März 2023
11. Jahrg.
Seite 1 – 92

RAW

1

Recht ■ Automobil ■ Wirtschaft
Unternehmen | Technologie | Beratung

dfv Mediengruppe · Frankfurt am Main

Elisabeth Macher, LL.M. (Birmingham), Paul Schmitz, beide Köln und Dr. Frank-Bernd Weigand, LL.M. (London), Weiden i. d. OPf.*

Im Spannungsfeld zwischen Cybersecurity und Wettbewerb – (wie) darf der Fahrzeughersteller den Zugang zum OBD-Port kontrollieren?

Der Markt für Fahrzeugreparatur und -wartung befindet sich im Umbruch: Moderne Fahrzeuge erinnern immer mehr an fahrende Computer. Ohne Zugriff auf die elektronischen Steuergeräte eines Fahrzeugs, beispielsweise das Auslesen von Fehlercodes, ist eine Diagnose, Reparatur oder Wartung nicht mehr möglich. Der „Blick unter die Motorhaube" genügt nicht mehr.
Dreh- und Angelpunkt für diese Arbeiten ist der gesetzlich vorgeschriebene OBD-Port (On-Board-Diagnose-Port), mit dem jedes Fahrzeug standardmäßig vom Hersteller ausgerüstet wird. Über den OBD-Port kann ein Mechatroniker ein Diagnosegerät an das Fahrzeug anschließen und so in der Werkstatt auf den Datenstrom des Fahrzeugs zugreifen. Kaum ein Service kann ohne diese elektronische Fahrzeugdiagnose ausgeführt werden. Der einfache und direkte Zugriff über den OBD-Port ist dementsprechend für Werkstätten überlebenswichtig. Fahrzeughersteller sind daher verpflichtet, Marktteilnehmern (insbesondere freien, d. h. nicht markengebundenen Werkstätten) Zugang zum Fahrzeugdatenstrom über den OBD-Port zu ermöglichen.
Gleichzeitig ist das Thema Cybersecurity omnipräsent: Der Zugriff auf den Fahrzeugdatenstrom kann Gefahren bergen. Die Furcht vor Fernmanipulationen an fahrenden Autos ist groß. Neue Vorschriften verpflichten Fahrzeughersteller zum Schutz ihrer Fahrzeuge auch und gerade vor Cyberangriffen. Es herrscht daher große Unsicherheit, welche Maßnahmen Fahrzeughersteller zur Sicherstellung der Cybersecurity ergreifen müssen bzw. dürfen, ohne gleichzeitig ihre Pflicht zur Bereitstellung der Fahrzeugdaten mittels des OBD-Ports zu verletzen. Aktuell ist diese Frage auch Thema eines Vorabentscheidungsverfahrens vor dem Europäischen Gerichtshof (EuGH, Rs. C-296/22).[1]

I. Der OBD-Port und seine Bedeutung

Einleitend soll kurz der OBD-Port als solcher und seine Bedeutung für die Fahrzeugreparatur erläutert werden. Der OBD-Port bzw. die OBD-Schnittstelle ist eine Buchse im Fahrzeuginneren, über die Diagnosegeräte an das Fahrzeug angeschlossen werden können. Diese Diagnosegeräte wiederum sind für die Arbeit der Werkstatt unerlässlich. Sie greifen auf den Fahrzeugdatenstrom zu, lesen beispielsweise von den Steuergeräten des Fahrzeugs gemeldete Fehlercodes aus und fragen Informationen zum Fahrzeugzustand ab. Die Werkstatt kann so genau diagnostizieren, ob und an welcher Stelle ein technisches Problem vorliegt. Über diesen sog. Lesezugriff hinaus können mittels des Diagnosegeräts über den OBD-Port auch Reparaturen oder Wartungen vorgenommen werden. Dafür ist regelmäßig ein sog. Schreibzugriff erforderlich.

Für die Reparatur selbst ist es häufig erforderlich, dass Anlernprozesse und Kalibrierungen, d. h. Schreibvorgänge, durchgeführt werden. Wird beispielsweise eine Windschutzscheibe ausgetauscht, müssen danach Sensoren und Kameras neu justiert („kalibriert") werden, damit Fahrassistenzsysteme weiterhin wie vorgesehen arbeiten. Neu verbaute Komponenten müssen im Fahrzeug elektronisch „angelernt", also gewissermaßen installiert werden, damit sie ordnungsgemäß funktionieren. Vorhandene Fehlercodes in den Steuergeräten müssen nach erfolgter Reparatur wieder gelöscht werden. Darüber hinaus müssen Warnhinweise an den Fahrer (z. B., dass eine Wartung durchzuführen ist) nach erfolgtem Service entfernt werden. Fahrzeugmodelle der heutigen Generation unterscheiden sich in dieser Hinsicht erheblich von ihren „analogen" Vorgängern. Zur rein mechanischen Reparatur und Wartung kommen digital durchzuführende Vorgänge hinzu. Dafür ist zwingend der Zugang zum Fahrzeugdatenstrom per Diagnosegerät über die OBD-Schnittstelle erforderlich.

Diagnosegeräte werden zum einen von den Fahrzeugherstellern selbst für ihre jeweiligen Marken angeboten; zum anderen sind auf dem Markt auch generische (Mehrmarken-)Diagnosegeräte erhältlich, die universell und nicht nur für Fahrzeuge eines bestimmten Herstellers einsetzbar sind. Gerade freie Werkstätten, die Services für mehrere Marken anbieten, sind für ihre Arbeit auf diese generischen Diagnosegeräte angewiesen.

II. Der Zugangsanspruch des freien Marktes

Auf dem Reparatur- und Ersatzteilmarkt stehen mit dem Hersteller vertraglich verbundene Markenwerkstätten und freie Werkstätten in direktem Wettbewerb. Zur Gewährleistung des Wettbewerbs auf diesem Markt[2] (und damit letztlich im Interesse des Verbrauchers) hat der EU-Gesetzgeber im Typgenehmigungsrecht Zugangsansprüche des freien Marktes zu Fahrzeugen und technischen Informationen normiert. So sind Fahrzeughersteller nach Anhang X, Ziff. 2.9 der Verordnung (EU) 2018/858 gesetzlich verpflichtet, den Zugriff auf den Fahrzeugdatenstrom über den OBD-Port zu ermöglichen. Anhang X, Ziff. 2.9 lautet:

„Für die Zwecke der Fahrzeug-OBD sowie der Fahrzeugdiagnose, -reparatur und -wartung ist der direkte Fahr-

* Mehr über die Autoren erfahren Sie auf S. III und IV.

1 Das Vorabentscheidungsverfahren geht auf eine Vorlage des Landgerichts Köln in einem wettbewerbsrechtlichen Musterverfahren zurück, das die Unternehmen *A.T.U Auto-Teile-Unger* und *Carglass* gegen den Fahrzeughersteller *FCA Italy* angestrengt haben. Die Autoren sind an dem Verfahren vor dem Landgericht Köln und dem Vorabentscheidungsverfahren als Partei (A.T.U Auto-Teile-Unger, Frank-Bernd Weigand) bzw. als Prozessbevollmächtigte (Elisabeth Macher, Paul Schmitz) beteiligt.

2 Erwägungsgrund 52 der Verordnung (EU) 2018/858 stellt das gesetzgeberische Ziel heraus, dass „der unabhängige Markt der Fahrzeugreparatur und Fahrzeugwartung insgesamt mit Vertragshändlern konkurrieren kann".

zeugdatenstrom über einen seriellen genormten Datenübertragungsanschluss gemäß der UN-Regelung Nr. 83 Anhang 11 Anlage 1 Nummer 6.5.1.4 und der UN-Regelung Nr. 49 Anhang 9B Nummer 4.7.3 bereitzustellen.

Befindet sich das Fahrzeug in Bewegung, so darf auf die Daten nur im Lesemodus zugegriffen werden."

Aus dem zweiten Satz („Befindet sich das Fahrzeug in Bewegung, …") folgt im Umkehrschluss, dass bei stehenden Fahrzeugen nicht nur der Lesemodus, sondern zusätzlich auch der Schreibzugriff zu ermöglichen ist. Dieser ist, wie eingangs aufgezeigt, während und nach einem Servicevorgang unabdingbar, um eine Werkstattleistung ordnungsgemäß erbringen und abschließen zu können.

Abseits der Bedingung, dass sich das Fahrzeug für den Schreibzugriff nicht in Bewegung befinden darf, existieren (nur) in sensiblen Spezialbereichen, nämlich der Diebstahlsicherung und der Emissionskalibrierung, weitere gesetzliche Voraussetzungen für die Bereitstellung des Fahrzeugdatenstroms. So sieht Anhang X, Ziff. 6.2 der Verordnung (EU) 2018/858 für den Bereich der Diebstahlsicherung vor, dass „Sicherheitsmerkmale" der Fahrzeuge durch „Sicherheitstechnik" geschützt werden müssen. Dazu gehört u. a., dass sich freie Werkstätten für den Zugriff auf diebstahlsrelevante Informationen und Funktionen („SERMI")[3] des Fahrzeugs zunächst bei einer unabhängigen Prüfstelle akkreditieren lassen müssen.[4] Erst wenn sie so autorisiert sind, muss der Fahrzeughersteller ihnen Zugriff auf diese Sicherheitsmerkmale einräumen.

Ebenso hat der Gesetzgeber für den – insbesondere politisch sensiblen – Bereich der Emissionskalibrierung Schutzmaßnahmen vorgesehen. Rechner für die Emissionsbegrenzung im Fahrzeug müssen technisch gegen unbefugte Eingriffe geschützt werden, sodass Veränderungen nicht ohne Genehmigung des Herstellers vorgenommen werden können.[5] Das Gesetz hält jedoch ausdrücklich fest, dass „lediglich Funktionen, die unmittelbar mit der Emissionskalibrierung oder der Diebstahlsicherung zusammenhängen", auf diese Weise geschützt werden dürfen.[6]

Schließlich sieht Art. 63 der Verordnung (EU) 2018/858 noch vor, dass Hersteller den Zugang zu Reparatur- und Wartungsinformationen (also statischen, auf Webseiten abrufbaren Informationen wie etwa Teilekatalogen und Reparaturanleitungen) von der Entrichtung einer Gebühr abhängig machen können. Für den Zugang auf die Live-Daten (den Fahrzeugdatenstrom) eines Fahrzeugs über den OBD-Port gibt es eine solche Vorschrift hingegen nicht.

III. Cybersecurity-Risiken und -Vorgaben

Während Fahrzeughersteller also einerseits zur weitgehend unbeschränkten Bereitstellung des OBD-Ports verpflichtet sind, sehen sie sich andererseits zunehmend Vorgaben zur Fahrzeugsicherheit, insbesondere zur Cybersecurity gegenüber. So gibt es nicht nur neue bzw. überarbeitete Vorschriften zur allgemeinen Fahrzeugsicherheit (Verordnung (EU) 2019/2144, sog. General Safety Regulation), sondern auch spezifische Rechtsakte zur Cybersecurity im Automobilbereich.

Die UN/ECE-Verordnungen R155 und R156 definieren Anforderungen an die Cybersecurity und wurden jüngst in den europäischen Typgenehmigungsrahmen implementiert.[7] Fahrzeughersteller müssen danach künftig ein Cybersecurity-Management-System implementieren und aufrechterhalten und entsprechende Nachweise erbringen, dass sie potenziellen Cyberattacken wirkungsvoll begegnen können.

Für die OBD-Schnittstelle besonders relevant ist dabei die Vorschrift der UN/ECE R155, Teil B, Ziff. 18.3, die vorschreibt, dass „an externen Schnittstellen […] Sicherheitsmaßnahmen anzuwenden" seien. Konkretere Vorgaben zu den anzuwendenden Sicherheitsmaßnahmen macht die Verordnung jedoch nicht. Die UN/ECE R155 spezifiziert keine konkreten Minderungs- oder Abwehrmaßnahmen, sondern legt die Wahl der Mittel grundsätzlich in die Hand des Fahrzeugherstellers.

Die Praxis der Fahrzeughersteller zum Schutz des OBD-Ports besteht zumeist darin, den zentralen Server des Herstellers zwischen Fahrzeug und Diagnosegerät zu schalten und so den Zugang zum OBD-Port zu kontrollieren. Die Kontrolle reicht von Registrierungserfordernissen über Zertifikatslösungen bis hin zur kompletten Sperrung von Schreibzugriffen über den OBD-Port für freie Werkstätten.

IV. (Wie) lässt sich das Spannungsfeld zwischen Cybersecurity und Wettbewerb auflösen?

Auf den ersten Blick scheinen Fahrzeughersteller mit einem Dilemma konfrontiert zu sein: Wie können sie den eindeutigen Anforderungen an die Bereitstellung des Fahrzeugdatenstroms genügen, ohne gleichzeitig erforderliche Maßnahmen zur Gewährleistung der Fahrzeugsicherheit zu vernachlässigen?

1. Spannungsfeld zwischen Cybersecurity und Wettbewerb

Die UN/ECE R155 benennt zwar Risiken, gibt jedoch keine konkreten Abwehr- bzw. Minderungsmaßnahmen vor und räumt den Fahrzeugherstellern insoweit einen Spielraum bei der Umsetzung ein.[8] Gerade dieser Spielraum bei der Implementierung von Sicherheitsmaßnahmen kann zu (Rechts-)Unsicherheit führen: Welche Maßnahmen darf der Fahrzeughersteller ergreifen? Selbst das Aufstellen vergleichsweise niedrigschwelliger Bedingungen wie etwa das Erfordernis, dass ein Mechatroniker sich vorab bei dem Hersteller registriert, stellt eine Einschränkung des Zugangsanspruchs dar. Wird Zugang erst bei Erfüllung einer Bedingung gewährt, wird er zunächst verweigert. Erst recht gilt dies, wenn Bedingungen prohibitiver werden und über die oben genannten Beispiele aus der derzeitigen Praxis hinausgehen. Zu denken ist etwa an hohe Gebühren oder die Beibringung personenbezogener Daten einzelner Werkstattmitarbeiter oder den Nachweis besonderer Qualifikationen. Zusätzlich birgt der zwischengeschaltete Server des

3 Security-related repair and maintenance information bzw. sicherheitsrelevante Reparatur- und Wartungsinformationen; s. Delegierte Verordnung (EU) 2021/1244, Anhang Ziff. 7 zur neuen Anlage 3, dort Ziff. 2.1.3. Die Delegierte Verordnung wird zum 23.7.2023 wirksam.

4 Delegierte Verordnung (EU) 2021/1244, Anhang Ziff. 7 zur neuen Anlage 3, dort Ziff. 3.

5 Verordnung (EU) 2017/1151, Anhang I, Ziff. 2.3.1 in der konsolidierten Fassung vom 25.1.2020.

6 Ebenda.

7 In der General Safety Regulation, Anhang II wurde für die Anforderung „D4 – Schutz des Fahrzeugs gegen Cyberangriffe" ein entsprechender Verweis auf die UN/ECE R155 eingefügt.

8 Vgl. dazu auch *Harms*, RAW 2022, 153, 156.

Herstellers stets das Risiko, dass ein Zugriff zeitweise schon aufgrund technischer Probleme nicht möglich ist, etwa weil der Server des Herstellers ausfällt oder sonst nicht erreichbar ist. Der Zugangsanspruch wird in diesen Zeitspannen nicht erfüllt.

Muss der Fahrzeughersteller also selbst eine Abwägung zwischen scheinbar widerstreitenden Vorgaben und Interessen vornehmen und sich dem Risiko aussetzen, entweder die Sicherheit außer Acht zu lassen oder seinen wettbewerbsbezogenen Verpflichtungen nicht nachzukommen? Diese Situation wäre auch für freie Werkstätten, für deren tägliche Arbeit der Zugriff auf die genormte OBD-Schnittstelle essenziell ist, mehr als unbefriedigend: Anstatt – wie durch die Normung der Schnittstelle intendiert – mit universell einsetzbaren Diagnosegeräten auf den Fahrzeugdatenstrom zugreifen zu können,[9] könnten sie sich mit einem Flickenteppich individueller Zugangshürden konfrontiert sehen. Je nach Fahrzeug und Fahrzeughersteller müssten sie dann unterschiedliche, sich ggf. auch verändernde Registrierungs- und Zugangssysteme überwinden und für diese Mehrbelastung womöglich noch besondere Entgelte entrichten. Dies würde das Geschäftsmodell der freien (nicht markengebundenen) Werkstätten und so den Wettbewerb auf dem Markt ernsthaft gefährden.

2. Gesetzgeberische Vorgabe: Vorrang des Zugangsanspruchs

Tatsächlich hat der Gesetzgeber das beschriebene Spannungsverhältnis jedoch erkannt und aufgelöst. Das EU-Typgenehmigungsrecht gibt vor, wie die verschiedenen Verpflichtungen in Einklang zu bringen sind und lässt die Rechtsanwender nicht im Ungewissen.

a) General Safety Regulation

Inwiefern Fahrzeughersteller Maßnahmen zur Gewährleistung der Fahrzeugsicherheit treffen müssen, ist im Typgenehmigungsrecht insbesondere in der General Safety Regulation (GSR) geregelt. Art. 4 Abs. 4 und 5 der GSR geben dem Fahrzeughersteller auf, sicherzustellen, dass Fahrzeuge so konstruiert sind, dass die Gefahr von Verletzungen für die Fahrzeuginsassen und andere Fahrzeugteilnehmer möglichst gering ist. Zudem muss sichergestellt sein, dass die Fahrzeuge mit Anforderungen u. a. zum „Schutz vor unbefugter Verwendung einschließlich Cyberangriffen" übereinstimmen.

Wie diese Sicherheitsvorgaben und die Bereitstellungspflicht des Herstellers hinsichtlich des Fahrzeugdatenstroms in Einklang zu bringen sind, gibt die GSR selbst vor. In den Erwägungsgründen 26 und 27 heißt es:

„(26) Die Vernetzung und Automatisierung von Fahrzeugen erhöht die Möglichkeit des unbefugten drahtlosen („over-the-air") Fernzugriffs auf Fahrzeugdaten sowie entsprechender rechtswidriger Änderungen der Software. Um solchen Risiken Rechnung zu tragen, sollten die UN-Regelungen und andere Rechtsakte zur Cybersicherheit möglichst bald nach ihrem Inkrafttreten verbindlich Anwendung finden.

(27) […] Daher sollten UN-Regelungen und andere Rechtsakte betreffend Software-Aktualisierungsverfahren möglichst bald nach ihrem Inkrafttreten verbindlich Anwendung finden. *Diese Sicherheitsmaßnahmen sollten jedoch nicht die Verpflichtungen des Fahrzeugherstellers berühren, Zugang zu umfassenden Diagnoseinformationen und Fahrzeugdaten zu gewähren, die für die Reparatur und Wartung eines Fahrzeugs relevant sind.*"

Damit legt die GSR das grundsätzliche Verhältnis von Zugangsanspruch und Sicherheitserwägungen eindeutig fest: Der Zugangsanspruch ist stets zu erfüllen. Es dürfen nur solche Sicherheitsmaßnahmen umgesetzt werden, die den Zugriff auf den Fahrzeugdatenstrom (über die OBD-Schnittstelle) nicht berühren. Zu einer Pflichtenkollision der Hersteller kommt es gerade nicht.

b) UN/ECE R155

Derselbe Grundsatz findet sich auch in der Regelung UN/ECE R155 zu Cybersecurity. Die UN/ECE R155 schreibt zwar für den OBD-Port vor, dass „an externen Schnittstellen […] Sicherheitsmaßnahmen anzuwenden" seien. Wie die GSR legt aber auch die UN/ECE R155 einen Vorrang der Bereitstellungspflicht fest. Ziffer 1.3 lautet:

„Diese Regelung gilt unbeschadet anderer UN-Regelungen sowie regionaler oder nationaler Rechtsvorschriften, die den Zugang befugter Parteien zu dem Fahrzeug, dessen Daten, Funktionen und Ressourcen sowie die Zugangsbedingungen regeln. […]"

Fahrzeughersteller sind also aufgefordert, nur solche Sicherheitsmaßnahmen zu implementieren, die nicht mit ihrer Bereitstellungspflicht kollidieren. Die Norm nennt ausdrücklich „Zugangsbedingungen", die durch UN/ECE R155 nicht berührt werden sollen. Solche Bedingungen – welche die Verordnung (EU) 2018/858 selbst nicht vorsieht – können folglich nicht auf UN/ECE R155 gestützt werden. Das gilt auch bei der Beobachtung möglicher Cyberrisiken. Dies ist in Ziff. 7.2.2.4b) UN/ECE R155 als Pflicht des Fahrzeugherstellers zwar vorgesehen; in der gleichen Vorschrift wird aber wiederum auf Ziffer 1.3 der UN/ECE R155 verwiesen, wonach der Zugang zu Fahrzeugdaten und -funktionen nicht eingeschränkt werden darf.

Während die UN/ECE R155 also grundsätzlich den Fahrzeugherstellern überlässt, welche konkreten Maßnahmen sie zur Gewährleistung der Fahrzeugsicherheit treffen, endet diese Freiheit dort, wo Sicherheitsmaßnahmen mit der Bereitstellungsverpflichtung kollidieren würden. Der Fahrzeughersteller gerät daher nicht in die Lage, selbst eine Abwägung vornehmen zu müssen, ob eine Beschränkung des Zugangs zum Fahrzeugdatenstrom über die OBD-Schnittstelle aufgrund vorrangiger Sicherheitsinteressen ggf. noch gerechtfertigt sein könnte.

Der Gesetzgeber hat diese Abwägung bereits selbst vorgenommen und geregelt, in welchen Fällen besondere (Schutz-)Maßnahmen ergriffen werden müssen (s. oben, II.). Dieser gesetzgeberischen Wertung würde es zuwiderlaufen, wenn Fahrzeughersteller abseits dieser klar definierten Bereiche ebenfalls besondere Sicherheitsmaßnamen einrichten könnten bzw. müssten, die den Zugang

9 Aus Anhang X, Anlage 2, sowie aus Art. 61 Abs. 7 der Verordnung (EU) 2018/858, wonach Fahrzeughersteller interessierten Marktteilnehmern die erforderlichen Informationen zur „Herstellung von OBD-kompatiblen […] Diagnose- und Prüfgeräten" bereitstellen müssen, folgt ebenfalls, dass der Zugriff auf den OBD-Port mit Hilfe eines generischen Diagnosegeräts möglich sein muss. Anhang II, Anlage 1, Tabelle 1, 2A, Tabelle 2, 2A; Anlage 2, Punkt 4, Teil 1, 2A; Teil 2, 2A der Verordnung schreiben zudem vor, dass die OBD-Schnittstelle „mit herkömmlichen Diagnosegeräten kommunizieren können" muss.

zur OBD-Schnittstelle beeinträchtigen.[10] Auch die mit der Normung der OBD-Schnittstelle bezweckte Vereinheitlichung zur Förderung des Wettbewerbs könnte nicht erreicht werden. Außerhalb der oben angesprochenen Spezialbereiche ist eine Beschränkung schlicht nicht gerechtfertigt – auch nicht vor dem Hintergrund von Cybersecurity-Bedenken.

Das bedeutet: Vom Mitarbeiter in der Werkstatt darf nicht mehr verlangt werden, als das Diagnosegerät an den OBD-Port anzuschließen. Solange sich das Fahrzeug im Stillstand befindet und nicht auf diebstahls- oder emissionsrelevante Funktionen zugegriffen werden soll, muss allein das Verbinden mit dem Diagnosegerät den Datenfluss über den OBD-Port ermöglichen, ohne dass noch weitere Voraussetzungen (wie etwa die Verbindung mit dem Server des Herstellers) dazukommen.

Nur dieses Verständnis deckt sich auch mit der einschlägigen Rechtsprechung des EuGH. Dieser hat jüngst mit Blick auf den ebenfalls in Art. 61 der Verordnung (EU) 2018/858 geregelten Zugangsanspruch zu Reparatur- und Wartungsinformationen bekräftigt, dass Fahrzeughersteller diesen Zugang nicht von Bedingungen abhängig machen dürfen, die die Verordnung nicht vorsieht.[11] Diese Wertung ist ohne weiteres auf den Zugang zur OBD-Schnittstelle übertragbar. Im Zuge seines regulatorischen Eingriffs hat der Gesetzgeber die Zugangsbedingungen abschließend geregelt. Die Vorgaben des Typgenehmigungsrechts sind bereits das Ergebnis einer vom Gesetzgeber vorgenommen Abwägung zwischen Sicherheit und Wettbewerb, deren Ergebnis nicht durch Einführung abweichender individueller Bedingungen unterlaufen werden darf.

3. Praktische Lösung: Security by Design

Die Fahrzeughersteller sind daher aufgerufen, etwaige Sicherheitsrisiken, die die Ausrüstung mit (gesetzlich vorgeschriebenen) Schnittstellen mitbringt, bereits beim Fahrzeug-Design zu berücksichtigen und Sicherheitsmechanismen zu implementieren („security by design"). Fahrzeuge müssen so konstruiert werden, dass bestimmte sicherheitsgefährdende Einstellungen nicht vorgenommen werden können, aber der grundsätzliche Zugriff auf den Fahrzeugdatenstrom für Zwecke der Diagnose, Wartung und Reparatur nicht berührt wird. Die Sicherheitssysteme sind *im Fahrzeug selbst* zu installieren (etwa durch Blockieren schadhafter Befehle oder sicherheitsrelevanter Steuergeräte), damit sicherheitsgefährdende Veränderungen nicht vorgenommen werden können. Der Gedanke des „security by design" findet sich explizit in den maßgeblichen Rechtsakten. Art. 4 Abs. 4 der GSR schreibt beispielsweise vor, dass „Fahrzeuge so konstruiert, gebaut und zusammengebaut sind", dass Gefahren vermieden werden.

V. Exkurs: Warum der „Jeep-Fall" keine Rolle spielt

Im Zusammenhang mit Fahrzeug-Schnittstellen und Cybersecurity wird ein Thema immer wieder genannt: der „Jeep-Hack" im Jahr 2015 in den USA. Dort war es „Hackern" gelungen, per Fernzugriff auf einen fahrenden Jeep Cherokee einzuwirken, d. h. unter anderem die Kontrolle über Lenkrad und Bremsen zu übernehmen.

Tatsächlich hat jedoch dieser Vorfall nichts mit der Bereitstellung des OBD-Ports zu tun. Es lohnt sich, genauer hinzusehen: Es handelte sich nicht um einen kriminellen Angriff auf einen nichts ahnenden Fahrer. Vielmehr hatte sich ein Journalist, der den Jeep zum fraglichen Zeitpunkt fuhr, absichtlich für dieses Experiment zur Verfügung gestellt. Der Zugriff war geplant. Die „Hacker" waren *Dr. Charlie Miller* und *Chris Valasek*, Experten für Computersicherheit, die sich zuvor jahrelang mit Fahrzeugsicherheitssystemen beschäftigt hatten. Und: Der Zugriff erfolgte nicht über den OBD-Port, sondern über das Infotainment-System des Fahrzeugs. Bei Modellen für den US-Markt waren diese Systeme über das Mobilfunknetz mit dem Internet verbunden. Das dafür benötigte, werkseitig vergebene Passwort war leicht zu erraten. Mit Hilfe dieses Passworts gelangten die Forscher in das Infotainment-System und – nach Installation eines manipulierten „Upgrades" – über ungesicherte Schnittstellen zur restlichen Fahrzeugarchitektur auch in sicherheitsrelevante Steuergeräte.[12]

Es handelte sich also um einen aufwendig inszenierten Vorfall, die Forscher gelangten nicht über den OBD-Port in die Fahrzeugsysteme und anders als bei einem Werkstattzugriff per Steckverbindung auf den OBD-Port wurde „over-the-air" auf ein fahrendes Fahrzeug zugegriffen. Nichts davon gibt Anlass oder kann es rechtfertigen, den Zugriff von Werkstätten auf stehende Fahrzeuge über den OBD-Port einzuschränken.

VI. Ausblick

Die Praxis zeigt, dass die Umsetzung sowohl der neuen Regelungen zur Fahrzeugsicherheit als auch der wettbewerbsbezogenen Verpflichtungen zur Zugangsgewährung zu Fahrzeugdaten und -informationen für die Marktteilnehmer noch mit vielen Fragen und Schwierigkeiten verbunden ist. Das kann zu erheblichen Hemmnissen im Wettbewerb führen, die teils nur durch eine in der gesamten Europäischen Union verbindliche Klärung der maßgeblichen (Auslegungs-)Fragen durch den EuGH beseitigt werden können. Dieser befasst sich gegenwärtig auch mit der hier aufbereiteten Frage des Verhältnisses zwischen dem im Typgenehmigungsrecht verankerten Anspruch auf Zugang zum Fahrzeugdatenstrom über die OBD-Schnittstelle und den zu erfüllenden (Cyber-)Sicherheitsanforderungen und wird dazu in Kürze eine Entscheidung fällen.[13]

Sollte sich in der Zukunft zeigen, dass die derzeit geltenden Sicherheitsanforderungen nicht (mehr) genügen, um Cyberangriffen über die OBD-Schnittstelle wirkungsvoll entgegenzutreten, wäre der Gesetzgeber aufgerufen, nachzubessern. Es ist aber nicht an den Fahrzeugherstellern, sich selbst vorauseilend über die aktuellen Bestimmungen hinwegzusetzen und Maßnahmen zu treffen, die mit diesen Bestimmungen nicht in Einklang zu bringen sind. Damit wäre – auch im Sinne der Rechtssicherheit – letztlich niemandem gedient.

10 Zumal etwa im Zusammenhang mit SERMI gerade nicht der Fahrzeughersteller die Entscheidung trifft, wem Zugang gewährt wird, sondern eine unabhängige Stelle; dazu bereits oben.

11 EuGH, Urt. v. 27.10.2022 – C-390/21, BeckRS 2022, 28847, Rn. 29 ff.

12 https://www.kaspersky.de/blog/blackhat-jeep-cherokee-hack-explained/5940/; https://www.heise.de/security/meldung/Hacker-steuern-Jeep-Cherokee-fern-2756331.html.

13 EuGH, Rs. C-296/22 (anhängig); vgl. Fn. 1.

VII. Zusammenfassung/Summary

Die Automobilwelt ist im Umbruch. Bedrohungen der Cybersecurity verlangen von Fahrzeugherstellern angemessene Reaktionen. Gleichzeitig muss der Wettbewerb auf dem Reparatur- und Ersatzteilmarkt geschützt werden. Wirksamer Wettbewerb lebt von einem unbeschränkten Zugang zum Fahrzeug; hierzu gehört zwingend der Zugang zum Fahrzeugdatenstrom über den OBD-Port. Tatsächlich ist jedoch das Spannungsverhältnis zwischen Fahrzeugsicherheit und wirksamem Wettbewerb keines, das der Fahrzeughersteller lösen muss; es ist durch den Gesetzgeber bereits bedacht und entsprechend geregelt worden. Der Schutz des Fahrzeugs vor Cybersecurity-Angriffen ist richtig und wichtig. Er darf aber nicht dazu führen, dass der Zugang freier Werkstätten zum Fahrzeug beschränkt wird.

Für die Praxis bedeutet das: Cybersecurity-Maßnahmen können und müssen über das technische Design des Fahrzeugs umgesetzt werden, so dass etwa die Ausführung schadhafter Befehle während der Fahrt von vornherein nicht möglich ist. Die Einschränkung des Zugangs zum OBD-Port insgesamt ist dagegen keine rechtmäßige Option. Der Gesetzgeber wollte gerade vermeiden, dass der Hersteller über die Bestimmung von Zugangsbedingungen kontrolliert, wer mit ihm bzw. mit den mit ihm verbundenen Markenwerkstätten auf dem Reparatur- und Ersatzteilmarkt in Wettbewerb treten kann. Die Bedingungen für den Zugang hat er daher (selbst) abschließend geregelt.

The automotive world is changing. Cybersecurity threats require appropriate responses from vehicle manufacturers. At the same time, competition in the automotive aftermarket needs to be protected. Effective competition thrives on unrestricted access to the vehicle; this necessarily includes access to the vehicle data stream via the OBD port. However, this tension between vehicle security and effective competition is not one that the vehicle manufacturer needs to resolve; it has already been considered by the legislator and regulated accordingly. Protecting the vehicle from cybersecurity attacks is legitimate and important. But it must not lead to restrictions on access to the vehicle by independent workshops.

In practice, this means that cybersecurity measures can and must be implemented via the technical design of the vehicle so that, for example, it is not possible to execute malicious commands while the vehicle is in motion. Restricting access to the OBD port altogether, on the other hand, is not a legitimate option. The legislator's intention was precisely to prevent the manufacturer from controlling who can compete with it or its affiliated workshops on the aftermarket by determining access conditions. The conditions for access have, therefore, been conclusively determined by the legislator itself.

Rechtsprechung

Kompakt

Ass. iur. Paul Harenberg, Frankfurt a. M.

EuGH: „Umweltverbandsklage" und „Thermofenster" – Klagebefugnis des Deutsche Umwelthilfe e. V.

Tenor des Gerichts:

1. Art. 9 Abs. 3 des am 25.6.1998 in Aarhus unterzeichneten und im Namen der Europäischen Gemeinschaft mit dem Beschluss 2005/370/EG des Rates vom 17.2.2005 genehmigten Übereinkommens über den Zugang zu Informationen, die Öffentlichkeitsbeteiligung an Entscheidungsverfahren und den Zugang zu Gerichten in Umweltangelegenheiten in Verbindung mit Art. 47 der Charta der Grundrechte der Europäischen Union ist dahin auszulegen, dass es einer Umweltvereinigung, die nach nationalem Recht zur Einlegung von Rechtsbehelfen berechtigt ist, nicht verwehrt werden darf, eine Verwaltungsentscheidung, mit der eine EG-Typgenehmigung für Fahrzeuge erteilt oder geändert wird, die möglicherweise gegen Art. 5 Abs. 2 der Verordnung (EG) Nr. 715/2007 des Europäischen Parlaments und des Rates vom 20.6.2007 über die Typgenehmigung von Kraftfahrzeugen hinsichtlich der Emissionen von leichten Personenkraftwagen und Nutzfahrzeugen (Euro 5 und Euro 6) und über den Zugang zu Reparatur- und Wartungsinformationen für Fahrzeuge verstößt, vor einem innerstaatlichen Gericht anzufechten.

2. Art. 5 Abs. 2 Buchst. a der Verordnung Nr. 715/2007 ist dahin auszulegen, dass eine Abschalteinrichtung nur dann nach dieser Bestimmung zulässig sein kann, wenn nachgewiesen ist, dass diese Einrichtung ausschließlich notwendig ist, um die durch eine Fehlfunktion eines Bauteils des Abgasrückführungssystems verursachten unmittelbaren Risiken für den Motor in Form von Beschädigung oder Unfall zu vermeiden, Risiken, die so schwer wiegen, dass sie eine konkrete Gefahr beim Betrieb des mit dieser Einrichtung ausgestatteten Fahrzeugs darstellen. Außerdem ist eine Abschalteinrichtung nur dann „notwendig" im Sinne