie der zuständigen Behörde oder dem sog. Computer Security Incident Response Teams (CSIRT)

[40] Zum Umgang mit Risiken im Recht und der Technikregulierung *Steege*, NZV 2022, 257.

Sicherheitsvorfälle mit erheblichen Auswirkungen auf die Verfügbarkeit der bereitgestellten wesentlichen Dienste unverzüglich melden.

Die nationale Umsetzung der NIS-Richtlinie findet sich in Deutschland im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG).[41]

d. Produktsicherheitsrecht

Die europäische Produktsicherheits-Richtlinie 2001/95/EG[42] wird in Deutschland im Produktsicherheitsgesetz (ProdSG) umgesetzt. Die Richtlinie ist anwendbar, sofern es sich um Produkte handelt, die zur Benutzung durch Verbraucher vorgesehen sind.[43] Eine Anwendbarkeit ist aber auch dann gegeben, wenn vernünftigerweise zu erwarten ist, dass das Produkt von Verbrauchern benutzt werden kann (Art. 2 lit. a Richtlinie 2001/95/EG).

Die Benutzung von Testfeldern erfolgt indes nicht durch Verbraucher, sondern durch Unternehmen. Hinzu kommt, dass es sich nicht um ein einzelnes Produkt handelt, dass genutzt wird, sondern dass von Unternehmen einzelne Funktionen, wie etwa Sensorik, oder eine vernetzte Infrastruktur zu Testzwecken genutzt werden darf.

e. Vertragsrecht, Kaufrecht und Verbraucherschutzrecht

Vertragliche Anforderungen an Produkte finden sich im Rahmen der Warenkauf-Richtlinie (EU) 2019/771[44] sowie der Digitale-Inhalte-Richtlinie 2019/770.[45] Im Unterschied zu Verordnungen müssen Richtlinien in nationales Recht umgesetzt werden, wobei ein gewisser Umsetzungsspielraum besteht. Die Digitale-Inhalte-Richtlinie wurde in den §§ 327 ff. BGB umgesetzt und die Warenkauf-Richtlinie in den §§ 434 ff. BGB.

Beide Richtlinien und ihre Umsetzungen im nationalen Recht erscheinen im Hinblick auf die Betreiber von Testfeldern nicht relevant.

Gemäß § 327 Abs. 1 BGB sind die §§ 327 ff. BGB (Umsetzung der Digitalen-Inhalte-Richtlinie) auf Verbraucherverträge anzuwenden, welche die Bereitstellung digitaler Inhalte oder digitaler Dienstleistungen durch den Unternehmer gegen Zahlung eines Preises zum Gegenstand haben. Bei vertraglichen Konstellationen im Zusammenhang mit der Nutzung von Testfeldern für autonome und vernetzte Mobilität fehlt es schon daran, dass der Nutzer des Testfelds ein Verbraucher ist, sodass kein Verbrauchervertrag vorliegt. Vielmehr handelt es sich um reine Business-to-Business Beziehungen. Selbst wenn dies anders wäre, würde die Eröffnung des Anwendungsbereichs daran scheitern, dass es sich bei der Nutzung von Testfeldern und der damit einhergehenden Verwendung von Sensoren, Messgeräten und

[41] Dazu untenstehend.
[42] Richtlinie 2001/95/EG des Europäischen Parlamentes und des Rates vom 3.12.2001 über die allgemeine Produktsicherheit, ABl. 2002 L 11, 4; sie ersetzt die erste Produktsicherheits-Richtlinie 92/59/EWG des Rates vom 29.6.1992, ABl. 1992 L 228, 24.
[43] *Langner/Klindt/Schucht*, in: Dauses/Ludwigs, Handbuch des EU-Wirtschaftsrechts, Stand: 58. EL April 2023, Rn. 60.
[44] Richtlinie (EU) 2019/771 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte des Warenkaufs, zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie 2009/22/EG sowie zur Aufhebung der Richtlinie 1999/44/EG.
[45] Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen.

Infrastruktur nicht um digitale Inhalte i.S. des § 327 Abs. 2 S. 1 BGB handelt. Beispiele für digitale Inhalte ergeben sich aus ErwG 19 Digitale-Inhalte-RL und sind etwa Computerprogramme, Apps, Videodateien, Musikdateien sowie digitale Spiele oder elektronische Bücher.[46] Es handelt sich zudem auch nicht um digitale Dienstleistungen, da die Voraussetzungen hierfür nicht erfüllt sind, da einem Verbraucher die Erstellung, Verarbeitung oder Speicherung von Daten in digitaler Form ermöglicht werden muss.[47]

Hinsichtlich der Warenkauf-Richtlinie fehlt es bei der Nutzung eines Testfelds und der Vertragsbeziehung zwischen Testfeldbetreiber und Nutzer schon an einem Kaufvertrag. Insofern sind auch diese Regelungen im Hinblick auf Testfelder zu vernachlässigen.

f. Kooperative intelligente Verkehrssysteme

Kooperative intelligente Verkehrssysteme (engl: Cooperative Intelligent Transport Systems, „C-ITS“) sind die Grundlage für die Kommunikation zwischen Kraftfahrzeugen und der Verkehrsinfrastruktur. Neben Gefahrenmeldungen, wie etwa Staus oder Gefahrenstellen, können die gesendeten Nachrichten auch Informationen zum Fahrzeugzustand enthalten. Möglich ist dieser Austausch zwischen dem Fahrzeug und der gesamten Infrastruktur wie bspw. Ampeln, Baustellen etc. Dieses Thema ist nicht nur auf europäischer Ebene, sondern auch national relevant.[48] Das BSI hat in diesem Zusammenhang die Technische Richtlinie BSI TR-03164 veröffentlicht und konkretisiert darin Vorgaben zu den Zertifikaten mit Blick auf den sicheren Betrieb von sog. Publik-Key Infrastrukturen (PKI). Enthalten sind neben einer harmonisierten Interpretationsgrundlage der relevanten Vorgaben Empfehlungen für die Umsetzung, sofern Ermessensspielräume bestehen.

Auf europäischer Ebene hat die Europäische Kommission am 30.11.2016 eine europäische Strategie zu kooperativen intelligenten Verkehrssystemen verabschiedet.[49]

3. Nationaler Rechtsrahmen

In Deutschland existiert kein zusammenhängendes Gesetz zur IT-Sicherheit i.S. einer Lex Cyber- und Informationssicherheitsrecht.[50] Vielmehr ist die IT-Sicherheit zerstückelt in zahlreichen Gesetzen geregelt und nimmt des Öfteren in der Praxis trotz der erheblichen Relevanz eine eher untergeordnete Rolle ein. Daran hat 2015 auch das IT-Sicherheitsgesetz nichts geändert.[51] Denn dadurch wurden bspw. das BSI-Gesetz (BSIG), das Atomgesetz (AtG), das Energiewirtschaftsgesetz (EnWG), das Telemediengesetz (TMG), das

[46] BeckOGK/*Fries*, 1.7.2023, BGB § 327 Rn. 8.
[47] BeckOGK/*Fries*, 1.7.2023, BGB § 327 Rn. 9.
[48] Siehe etwa diesbezügliche Informationen des BSI unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Automotive/Kooperative_Intelligente_Verkehrssysteme/Kooperative_Intelligente_Verkehrssysteme.html (zuletzt abgerufen am 8.11.2023).
[49] Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Eine europäische Strategie für Kooperative Intelligente Verkehrssysteme – ein Meilenstein auf dem Weg zu einer kooperativen, vernetzten und automatisierten Mobilität, vom 30.11.2016, COM(2016) 766 final.
[50] *Wagner*, Das neue Mobilitätsrecht, 2021, S. 194.
[51] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015, BGBl I. S. 1324.

Telekommunikationsgesetz (TKG), das Bundeskriminalamtsgesetz (BKAG) und weitere geändert. Dieser Umstand wird auch nicht durch das IT-Sicherheitsgesetz 2.0 geändert.[52]

a. Betreiber kritischer Infrastrukturen i.S. des BSIG

Die europäische NIS-Richtlinie wurde national im BSIG umgesetzt. Allerdings handelt es sich nicht um eine Verordnung, sondern um eine Richtlinie, sodass die Mitgliedstaaten die NIS-Richtlinie mit einem gewissen Spielraum umsetzen können. Insofern ist die rechtliche Bewertung, ob Testfeldbetreiber gleichzeitig Betreiber einer kritischen Infrastruktur sind, analog zur obigen Betrachtung im Zusammenhang mit der NIS-Richtlinie. Gleichwohl soll kurz auf den nationalen Rechtsrahmen eingegangen werden.

Mit Blick auf die Sicherheit kritischer Infrastrukturen in der Informationstechnik ist § 8a BSIG relevant. Nach § 8a Abs. 1 BSIG müssen Betreiber von kritischen Infrastrukturen angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden.[53]

In § 8a Abs. 1 BSIG findet sich zudem die Antwort auf die Frage, wann die organisatorischen und technischen Maßnahmen angemessen sind. Dies ist dann der Fall, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Infrastruktur steht. Ob Betreiber von Testfeldern diese Vorkehrungen treffen müssen, hängt davon ab, ob sie mit ihrem Testfeld Betreiber einer kritischen Infrastruktur sind.

§ 2 Abs. 10 BSIG regelt, wann es sich um kritische Infrastrukturen i.S. des BSIG handelt. Dies sind Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören und (kumulativ) von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. In dieser abschließenden Auflistung sind in § 2 Abs. 10 Nr. 1 BSIG auch Transport und Verkehr genannt. Allerdings kann nicht jede Anlage im Bereich Transport und Verkehr eine kritische Infrastruktur darstellen.

Um zu bestimmen, wann eine kritische Infrastruktur im Bereich Transport und Verkehr vorliegt, wurde die KritisV veröffentlicht.[54] In § 8 KritisV ist geregelt, wann eine kritische Infrastruktur im Kontext von Transport und Verkehr vorliegt. Beim Personen- und Güterverkehr handelt es sich gem. § 8 Abs. 1 KritisV aufgrund seiner besonderen Bedeutung für das Funktionieren des Gemeinwesens hinsichtlich der Versorgung der Allgemeinheit mit Leistungen zum Transport von Personen und Gütern um eine kritische Dienstleistung i.S. des

[52] Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) vom 18. Mai 2021, BGBl I. S. 1122.
[53] Strenger sind Anforderungen, die die Einhaltung des Stands von Wissenschaft und Technik verlangen. Hierzu im Rahmen der Produktentwicklung *Steege*, in: Automatisierte Systeme, Buck-Heeb/Oppermann (Hrsg.), 2022, Kap. 3.11 Rn. 70 f.
[54] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) vom 22. April 2016 (BGBl I. S. 958).

§ 10 Abs. 1 S. 1 BSIG. Bei Testfeldern handelt es sich derzeit nicht um einen unmittelbaren Bestandteil des Personen- und Güterverkehrs noch um einen mittelbaren. Insofern handelt es sich bei Testfeldbetreibern nicht um Betreiber einer kritischen Dienstleistung i.S. des § 10 Abs. 1 S. 1 BSIG. Allerdings könnte es sich um eine kritische Infrastruktur handeln, da die Testfelder mit ihren intelligenten Sensoren einen Teil der Straßenverkehrsinfrastruktur darstellen. Wann eine kritische Infrastruktur im Bereich Transport und Verkehr vorliegt, richtet sich nach § 8 Abs. 3 KritisV. Danach müssen die Anlagen den in Anhang 7 Teil 3 Spalte B genannten Kategorien zugeordnet sein und (kumulativ) den Schwellenwert nach Anhang 7 Teil 3 Spalte D erreichen oder überschreiten.

Anhang 7 Teil 3 Spalte B der KritisV nennt unter Ziffer 1.4 den Straßenverkehr. Dazu zählen gem. Ziffer 1.4.1 Verkehrssteuerungs- und Leitsysteme. Hierzu zählen Testfelder allerdings nicht, solange ihr Zweck nicht geändert wird. Ziffer 1.4.2 nennt Verkehrssteuerungs- und Leitsysteme im kommunalen Straßenverkehr. Hierzu zählen Testfelder ebenfalls nicht. Letztlich nennt Ziffer 1.4.3 noch intelligente Verkehrssysteme. Auch hierzu zählen Testfelder nicht. Selbst wenn der Zweck von Testfeldern umgewidmet wird und sie unter die soeben genannten Systeme subsumiert werden, müssen die in Anhang 7 Teil 3 Spalte D KritisV genannten Schwellenwerte erreicht oder überschritten werden. Systeme i.S. der Ziffer 1.4.1 müssen danach auf der Bundesautobahn errichtet sein. Systeme nach Ziffer 1.4.2 müssen 500.000 Einwohner pro Stadt versorgen und intelligente Verkehrssysteme i.S. der Ziffer 1.4.3 müssen 500.000 angeschlossene Nutzer oder durchschnittlich im Versorgungsgebiet versorgte Nutzer umfassen. In Ziffer 1.5 ist der ÖPNV genannt. Erfasst sind nach Ziffer 1.5.1 Schienennetze und Stellwerke des öffentlichen Straßenpersonenverkehrs (ÖSPV) sowie nach Ziffer 1.5.2 die Leitzentrale des ÖSPV. Die Schwellenwerte liegen hier bei 125.000.000 unternehmensbezogenen Fahrgastfahrten pro Jahr. Auch hierzu zählen Testfelder nicht. Testfelder werden in Anhang 7 Teil 3 Spalte A KritisV nicht genannt. Folglich handelt es sich dabei nicht um eine kritische Infrastruktur im Kontext von Transport und Verkehr. Hierfür bedarf es einer Zweckänderung und einer relevanten Rolle, sodass die geforderten Schwellenwerte erreicht werden.

Auch nach nationalem Recht handelt es sich – wenig überraschend – bei Testfeldern nicht um kritische Infrastrukturen. Dies kann sich in Zukunft allerdings je nach konkreter Ausgestaltung der Testfelder ändern, da die rechtliche Bewertung von den faktischen Umständen abhängt. Sobald dies der Fall sein sollte, müssten Testfelder zahlreiche Anforderungen erfüllen, welche vom BSI überprüft werden können. Gleichwohl wären die Regelungen nicht unmittelbar auf das automatisierte und autonome Fahren anwendbar.[55]

b. Produktsicherheitsrecht

Für Produkte von besonderer Relevanz ist das Produktsicherheitsgesetz (ProdSG),[56] welches Anforderungen an deren Sicherheit stellt. Der Anwendungsbereich des ProdSG erfasst gem. § 1 Abs. 1 ProdSG Produkte, wenn sie im Rahmen einer Geschäftstätigkeit auf dem Markt bereitgestellt, ausgestellt oder erstmals verwendet werden. Ausnahmen finden sich in § 1 Abs. 2, 3 ProdSG. Behördliche Befugnisse waren in § 26 Abs. 2 ProdSG aF vorgesehen. Nunmehr ermächtigt § 8 ProdSG, dass Rechtsverordnungen bspw. die Beschaffenheit von Produkten,

[55] *Wagner*, Das neue Mobilitätsrecht, 2021, S. 195; *Ensthaler/Gollrad*, Rechtsgrundlagen des automatisierten Fahrens, 2019, S. 155.
[56] Gesetz über die Bereitstellung von Produkten auf dem Markt (Produktsicherheitsgesetz – ProdSG) vom 8. November 2011 (BGBl. I S. 2178, 2179; 2012 I S: 131.

deren Kennzeichnung oder deren Ausstellung regeln können. Mittlerweile existieren zahlreiche Verordnungen zum ProdSG.[57] Die zuständigen Marktüberwachungsbehörden können zahlreiche Maßnahmen treffen. Für Fahrzeuge ist das Kraftfahrt-Bundesamt die zuständige Marktüberwachungsbehörde. In diesem Zusammenhang sind zahlreiche nationale sowie europäische Rechtsquellen relevant.

c. Haftungsrecht

Anforderungen an die Sicherheit von Systemen und den Schutz von Daten folgen auch aus dem Haftungsrecht, insbesondere aus der Produkt- und Produzentenhaftung. Aufgrund der Relevanz wird die Produkt- und Produzentenhaftung gesondert betrachtet.[58]

IV. Hoch- und vollautomatisiertes Fahren

Rechtliche Anforderungen an hoch- und vollautomatisierte Fahrfunktionen existieren in Deutschland seit 2017. Am 21.6.2017 ist das Achte Gesetz zur Änderung des Straßenverkehrsgesetzes in Kraft getreten. In den §§ 1a ff. StVG ist seither das hoch- und vollautomatisierte Fahren geregelt.[59] Wenngleich die verwendeten Begrifflichkeiten vermuten lassen, dass damit die SAE J3016 Stufen 3 und 4 geregelt sind, so ist lediglich Stufe 3 erfasst.[60]

1. Anforderungen an den Betrieb von Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion

§ 1a StVG enthält Anforderungen an den Betrieb von Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion. Nach § 1a Abs. 1 StVG ist der Betrieb eines Kraftfahrzeugs mit hoch- und vollautomatisierter Fahrfunktion zulässig, sofern eine bestimmungsgemäße Verwendung vorliegt. Wann dies der Fall ist, konkretisiert § 1a StVG nicht. Vielmehr obliegt es jedem einzelnen Hersteller für seine Kraftfahrzeuge in seiner Systembeschreibung zu definieren, wann eine bestimmungsgemäße Verwendung vorliegt. Für Fahrzeugführer bedeutet dies, dass sich ihre Sorgfaltspflichten und somit ihre Haftung nach der Systembeschreibung richten. Die eingehende Lektüre der Systembeschreibung vor Fahrtantritt ist notwendig.

§ 1a Abs. 2 StVG enthält Anforderungen an die technische Ausrüstung der Fahrfunktion. Diese muss die Fahraufgabe (einschließlich Längs- und Querführung) wahrnehmen können. Zudem muss sie die an die Fahrzeugführung gerichteten Verkehrsvorschriften einhalten und vom Fahrzeugführer jederzeit manuell übersteuert und deaktiviert werden können. Darüber hinaus muss die Fahrfunktion erkennen können, wann es notwendig ist, dass der Fahrzeugführer die Steuerung übernimmt, und sie muss in der Lage sein, mit ausreichend Zeitreserve die Notwendigkeit der Steuerungsübernahme anzuzeigen. Letztlich muss auf eine unzulässige Verwendung hingewiesen werden.

Der Hersteller muss gem. § 1a Abs. 2 S. 1 StVG in der Systembeschreibung verbindlich erklären, dass die Fahrfunktion die Anforderungen des § 1a Abs. 2 S. 1 StVG erfüllt.

---

[57] Ein Überblick findet sich bei NK-ProdR/*Ludger Giesberts/Michael Gayger*, 1. Aufl. 2022, ProdSG § 8 Rn. 19-76.
[58] Siehe hierzu untenstehend.
[59] *Steege*, PHi 2021, 210, 215.
[60] Eingehend zu den Stufen des automatisierten Fahrens und den im StVG verwendeten Begriffen *Steege*, Automatisierte Rechtsanwendung, 2022, S. 46-50.

2. Rechte und Pflichten des Fahrzeugführers bei Nutzung einer hoch- oder vollautomatisierten Fahrfunktion

In § 1b StVG finden sich sodann Rechte und Pflichten des Fahrzeugführers bei Nutzung einer hoch- oder vollautomatisierten Fahrfunktion. So darf sich der Fahrzeugführer vom Verkehrsgeschehen und der Fahrzeugsteuerung abwenden. Gleichzeitig muss er in einer solchen Art und Weise wahrnehmungsbereit sein, dass er seine Pflicht zur Übernahme der Fahrzeugsteuerung nach § 1b Abs. 2 StVG jederzeit erfüllen kann.[61]

Sowohl § 1a als auch § 1b StVG enthalten keinerlei Anforderungen an den Schutz von Daten vor Angriffen auf das Fahrzeug.

3. Datenverarbeitung beim hoch- oder vollautomatisierten Fahren

Mit § 63a StVG wurde eine Vorschrift zur Datenverarbeitung beim hoch- oder vollautomatisierten Fahren eingefügt.[62] § 63a Abs. 1 StVG schreibt vor, dass bei einem Wechsel der Fahrzeugsteuerung zwischen Fahrzeugführer und Fahrfunktion die Positions- und Zeitangaben gespeichert werden. Diese Daten sollen zudem gespeichert werden, wenn die Fahrfunktion den Menschen auffordert, die Steuerung zu übernehmen sowie in Fällen einer technischen Systemstörung.[63] In den weiteren Absätzen ist etwa die Datenweitergabe an Behörden sowie zum Zwecke der Forschung im Rahmen der Unfallforschung geregelt.[64]

Regelungen zum Schutz von Daten vor Hackerangriffen sowie generell Anforderungen an die Sicherheit der Systeme enthält § 63a StVG nicht.

Gleichwohl trifft den Hersteller eines Fahrzeugs die Pflicht, das Fahrzeug derart zu konstruieren, dass die Anforderungen nach § 63a StVG erfüllt werden. Dies betrifft beispielsweise die Speicherdauer der Daten.

Die Anforderungen in § 63a StVG richten sich an den Hersteller eines Fahrzeugs mit hoch- oder vollautomatisierter Fahrfunktion sowie den Fahrzeughalter und Behörden. Betreiber von Testfeldern sind nicht Adressat der Regelung. Aus § 63a StVG lassen sich daher auch keine Anforderungen an die Datenverarbeitung im Zusammenhang mit Testfeldern entnehmen. Ebenso wenig kommt § 63a StVG als gesetzliche Verpflichtung – also als Erlaubnistatbestand – i.S. des Art. 6 Abs. 1 lit. c DS-GVO in Betracht.

4. Zwischenergebnis

Anforderungen an den Schutz von Daten, an die Sicherheit der Systeme sowie allgemeine Pflichten zum Schutz vor Hackerangriffen existieren in den Vorschriften zum hoch- und vollautomatisierten Fahren im Straßenverkehrsgesetz nicht. Der Gesetzgeber hat dahingehend keinerlei Regelungen getroffen.

---

[61] *Steege*, PHi 2021, 210, 215.
[62] Für autonome Fahrzeuge i.S. des § 1d StVG ist § 1g StVG lex specialis. Dazu *Steege*, SVR 2021, 128, 134.
[63] *Steege*, PHi 2021, 210, 217.
[64] *Stender-Vorwachs/Steege*, in: Oppermann/Stender-Vorwachs (Hrsg.), Autonomes Fahren, 2020, Kap. 3.6.1, S. 414-423.

Die Anforderungen richten sich an den Automobilhersteller und den Fahrzeugführer. Betreiber von Testfeldern sind keine Adressaten dieser Regelungen. Regelungen, die sich auf den Betrieb von Testfeldern beziehen, existieren nicht. Betreiber von Testfeldern sind höchstwahrscheinlich nicht personenidentisch mit den Adressaten der §§ 1a ff. StVG, da sie dafür zugleich Automobilhersteller oder Fahrzeugführer (natürliche Person) sein müssten.

V. Autonomes Fahren

Deutschland hat 2021 mit den neu eingefügten §§ 1d ff. StVG[65] einen Rechtsrahmen für das sog. autonome Fahren (§ 1d Abs. 1 StVG) geschaffen.[66] Die neuen Vorschriften betreffen zahlreiche Aspekte und reichen von der Datenspeicherung bis hin zu Pflichten der Beteiligten. Adressaten der Vorschriften sind primär Automobilhersteller, Betreiber der Fahrzeuge, involvierte Behörden sowie die Technische Aufsicht. Betreiber von Testfeldern werden nicht adressiert. Diese können nur dann betroffen sein, wenn sie etwa ein Fahrzeug mit autonomer Fahrfunktion betreiben.

1. Anwendungsbereich

Wenngleich der Wortlaut des § 1d Abs. 1 StVG von autonomer Fahrfunktion spricht, ist nicht das autonome Fahren i.S. der Stufe 5 SAE J3016 gemeint, sondern Stufe 4. Diese Terminologie ist misslich.[67]

2. Testfelder als festgelegter Betriebsbereich

Für Betreiber von Testfeldern relevant ist der festgelegte Betriebsbereich, welcher in § 1d Abs. 2 StVG legaldefiniert ist: „Ein festgelegter Betriebsbereich im Sinne dieses Gesetzes bezeichnet den örtlich und räumlich bestimmten öffentlichen Straßenraum, in dem ein Kraftfahrzeug mit autonomer Fahrfunktion bei Vorliegen der Voraussetzungen gemäß § 1e Absatz 1 betrieben werden darf."

Auch Testfelder können sowohl im Rahmen der Erprobung von autonomen Fahrfunktionen einen späteren regulären Betriebsbereich simulieren, bspw. wenn es sich um einen räumlich abgetrennten Bereich handelt, als auch im Regelbetrieb einen festgelegten Betriebsbereich i.S. des § 1d Abs. 2 StVG darstellen. Zu beachten ist allerdings, dass das Testfeld geografische Voraussetzungen erfüllt. Damit kommt es insbesondere auf die Größe des Testfelds an.

Anforderungen an die Datensicherheit oder den Datenschutz enthält § 1d Abs. 2 StVG nicht.

3. Erprobung von automatisierten und autonomen Fahrfunktionen

Die Erprobung von automatisierten und autonomen Fahrfunktionen ist in § 1i StVG geregelt. Diese Vorschrift betrifft allerdings primär den Halter, da gem. § 1i Abs. 2 StVG die Erprobungsgenehmigung vom Kraftfahrt-Bundesamt auf Antrag des Halters erteilt wird. Betreiber von Testfeldern können folglich nur dann Normadressat sein, wenn sie als Halter

[65] BGBl. Teil I, S. 3108.
[66] Eingehend zum Gesetzesentwurf *Steege*, SVR 2022, 161 ff. und zum finalen Gesetz *Steege*, PHi 5-6/2021, 210 ff.; 1/2022, 18 ff.
[67] Ausführlich zur sprachlichen Verwirrung und den Auswirkungen *Steege*, SVR 2021, 128, 130.

eines Fahrzeugs mit automatisierter oder autonomer Fahrfunktion eine Erprobungsgenehmigung nach § 1i Abs. 1 Nr. 1 beantragen.

In § 1i StVG ist die Rede von automatisierten und autonomen Fahrfunktionen. Autonome Fahrfunktionen meint eindeutig solche i.S. von § 1d Abs. 1 StVG. Unklar ist allerdings, worauf sich der Begriff automatisierte Fahrfunktionen bezieht. Erfasst sein könnten davon auch hoch- und vollautomatisierte Fahrfunktionen i.S. von § 1a StVG. Hiergegen spricht jedoch die systematische Stellung des § 1i StVG. Automatisiert ist allerdings der übergeordnete Begriff, sodass davon sämtliche Automatisierungsstufen umfasst sein könnten.[68] Dies wirkt sich unmittelbar im Rahmen des Genehmigungsprozesses aus, da unmittelbar die Zuständigkeit des Kraftfahrt-Bundesamtes tangiert ist. Amtshaftungsansprüche sind aufgrund der Erteilung der Erprobungsgenehmigung durch das Kraftfahrt-Bundesamt denkbar.[69]

VI. Autonome-Fahrzeuge-Genehmigungs- und Betriebs-Verordnung (AFGBV)

Zur Konkretisierung des Rechtsrahmens zum autonomen Fahren durch die §§ 1d ff. StVG hat der Gesetzgeber 2022 die „Verordnung zur Genehmigung und zum Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen (Autonome-Fahrzeuge-Genehmigungs- und-Betriebs-Verordnung – AFGBV)“ erlassen.[70]

Der Regelungsgehalt der AFGBV umfasst gem. § 1 Abs. 2:

- zunächst die Erteilung von Betriebserlaubnissen für Kraftfahrzeuge mit autonomer Fahrfunktion i.S. des § 1d StVG sowie von Genehmigungen für nachträglich aktivierbare automatisierte und autonome Fahrfunktionen,
- die Genehmigung festgelegter Betriebsbereiche,
- die Zulassung von Kraftfahrzeugen mit autonomer Fahrfunktion zum Straßenverkehr,
- die Marktüberwachung von Kraftfahrzeugen mit autonomer Fahrfunktion mit aufgrund der AFGBV erteilter oder zu erteilender Betriebserlaubnisse sowie von nachträglich aktivierten automatisierten und autonomen Fahrfunktionen und Fahrzeugteilen und
- die Anforderungen an und Pflichten für den Hersteller, den Halter und die Technische Aufsicht von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen und von Kraftfahrzeugen mit automatisierter oder autonomer Fahrfunktion nach § 1f des Straßenverkehrsgesetzes.

Betreiber von Testfeldern zur Erforschung autonomer Fahrfunktionen sind somit nicht im Fokus des Regelungsgehalts der AFGBV.

VII. Teleoperiertes Fahren

[68] Dazu *Steege*, PHi 1/2022, 18, 26 f. Zur möglichen Amtshaftung durch eine Landesbehörde bei Erteilung der Erprobungsgenehmigung anstelle des Kraftfahrt-Bundesamtes i.S. des § 1i StVG *Porsch/Moench*, Gutachten zur Frage der Zuständigkeit für die Erteilung von Erprobungsgenehmigungen für die Entwicklung automatisierter und autonomer Fahrfunktionen und zu möglichen haftungsrechtlichen Konsequenzen bei der Erteilung der Erprobungsgenehmigungen durch das Land, vom 4.5.2023, unveröffentlicht.
[69] Umfassend zur Amtshaftung NK-BGB/*Steege/Muthers*, 4. Aufl., § 839 BGB.
[70] BGBl. I S. 986.

Gesetzliche Regelungen zum sog. teleoperierten Fahren existieren in Deutschland nicht.[71] Folglich gibt es keinerlei spezielle Regelungen, die die Cybersicherheit von teleoperierten Fahrzeugen sowie die Datenverarbeitung adressieren. Dies führt sowohl für Automobilhersteller als auch für Betreiber von teleoperierten Fahrzeugen und Betreibern von Testfeldern zu Herausforderungen.

VIII. Datenschutzrecht – DS-GVO

Je nach Art der Daten können Anforderungen aus dem Datenschutz auch die Sicherheit der Daten umfassen.
Zu unterscheiden ist zunächst zwischen personenbezogenen Daten i.S. des Art. 4 Nr. 1 DS-GVO und neutralen, technischen Daten.[72] Erstere unterfallen dem Anwendungsbereich der Datenschutz-Grundverordnung (DS-GVO)[73] bzw. dem Bundesdatenschutzgesetz (BDSG).[74] Neutrale Daten fallen im Umkehrschluss nicht in den Anwendungsbereich der DS-GVO, sodass die dortigen Maßnahmen und Anforderungen für sie nicht gelten.

1. Anwendungsbereich – personenbezogene Daten

Da nur personenbezogene Daten in den Anwendungsbereich der DS-GVO fallen, ist die Definition von personenbezogenen Daten in der Praxis äußerst relevant. Gemäß Art. 4 Nr. 1 DS-GVO sind „‘personenbezogene Daten‘ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“.

Entscheidend ist hierbei die Identifizierbarkeit. Umfasst sind ausgehend vom Wortlaut sowohl „identifizierte“ als auch „identifizierbare“ natürliche Personen.[75] Juristische Personen sind vom Schutzbereich der DS-GVO nicht umfasst. Die Informationen müssen sich vielmehr auf eine natürliche Person beziehen. Gegen eine Anwendbarkeit auf juristische Personen spricht ausdrücklich Erwägungsgrund 14 DS-GVO. Insofern handelt es sich bei dem Dritten als Unternehmen, der das Testfeld nutzt, nicht um eine betroffene Person. Bei Testfahrten im Rahmen der Nutzung von Testfeldern ist die betroffene Person in der Regel der Testfahrer. Dies kann bspw. dann der Fall sein, wenn er von einer Innenraumkamera aufgenommen wird. Erfasst das Fahrzeug mittels Kamera oder anderer Sensoren die Fahrzeugumgebung, so sind die in diesem Kontext erfassten Personen die jeweils betroffene Person. Bei wem es sich um die betroffene Person handelt, wirkt sich auch im Rahmen der Rechtmäßigkeit der Datenverarbeitung aus.

[71] *Hartmann/Seebach/Walter*, SVR 2023, 169, 175.
[72] *Stender-Vorwachs/Steege*, NJOZ 2018, 1361, 1362.
[73] Verordnung Nr. 2016/679 des Europäischen Parlaments und Rates vom 27.4.2016, in Kraft getreten am 25.5.2018.
[74] Artikel 1 des Gesetzes vom 30.06.2017 (BGBl. I S. 2097), in Kraft getreten am 25.05.2018.
[75] *Steege*, PHi 4-5/2022, 164, 166.

Die Definition des personenbezogenen Datums ist sehr weit gefasst,[76] da es ausreichend ist, wenn die natürliche Person identifizierbar ist. Dadurch ist es ausreichend, wenn die betroffene Person mittels Kombination mit weiteren Daten identifizierbar ist.[77] Zur Abgrenzung, ob personenbezogene Daten vorliegen oder nicht, kommt es folglich maßgeblich auf das Verständnis vom Personenbezug an. Unterschieden wird zwischen einem relativen und absoluten Personenbezug.[78]

Die Rechtsprechung neigt dazu, einen sehr weiten Personenbezug anzunehmen.[79] So führt der EuGH aus: „Wie der Gerichtshof bereits festgestellt hat, ist der Anwendungsbereich der RL 95/46 sehr weit und […] die von ihr erfassten personenbezogenen Daten vielfältig […]".[80] Bereits das Bundesverfassungsgericht stellte fest, dass die umfassenden Verarbeitungs- und Verknüpfungsmöglichkeiten von Daten dazu führen, dass es kaum Daten ohne Personenbezug gibt.[81] Auch dem Europäischen Gerichtshof lässt sich ein weites Verständnis des Begriffs „personenbezogene Daten" entnehmen. So führte er aus: „Wie der Gerichtshof bereits festgestellt hat, ist der Anwendungsbereich der RL 95/46 sehr weit und […] die von ihr erfassten personenbezogenen Daten vielfältig […]".[82] Allerdings lässt sich in jüngster Rechtsprechung des Europäischen Gerichts erkennen, dass es verstärkt darauf ankommen soll, ob weitere Daten, die zu einem Personenbezug führen, für den Verantwortlichen zugänglich sind oder nicht. Dies spricht gegen einen absoluten und für einen relativen Personenbezug, bei dem es maßgeblich darauf ankommt, ob der Verantwortliche an zusätzliche Daten gelangt und wie schwer dies ist. Ob ein Personenbezug vorliegt oder nicht hängt jedoch maßgeblich vom Einzelfall ab.

Im Kontext von Testfeldern autonomer Mobilität sind daher je nach Ausgestaltung des Testfelds und der übermittelten Daten zahlreiche personenbezogene Daten denkbar. Für Betreiber der Testfelder ist es daher unerlässlich bei der Planung der Dienstleistungen zu prüfen, welche datenschutzrechtliche Rolle der Testfeldbetreiber einnimmt und ob die daraus resultierenden Anforderungen umgesetzt werden können. Eine Pauschalisierung ist nicht möglich, sodass einzelfallabhängig im jeweiligen Projekt bzw. ausgehend von der jeweiligen Dienstleistung zu prüfen ist, ob personenbezogene Daten generiert werden und welche datenschutzrechtlichen Konsequenzen daraus folgen.

Exemplarisch seien einige personenbezogene Daten im Rahmen von Testfeldern genannt:
- Vor- und Nachname
- Berufliche Kontaktdaten wie E-Mail-Adresse und Telefonnummer
- Audio- und Videoaufzeichnungen von Testfahrern
- Audio- und Videoaufzeichnungen von Straßenverkehrsteilnehmern mit Zeitstempel und / oder Geoinformationen wie GPS-Positionsdaten[83]
- Kfz-Kennzeichen[84]
- Cookies

---

[76] Paal/Pauly/*Ernst*, 3. Aufl. 2021, DS-GVO Art. 4 Rn. 3; *Steege*, PHi 4-5/2022, 164, 166.
[77] *Steege*, PHi 4-5/2022, 164, 166.
[78] *Steege*, PHi 4-5/2022, 164, 166.
[79] *Steege*, PHi 4-5/2022, 164, 166.
[80] EuGH, NJW 2018, 767 Rn. 33. Zwar bezieht sich dieses Postulat auf die der DS-GVO vorangegangene Richtlinie, allerdings wurde die Definition des personenbezogenen Datums inhaltlich nicht geändert.
[81] BVerfGE 65, 1, Rn. 176 = NJW 1984, 419.
[82] EuGH, NJW 2018, 767 Rn. 33. Das Urteil bezieht sich auf die vorherige Datenschutzrichtlinie, allerdings hat sich die Definition des personenbezogenen Datums in der DS-GVO nicht geändert.
[83] EuGH, NJW 2015, 463 Rn. 22.
[84] OVG Münster, NVwZ 2018, 742; *v. Schönfeld*, DAR 2015, 617, 619.

- (dynamische) IP-Adresse[85]
- Fahrzeug-Identifikationsnummer (FIN)
- Anschrift von Testfahrern
- Log-Files[86]
- elektronische Zertifikate
- GPS-Daten zur Ortung eines Firmenwagens[87]

2. Datenschutzrechtliche Rolle des Testfeldbetreibers (Verantwortlicher oder Auftragsverarbeiter)

Adressat der zahlreichen Pflichten aus der DS-GVO ist der Verantwortliche im datenschutzrechtlichen Sinne. Aber auch den Auftragsverarbeiter treffen Pflichten im Umgang mit der Datenverarbeitung. Die Unterscheidung dieser beiden Rollen ist zur Bestimmung der Pflichten essenziell.

a. Verantwortlicher

Eine Legaldefinition findet sich in Art. 4 Nr. 7 DS-GVO: „‘Verantwortlicher‘ [meint] 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; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.“

Verantwortlicher i.S. der DS-GVO ist folglich derjenige, der über Zweck und Mittel der Datenverarbeitung entscheidet.

b. Auftragsverarbeiter

Wird nicht über die Zwecke und Mittel der Datenverarbeitung entschieden, sondern erfolgt lediglich – weisungsgebunden – eine Auftragsdatenverarbeitung, so ist die datenschutzrechtliche Rolle die des Auftragsverarbeiters. Der Auftragsverarbeiter ist in Art. 4 Nr. 8 DS-GVO legaldefiniert.
Dies ist „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“.

Konkrete Anforderungen an den Auftragsverarbeiter sind in Art. 28 DS-GVO geregelt.

c. Bedeutung für Testfelder

Bei Testfeldern kommt es mithin darauf an, wer über Zweck und Mittel der Datenverarbeitung entscheidet. So kann der Betreiber eines Testfelds Verantwortlicher sein, wenn er darüber entscheidet, zu welchem Zweck welche Daten aus den Fahrzeugen ausgeleitet werden und wie diese sodann verarbeitet werden. Insgesamt sind jedoch mehrere Konstellationen denkbar. Zu

[85] EuGH, GRUR 2012, 265.
[86] Dazu *Steege*, MMR 2019, 509, 510.
[87] VG Lüneburg, ZD 2019, 331.

beachten ist jedoch stets, dass sich mit jeder neuen Datenverarbeitung auch die datenschutzrechtliche Rolle ändern kann. Dies bedeutet, dass der Betreiber eines Testfeldes in dem einen Fall lediglich Auftragsverarbeiter ist und ein Dritter, der Tests durchführt, Verantwortlicher ist und im nächsten Fall der Betreiber des Testfeldes selbstständig Tests durchführt und daher Verantwortlicher ist.

Können Dritte Testfelder zum Testen ihrer Fahrzeuge und Fahrfunktionen nutzen und entscheiden diese allein über Zweck und Mittel der Datenverarbeitung, so sind diese Verantwortliche i.S. des Art. 4 Nr. 7 DS-GVO. Verarbeitet der Testfeldbetreiber personenbezogene Daten lediglich weisungsgebunden für Dritte, so ist der Testfeldbetreiber lediglich Auftragsverarbeiter i.S. des Art. 4 Nr. 8 DS-GVO.[88]

Entscheiden Dritte und Testfeldbetreiber jedoch gemeinsam über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten, so liegt eine gemeinsame Verantwortlichkeit i.S. des Art. 26 Abs. 1 DS-GVO vor. Dies kann auch im Rahmen von gemeinsamen Forschungsprojekten der Fall sein, bei denen der Testfeldbetreiber Konsortialpartner ist.

Letztlich ist auch eine getrennte Verantwortlichkeit denkbar, wenn Betreiber des Testfelds und Dritte getrennt über Zwecke und Mittel der Datenverarbeitung entscheiden. Entscheidend ist dabei, dass nicht gemeinsam über Mittel und Zwecke der Verarbeitung entschieden wird.[89] Daran ändert es auch nichts, wenn Dritter und Betreiber des Testfelds die Daten unabhängig voneinander in einem System speichern. Dies ist beispielsweise denkbar, wenn der Betreiber des Testfelds aus eigenen Interessen Systemdaten verarbeitet, die für den Dritten uninteressant sind.

d. Bedeutung für Betreiber von Testfeldern

Bei der Beurteilung der datenschutzrechtlichen Rolle des Testfeldbetreibers kommt es maßgeblich auf die konkrete Ausgestaltung der Nutzung des Testfelds an. Dabei ist zu berücksichtigen, wer über Zweck und Mittel der Datenverarbeitung entscheidet. Die datenschutzrechtliche Rolle ist keinesfalls starr, sondern kann sich von Testbetrieb zu Testbetrieb ändern, wenn damit auch eine Änderung in den Umständen der Datenverarbeitung einhergeht. Dies bedeutet, dass sich die Rolle auch bei ein und demselben Dritten ändern kann. Das ist dann der Fall, wenn der Betreiber eines Testfeldes einmal selbst über die zu erhebenden Daten und deren Verarbeitung entscheidet und beim anderen Mal der Dritte zusammen mit dem Betreiber des Testfelds, etwa im Rahmen eines Forschungsprojekts. Führt der Testfeldbetreiber selbst Tests durch und entscheidet er über den Umfang der Datenverarbeitung, so ist er Verantwortlicher. Setzt er zur Datenverarbeitung – etwa zur Auswertung – einen Dienstleister ein, der weisungsgebunden agiert, so ist dieser Auftragsverarbeiter. Umgekehrt kann der Testfeldbetreiber Auftragsverarbeiter sein, wenn der Dritte über Zweck und Mittel der Datenverarbeitung entscheidet und der Betreiber des Testfelds lediglich innerhalb der Weisungen des Dritten agiert. Verarbeitet der Testfeldbetreiber aus eigenem Interesse eigenständig anfallende Daten aus den Systemen und Tests, so kann eine getrennte Verantwortlichkeit vorliegen. Wird ein Testfeld in unterschiedlichen Konstellationen genutzt und unterscheiden sich die Rollen der beteiligten Akteure, so sollte vor jedem Testbetrieb überprüft werden, welche datenschutzrechtlichen Rollen die Beteiligten haben und welches entsprechende Datenschutzkonzept angewendet werden muss.

[88] Zu den Auswirkungen sogleich unter Bedeutung für Betreiber von Testfeldern.
[89] *Jung/Hansch*, ZD 2019, 143, 144.

Die Frage, wer Verantwortlicher i.S. der DS-GVO ist, ist deshalb so relevant, weil ihn die Anforderungen aus der DS-GVO treffen. Gleiches gilt für den Auftragsverarbeiter, den spezielle Pflichten treffen. Ganz erheblich wirkt sich das unterschiedliche Anforderungsprofil aus. So treffen den Verantwortlichen bestimmte Pflichten, die nicht in der Sphäre des Auftragsverarbeiters liegen. Dies betrifft etwa die Rechtsgrundlage der Datenverarbeitung ebenso wie die Erarbeitung eines Löschkonzepts oder die Umsetzung der in Art. 25 DS-GVO genannten Prinzipien.

Nutzt ein Dritter das Testfeld zur Erprobung und Erforschung seiner Fahrzeuge und ist er Verantwortlicher i.S. der DS-GVO und ist der Betreiber des Testfelds dessen Auftragsverarbeiter, so hat der Testfeldbetreiber die Anforderungen des Art. 28 DS-GVO zu berücksichtigen.

3. Rechtmäßigkeit der Datenverarbeitung

Die Datenverarbeitung muss rechtmäßig sein, da die Datenverarbeitung für die betroffene Person einen Grundrechtseingriff darstellt. Art. 6 DS-GVO zählt abschließend Rechtmäßigkeitsgrundlagen auf.[90] Diese Rechtmäßigkeitsgrundlagen sind im Verhältnis zueinander gleichwertig. Bei sensiblen Daten ist jedoch Art. 9 DS-GVO zu beachten.

a. Kein Erfordernis einer behördlichen Genehmigung

Oftmals ist im Zusammenhang mit der Zulässigkeit der Datenverarbeitung von einem Verbot mit Erlaubnisvorbehalt die Rede.[91] Diese Bezeichnung geht dogmatisch fehl.[92] Dies folgt aus dem grundrechtlichen Eingriff, der in einer Datenverarbeitung zu sehen ist. Ein Eingriff in die Grundrechte auf Privatleben nach Art. 7 GRCh, auf Datenschutz nach Art. 8 GRCh sowie in die informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ist lediglich dann rechtmäßig, wenn eine gesetzliche Rechtsvorschrift dies erlaubt (sog. Vorbehalt des Gesetzes).[93]

Für Betreiber von Testfeldern folgt daraus, dass sofern sie Verantwortlicher sind und damit für die Rechtsgrundlage verantwortlich sind, eine behördliche Genehmigung nicht erforderlich ist. Eine Abstimmung bzw. Anfrage um Erlaubnis der Datenverarbeitung mit dem jeweiligen Landesbeauftragten für Datenschutz ist daher nicht notwendig.

b. Rechtsgrundlagen des Art. 6 DS-GVO

Art. 6 Abs. 1 DS-GVO sieht u.a. folgende Rechtsgrundlagen einer Datenverarbeitung vor:[94]
- Einwilligung (lit. a),

---

[90] *Steege*, PHi 4-5/2022, 164, 169.
[91] *Ziegenhorn/v. Heckel*, NVwZ 2016, 1585, 1586 ff.; *Buchner*, DuD 2016, 155, 157 f.
[92] *Steege/Kuß*, in: Chibanguza/Kuß/Steege (Hrsg.), Künstliche Intelligenz, 2022, Kapitel § 2 C. Rn. 30; so auch BeckOK DatenschutzR/*Albers/Veit*, 44. Ed. 1.5.2023, DS-GVO Art. 6 Rn. 11; *Roßnagel*, NJW 2019, 1 ff.
[93] So auch *Roßnagel*, NJW 2019, 1 ff.
[94] Grundlegend zu den Rechtsgrundlagen *Steege/Kuß*, in: Chibanguza/Kuß/Steege (Hrsg.), Künstliche Intelligenz, 2022, Kapitel § 2 C. Rn. 30-50; umfassend zu den Rechtsgrundlagen im Kontext der Erprobung automatisierter und autonomer Fahrzeuge *Steege/Stender-Vorwachs*, in: Chibanguza/Kuß/Steege (Hrsg.), Künstliche Intelligenz, 2022, Kapitel § 3 K. Rn. 27-40.

- Vertragserfüllung und Durchführung vorvertraglicher Maßnahmen (lit. b),
- Verarbeitung aufgrund einer rechtlichen Verpflichtung (lit. c),
- sowie aufgrund eines berechtigten Interesses des Verantwortlichen (lit. f.).

c. Besonderheiten bei der Verarbeitung besonderer Kategorien personenbezogener Daten

Im Kontext von sensitiven Daten geht Art. 9 DS-GVO vor. Bei u.a. medizinischen Daten bedarf es gem. Art. 9 Abs. 2 lit. a DS-GVO einer Einwilligung.[95] Ein berechtigtes Interesse o.Ä., wie es Art. 6 DS-GVO vorsieht, enthält Art. 9 DS-GVO nicht.[96] Diese im Vergleich zu Art. 6 DS-GVO bestehende Einschränkung muss der Verantwortliche, der für die Rechtsgrundlage zuständig ist, beachten. Der Anwendungsbereich der Vorschrift dürfte im Zusammenhang mit Testfeldern autonomer Mobilität in den allermeisten Fällen nicht eröffnet sein, sofern beim Testen nicht explizit Daten im Kontext von sog. Automotive Health-Anwendungen anfallen oder vom Testfahrer etwa Puls und Herzrate aufgezeichnet werden. Werden jedoch Tests durchgeführt, bei denen Daten i.S. des Art. 9 DS-GVO anfallen, so ist dessen Anwendungsbereich eröffnet und der Verantwortliche im datenschutzrechtliche Sinne muss dies bei der Datenerhebung beachten.

d. Wahl der Rechtsgrundlage

Die Wahl der Rechtsgrundlage wird maßgeblich durch die Lebenswirklichkeit beeinflusst. Bei Testfahrern kann neben einer Einwilligung insbesondere der Arbeitsvertrag die Rechtsgrundlage darstellen.[97] Personen außerhalb des Fahrzeugs können allerdings weder während des Fahrvorgangs einwilligen,[98] noch dient die Erhebung ihrer Daten der Vertragserfüllung oder erfolgt aufgrund einer rechtlichen Verpflichtung.[99] Damit bleibt das berechtigte Interesse des Verantwortlichen, sodass die Interessenabwägung maßgeblich ist. Diese erfordert, dass die sich gegenüberstehenden Interessen abgewogen werden. Welches Interesse überwiegt, hängt nicht nur vom Interesse der Beteiligten an der Datenverarbeitung und damit dem Zweck ab, sondern auch ganz erheblich von der Eingriffsintensität. Unter Interesse sind nicht nur rechtliche Interessen des Verantwortlichen, sondern auch wirtschaftliche und ideelle Interessen zu verstehen.

4. Datenschutzgrundsätze

Datenschutzgrundsätze finden sich in Art. 5-11 DS-GVO. Für die Datenverarbeitung im Kontext von Testfeldern für autonome Mobilität sowie beim automatisierten und autonomen Fahren ist höchstwahrscheinlich lediglich Art. 5 DS-GVO von Relevanz.

Art. 5 Abs. 1 DS-GVO nennt verschiedene Datenschutzgrundsätze, die bei der Datenverarbeitung berücksichtigt werden müssen.

---

[95] *Steege*, PHi 4-5/2022, 164, 169.
[96] *Steege/Kuß*, in: Chibanguza/Kuß/Steege (Hrsg.), Künstliche Intelligenz, 2022, Kapitel § 2 C. Rn. 49.
[97] *Steege*, MMR 2019, 509, 511.
[98] *Klink-Straub/Straub*, NJW 2018, 3201, 3205.
[99] *Steege*, MMR 2019, 509, 511.

a. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben sowie Transparenz

Gemäß Art. 5 Abs. 1 lit. a DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Dies meint die Grundsätze Rechtmäßigkeit, Verarbeitung nach Treu und Glauben sowie Transparenz.

b. Zweckbindung

Art. 5 Abs. 1 lit. b DS-GVO sieht eine Zweckbindung vor. Danach dürfen personenbezogene Daten lediglich für festgelegte, eindeutige und legitime Zwecke erhoben werden. Eine Datenverarbeitung, die diesen Zwecken zuwiderläuft, ist unzulässig. Eine nachträgliche Nutzung zu anderen Zwecken ist also nicht einfach möglich.

Etwas anderes gilt allerdings im Zusammenhang mit der Datenverarbeitung zu Forschungszwecken. Art. 5 Abs. 1 lit. b 2. HS DS-GVO sieht eine Privilegierung für wissenschaftliche Forschungszwecke vor. Die gleiche Privilegierung findet sich in Art. 89 Abs. 1 DS-GVO, worauf auch Art. 5 Abs. 1 lit. b 2. HS DS-GVO verweist. Es handelt sich um eine Fiktion, wonach der Sekundärzweck der wissenschaftlichen Forschung als mit dem Primärzweck vereinbar gilt.[100] Ohne diese Fiktion wäre eine Datenverarbeitung zu wissenschaftlichen Forschungszwecken mit dem Primärzweck unvereinbar, sofern der primäre Zweck der Datenerhebung nicht bereits in einer wissenschaftlichen Forschung liegt.

Für die Entwicklung automatisierter und autonomer Fahrzeuge und den Betrieb von Testfeldern für autonome Mobilität bedeutet dies, dass die Datenverarbeitung von zu eigentlich anderen Zwecken erhobenen Daten zulässig ist, sofern dies zu wissenschaftlichen Forschungszwecken geschieht. Eine pauschale Privilegierung existiert allerdings nicht, sodass es im jeweiligen Einzelfall auf die konkrete Ausgestaltung der Datenverarbeitung ankommt.[101]

Da die angebotenen Dienstleistungen der Testfelder autonomer Mobilität divergieren, ist im Einzelfall zu prüfen, ob es sich bei der konkreten Nutzung um wissenschaftliche Forschung handelt. Zuvor ist maßgeblich, was unter wissenschaftlicher Forschung i.S. des Art. 5 Abs. 1 lit. b 2. HS DS-GVO zu verstehen ist.[102]

c. Datenminimierung

Personenbezogene Daten müssen zudem gem. Art. 5 Abs. 1 lit. c DS-GVO dem Zweck der Datenverarbeitung angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

d. Richtigkeit

Personenbezogene Daten müssen darüber hinaus gem. Art. 5 Abs. 1 lit. d DS-GVO sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Der Verantwortliche muss alle

[100] Paal/Pauly/*Frenzel*, 3. Aufl. 2021, DS-GVO Art. 5 Rn. 32.
[101] Paal/Pauly/*Frenzel*, 3. Aufl. 2021, DS-GVO Art. 5 Rn. 32.
[102] Mit der Forschungsprivilegierung befasst sich etwa *Weichert*, ZD 2020, 18 ff.

Maßnahmen treffen, die angemessenen sind, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

e. Speicherbegrenzung

Art. 5 Abs. 1 lit. e DS-GVO sieht vor, dass personenbezogene Daten nur so lange gespeichert werden, wie es für den Zweck der Datenverarbeitung erforderlich ist. Daneben können gesetzliche Bestimmungen bestehen, die eine längere Aufbewahrungsfrist vorsehen. Im Bereich des Straßenverkehrs findet sich eine solche Regelung etwa mit Blick auf hoch- und vollautomatisierte Kraftfahrzeuge in § 63a Abs. 4 StVG. Eine Pflicht zur Datenspeicherung sieht auch § 1g Abs. 1, 2 StVG vor.

Existieren keine gesetzlichen Aufbewahrungs- oder Speicherfristen, hängt die Speicherdauer vom jeweiligen Einzelfall ab. Eine pauschale, d.h. starre Frist, kann nicht vorgegeben werden. Dies würde der Datenschutz-Grundverordnung zuwiderlaufen. Denn es hängt vom konkreten Einzelfall ab, wann der jeweilige Zweck der Datenverarbeitung erreicht ist, sodass die Daten gelöscht werden können. Verantwortliche müssen daher vor der Datenverarbeitung bei der Erstellung des jeweiligen datenschutzrechtlichen Konzepts überlegen, wann der Zweck erreicht ist und ob sich dies im Vorhinein bereits mit einer Zeitangabe bemessen lässt. Wie schnell der Zweck erreicht ist, liegt ebenfalls in der Sphäre des Verantwortlichen. Damit kommt es maßgeblich darauf an, was i.R. der Nutzung des Testfelds gemacht wird. Dies ist bei der Erstellung eines Löschkonzepts zu berücksichtigen.

Zu berücksichtigen ist zudem, in welcher datenschutzrechtlichen Rolle der Betreiber eines Testfelds ist. Sofern er Verantwortlicher ist, ist er für die Bestimmung der Löschfristen verantwortlich. Ist der Testfeldbetreiber Auftragsverarbeiter i.S. des Art. 28 DS-GVO, so sind bei der Löschung der Daten die Vorgaben des Art. 28 Abs. 3 lit. g DS-GVO zu beachten, sofern aus dem Unionsrecht oder dem Recht der Mitgliedstaaten keine Verpflichtung zur Speicherung der personenbezogenen Daten besteht, die über den Verarbeitungszeitraum hinausgeht.

f. Integrität und Vertraulichkeit

Die Datenverarbeitung personenbezogener Daten muss gem. Art. 5 Abs. 1 lit. f DS-GVO in einer Weise geschehen, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Dies umfasst den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung durch geeignete technische und organisatorische Maßnahmen.

Gegenstand von Art. 5 Abs. 1 lit. f DS-GVO ist nicht die Frage, ob die Datenverarbeitung zulässig ist, sondern wie die Datenverarbeitung erfolgen soll. Diese Vorgaben beziehen sich auf die Datensicherheit.[103]

Die nach Art. 25 und 32 DS-GVO notwendigen technischen und organisatorischen Maßnahmen konkretisieren den in Art. 5 Abs. 1 lit. f DS-GVO aufgestellten Datenschutzgrundsatz der Vertraulichkeit und Integrität.

[103] Gola/Heckmann/*Pötters*, 3. Aufl. 2022, DS-GVO Art. 5 Rn. 29.

g. Verantwortlichkeit für die Einhaltung der Datenschutzgrundsätze

Art. 5 Abs. 2 DS-GVO sieht vor, dass der Verantwortliche für die Einhaltung des Abs. 1 verantwortlich ist und dessen Einhaltung etwa gegenüber der Behörde nachweisen können muss (Rechenschaftspflicht).

5. Informationspflichten des Verantwortlichen

Findet eine Verarbeitung personenbezogener Daten statt, so muss der Verantwortliche der betroffenen Person Informationen mitteilen. Diese Informationen sind in Art. 13 Abs. 1, 2 DS-GVO enumerativ aufgelistet. Diese Informationspflicht besteht gem. Art. 13 Abs. 1 DS-GVO bereits mit Erhebung der Daten.

Von der Informationspflicht umfasst sind:

- der Name und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters (Abs. 1 lit. a),
- gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten (Abs. 1 lit. b),
- die Zwecke der Datenverarbeitung sowie die jeweilige Rechtsgrundlage (Abs. 1 lit. c),
- sofern die Verarbeitung auf ein berechtigtes Interesse gestützt wird, ist dieses zu benennen (Abs. 1 lit. d),
- gegebenenfalls die Empfänger oder Kategorien von Datenempfängern (Abs. 1 lit. e),
- beabsichtigte Drittstaatentransfers (Abs. 1 lit. f),
- die Speicherdauer (Abs. 2 lit. a),
- die Nennung der Rechte der betroffenen Person (Abs. 2 lit. b),
- der Hinweis auf das bestehende Widerrufsrecht der erteilten Einwilligung (Abs. 2 lit. c),
- Beschwerderechte der betroffenen Person bei einer Aufsichtsbehörde (Abs. 2 lit. d),
- die gesetzliche oder vertragliche Erforderlichkeit der Datenverarbeitung sowie ob die betroffene Person die Daten bereitstellen muss und welche Konsequenzen das Missachten hat (Abs. 2 lit. e),
- sowie das Vorliegen einer automatisierten Entscheidungsfindung i.S. des Art. 22 DS-GVO (Abs. 2 lit. f).

Wie die Informationspflichten erfüllt werden können, hängt von der konkreten Ausgestaltung des Testfelds und seiner Nutzung ab. Denkbar ist einerseits, dass eine Datenverarbeitung lediglich durch die Testfahrzeuge erfolgt. Andererseits kann eine Datenverarbeitung aber auch durch die Sensorik in der Infrastruktur erfolgen, etwa wenn Ampeln auch mit Kameras ausgestattet sind und eine Kreuzung filmen oder mittels Vehicle-to-Infrastructure-Kommunikation mit den Fahrzeugen kommunizieren und dabei Daten anfallen.

Erfasst das Fahrzeug, welches auf dem Testfeld fährt, die Fahrzeugumgebung mittels Kamera, so ist darauf hinzuweisen. In der Praxis hat sich ein entsprechendes Labeling der Fahrzeuge als Kamerafahrzeuge durchgesetzt.[104] Zusätzlich zu dem Hinweis der Aufzeichnung sollte die Homepage, der die notwendigen Informationen zu entnehmen sind, genannt werden oder mittels QR-Code erreichbar sein. Die Homepage muss sodann die nach Art. 13 DS-GVO erforderlichen Informationen enthalten. Handelt es sich bei dem Betreiber des Testfelds nur um einen Auftragsverarbeiter, obliegt nicht ihm, sondern dem Verantwortlichen die

[104] So schon *Steege*, MMR 2019, 509, 512.

Informationspflicht, d.h. dieser muss das Labeling vornehmen und die Informationen bereitstellen. Etwas anderes gilt dann, wenn der Testfeldbetreiber Verantwortlicher im datenschutzrechtlichen Sinne ist.

Informationspflichten bestehen ebenfalls hinsichtlich der im Testfeld eingesetzten bzw. verbauten Sensorik (etwa Kameras, Vehicle-to-Infrastructure-Kommunikation). Hier ist es für den Betreiber des Testfelds möglich, durch entsprechende Schilder die Verkehrsteilnehmer auf die Datenverarbeitung aufmerksam zu machen. Ist der Testfeldbetreiber Verantwortlicher, so ist er auch für die Informationen auf einer Homepage verantwortlich. Da die Nutzer des Testfelds wechseln können und es sich in den allermeisten Fällen wahrscheinlich um Dritte handelt und der Betreiber des Testfelds lediglich Auftragsverarbeiter ist, bietet es sich an, auf den Schildern lediglich auf die Datenverarbeitung im Rahmen des Testfelds und etwa die Aufnahme von Videodaten hinzuweisen und auf der Homepage auf die jeweiligen Informationen des Verantwortlichen zu verweisen, sodass der Testfeldbetreiber einen flexiblen Ansatz verfolgt, der es ermöglicht, auch bei wechselnden Nutzern und Anwendungsfällen der Informationspflicht hinreichend nachzukommen.

Von praktischer Bedeutung ist die Reichweite der Informationspflichten. Nicht jeder Verkehrsteilnehmer wird die Schilder beachten und noch wenigere werden in der Lage sein, die URL zu erkennen oder einzelne Details zu lesen. Damit stellt sich die Frage, ob der Informationspflicht entsprochen wird, wenn gleichwohl lediglich mittels eines Schildes bzw. Labels am Fahrzeug und Verweis auf eine Homepage informiert wird. Noch weitreichender wäre eine Kampagne, um die Öffentlichkeit zu informieren. Je nach Reichweite des Art. 13 DS-GVO werden die Anforderungen an den Verantwortlichen kaum erfüllbar. Eine Begrenzung der Reichweite der Informationspflichten findet sich in Art. 13 Abs. 4 DS-GVO. Danach findet Art. 13 Abs. 1, 2, 3 DS-GVO keine Anwendung, sofern die betroffene Person bereits über die in Art. 13 DS-GVO genannten Informationen verfügt. Eine Begrenzung der Reichweite der Informationspflichten findet sich auch in Art. 14 Abs. 5 DS-GVO, wobei sich diese Ausschlussgründe lediglich auf die Informationspflichten nach Art. 14 DS-GVO beziehen. Eine Heranziehung dieser Gründe für Art. 13 DS-GVO erscheint contra legem. Auch eine Analogie wird größtenteils abgelehnt, da es an einer planwidrigen Regelungslücke fehlt.[105]

Ob Art. 13 DS-GVO oder Art. 14 DS-GVO einschlägig ist, hängt davon ab, ob die Daten „bei der betroffenen Person“ erhoben werden.[106] Ist dies der Fall, so ist Art. 13 DS-GVO anwendbar. Werden die Daten hingegen nicht „bei der betroffenen Person“ erhoben, so ist Art. 14 DS-GVO anwendbar. Die Abgrenzung ist nicht immer einfach. Im Bereich der Videoaufnahmen wird gemeinhin darauf abgestellt, ob es sich um eine offene Videoüberwachung mit entsprechendem Hinweisschild handelt oder um eine geheime Überwachung. Im ersten Fall ist Art. 13 DS-GVO einschlägig, bei Letzterem ist Art. 14 DS-GVO anwendbar.[107] Wird durch ein entsprechendes Labeling der Fahrzeuge sowie Hinweisschilder im Bereich der Testfelder auf die Datenverarbeitung aufmerksam gemacht, so handelt es sich um eine offene Videoüberwachung des Straßenraums, sodass nach allen Ansichten Art. 13 DS-GVO anwendbar ist.[108] Damit

[105] BeckOK DatenschutzR/*Schmidt-Wudy*, 44. Ed. 1.5.2023, DS-GVO Art. 13 Rn. 95.
[106] Zum Konzept einer Abgrenzung von Art. 13 und Art. 14 DS-GVO siehe nur *Jaksch/Hoffmann*, ZD 2022, 605 ff.
[107] BeckOK DatenschutzR/*Schmidt-Wudy*, 44. Ed. 1.5.2023, DS-GVO Art. 14 Rn. 31.2; Paal/Pauly/*Paal/Hennemann*, 3. Aufl. 2021, DS-GVO Art. 13 Rn. 11b; Gola/Heckmann/*Franck*, 3. Aufl. 2022, DS-GVO Art. 14 Rn. 2; a.A. EDSA-Leitlinien zur Datenverarbeitung durch Videogeräte, Rn. 110, wonach auch bei verdeckten Aufnahmen Art. 13 DS-GVO anwendbar sein soll.
[108] So auch für Erprobungsfahrten automatisierter und autonomer Fahrzeuge *Steege*, MMR 2019, 509, 512.

müssen die Informationspflichten erfüllt werden, sofern die betroffene Person nicht bereits über die Informationen verfügt (Art. 13 Abs. 4 DS-GVO). Sämtliche Daten des Art. 13 Abs. 1, 2 DS-GVO müssen nicht auf den Hinweisschildern oder dem Labeling genannt werden. Dies würde dem Sinn und Zweck der Informationspflichten zuwiderlaufen, da dadurch keine Transparenz erzeugt wird. Daher sollten die wesentlichen Informationen gut lesbar sein und sich die weiteren Informationen auf einer Homepage finden lassen.[109] Vorgaben für eine Schriftgröße sieht die DS-GVO nicht vor. Es kommt lediglich darauf an, dass die wesentlichen Informationen für Verkehrsteilnehmer im fließenden Straßenverkehr lesbar und erkennbar sind. Am Straßenrand von Testfeldern können zudem große, gut sichtbare Schilder mit Hinweisen auf das entsprechende Testfeld und zur Art der Datenerhebung aufgestellt werden.

6. Datensicherheit – technische und organisatorische Maßnahmen

Art. 5 Abs. 1 lit. f DS-GVO fordert eine angemessene Sicherheit der personenbezogenen Daten. Dies soll durch technische und organisatorische Maßnahmen gewährleistet werden. Diese wiederum finden ihre Konkretisierung in den Art. 25 und 32 DS-GVO.

a. Datenschutz durch Technikgestaltung

In Art. 25 DS-GVO findet sich der Ansatz des Datenschutzes durch Technikgestaltung. Art. 25 Abs. 1 DS-GVO steht dabei unter dem Motto „Data Protection by Design“. Die Gestaltung und der Einsatz von Technik sollen datenschutzfreundlich erfolgen. Der Unionsgesetzgeber verfolgt damit das Ziel, dass bereits bei der Entwicklung von Technik die Weichen der späteren Datenverarbeitung gelegt werden, sodass zu einem solch frühen Zeitpunkt bereits eine effektive Datensparsamkeit vorgegeben werden kann.[110] Art. 25 Abs. 1 DS-GVO zählt als konkrete Maßnahme allerdings lediglich die Pseudonymisierung auf,[111] sodass unklar ist, welche Maßnahmen zu treffen sind. Dies führt in der Praxis zu großen Herausforderungen aufgrund bestehender Rechtsunsicherheit und mündet in einer Einzelfallentscheidung. Da ein Verstoß gegen Art. 25 DS-GVO mit einem Bußgeld verhängt werden kann, hat die Vorschrift praktische Bedeutung.

aa) Normadressat

Normadressat ist der Verantwortliche. Ihn treffen die Pflichten aus Art. 25 Abs. 1 DS-GVO. Auftragsverarbeiter sind deshalb nicht unmittelbar von den Pflichten erfasst.[112]

bb) Umsetzung der technisch-organisatorischen Maßnahmen

Ausgehend vom Wortlaut des Art. 25 Abs. 1 DS-GVO trifft den Verantwortlichen zum Zeitpunkt der Datenverarbeitung die Pflicht, geeignete technische und organisatorische Maßnahmen zu treffen. Diese sollen dazu ausgelegt sein, die Datenschutzgrundsätze

[109] *Steege*, MMR 2019, 509, 512.
[110] *Steege*, MMR 2019, 509, 512.
[111] *Hartung*, in: Kühling/Buchner, DS-GVO Art. 25 Rn. 1.
[112] *Hartung*, in: Kühling/Buchner, DS-GVO Art. 25 Rn. 12.

umzusetzen. Art. 25 Abs. 1 DS-GVO nennt dabei explizit die Pseudonymisierung (Art. 4 Nr. 5 DS-GVO) als Beispiel für die Datenminimierung nach Art. 5 Abs. 1 lit. c DS-GVO. Dies ist allerdings nur beispielhaft zu verstehen. Selbstverständlich sind auch die übrigen in Art. 5 Abs. 1 DS-GVO genannten Datenschutzgrundsätze umzusetzen.[113]

Darüber hinaus sind als zu treffende Maßnahmen die Verschlüsselung der Daten sowie Zugangs- und Zutrittskontrollen geeignet.[114]

Darüber hinaus wirkt sich auch der Speicherort der Daten – etwa im Fahrzeug oder auf Servern des Testfeldbetreibers – auf die Sicherheit der Daten aus. Aber auch die Architektur wirkt sich unmittelbar auf die Datensicherheit aus.[115]

Vom Einzelfall hängt es zudem ab, welche Maßnahmen der Verantwortliche konkret treffen kann und muss. Diese Einzelfallbezogenheit bei gleichzeitig nebulöser Pflicht führt für die Praxis zu großen Herausforderungen.[116] Insbesondere enthält Art. 25 DS-GVO kein Schema, mittels dessen Verantwortliche vorgehen können.[117] Für Betreiber von Testfeldern bleibt damit nur, in Abhängigkeit der jeweils angebotenen Dienstleistungen und der dabei anfallenden Daten Maßnahmen zu bestimmen. Diese können allerdings von Dienstleistung zu Dienstleistung abweichen und sich von Testfeld zu Testfeld unterscheiden. Entwickeln Testfeldbetreiber ein Schema, so kann dies höchstens einen Anhaltspunkt bieten. Der jeweilige Testfeldbetreiber wird indes nicht davon befreit, für seine konkreten Datenverarbeitungen entsprechende Maßnahmen zu treffen.

Im Zusammenhang mit Kraftfahrzeugen und Testfeldern bietet es sich an, Schnittstellen hinreichend zu schützen bzw. zu reduzieren, um vor Hackerangriffen geschützt zu sein. Eine Entkopplung von Steuergeräten und bspw. den jeweiligen Schnittstellen von Infotainmentsystemen sowie ein eingeschränkter Zugriff auf die Daten bietet sich ebenfalls an.[118]

b. Technische und organisatorische Maßnahmen nach Art. 24 DS-GVO

Art. 24 DS-GVO regelt die Verantwortung des Verantwortlichen und sieht ebenfalls technische und organisatorische Maßnahmen vor. Dabei handelt es sich jedoch nicht um eine Konkretisierung dieser Maßnahmen. Vielmehr ist Art. 24 DS-GVO lex generalis gegenüber Art. 25, 32, 35 DS-GVO, welche im Verhältnis zu Art. 24 DS-GVO lex specialis sind.[119] Die Pflichten in Art. 24 DS-GVO werden folglich durch die Inhalte der Art. 25, 32, 35 DS-GVO näher ausgestaltet.

c. Sicherheit der Datenverarbeitung nach Art. 32 DS-GVO

Art. 32 DS-GVO regelt die Sicherheit der Datenverarbeitung. Diese Anforderungen erlangen insbesondere aufgrund von Hackerangriffen sowie Computerviren und weiteren kriminellen

[113] So auch *Hartung*, in: Kühling/Buchner, DS-GVO Art. 25 Rn. 16.
[114] Esslinger/Marques, DuD 2018, 101.
[115] *Hartung*, in: Kühling/Buchner, DS-GVO Art. 25 Rn. 16.
[116] *Steege*, PHi 4-5/2022, 164, 172.
[117] Kritisch statt vieler *Hartung*, in: Kühling/Buchner, DS-GVO Art. 25 Rn. 17.
[118] *Stender-Vorwachs/Steege*, Autonomes Fahren, Kap. 3.6.1. Rn. 159.
[119] Paal/Pauly/*Martini*, 3. Aufl. 2021, DS-GVO Art. 24 Rn. 1.

Handlungen – insbesondere bei der Erprobung von automatisierten, autonomen sowie vernetzten Fahrzeugen – hohe Relevanz. Denn Datenschutz ohne hinreichende Datensicherheit ist unwirksam. Während Datenschutz darauf abzielt, es dem Einzelnen – der betroffenen Person – zu ermöglichen, seine Autonomie im Umgang mit seinen personenbezogenen Daten zu wahren und zu schützen, zielt die Datensicherheit auf den Schutz dieser Daten ab und verhindert etwa einen unzulässigen Zugriff.[120] Die Datensicherheit soll die Vertraulichkeit, Integrität sowie Verfügbarkeit der Daten durch technische und organisatorische Maßnahmen sicherstellen.[121]

Teilweise ergeben sich zu treffende Maßnahmen aus Art. 32 Abs. 1 HS. 2 DS-GVO, denn diese Aufzählung ist nicht abschließend. Neben konkreten Maßnahmen finden sich Zielvorgaben (lit. b und c).[122]

Danach handelt es sich um die folgenden:
- Pseudonymisierung und Verschlüsselung der personenbezogenen Daten (lit. a),
- die Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Kontext der Verarbeitung auf Dauer zu gewährleisten (lit. b),
- die Möglichkeit, die Verfügbarkeit der personenbezogenen Daten sowie den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (lit. c),
- sowie ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung (lit. d).

Allerdings enthält Art. 32 Abs. 1 DS-GVO zahlreiche unbestimmte Rechtsbegriffe, die dazu führen, dass für den Normadressaten ein weiter Ermessensspielraum besteht und gleichzeitig Rechtsunsicherheit besteht. Mit Blick auf die Interessen der betroffenen Person kann auch von einem Makel des Art. 31 Abs. 1 DS-GVO gesprochen werden, denn dieser sieht vor, dass sowohl der Stand der Technik, als auch die Implementierungskosten, die Art des Umfangs, die Umstände und Zwecke der Datenverarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und die Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen berücksichtigt werden und aufgrund dessen durch den Verantwortlichen und den Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen getroffen werden, um „ein dem Risiko angemessenes Schutzniveau zu gewährleisten“.

d. Mögliche zu treffende Maßnahmen

In der Gesamtschau der zahlreichen datenschutzrechtlichen Anforderungen lassen sich einige mögliche Maßnahmen ausmachen, die Betreiber von Testfeldern sowohl in der Rolle des Verantwortlichen als auch des Auftragsverarbeiters treffen können, um Datenschutz und Datensicherheit zu gewährleisten und die bereits durch Betreiber von Testfeldern zum Einsatz kommen. Diese sind keinesfalls abschließend, bieten aber neben den Zielbestimmungen des Datenschutzes und der Datensicherheit mögliche Ansatzpunkte, um einen effektiven Datenschutz ebenso zu gewährleisten wie eine Datensicherheit. Denn die jeweils zu treffenden Maßnahmen werden von den Umständen des jeweiligen Einzelfalls und insbesondere den betroffenen Datenkategorien determiniert.
Mögliche Maßnahmen sind:

[120] Paal/Pauly/*Martini*, 3. Aufl. 2021, DS-GVO Art. 32 Rn. 1b.
[121] *Schulte/Wambach*, DuD 2020, 462, 463.
[122] Paal/Pauly/*Martini*, 3. Aufl. 2021, DS-GVO Art. 32 Rn. 30.

- Pseudonymisierung oder Anonymisierung der Daten,
- Verschlüsselung der Daten,
- Nutzung eines Virtual Private Network (VPN),
- Berücksichtigung der ISO/IEC 27002, veröffentlicht in der zweiten Ausgabe als ISO/IEC 27002:2013 Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmaßnahmen,
- Videoaufnahmen mit verringerter Bildqualität, sofern dies für die Erreichung des Zwecks der Datenerhebung irrelevant ist,
- Erstellung eines Back-Ups der gespeicherten Daten,
- Nutzung einer Public Key Infrastruktur (PKI),
- Verschlüsselung von Festplatten und sonstigen Datenspeichern,
- Implementierung einer Firewall,
- Lokale Speicherung der Daten und Beachtung von Datenschutzanforderungen bei der Speicherung in einer Cloud. Insbesondere hinsichtlich der Datensicherheit als auch des geeigneten Datenschutzniveaus sowie mit Blick auf einen möglichen Drittstaatentransfer,
- Nutzung eines eigenen Mobilfunkpunkts (APN),
- Betreiben / Hosten eines eigenen Servers,
- Beachtung des BSI-Grundschutzes,
- Entsprechender Schutz von Hardware, etwa durch einen Schaltschrank und Zutrittssysteme in Form von Schlüsseln und Zutritts- sowie Berechtigungskonzepten,
- Installation einer Alarmanlage und weiterer Mechanismen zum Schutz.

IX. Produkt- und Produzentenhaftung

Die Produkthaftung fußt auf zwei Säulen. Dies ist zum einen die nationale, deliktische Produzentenhaftung nach § 823 Abs. 1 BGB und zum anderen die harmonisierte Produkthaftung nach dem Produkthaftungsgesetz (ProdHaftG),[123] welches auf der europäischen Produkthaftungsrichtlinie basiert.[124] Wenngleich gemeinhin angenommen wird, dass es sich bei letzterer um eine verschuldensunabhängige Haftung handelt, liegt beides Mal eine Sorgfaltspflichtverletzung des Herstellers zugrunde, auch wenn eine solche im Rahmen der Haftung nach dem ProdHaftG nicht von Nöten ist.[125] Anwendungsbereich und erfasste Produkte der beiden Anspruchsgrundlagen divergieren, was sich etwa im Hinblick auf Software auswirkt.[126] Die Rechtsprechung hat früh begonnen, zahlreiche Pflichten (Sorgfaltspflichten in Form von Verkehrssicherungspflichten und Verkehrspflichten sowie Organisationspflichten) zu normieren.[127] Unterscheiden lassen sich Pflichten vor und nach der Inverkehrgabe.[128] Dabei wurden verschiedene Fehlerkategorien entwickelt.[129]

Nicht nur die Informations- und Cybersicherheit sind Bestandteil der Herstellerhaftung. Mit Blick auf Betreiber von Testfeldern stellt sich zunächst die Frage, in welcher Konstellation sie von der Produkt- und Produzentenhaftung erfasst sein können. Dies hängt maßgeblich von deren Aktivitäten ab. Sofern von einer Herstellerstellung auszugehen ist, müssen die Pflichten

[123] ProdHaftG vom 15.12.1989 (BGBl. 1989 I. S. 2198), in Kraft getreten am 1.1.1990.
[124] *Steege*, SVR 2023, 9, 13.
[125] *Steege*, in Buck-Heeb/Oppermann (Hrsg.), Automatisierte Systeme, 2022, Kap. 3.11, S. 374; *Wagner*, AcP 217 (2017), 707, 711.
[126] *Steege*, NZV 2021, 6, 7.
[127] *Steege*, Organisationspflichten und Organisationsverschulden, 2022, S. 133.
[128] *Steege*, in Buck-Heeb/Oppermann (Hrsg.), Automatisierte Systeme, 2022, Kap. 3.11, S. 382.
[129] Dazu Steege, *Steege*, in Haus/Krumm/Quarch, Gesamtes Verkehrsrecht, 3. Aufl. 2021, Anh. III zu §§ 1a-1c StVG, Rn. 59 ff.

und deren Inhalt und Umfang im Einzelfall bestimmt werden. Naheliegender sind bspw. Pflichten von Automobilherstellern, die für Produktfehler und daraus resultierende Schäden ihrer Erprobungsfahrzeuge haften. Virulent wird insbesondere die Schaffung einer Absicherung gegenüber Cyberangriffen Dritter.[130]

X. Technical Compliance

Der Aspekt der Technical Compliance ist insbesondere für Automobilhersteller von zentraler Bedeutung. Aber auch Betreiber von Testfeldern, die Sensorik bzw. Infrastruktur bauen, sollten nationale und internationale Normen und Standards im Blick behalten. Allgemeinhin bekannt sind etwa ISO- und DIN-Normen. Diese können allerdings auch mit Blick auf den Aufbau der jeweiligen juristischen Person relevant werden, sodass hinsichtlich des Testfeldbetreibers Anforderungen an dessen Aufbau- und Ablauforganisation bestehen.[131]

Bei diesen Normen handelt es sich um eine Selbstregulierung im Privatrecht, sodass es sich nicht um Rechtsquellen handelt, wodurch sie keine bindende Wirkung entfalten.[132] Dies kann sich allerdings immer dann ändern, wenn ihr Inhalt durch ein Gesetz bindend wird. Verweist ein Gesetz etwa auf den Stand der Technik oder gar unmittelbar auf eine Norm, so sind deren Anforderungen zu berücksichtigen. Insbesondere im Rahmen des Produkthaftungsrechts werden daher (technische) Normen virulent. Dies folgt daraus, dass sie das vom Verkehrskreis zu erwartende Sicherheitsniveau des jeweiligen Produkts bestimmen können.[133] Durch den Stand der Technik wird deutlich, was technisch möglich ist und welches Sicherheitsniveau für den Hersteller zumutbar ist.[134] Werden private Standards eingehalten, bedeutet dies nicht, dass dadurch eine Haftung ausgeschlossen wird.[135]

Für Betreiber von Testfeldern können Normen relevant werden, die die Datensicherheit betreffen. Aber auch organisatorische Normen, die die Aufbau- und Ablauforganisation des Betreibers selbst betreffen, sind zu beachten. Damit sind verschiedene Ebenen betroffen. Einerseits das Unternehmen des Testfeldbetreibers und dessen Aufbau sowie die einzelnen Arbeitsabläufe und andererseits die Herstellung und der Betrieb von Versuchsträgern und Einrichtungen und etwaige Anforderungen an diese.

XI. Ergebnis

Ein einheitliches Gesetz für Testfelder autonomer Mobilität existiert nicht. Anforderungen an die Informations- und Cybersicherheit sind ebenfalls nicht in einer einzigen Rechtsquelle kodifiziert, sondern existieren in unterschiedlichen Gesetzen und verschiedenen Rechtsgebieten. Lediglich der Datenschutz ist innerhalb der europäischen Union einheitlich in der DS-GVO geregelt, sodass dadurch eine Vollharmonisierung erreicht wird.

---

[130] Hierzu auch *Hartmann*, DAR 2015, 122, 123.
[131] Zur Anknüpfung von Organisationspflichten an die Aufbau- und Ablauforganisation sowie ökonomische Implikationen siehe *Steege*, Organisationspflichten und Organisationsverschulden, 2022, S. 44 ff.
[132] *Steege*, Organisationspflichten und Organisationsverschulden, 2022, S. 239.
[133] Zu haftungsrechtlichen Implikationen von technischen Normen und Standards siehe *Rockstroh/Kunkel*, MMR 2017, 77, 81.
[134] *Steege*, Organisationspflichten und Organisationsverschulden, 2022, S. 239; BGH, VersR 1984, 270; *Marburger*, VersR 1983, 597, 600 f.
[135] *Steege*, Organisationspflichten und Organisationsverschulden, 2022, S. 241.

Anforderungen an Betreiber von Testfeldern gibt es zahlreiche. Welche Gesetze einschlägig sind, hängt von der konkreten Ausgestaltung und den jeweiligen Angeboten der Testfelder ab, sodass Anforderungen nicht für alle Testfelder pauschal gelten, sondern es vielmehr auf den jeweiligen Einzelfall ankommt.

C. Frage 3: Erläuterung der aktuellen Rechtsauslegung bzgl. Datenschutz innerhalb der V2X (Vehicle-2-Everything) - Kommunikation

I. Umfang des Gutachtens

Gewünscht ist die Erläuterung der aktuellen Rechtslage hinsichtlich des Datenschutzes im Kontext der Vehicle-2-Everything-Kommunikation (V2X-Kommunikation). Konkret soll untersucht werden, welche datenschutzrechtlichen Anforderungen bei der Übertragung von Fahrzeuginformationen über den Nachrichtentyp CAM (Cooperative Awareness Message) via Broadcast bestehen. Zudem soll untersucht werden, ob es einen Unterschied macht, ob dieser Datentransfer kommerziell oder zu Forschungszwecken erfolgt.

II. Einleitung

Nicht nur die zunehmende Automatisierung prägt den Straßenverkehr, sondern auch die voranschreitende Vernetzung der Fahrzeuge mit der Fahrzeugumgebung. Im Fahrzeug generierte Daten können dabei an andere Empfänger übermittelt werden. Dabei wird unterschieden zwischen der sog. Car to Car (C2C) Kommunikation, bei der Daten an andere Fahrzeuge übermittelt werden, Car to Infrastructure (C2I) sowie Car to Anything (C2X).[136]

Kooperative intelligente Verkehrssysteme ermöglichen vernetzten Kraftfahrzeugen den Austausch von digitalen Funknachrichten mit der Verkehrsinfrastruktur. Gegenstand der Informationen können dabei das Verkehrsgeschehen sowie der Fahrzeugzustand sein. Fahrzeuge können dabei mit Ampeln, Schilderbrücken und Baustelleneinrichtungen kommunizieren, wodurch die Verkehrssicherheit erhöht werden soll. Dadurch sollen Unfälle minimiert bzw. verhindert und der Verkehrsfluss optimiert werden.[137] Ganz konkret können Autofahrer so bspw. vor Baustellen oder Stauenden gewarnt werden. Aber auch Verkehrszeichen können über sog. In-Vehicle-Information-Nachrichten (IVI-Nachrichten) zum Fahrzeug gesendet und im Cockpit dargestellt werden.

III. Datenschutzrechtliche Anforderungen

1. Anwendbarkeit der DS-GVO – personenbezogene Daten

Die Datenschutzgrundverordnung ist bei sog. CAM-Nachrichten anwendbar, sofern es sich dabei um personenbezogene Daten handelt.

Da nur personenbezogene Daten in den Anwendungsbereich der DS-GVO fallen, ist die Definition von personenbezogenen Daten in der Praxis äußerst relevant. Gemäß Art. 4 Nr. 1

[136] *Stender-Vorwachs/Steege*, in: Oppermann/Stender-Vorwachs (Hrsg.), Autonomes Fahren, 2020, Kap. 3.6.1, S. 406.

[137] Vgl. Bundesamt für Sicherheit in der Informationstechnik, Kooperative Intelligente Verkehrssysteme (C-ITS), abrufbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Automotive/Kooperative_Intelligente_Verkehrssysteme/Kooperative_Intelligente_Verkehrssysteme.html (zuletzt abgerufen am 10.12.2023).

DS-GVO sind „‘personenbezogene Daten‘ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“.

Entscheidend ist hierbei die Identifizierbarkeit. Umfasst sind ausgehend vom Wortlaut sowohl „identifizierte“ als auch „identifizierbare“ natürliche Personen.[138] Juristische Personen sind vom Schutzbereich der DS-GVO nicht umfasst. Die Informationen müssen sich vielmehr auf eine natürliche Person beziehen. Gegen eine Anwendbarkeit auf juristische Personen spricht ausdrücklich Erwägungsgrund 14 DS-GVO. Insofern handelt es sich bei dem Dritten als Unternehmen, der das Testfeld nutzt, nicht um eine betroffene Person. Bei Testfahrten im Rahmen der Nutzung von Testfeldern ist die betroffene Person in der Regel der Testfahrer. Dies kann bspw. dann der Fall sein, wenn er von einer Innenraumkamera aufgenommen wird. Erfasst das Fahrzeug mittels Kamera oder anderer Sensoren die Fahrzeugumgebung, so sind die in diesem Kontext erfassten Personen die jeweils betroffene Person. Bei wem es sich um die betroffene Person handelt, wirkt sich auch im Rahmen der Rechtmäßigkeit der Datenverarbeitung aus. Aber auch vom Fahrzeug übermittelte Informationen können personenbezogen sein, wobei es auf die konkret übermittelten Daten ankommt.

Die Definition des personenbezogenen Datums ist sehr weit gefasst,[139] da es ausreichend ist, wenn die natürliche Person identifizierbar ist. Dadurch ist es ausreichend, wenn die betroffene Person mittels Kombination mit weiteren Daten identifizierbar ist.[140] Zur Abgrenzung, ob personenbezogene Daten vorliegen oder nicht, kommt es folglich maßgeblich auf das Verständnis vom Personenbezug an. Unterschieden wird zwischen einem relativen und absoluten Personenbezug.[141]

Die Rechtsprechung neigt dazu, einen sehr weiten Personenbezug anzunehmen.[142] So führt der EuGH aus: „Wie der Gerichtshof bereits festgestellt hat, ist der Anwendungsbereich der RL 95/46 sehr weit und […] die von ihr erfassten personenbezogenen Daten vielfältig […]“.[143] Bereits das Bundesverfassungsgericht stellte fest, dass die umfassenden Verarbeitungs- und Verknüpfungsmöglichkeiten von Daten dazu führen, dass es kaum Daten ohne Personenbezug gibt.[144] Auch dem Europäischen Gerichtshof lässt sich ein weites Verständnis des Begriffs „personenbezogene Daten“ entnehmen. So führte er aus: „Wie der Gerichtshof bereits festgestellt hat, ist der Anwendungsbereich der RL 95/46 sehr weit und […] die von ihr erfassten personenbezogenen Daten vielfältig […]“.[145] Allerdings lässt sich in jüngster Rechtsprechung des Europäischen Gerichts erkennen, dass es verstärkt darauf ankommen soll, ob weitere Daten, die zu einem Personenbezug führen, für den Verantwortlichen zugänglich sind oder nicht. Dies spricht gegen einen absoluten und für einen relativen Personenbezug, bei

[138] *Steege*, PHi 4-5/2022, 164, 166.
[139] Paal/Pauly/*Ernst*, 3. Aufl. 2021, DS-GVO Art. 4 Rn. 3; *Steege*, PHi 4-5/2022, 164, 166.
[140] *Steege*, PHi 4-5/2022, 164, 166.
[141] *Steege*, PHi 4-5/2022, 164, 166.
[142] *Steege*, PHi 4-5/2022, 164, 166.
[143] EuGH, NJW 2018, 767 Rn. 33. Zwar bezieht sich dieses Postulat auf die der DS-GVO vorangegangene Richtlinie, allerdings wurde die Definition des personenbezogenen Datums inhaltlich nicht geändert.
[144] BVerfGE 65, 1, Rn. 176 = NJW 1984, 419.
[145] EuGH, NJW 2018, 767 Rn. 33.

dem es maßgeblich darauf ankommt, ob der Verantwortliche an zusätzliche Daten gelangt und wie schwer dies ist. Ob ein Personenbezug vorliegt oder nicht, hängt jedoch maßgeblich vom Einzelfall ab. Denn während für eine Person Informationen personenbezogene Daten darstellen können, kann sich dies für eine andere Person vollständig anders darstellen. Die Annahme des Personenbezugs ist also kontextualisiert und nicht absolut.

Um zu beurteilen, ob es sich bei CAM-Nachrichten um personenbezogene Daten handelt, kommt es auf die einzelnen Informationen an, die in diesen enthalten sind. Die Daten, die eine CAM-Nachricht enthalten kann, sind im Standard des ETSI in den Anhängen A und B aufgeführt.[146] Diese Informationen beziehen sich auf das Fahrzeug, welches die Informationen sendet, sodass sie, wenn überhaupt, lediglich personenbezogene Daten des Testfahrers darstellen können. Im regulären Einsatz ist nicht ohne Weiteres nachvollziehbar, wessen Daten empfangen werden, da ein normaler Fahrzeugführer lediglich Informationen über Gefahrenstellen in seinem Display angezeigt bekommt. Sowohl der Kunde des Testfelds als auch der Testfeldbetreiber wissen jedoch, wem die gesendeten Daten zuzuordnen sind. So werden die an sich neutralen Daten zu personenbezogenen Daten des Testfahrers. Je nach Ausgestaltung des Testfelds und je nach Einsatz bzw. Erprobung kann es sein, dass es sich nicht um personenbezogene Daten handelt. Dies hängt maßgeblich davon ab, wer die Daten erhält und ob damit Rückschlüsse möglich sind etc.

2. Datenschutzrechtliche Rolle des Testfeldbetreibers

Adressat der zahlreichen Pflichten aus der DS-GVO ist der Verantwortliche im datenschutzrechtlichen Sinne. Aber auch den Auftragsverarbeiter treffen Pflichten im Umgang mit der Datenverarbeitung. Die Unterscheidung dieser beiden Rollen ist zur Bestimmung der Pflichten essenziell. Bei der Versendung von CAM-Nachrichten stellt sich die Frage, wer datenschutzrechtlich besehen die verantwortliche Person ist, falls es sich dabei um personenbezogene Daten handeln sollte.

a) Verantwortlicher

Eine Legaldefinition findet sich in Art. 4 Nr. 7 DS-GVO: „‘Verantwortlicher‘ [meint] 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; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.“

Verantwortlicher i.S. der DS-GVO ist folglich derjenige, der über Zweck und Mittel der Datenverarbeitung entscheidet.

b) Auftragsverarbeiter

[146] ETSI EN 302 637-2, V1.3.1 (2014-09), abrufbar unter: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjl87vZpIWDAxWKPOwKHfIwBEcQFnoECA0QAQ&url=https%3A%2F%2Fwww.etsi.org%2Fdeliver%2Fetsi_en%2F302600_302699%2F30263702%2F01.03.01_30%2Fen_30263702v010301v.pdf&usg=AOvVaw1e1kWOVPinL8jZ2UaRsqaV&opi=89978449 (zuletzt abgerufen am 10.12.2023).

Wird nicht über die Zwecke und Mittel der Datenverarbeitung entschieden, sondern erfolgt lediglich – weisungsgebunden – eine Auftragsdatenverarbeitung, so ist die datenschutzrechtliche Rolle die des Auftragsverarbeiters. Der Auftragsverarbeiter ist in Art. 4 Nr. 8 DS-GVO legaldefiniert.
Dies ist „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet".

Konkrete Anforderungen an den Auftragsverarbeiter sind in Art. 28 DS-GVO geregelt.

c) Bedeutung für CAM-Nachrichten

Werden i.R. der Nutzung von Testfeldern Kraftfahrzeuge genutzt, welche zu Testzwecken CAM-Nachrichten versenden, so beziehen sich die Daten aus dem Fahrzeug, die versendet werden, lediglich auf den Testfahrer. Diese Rechtsgrundlage zur Datenverarbeitung wird höchstwahrscheinlich schon aus seinem Arbeitsvertrag folgen, wenn er zu solchen Zwecken beschäftigt wird. Ansonsten kommt die Einwilligung als Rechtsgrundlage in Betracht. Je nachdem, was mit den versendeten Daten passiert und wer diese bearbeitet, bestimmen sich die datenschutzrechtlichen Rollen der Beteiligten. Der Nutzer des Testfelds, d.h. der Eigentümer des Fahrzeugs wird höchstwahrscheinlich Verantwortlicher im datenschutzrechtlichen Sinne sein. Der Betreiber des Testfelds kann Auftragsverarbeiter sein, wenn er weisungsgebunden die Daten für den Nutzer verarbeitet. Darf er die Daten zu eigenen Zwecken nutzen, so liegt eine getrennte Verantwortlichkeit vor. Werden die Daten gemeinsam genutzt, so liegt eine gemeinsame Verantwortlichkeit vor.

Auch wenn CAM-Nachrichten eine alle paar Minuten wechselnde User-ID nutzen, so handelt es sich für den Eigentümer des Kraftfahrzeugs um personenbezogene Daten. Je nachdem, was der Testfeldbetreiber an Daten empfängt bzw. auslesen darf, handelt es sich auch für ihn um personenbezogene Daten.

IV. Ergebnis

Die datenschutzrechtliche Beurteilung von CAM-Daten zeigt, dass sich die Versendung von Daten zu Forschungs- und Erprobungszwecken zum Regelbetrieb unterscheidet. Während im Regelbetrieb aufgrund der sich ständig wechselnden User-ID und den für sich genommen ungenauen Angaben nicht ohne Weiteres nachvollzogen werden kann, welches Fahrzeug in der Umgebung diese Nachrichten sendet und unklar ist, wem sie zuzuordnen sind, stellt sich dies i.R. von Testzwecken anders dar. Hier wissen Sender und Empfänger welcher Fahrer dem Fahrzeug zuzuordnen ist.

Je nach konkreter Ausgestaltung der Nutzung bestimmen sich die datenschutzrechtlichen Rollen. Ob es sich im konkreten Fall um personenbezogene Daten des Testfahrers handelt, hängt einerseits von den in den CAM-Nachrichten enthaltenen Daten ab und andererseits davon, wer diese Daten empfängt. Der Eigentümer des Fahrzeugs wird Verantwortlicher im datenschutzrechtlichen Sinn sein, sodass ihn die primären Anforderungen aus der DS-GVO treffen. Ist der Testfeldbetreiber lediglich Auftragsverarbeiter, so muss er die Pflichten aus Art. 28 DS-GVO erfüllen.

Für Betreiber von Testfeldern empfiehlt sich daher je nach Use-Case eine einzelne datenschutzrechtliche Bewertung des Sachverhalts.

D. Frage 4: Erläuterung des rechtspolitischen Ausblickes in Bezug auf die Gesetzgebung zur Autonomen Mobilität

I. Einführung

Die Beantwortung der vierten Frage zielt auf den rechtspolitischen Ausblick in Bezug auf die Gesetzgebung zur autonomen Mobilität. Hierfür zunächst ist eine Umgrenzung der untersuchten Rechtsbereiche erforderlich. Das Mobilitätsrecht erfasst die Bereiche Straßenverkehrsrecht, Haftungsrecht, Datenschutzrecht, IT-Sicherheitsrecht, Strafrecht und Wettbewerbsrecht. Vorliegend sind entsprechend der Auftragsvergabe insbesondere straßenverkehrsrechtliche Vorschriften – konkret §§ 1a-1c, 1d-1f, § 63a StVG nebst AFGBV – zu untersuchen. Die vorliegende Untersuchung beschränkt sich daher auf die Untersuchung des Straßenverkehrsrechts sowie in dem dargestellten Rahmen des Datenschutzrechts. Dabei werden Lücken, Rechtsunsicherheiten oder Rechtsunklarheiten herausgearbeitet. Hierauf aufbauend werden rechtspolitische Handlungsempfehlungen formuliert, wobei zwischen Entwicklern und Testfeldbetreibern unterschieden wird.

II. Darstellung der Rechtslage

§ 1 Abs. 1 S. 1 StVG i. V. m. § 3 Abs. 1 S. 1 FZV statuiert die Zulassungspflichtigkeit von Fahrzeugen auf öffentlichen Straßen, die auch für Fahrzeuge mit automatisierten Fahrfunktionen gilt. Für Fahrzeuge mit automatisierten und autonomen Fahrfunktionen enthalten die §§ 1a ff. und 1d ff. StVG spezialisierte Regelungen.

1. StVG-Novelle 2017

a) § 1a StVG

Mit dem Achten Gesetz zur Änderung des Straßenverkehrsgesetzes vom 16.6.2017 (sog. StVG-Novelle 2017) hat der Gesetzgeber durch die Einführung der §§ 1a – 1c, 63a, 63b StVG den rechtlichen Rahmen für den Betrieb von Fahrzeugen mittel hoch- und vollautomatisierter Fahrfunktionen verabschiedet. § 1a Abs. 2 S. 1 StVG enthält eine Begriffsbestimmung für Kraftfahrzeuge mit „hoch- oder vollautomatisierter Fahrfunktion“, womit nach allgemeiner Auffassung die SAE L3 und L4 gemeint sind.[147] Vom gesetzgeberischen Anwendungsbereich umfasst, sind (jedoch) nur solche Kraftfahrzeuge, die über die in Abs. 2 S. 1 näher konkretisierte technische Ausrüstung verfügen. Trotz des Wortlauts „hoch- und vollautomatisiert“ adressieren

[147] Vgl. nur Leupold/Wiebe/Glossner/*Beck*, Münchener Anwaltshandbuch IT-Recht, 4. Auflage 2021, Teil 9.2. Rn. 56.

die Regelungen im Kern Stufe 3. Diese unklare Normstruktur wird von verschiedenen Seiten kritisiert.[148]

Schwierigkeiten ergeben sich insbesondere aus der in Nr. 2 formulierten Anforderung, dass die technische Ausrüstung in der Lage sein muss, während der hoch- oder vollautomatisierten Fahrzeugsteuerung den an die Fahrzeugführung gerichteten Verkehrsvorschriften zu entsprechen.[149] Dies ergibt sich insbesondere mit Blick auf Testfelder, die gerade der Erprobung des ordnungsgemäßen Funktionierens der Fahrzeuge im Verkehr dienen.

Nach Abs. 1 des § 1a StVG ist der Betrieb eines solchen Fahrzeugs zulässig, wenn die Fahrfunktion „bestimmungsgemäß verwendet" wird. Eine Verwendung der Fahrfunktion außerhalb der seitens des Herstellers erfolgenden Zweck- und Nutzungsbestimmung ist daher unzulässig.[150] Der Begriff „bestimmungsgemäß" bezieht sich dabei vor allem auf die in der Systembeschreibung des Herstellers enthaltenen Systemgrenzen. So kann ein Fahrzeug bspw. auf den Betrieb auf Autobahnen beschränkt sein.[151]

Abs. 3 des § 1a StVG stellt klar, dass nur solche Fahrfunktionen von § 1a StVG umfasst sind, die nach den dort genannten[152] technischen Anforderungen zugelassen sind.

Abs. 4 des § 1a StVG bestimmt, dass Fahrzeugführer im Sinne des Gesetzes auch derjenige ist, der eine automatisierte Fahrfunktion aktiviert und zur Fahrzeugsteuerung verwendet, auch wenn er das Fahrzeug nicht eigenhändig steuert. In Zusammenschau mit anderen Vorschriften (vgl. etwa § 18 StVG) lässt sich hieraus die Notwendigkeit der Anwesenheit des Fahrzeugführers ableiten.[153]

b) § 1b StVG

§ 1b StVG enthält Rechte und Pflichten des Fahrzeugführers bei der Nutzung hoch- oder vollautomatisierter Fahrfunktionen. Besonders hervorzuheben ist hierbei die stetige Pflicht zur Wahrnehmungsbereitschaft nach Abs. 1, die jedoch keine dauerhafte Verkehrsbeobachtung erfordert.[154] Aus § 23 Abs. 1a S. 5 StVO, der festhält, dass § 1b StVG durch die Regelung in §

[148] Vgl. bspw. *Sesing*, „Fahrzeuge als (mittelbare) Normadressaten? Implikationen des Gesetzes zum autonomen Fahren", DSRITB 2021, 571 ff.; *Wagner*, Smart Mobility – Rechtliche Aspekte, FZI Forschungszentrum Informatik, S. 10.
[149] Mit entsprechendem Hinweis Leupold/Wiebe/Glossner/*Beck*, Münchener Anwaltshandbuch IT-Recht, 4. Auflage 2021, Teil 9.2. Rn. 60.
[150] Leupold/Wiebe/Glossner/*Beck*, Münchener Anwaltshandbuch IT-Recht, 4. Auflage 2021, Teil 9.2. Rn. 57 f.
[151] *Wagner*, Das neue Mobilitätsrecht, 2021, S. 55.
[152] Dies sind ECE-Regelungen oder abweichenden Bestimmungen in Art. 20 der Richtlinie 2007/46/EG bzw. ab 1. 9. 2020 Art. 39 der Verordnung (EU) 2018/858.
[153] Leupold/Wiebe/Glossner/*Beck*, Münchener Anwaltshandbuch IT-Recht, 4. Auflage 2021, Teil 9.2. Rn. 62.
[154] Leupold/Wiebe/Glossner/*Beck*, Münchener Anwaltshandbuch IT-Recht, 4. Auflage 2021, Teil 9.2. Rn. 63.

23a Abs. 1a S. 1-4 unberührt ist, lässt sich zudem ableiten, dass die Nutzung von Smartphones oder Notebooks während der Fahrzeugführung mittels hoch- oder vollautomatisierter Fahrfunktion iSd § 1a StVG grundsätzlich zulässig ist.[155] Auch der Gesetzgeber hat deutlich gemacht, dass Tätigkeiten wie das Bearbeiten von E-Mails oder die Nutzung des Infotainmentsystems möglich sein sollen.[156] Hierfür können FahrerInnen – je nach Systembeschreibung des Herstellers – die Hände vom Lenkrad nehmen und den Blick von der Straße nehmen.[157] In Zusammenschau mit der Pflicht zur Wahrnehmungsbereitschaft entsteht hieraus jedoch ein Kontrolldilemma.[158] Problematisch ist insbesondere die Vorgabe, dass der Fahrer in diesem Fall die Fahrzeugsteuerung *unverzüglich* übernehmen können muss (vgl. § 1b Abs. 2 StVG). Das BMVI versteht darunter, die die Fahraufgabe nach Aufforderung mit einer „angemessenen Zeitreserve" wieder vollständig und sicher übernommen werden muss.[159] In § 121 BGB wird unverzüglich konkretisiert als Handeln „ohne schuldhaftes Zögern"; dieses Begriffsverständnis wird auch auf andere gesetzliche Regelungen übertragen. Für den Bereich des automatisierten und autonomen Fahrens erklärt diese Formulierung jedoch nicht, wie sich der Fahrer während der Fahrt verhalten darf.[160] Der durch die automatisierte Steuerung erhoffte und versprochene Zugewinn an Bewegungsfreiheit und Entspannung wird daher geringer ausfallen, als ursprünglich erhofft.[161] Auch hier wird die mangelnde Gesetzesschärfe kritisiert.[162] Andererseits scheint es praktisch kaum möglich, aufgrund der Vielzahl möglicher Verkehrssituationen eine abschließende oder auch nur exemplarische Auflistung konkreter Wahrnehmungspflichten vorzunehmen. Vereinzelt findet sich der Vorschlag besonders prägnante Gefahrensituationen besonders hervorzuheben.[163]

Nach Abs. 2 ist der Fahrzeugführer verpflichtet, die Fahrzeugsteuerung unverzüglich wieder zu übernehmen, wenn ihn das hoch- oder vollautomatisierte System dazu auffordert (Nr. 1) oder wenn er erkennt oder auf Grund offensichtlicher Umstände erkennen muss, dass die Voraussetzungen für eine bestimmungsgemäße Verwendung der hoch- oder vollautomatisierten Fahrfunktionen nicht mehr vorliegen (Nr. 2). Dies ist etwa dann der Fall, wenn offensichtlich erkennbar ist, dass das System durch eine Fehlfunktion gestört ist.[164]

c) § 1c StVG

[155] Leupold/Wiebe/Glossner/*Beck*, Münchener Anwaltshandbuch IT-Recht, 4. Auflage 2021, Teil 9.2. Rn. 63.
[156] BT-Drs. 18/11776, S. 10.
[157] BT-Drs. 18/11776, S. 10.
[158] Vgl. *Wagner*, Das neue Mobilitätsrecht, 2021, S. 58. Zur Kritik *Armbrüster*, ZRP 2017, 83 (83 ff.); *König*, NZV 2017, 123 (123 ff.).
[159] BMVI, Strategie automatisiertes und vernetztes Fahren, S. 5.
[160] *Schirmer*, NZV 2017, 253 (255) mit Bsp.
[161] Zu dieser Problematik *Wagner*, Das neue Mobilitätsrecht, 2021, S. 58.
[162] *Wagner*, Smart Mobility – Rechtliche Aspekte, FZI Forschungszentrum Informatik, S. 19; *dies.*, Das neue Mobilitätsrecht, 2021, S 56 ff.
[163] In Betracht kommen typische akustische Signale wie ein Martinshorn oder das Hupen anderer Verkehrsteilnehmender (s. etwa Lange, NZV 2017, 345 (350)).
[164] BT-Drs. 18/11300, S. 22.

§ 1c StVG ergänzt diese Regelungen durch eine Pflicht zur wissenschaftlichen Evaluierung nach Ablauf des Jahres 2019.

d) § 63a StVG

§ 63a StVG regelt die Datenverarbeitung bei Fahrzeugen mit hoch- und vollautomatisierter Fahrfunktion. Die Vorschrift nimmt Bezug darauf, dass gemäß § 1a StVG die durch ein Satellitennavigationssystem ermittelten Positions- und Zeitangaben speichern, sobald ein Wechsel der Fahrzeugsteuerung zwischen Fahrzeugführer und dem hoch- oder vollautomatisierten System erfolgt. Damit wird von Seiten des Gesetzgebers zunächst unterstellt, dass die Speicherung dieser Daten DSGVO-konform möglich ist. Diesbezüglich ist auf die unter Frage 1 behandelten Aspekte zu verweisen.

Der Regelung des § 63a StVG wird unter dieser Annahme eine Verantwortungszuweisung nach Art. 4 Nr. 7 2. Hs. DSGVO entnommen. *Datenverantwortlicher* sind nach Art. 4 Nr. 7 1. Hs. DSGVO die natürlichen oder juristischen Personen, Behörden, Einrichtungen oder anderen Stellen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Im Bereich des autonomen und automatisierten Fahrens ist diese Zuweisung problematisch. Prinzipiell kommen als Datenverantwortliche Fahrer, Halter und Hersteller in Betracht.[165] Art. 4 Nr. 7 2. Hs. DSGVO sieht allerdings auch die Möglichkeit vor, bestimmte Kriterien der Benennung des Datenverantwortlichen durch das Unionsrecht oder das mitgliedstaatliche Recht vorgesehen werden können.

Eine detaillierte Auslegung des § 63a StVG führt allerdings insofern zu keinem eindeutigen Ergebnis.[166]

2. StVG-Novelle 2021

Die StVG-Novelle 2021 betraf Änderungen durch das Gesetz zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes (Gesetz zum autonomen Fahren). Hierdurch wurden die §§ 1d-1e StVG zu verschiedenen Rechtsfragen im Kontext autonomer Fahrzeuge (SAE Level 4) eingefügt.

a) § 1d StVG

Gemäß § 1d StVG ist der Regelbetrieb von Kfz mit autonomer Fahrfunktion von vier kumulativen Voraussetzungen abhängig: der Erfüllung der technischen Anforderungen, der

[165] Hierzu im Detail *Werner/Wagner/Pieper*, RDV 2020, 111 (112 ff.).
[166] Siehe *Werner/Wagner/Pieper*, RDV 2020, 111 (112 ff.).

Betriebserlaubnis durch das Kraftfahrt-Bundesamt, der Genehmigung des festgelegten Betriebsbereichs durch die nach Landesrecht zuständige Behörde und der Zulassung durch die Zulassungsbehörde.

Ein festgelegter Betriebsbereich ist nach § 1d Abs. 2 StVG der örtlich und räumlich bestimmte Straßenraum, in dem ein Kfz mit autonomer Fahrfunktion bei Vorliegen der Voraussetzungen gemäß § 1e Abs. 1 StVG betrieben werden darf. Dieser soll durch eine nach Landesrecht zuständige Behörde genehmigt werden, da diese über bessere Ortskenntnis verfügt. Genauere Eignungskriterien regelt § 9 Abs. 2 AFGBV. Es ist zu beachten, dass auch Testfelder im Rahmen der Erprobung von autonomen Fahrfunktionen einen späteren regulären Betriebsbereich simulieren können, wenn es sich um einen räumlich abgetrennten Bereich handelt und diese die Maßgaben des § 9 Abs. 2 AFGBV einhalten.

Gemäß § 1d Abs. 3 StVG liegt die menschliche Entscheidungsbefugnis und Verantwortung nicht mehr allein bei dem Fahrzeugführer oder der Fahrzeugführerin. Stattdessen wird die sog. Technische Aufsicht damit betraut: Dabei handelt es sich um diejenige natürliche Person, die dieses Kraftfahrzeug während des Betriebs gemäß § 1e Absatz 2 Nummer 8 deaktivieren und für dieses Kraftfahrzeug gemäß § 1e Absatz 2 Nummer 4 und Absatz 3 Fahrmanöver freigeben kann. Die letzte Verantwortung verbleibt damit beim Menschen. Eine endgültige Übertragung der Verantwortung auf das autonome Fahrzeug ist somit (noch) nicht vorgesehen. Gemäß § 14 AGBFV muss eine sachkundige und zuverlässige Aufsicht über einen Studienabschluss oder Abschluss als staatlich geprüfter Techniker der Fachrichtung Maschinenbau, Fahrzeugtechnik, Elektrotechnik oder Luft- und Raumfahrttechnik oder Luftfahrzeugtechnik verfügen.

b) § 1e StVG

Gemäß § 1e Abs. 1 S. 1 StVG ist der Betrieb eines autonomen Kfz nur zulässig, wenn das Fahrzeug den in Abs. 2 der Vorschrift konkretisierten technischen Voraussetzungen entspricht, für das Kfz eine Betriebserlaubnis erteilt worden ist, das Kfz in einem festgelegten Betriebsbereich eingesetzt wird und das KfZ zur Teilnahme am öffentlichen Straßenverkehr zugelassen ist.

Nach Abs. 2 Nr. 2 muss das technische System im Übrigen so ausgestaltet sein, dass die grundrechtlichen Rechtsgüter Leben und körperliche Unversehrtheit bestmöglichen Schutz genießen und Dilemmasituationen im Einklang mit grundgesetzlichen Vorgaben, insbesondere Art. 1 Abs. 1 GG, gelöst werden. Dementsprechend muss das technische System in der Lage sein, den an die Fahrzeugführung gerichteten Verkehrsvorschriften zu entsprechen und die über ein System der Unfallvermeidung verfügt, das auf Schadensvermeidung und Schadensreduzierung ausgelegt ist, bei einer unvermeidbaren alternativen Schädigung unterschiedlicher Rechtsgüter die Bedeutung der Rechtsgüter berücksichtigt, wobei der Schutz menschlichen Lebens die höchste Priorität besitzt, und für den Fall einer unvermeidbaren

alternativen Gefährdung von Menschenleben keine weitere Gewichtung anhand persönlicher Merkmale vorsieht.

Zu den technischen Voraussetzungen nach Abs. 2 Nr. 3 gehört insbesondere eine technische Ausstattung, die es ermöglicht, das Kraftfahrzeug selbstständig in einen risikominimalen Zustand zu versetzen, wenn die Fortsetzung der Fahrt nur durch eine Verletzung des Straßenverkehrsrechts möglich wäre.

c) § 1f StVG

Nach § 1f Abs. 1 StVG ist der Halter eines Kfz mit autonomer Fahrfunktion schließlich zur Erhaltung der Verkehrssicherheit und der Umweltverträglichkeit des Kfz verpflichtet. Die hierfür erforderlichen Vorkehrungen werden in Abs. 1 S. 2 näher konkretisiert. Weitere Halterpflichten finden sich in Abs. 3 des § 1f StVG.

Weitere Pflichten für die Technische Aufsicht über Kfz mit autonomer Fahrfunktion werden in Abs. 2 des § 1f StVG.

3. Experimentierklausel und Ausnahmegenehmigung

Da es sich bei dem Betrieb von Testfeldern um Reallabore handelt, in denen die technologische Entwicklung von automatisierten und autonomen Fahrzeugen vorangetrieben wird, ist zuletzt zu untersuchen, inwieweit aktuell Abweichungsmöglichkeiten vom bestehenden Gesetzesrecht bestehen. Näher zu untersuchen sind § 46 StVO, § 70 StVZO und § 19 StVZO.

a) § 46 StVO

Nach § 46 StVO können bestimmte Ausnahmen von den Vorgaben der Straßenverkehrsordnung genehmigt werden. Diese Ausnahmen können sich entweder auf die Fahrzeugführer oder Fahrzeuge beziehen. Die einzelfallbezogenen Ausnahmevorschriften betreffen jedoch zum einen nur Vorschriften der StVO (und gerade nicht des StVG, insbesondere §§ 1a ff. sowie 1d ff.) und zugleich zum anderen individuelle Anwendungsfälle (personeller wie sachlicher Art) und können sich daher nicht auf ein geographisch abgegrenztes Testfeld beziehen.

Zu berücksichtigen ist dabei auch, dass hierdurch zwar einzelne verhaltensbezogene Vorschriften ausgesetzt werden können, die Anwendung dieser verhaltensbezogenen Normen

auf automatisierte und autonome Fahrzeuge aber ohne problematisch ist, wie an anderer Stelle ausgeführt.

b) § 70 StVZO

§ 70 StVZO sieht verschiedene Ausnahmen von den Vorgaben der StVZO vor, ist aber ebenfalls für Formen automatisierten und autonomen Fahrens, die sich durch eine Verantwortungsverschiebung von Mensch auf Maschine auszeichnen, nicht weiterführend. § 70 StVZO lässt nur bedingte, im Einzelnen aufgeführte Abweichungen vom allgemeinen gesetzlichen Rahmen zu. Dies liegt insbesondere daran, dass § 70 StVZO als verordnungsrechtliche Regelung bloß Ausnahmen „von allen Vorschriften dieser Verordnung", nicht jedoch von gesetzlichen Maßgaben zulässt.

c) § 19 StVZO

Für Umbauten an konventionellen Fahrzeugen, die bereits über eine Betriebserlaubnis verfügen, enthält § 19 Abs. 6 StVZO eine Experimentierklausel, welche einem Hersteller oder einer Forschungseinrichtung ermöglicht, Einzelfahrzeuge nachträglich zu Testzwecken zu verändern. Diese Vorschrift findet jedoch im Hinblick auf automatisierte oder autonome Fahrzeuge keine Anwendung.

III. Lücken und Unklarheiten in der bisherigen Gesetzgebung sowie Handlungsempfehlungen

1. Konkretisierung der Fahrfunktionen

§§ 1a-1c StVG beziehen sich auf hoch- und vollautomatisierte Fahrfunktionen, §§ 1d-f StVG beziehen sich auf autonome Fahrfunktionen. Der Gesetzgeber vermeidet es hierbei auf die international etablierten technischen Klassifizierungen zu verweisen. Dies wird in der rechtswissenschaftlichen Literatur – wie oben erörtert – zu Recht kritisiert.

Aufgrund der unklaren Begriffsbildung in §§ 1a-c StVG einerseits und §§ 1d-f StVG andererseits wäre eine Klarstellung des gesetzlichen Anwendungsbereichs und eine Abgleichung mit der international anerkannten Nomenklatur hilfreich. Eine solche wäre sowohl für Hersteller als auch für Testfeldbetreiber hilfreich.

2. Konkretisierung der Fahrerpflichten

Zugleich herrscht Unklarheit, wie genau die Fahrerpflichten ausgestaltet sind. Dies betrifft insbesondere den Begriff der „Wahrnehmungsbereitschaft“ in § 1b StVG, da bereits die Gesetzesbegründung hierzu unterschiedliche Gesetzeskonkretisierungen vorgenommen hat.

Wie bereits zuvor erörtert, führt dieses Fahrerdilemma zu Rechtsunsicherheiten, welche im Zuge einer Anpassung der gesetzlichen Regulierung (etwa durch Benennung einzelner Anwendungsfälle) verhindert werden. Dies wäre für Hersteller und Testfeldbetreiber hilfreich.

3. Verhaltensorientierte Pflichten

Als problematisch erweist sich auch, dass sich verschiedene StVO-Vorschriften an den Fahrzeugführer richten und von diesem bspw. Rücksichtnahme erfordern. Eine technologieoffene Auslegung vermag dieses Verständnis zwar auch auf autonome Fahrzeuge zu übertragen, indem diesen Fahrzeugen ein Fahrverhalten abverlangt wird, wie man es von einem rücksichtsvollen Fahrer erwarten würde. Eine Entsprechensklausel könnte die Rechtslage noch einmal klarstellen. Dennoch würde es sich auch hierbei um eine ‚Behelfsregelung‘ handeln, welche die Transformation des Verkehrswesens nur unzureichend aufnehmen würde.[167] Zurecht wird darauf hingewiesen, dass einzelne Pflichten der StVO (bspw. § 3 IIa StVO) von autonomen Fahrzeugen letztlich gar nicht mehr erfüllt werden können.[168]

Die bisherigen Anpassungen des StVG greifen daher nicht die notwendige Neugestaltung des Regelungsapparats auf, sondern erweisen sich gewissermaßen als Flickenteppich. Das bestehende Regelungsregime wird durch eine weitreichende Involvierung menschlicher Entscheidungsträger (in Form von LenkerInnen oder Technischer Aufsicht) aufrechterhalten, ohne hierdurch die Herausforderungen der neuen Fahrsysteme wirklich zu bewältigen.[169] Die hierdurch verursachte Verantwortungsverschiebung von Mensch zur Maschine wird durch die gesetzlichen Regelungen nicht hinreichend aufgegriffen. Der staatlichen Innovationsverantwortung,[170] welche die Begleitung technischer Innovationen durch

[167] Kritisch daher auch *Rodi*, Die Zulassung autonomer Fahrzeuge zum Straßenverkehr aus rechtlicher und rechtspolitischer Sicht, in: Oppermann/Stender-Vorwachs (Hrsg), Autonomes Fahren – Technische Grundlagen Rechtsprobleme Rechtsfolgen, 2020, 429, Rz 9, 38; lex2vehicle (abrufbar unter: https://projekte.ffg.at/anhang/625533a2394e2_lex2vehicle_Ergebnisbericht.pdf), zuletzt abgerufen am 14.12.2023, S. 36.

[168] *Wagner*, Smart Mobility – Rechtliche Aspekte, FZI Forschungszentrum Informatik, S. 21.

[169] In diesem Sinne auch die Kritik bei lex2vehicle (abrufbar unter: https://projekte.ffg.at/anhang/625533a2394e2_lex2vehicle_Ergebnisbericht.pdf), zuletzt abgerufen am 14.12.2023, S. 37.

[170] Grundsätzlich zum Konzept der Innovationsverantwortung *Eifert/Hoffmann-Riem (Hrsg.)*, Innovationsverantwortung, 2009; ein aktueller Beitrag findet sich bei *Bora*, Zukunftsfähigkeit und Zukunftsfähigkeit und Innovationsverantwortung – Zum gesellschaftlichen Umgang mit komplexer Temporalität, in: Reflexion des Rechts – Beiträge zur responsiven Rechtssoziologie, 2023, S. 311 ff.

entsprechende staatliche Regulierung verlangt, wird auf diesem Wege nicht hinreichend nachgekommen.[171]

Aus dieser Perspektive ist eine prinzipielle Überprüfung der Normen des StVG und der StVO angezeigt. Regelungen, die automatisierte und autonome Fahrzeuge adressieren, sollten die Besonderheiten dieser Fahrzeugtechnik erkennen und aufgreifen und ein entsprechendes Sicherheitskonzept entwickeln. Darauf aufbauende Gesetzesänderungen würden insbesondere für die Entwickler weitere Rechtssicherheit bedeuten.

4. Datenschutzrechtliche Verantwortlichkeit

Wie oben dargelegt, gibt es weitreichende Unklarheiten hinsichtlich der datenschutzrechtlichen Verantwortlichkeit von Fahrern, Haltern und Herstellern automatisierter und autonomer Fahrzeuge. Auch § 63a StVG bietet insofern keine Klarstellung. Es liegt daher im Interesse der Hersteller insoweit eine klarstellende Regelung einzufügen. Nach den Vorgaben der DSGVO wäre es wohl rechtlich möglich, eine alleinige Verantwortlichkeit des Herstellers anzunehmen. Da Fahrer und Halter nicht über die notwendigen faktischen Zugriffsmöglichkeiten verfügen, ist deren (alleinige) Datenverantwortlichkeit unionsrechtlich bereits ausgeschlossen.[172]

Im Hinblick auf die Vielzahl (auch weiterer) datenschutzrechtlicher Fragen wird vereinzelt der Erlass eines Mobilitätdatenschutzgesetzes vorgeschlagen,[173] welches den Besonderheiten der Anforderungen des Datenschutzes gerade im Bereich des automatisierten und autonomen Fahrens gerecht werden könnte. Aus kompetenzrechtlichen Gründen wäre ein solches Gesetz jedoch letztlich auf Unionsebene zu erlassen.[174]

5. Rechtlicher Umgang mit Testfeldern

Testfelder dienen als Reallabore zur Erforschung automatisierter und autonomer Fahrzeugtechniken. Die Deklaration eines Abschnitts des öffentlichen Straßenraums zum Testfeld entbindet jedoch nicht von der Pflicht zur Einhaltung des Zulassungs- und Verhaltensrechts; die Benennung eines Bereichs des öffentlichen Straßenverkehrsraums zum Testfeld hat daher keine straßenverkehrsrechtlichen Folgen.[175] Testungen, die erfolgen, ohne vorab eine straßenverkehrsrechtliche Zulassung einzuholen, sind nur auf privatem Grund möglich. Selbst bei Zulassungsfreiheit, die sich nach §§ 1, 3 FZV i.V.m. § 1 StVG bei einer

[171] Ähnlich lex2vehicle (abrufbar unter: https://projekte.ffg.at/anhang/625533a2394e2_lex2vehicle_Ergebnisbericht.pdf), zuletzt abgerufen am 14.12.2023, S. 37.
[172] *Werner/Wagner/Pieper*, RDV 2020, 111 (116).
[173] Nur exemplarisch *Wagner*, SVR 2021, 287 (291).
[174] In diesem Sinne auch *Wagner*, SVR 2021, 287 (291).
[175] *Wagner*, Smart Mobility – Rechtliche Aspekte, FZI Forschungszentrum Informatik, S. 42.

bauartbedingten Höchstgeschwindigkeit von weniger als 6 km/h ergibt (was etwa bei Lieferrobotern denkbar sein könnte), ist ein Betrieb nach § 16 StVZO nur möglich, wenn sämtliche Vorschriften der StVZO und der StVO erfüllt sind.

Nach § 2 AFGBV[176] ist für den Betrieb eines Kfz mit autonomer Fahrfunktion in festgelegten Betriebsbereichen im öffentlichen Straßenraum eine Betriebserlaubnis des Kraftfahrt-Bundesamt nach § 4 Abs. 1 AFGBV erforderlich. Diese Genehmigung ist nach § 3 Abs. 1 AFGBV durch den Hersteller beim Kraftfahrt-Bundesamt zu beantragen. Nach § 7 Abs. 1 AFGBV ist zudem die Festlegung des Betriebsbereichs genehmigungspflichtig: Danach dürfen Kfz mit autonomer Fahrfunktion im öffentlichen Straßenraum nur in festgelegten und genehmigten Betriebsbereich i.S.d. § 1d Abs. 2 StVG betrieben werden. Die Festlegung des Betriebsbereichs erfolgt nach § 7 Abs. 2 StVG durch den Halter des Kfz. Von diesem ist die nach § 8 AFGBV näher konkretisierte Genehmigung zu beantragen.

Aufgrund dieser Regelungen scheint es derzeit kaum möglich, ein Testfeld vorab als „festgelegten Betriebsbereich" i.S.d. § 1d Abs. 2 StVG genehmigen zu lassen. Dies könnte zwar Erleichterungen bei der Einholung der Betriebserlaubnis für Testfahrzeuge bedeuten. Allerdings sehen §§ 7, 8 AFGBV – wie dargelegt – einen Antrag des Halters für die Festlegung des Betriebsbereichs vor. Auch hierfür muss eine Betriebserlaubnis vorliegen. Die Genehmigung eines Betriebsbereichs ist bei reinen Erprobungsfahrzeugen nach § 1i StVG nicht vorgesehen; hier kann allerdings eine Nebenbestimmung den Betrieb auf einen bestimmten Betriebsbereich beschränken.

Im Folgenden ist daher zu untersuchen, inwiefern es sinnvoll wäre, die bestehenden StVG-Regelungen durch eine Experimentierklausel zu ergänzen.[177] Eine solche Experimentierklausel könnte insbesondere für Testfeldbetreiber Rechtssicherheit herbeiführen. Bislang ist die Erprobung von vollautomatisierten und autonomen Fahrfunktionen rechtlich nur unter Einbindung eines Sicherheitsfahrers genehmigungsfähig. Diese menschliche Rückfallebene ist jedoch dem rechtlichen und technologischen Dazulernen abträglich.[178] Zumindest für Fahrfunktionen des SAE-Levels 4 fehlt es bislang an Regelungen. Die rechtliche Möglichkeit, Ausnahmesituationen im Wege von Ausnahmegenehmigungen gemäß § 70 StVZO Rechnung zu tragen, hilft nicht weiter. Von dem Grundsatz eines vollverantwortlichen Fahrzeugführers

[176] Verordnung zur Genehmigung und zum Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen vom 24. Juni 2022 (BGBl. I S. 986), die durch Artikel 10 der Verordnung vom 20. Juli 2023 (BGBl. 2023 I Nr. 199).

[177] Einen Vorschlag für eine solche Experimentierklausel formuliert IKEM, Eine Experimentierklausel für Kraftfahrzeuge mit autonomer, vernetzter und teleoperierter Fahrfunktion im StVG, 2020 (abrufbar unter https://www.ikem.de/wp-content/uploads/2020/09/20200902_Experimentierklausel_StVG_autonomes-Fahren.pdf), zuletzt abgerufen am 14.12.2023, S. 1 f.

[178] So explizit IKEM, Eine Experimentierklausel für Kraftfahrzeuge mit autonomer, vernetzter und teleoperierter Fahrfunktion im StVG, 2020 (abrufbar unter https://www.ikem.de/wp-content/uploads/2020/09/20200902_Experimentierklausel_StVG_autonomes-Fahren.pdf), zuletzt abgerufen am 14.12.2023, S. 3.

kann eine Ausnahme nicht erteilt werden, weil keine dahingehende Rechtsgrundlage der Verwaltung vorliegt.

Eine solche Experimentierklausel ist eine Gesetzestechnik, mit deren Hilfe der Gesetz- oder Verordnungsgeber die Exekutive ermächtigt, zwecks Erprobung eines von der Verwaltung geplanten Vorhabens, das später auf der Grundlage gewonnener Erfahrungen endgültig normiert werden soll, von geltendem Recht abzuweichen oder zu dispensieren.[179] Der Experimentierklausel kommt daher der Charakter einer Dispensermächtigung zu.[180] Die Experimentierklausel dient als Reformklausel, die den Rahmen bietet, die erwartbare Transformation des Verkehrssystems zu erforschen. Sie ermöglicht das systematische Sammeln von Erfahrungen (im vorliegenden Fall bei der Fortentwicklung automatisierter und autonomer Fortbewegungsmodalitäten) mit dem Ziel, diese im Rahmen künftiger gesetzlicher Regelungen zu berücksichtigen.[181] Insofern ist die Verwendung von Experimentierklauseln gerade in einem Gebiet empfehlenswert, das – wie das vorliegende – in hohem Maße von technologischem Fortschritt und der Notwendigkeit ihrer rechtlichen Regulierung bestimmt ist.

Zu untersuchen bleibt dann, welche Anforderungen an eine Experimentierklausel zu stellen wären.[182] Zu beachten ist, dass derartige Experimentierklauseln das Verhältnis von Gesetzgeber und Verwaltung verschieben: Während der Gesetzgeber normalerweise berufen ist, den Steuerungsimpuls an die Verwaltung geben, welche die gesetzgeberischen Vorgaben ohne oder mit geringem Gestaltungsspielraum umsetzen muss, ermächtigt eine Experimentierklausel die Verwaltung zu einem deutlich weiteren Handlungsfeld. Um die demokratische Legitimation, die auf sachlich-inhaltlicher Ebene die Bindung der Verwaltung an das Gesetz fordert, dennoch zu gewährleisten, muss die Experimentierklausel bestimmten Voraussetzungen entsprechen. Abhängig von der Grundrechtsrelevanz des administrativen Handlungsspielraums muss die Experimentierklausel ein hinreichendes Maß an Bestimmtheit aufweisen.

Der gesetzgeberische Handlungsauftrag lässt sich auch aus dem grundrechtlichen Gesetzesvorbehalt ableiten. So dürfen Eingriffe in die hier betroffenen Grundrechte auf Leben und körperliche Unversehrtheit (Art. 2 Abs. 2 S. 1 GG) sowie auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) aufgrund oder durch eine gesetzliche Regelung erfolgen. Hier ist der parlamentarische Gesetzgeber gefragt, die tatsächlichen Grenzen der grundrechtlichen Freiheiten abzustecken, wobei er diese Grundrechte mit entgegenstehenden verfassungsrechtlichen Wertungen abwägen muss. Davon ausgehend, dass die Fortentwicklung automatisierten und autonomen Fahrens eine weitere Reduktion an Verkehrsunfällen sowie eine breite Teilhabe der Bevölkerung an motorisierter Fortbewegung

[179] *Maaß*, Experimentierklauseln für die Verwaltung und ihre verfassungsrechtlichen Grenzen, 2001, S. 39.
[180] *Beck/Schürmeier*, Die kommunalrechtliche Experimentierklausel als Reforminstrument, LKV 2004, 488 (488 f.).
[181] *Maaß*, Experimentierklauseln für die Verwaltung und ihre verfassungsrechtlichen Grenzen, 2001, S. 33.
[182] Beispielhaft wurde eine solche Experimentierklausel von IKEM („Eine Experimentierklausel für Kraftfahrzeuge mit autonomer, vernetzter und teleoperierter Fahrfunktion im StVG“) formuliert (abrufbar unter file:///C:/Users/danie/Desktop/DLR/Literatur/20200902_Experimentierklausel_StVG_autonomes-Fahren.pdf).

sicherstellen kann, sprechen für die Eröffnung eines experimentellen Handlungsspielraums ebenso Art. 2 Abs. 2 S. 1 GG und Art. 3 Abs. 1, 3 GG.

Um die notwendige Rechtssicherheit und Bestimmtheit der Regelung zu gewährleisten, muss die Experimentierklausel zwingend folgende Inhalte enthalten:

- Zwecksetzung der Abweichung

- Formale Voraussetzungen

  Unter den formalen Voraussetzungen ist insbesondere der Kreis der Antragsberechtigten zu bestimmen: Da auch die Novellierung durch die StVG 2021 keine Möglichkeiten eröffnet hat, ein Testfeld als festgelegten (Betriebs-)Bereich genehmigen zu lassen, da der Antrag durch die Fahrzeughalterin oder den Fahrzeughalter erfolgen müsste, wäre an dieser Stelle empfehlenswert den Kreis der Antragsberechtigten auf Testfeldbetreiber zu erweitern, um hierdurch tatsächliche Hürden für derartige Experimentierräume abzubauen.

  Als weitere formale Voraussetzung ist zugleich die Zuständigkeit zur Erteilung der Abweichung zu regeln.

- Inhaltliche Voraussetzungen

  Unter den inhaltlichen Voraussetzungen sollte zunächst der Anwendungsbereich spezifiziert werden, der auf Fälle des automatisierten, autonomen und teleoptierten Fahrens erstreckt werden sollte.

  Zugleich ist die räumliche Abgrenzung des Testfelds zu konkretisieren.

  Auch die Reichweite der Abweichungsbefugnis, also die Reichweite der Möglichkeit von einzelnen straßenverkehrsrechtlichen Vorschriften abzuweichen, ist im Gesetzestext genau zu bestimmen.

  Da dem Testfeld experimenteller Charakter zukommt, muss es auch Regelungen zur zeitlichen Befristung der Abweichungsbefugnis geben.

- Kenntlichmachung bei Testfeldern im Regelbetrieb

Entsprechende Vorgaben sind aus Gründen der Rechtssicherheit in die Experimentierklausel aufzunehmen.

- Befristung der Experimentierklausel und Evaluation

Da die Experimentierklausel der Erforschung und Erprobung neuer Innovationen dient, ist sie zugleich selbst zu befristen und einer Evaluationspflicht zu unterwerfen.

IV. Ergebnis

Anpassungsbedarf zeigen sich insbesondere mit Blick auf die Benennung und Beschreibung neuer Fahrfunktionen, die Konkretisierung der Fahrerpflichten, den Umgang mit verhaltensorientierten Pflichten, welche auf autonome Fahrzeige naturgemäß schlecht anwendbar sind, sowie die datenschutzrechtliche Verantwortlichkeit.

Im Hinblick auf Testfelder des autonomen und automatisierten Fahrens bleiben besonders viele Fragen offen, sodass die Einführung einer Experimentierklausel empfehlenswert wäre. Die Anforderungen an eine solche Experimentierklausel werden im Einzelnen aufgelistet.