März 2024
12. Jahrg.
Seite 1–88

RAW

1

Recht ■ Automobil ■ Wirtschaft
Unternehmen | Technologie | Beratung

dfv Mediengruppe · Frankfurt am Main

a) der Fahrzeugerwerber sich bei seinem Anspruch auf kleinen Schadenersatz auf den Schadenersatzbetrag die Vorteile der Nutzung des Fahrzeugs anrechnen lassen muss, soweit diese zusammen mit dem Restwert den gezahlten Kaufpreis abzüglich jenes Schadenersatzbetrags übersteigen?

b) der Anspruch des Fahrzeugerwerbers auf kleinen Schadenersatz auf maximal 15 % des gezahlten Kaufpreises begrenzt ist?

(LG Ravensburg, Beschl. v. 27.10.2023 – 2 O 331/19, 2 O 190/20, 2 O 425/20, 2 O 16/21, 2 O 57/21)

VG Düsseldorf: Rechtmäßiges Abschleppen eines an Ladesäule geparkten Fahrzeuges mit Verbrennungsmotor

Leitsatz des Gerichts:

Wird ein Motorrad/Kraftrad auf einem Sonderparkplatz für Elektrofahrzeuge abgestellt, rechtfertigt die damit einhergehende Funktionsbeeinträchtigung dieser Verkehrsfläche eine Abschleppmaßnahme regelmäßig auch ohne konkrete Behinderung eines im Sinne von § 2 EmoG bevorrechtigten Fahrzeugs, da die parkbevorrechtigten Benutzerkreise darauf vertrauen dürfen, dass der gekennzeichnete Parkraum ihnen unbedingt zur Verfügung steht.

Anmerkung der Redaktion:

Zu überprüfen hatte das VG Düsseldorf die Rechtmäßigkeit der Abschleppmaßnahme im Zuge der Klage des Fahrzeuginhabers gegen den korrespondierenden Leistungs- und Gebührenbescheid über rund 159 €. Die vorliegend durchgeführte Abschleppmaßnahme (Versetzung) sei sowohl als spezialgesetzliche Sicherstellung (§ 43 Nr. 1 PolG NRW) als auch als Ersatzvornahme einer Beseitigungsmaßnahme (§ 59 VwVG NRW) auf Grundlage der ordnungsrechtlichen Generalklausel rechtmäßig. Insbesondere könne dahingestellt bleiben, ob, wie zum Teil gefordert, das Gebot der Verhältnismäßigkeit hier ferner eine über das schlichte verbotswidrige Parken hinausgehende weitere Beeinträchtigung erfordere. Denn eine solche bestehe vorliegend in Form einer Funktionsbeeinträchtigung der relevanten Verkehrsfläche. Hiervon sei beim Abstellen eines Fahrzeuges mit Verbrennungsmotor im Bereich einer E-Ladestation regelmäßig auszugehen. Dabei bedürfe es keiner Überprüfung, ob durch das verbotswidrige Abstellen konkret ein bevorrechtigtes Elektrofahrzeug am Parken und Laden gehindert werde. Gleichermaßen sei das Abschleppen aus spezial- und generalpräventiven Zwecken gerechtfertigt: von einem an einer E-Tankstelle abgestellten Fahrzeug mit Verbrennungsmotor gehe eine negative Vorbildwirkung für andere Kraftfahrer aus. Der Gesetzgeber habe durch die Regelungen im Elektromobilitätsgesetz verdeutlicht, dass er der Bevorrechtigung von Elektrofahrzeugen im Allgemeinen und u. a. dem bevorzugten Parken im Besonderen eine hohe Bedeutung beimesse.

(VG Düsseldorf, Urt. v. 9.9.2023 – 14 K 7479/22)

Anmerkungen

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

Der OBD-Port muss offen bleiben – auch Cybersecurity ist kein Argument

Anmerkung zu EuGH, Urt. v. 5.10.2023 – C-296/22 – A.T.U und Carglass/FCA Italy

In einer wegweisenden Entscheidung hat der Europäische Gerichtshof (EuGH) am 5.10.2023 klargestellt, dass Fahrzeughersteller den Zugang unabhängiger Wirtschaftsakteure zum sog. OBD-Port (On-Board-Diagnose-Port) nicht beschränken dürfen, und zwar auch nicht aus Gründen der Cybersecurity. Das Urteil erging in einem Vorabentscheidungsverfahren, das durch eine Vorlage des LG Köln eingeleitet wurde (die Autoren berichteten hierzu in RAW 1/23, S. 64, „Im Spannungsfeld zwischen Cybersecurity und Wettbewerb – (wie) darf der Fahrzeughersteller den Zugang zum OBD-Port kontrollieren?“).

I. Sachverhalt

Ausgangspunkt war der folgende Sachverhalt:

Der Fahrzeughersteller FCA Italy (nunmehr: Stellantis Europe S. p. A.) rüstet seine Fahrzeuge mit sog. „Secure Gateways“ aus, die den Zugang zum Fahrzeugdatenstrom über den OBD-Port kontrollieren. Über den OBD-Port kann ein Mechatroniker ein Diagnosegerät an das Fahrzeug anschließen und so in der Werkstatt für Reparatur- und Wartungsarbeiten verschiedener Art auf den Datenstrom des Fahrzeugs zugreifen. Etwa um Schreibvorgänge durchführen zu können, Fehlercodes zu löschen und Rekalibrierungen vorzunehmen,[1] müssen bei Fahrzeugen von FCA/Stellantis so-

* Die hier besprochene Entscheidung 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 und Carglass GmbH, Kristina Heistermann) bzw. als Prozessbevollmächtigte (Elisabeth Macher, Paul Schmitz) beteiligt. Mehr zu den Autoren erfahren Sie auf S. III und IV.

1 Bei einem Windschutzscheibenaustausch ist mittlerweile z. B. in etwa 30 Prozent aller Fahrzeuge eine Kalibrierung des Fahrerassistenzsys-

wohl unabhängige Reparaturbetriebe als auch Vertragswerkstätten zunächst den Secure Gateway „öffnen", indem sie bestimmte, von FCA Italy festgelegte Anforderungen erfüllen. Diese bestehen unter anderem darin, dass der Werkstattmitarbeiter sich zunächst bei FCA mit seinen persönlichen Daten registriert und vor dem Reparaturvorgang bei einem von FCA bestimmten Server anmeldet, sowie dass die Werkstatt ein kostenpflichtiges Abonnement für die Nutzung generischer Diagnosegeräte erwirbt, die sie über das Internet mit diesem Server verbinden.

ATU und Carglass griffen diese Bedingungen vor dem Landgericht Köln mittels einer Unterlassungsklage an. Sie waren insbesondere der Ansicht, dass FCA durch die einseitige Auferlegung dieser Anforderungen gegen ihre Verpflichtungen aus Art. 61 Abs. 1 und 4 der Verordnung 2018/858 in Verbindung mit deren Anhang X Nr. 2.9 verstoße, wonach Fahrzeughersteller unabhängigen Wirtschaftsakteuren (wie Reparaturbetrieben) ungehinderten Zugang zum Fahrzeugdatenstrom bereitzustellen haben. FCA Italy war hingegen der Ansicht, die Zugangsbeschränkung sei insbesondere aus Gründen der Cybersicherheit gerechtfertigt. Der Zugang zum Fahrzeugdatenstrom müsse aus Sicherheitsgründen kontrolliert werden.

Das LG Köln legte dem EuGH folgende Auslegungsfrage vor:

„Ist Art. 61 Abs. 1 und 4 in Verbindung mit Anhang X Nr. 2.9 der Verordnung 2018/858 auch in Anbetracht der Anforderungen an den Fahrzeughersteller zur Gewährleistung der allgemeinen Fahrzeugsicherheit in Anhang II Teil I Nr. 63 dieser Verordnung […][2] so auszulegen, dass der Fahrzeughersteller stets, auch bei Implementierung entsprechender Sicherheitsmaßnahmen, sicherstellen muss, dass diese Fahrzeug-OBD, Fahrzeugdiagnose, -reparatur und -wartung einschließlich dafür erforderlicher Schreibvorgänge durch unabhängige Reparaturbetriebe mit Hilfe eines universellen, generischen Diagnosegerätes möglich bleibt, **ohne** dass die von der Verordnung nicht ausdrücklich vorgesehenen Voraussetzungen einer Internetverbindung des Geräts zu einem vom Fahrzeughersteller bestimmten Server und/oder einer vorherigen persönlichen Registrierung des Nutzers beim Fahrzeughersteller erfüllt werden müssen?"

II. Die Entscheidung des EuGH

Der EuGH folgt vollumfänglich der Ansicht der Kläger A.T.U und Carglass. Die Antwort auf die Vorlagefrage lautet:

„Art. 61 Abs. 1 und 4 in Verbindung mit Anhang X der Verordnung (EU) 2018/858 […] ist dahin auszulegen, dass er dem entgegensteht, dass ein Fahrzeughersteller den Zugang unabhängiger Wirtschaftakteure zu Fahrzeugreparatur- und -wartungsinformationen sowie zu Informationen des On-Board-Diagnosesystems, einschließlich den Schreibzugriff für diese Informationen, von anderen Voraussetzungen als von den in der Verordnung bestimmten abhängig macht."

In seiner Entscheidung ging der EuGH explizit auch auf das Cybersecurity-Argument des Fahrzeugherstellers ein.

1. Grundsätzlich uneingeschränkter Zugang: keine Bedingungen, die die Verordnung nicht vorsieht

Zunächst hob der EuGH hervor, dass Fahrzeughersteller den Zugang für unabhängige Wirtschaftsakteure nicht von Bedingungen abhängig machen dürfen, die in der Verordnung nicht vorgesehen sind. Insoweit knüpfte der Gerichtshof nahtlos an seine vorigen Feststellungen in der Entscheidung „ADPA und Gesamtverband Autoteile-Handel" an.[3] Während die Verordnung explizit Regelungen für den Zugang zu Sicherheitsmerkmalen des Fahrzeugs und besondere Anforderungen für die Reprogrammierung von Steuergeräten aufstellt, finden sich solche Bedingungen für den übrigen Zugang zum OBD-Port nicht. Der EuGH führt dementsprechend aus (Rz. 30):

„Was die systematische Auslegung der fraglichen Bestimmungen betrifft, so werden in Anhang X Nrn. 6.2 und 6.4 der Verordnung 2018/858 zum einen die Vorgaben für den Zugang zu Sicherheitsmerkmalen des Fahrzeugs (Diebstahlsicherung) und zur Emissionskalibrierung festgelegt. Wie die Europäische Kommission in ihren schriftlichen Erklärungen ausgeführt hat, sind in diesen Nummern die Fälle bestimmt, in denen der Zugang zu OBD-Informationen sowie zu Fahrzeugreparatur- und -wartungsinformationen aufgrund ihrer Bedeutung für die Sicherheit an bestimmte Bedingungen geknüpft werden kann. Liegt keiner dieser Fälle vor, müssen unabhängige Wirtschaftsakteure daher ein Recht auf Zugang zu diesen Informationen haben, ohne dass für sie andere als die in der Verordnung vorgesehenen Bedingungen gelten (vgl. in diesem Sinne Urteil vom 27.10.2022, ADPA und Gesamtverband Autoteile-Handel, C-390/21, EU:C:2022:837, Rn. 32)."

Diese Auslegung sieht der EuGH auch vom Sinn und Zweck der Verordnung gedeckt, namentlich wirksamen Wettbewerb auf dem Markt für Fahrzeugreparatur und -wartung sowie die entsprechenden Informationsdienste zu ermöglichen (Rz. 31; vgl. hierzu auch den o. g. Aufsatz in RAW 1/23, dort insbesondere S. 65). Insbesondere sieht der Gerichtshof den Wettbewerb auf dem Markt durch eine Zugangseinschränkung gefährdet: es „bestünde die Gefahr, dass sich die Anzahl der unabhängigen Werkstätten, die Zugang zu diesen Informationen haben, verringert, was möglicherweise zu einem Rückgang des Wettbewerbs auf dem Markt für Fahrzeugreparatur- und Fahrzeugwartungsinformationsdienste und damit zu einem verringerten Angebot für Verbraucher führt." (Rz. 32)

Nicht zuletzt bemüht der EuGH auch ein Dammbruchargument (das die Kläger ebenfalls vorgetragen hatten): „Könnten die Hersteller den Zugang zum direkten Fahrzeugdatenstrom im Sinne von Nr. 2.9 des Anhangs X der Verordnung nach Belieben beschränken, stünde es ihnen zudem frei, den Zugang zu diesem Datenstrom von Bedingungen abhängig zu machen, die ihn praktisch vereiteln könnten." (Rz. 32)

Die Bedingungen der Secure Gateways von FCA Italy, namentlich das Registrierungserfordernis und das Erfordernis einer Internetverbindung zu einem von FCA vorgesehenen Server, sind nach Ansicht des EuGH daher unzulässig. Ob diese Maßnahmen überhaupt zur Gewährleistung der Fahrzeugsicherheit tauglich gewesen wären, musste der EuGH nicht mehr prüfen.

Wichtig ist: Die Vorgabe, dass der Zugang zum Fahrzeugdatenstrom nicht eingeschränkt werden darf, gilt nicht nur

---

tems erforderlich. Diese Zahl wird weiter steigen, je mehr Neufahrzeuge mit Fahrerassistenzsystemen ausgestattet werden.

2 „in Verbindung mit der Verordnung Nr. 661/2009 im Hinblick auf vor dem 6. Juli 2022 typengenehmigte Fahrzeuge, dort insbesondere Art. 5 Abs. 1 und in Verbindung mit der ab dem 6. Juli 2022 geltenden Verordnung 2019/2144, dort insbesondere Art. 4 Abs. 4 und 5"; zur besseren Lesbarkeit im Text gekürzt.

3 EuGH, Urt. v. 27.10.2022 – C-390/21 – ADPA und Gesamtverband Autoteile-Handel, Rz. 32.

für den sog. Lesezugriff, d. h. das passive Auslesen beispielsweise von Fehlercodes, sondern auch für den Schreibzugriff, also etwa das Kalibrieren von Steuergeräten nach Einbau neuer Komponenten.

2. Spezialregelungen zur Cybersecurity stehen nicht entgegen

An dieser Bewertung ändert für den EuGH auch nichts, dass Vorschriften zur Sicherstellung der Cybersecurity existieren, an die sich Fahrzeughersteller ebenfalls halten müssen. Die Verordnung (EU) 2019/2144 (sog. „General Safety Regulation") verweist hinsichtlich des Schutzes vor Cyberangriffen auf die UN-Regelung Nr. 155, die (nicht näher definierte) Schutzmaßnahmen für externe Schnittstellen wie den OBD-Port vorsieht. Handelt es sich bei entsprechenden Maßnahmen also um „in der Verordnung vorgesehene Bedingungen", an die der Zugang zum OBD-Port geknüpft werden kann?

Nein, sagt der EuGH: Beide genannten Regelungen treten hinter den Zugangsvorschriften zurück. So heißt es in Art. 1.3 der UN-Regelung Nr. 155 ausdrücklich, dass diese unbeschadet von Rechtsvorschriften gelte, „die den Zugang befugter Parteien zu dem Fahrzeug, dessen Daten, Funktionen und Ressourcen sowie die Zugangsbedingungen regeln". Die General Safety Regulation wiederum sieht in Erwägungsgrund 27 vor, dass etwaige Sicherheitsmaßnahmen „nicht die Verpflichtungen des Fahrzeugherstellers berühren [sollten], Zugang zu umfassenden Diagnoseinformationen und Fahrzeugdaten zu gewähren, die für die Reparatur und Wartung eines Fahrzeugs relevant sind".

Der Gesetzgeber hat hier also bewusst eine Entscheidung getroffen: (Cyber-)Sicherheit ja, aber nicht auf Kosten des Zugangsanspruchs. Die Vorgaben des Typgenehmigungsrechts sind insoweit das Ergebnis einer vom Gesetzgeber vorgenommenen Abwägung zwischen Sicherheit und Wettbewerb (auch hierzu bereits RAW 1/23, S. 66). Für Fahrzeughersteller bedeutet das, dass sie die nötige Sicherheit anders gewährleisten müssen. Der EuGH betont in seiner Entscheidung (Rz. 37) die Vorgaben der General Safety Regulation, nach denen dies im Stadium der Entwicklung, der Konstruktion und des Zusammenbaus des Fahrzeugs zu geschehen hat („Security by Design") und nicht zum Nachteil unabhängiger Wirtschaftsakteure.

III. Einordnung und Ausblick/Bedeutung für die Praxis

Die Entscheidung des EuGH begründet keine neue Rechtslage. Vielmehr hat der EuGH lediglich klargestellt, wie das bereits geltende Recht zu verstehen ist. Seine Entscheidung bindet daher nicht lediglich die Parteien des (Ausgangs-)Rechtsstreits. Die klargestellten Anforderungen an die Zugangsgewährung gelten allgemeinverbindlich und unmittelbar für alle in der Europäischen Union tätigen Fahrzeughersteller.

1. Zäsur für die Fahrzeughersteller

Dennoch stellt die Entscheidung für die meisten Fahrzeughersteller eine Zäsur dar. Beschränkungen des Zugangs zum Fahrzeugdatenstrom sind zwischenzeitlich gängige Praxis geworden. Diverse Fahrzeughersteller waren offensichtlich dem Beispiel FCA gefolgt und haben vergleichbare Hürden aufgebaut. Nun müssen sich die Hersteller gehalten sehen, diese Mechanismen, soweit sie den Zugang zum OBD-Port einschränken, unverzüglich zu entfernen. Wo dies nicht ohne Weiteres aus der Ferne, also etwa serverseitig möglich ist, sondern Veränderungen am einzelnen Fahrzeug vorgenommen werden müssen, stehen gegebenenfalls Rückrufe der betroffenen Fahrzeuge im Raum. Bei neuen Fahrzeugmodellen muss von vornherein auf Secure Gateways und vergleichbare Mechanismen verzichtet werden. Auch wegen Verstößen in der Vergangenheit müssen sich Fahrzeughersteller möglicherweise mit Schadensersatzansprüchen konfrontiert sehen. Insofern kann es auch bedeutsam sein, wenn für das Öffnen des OBD-Ports von unabhängigen Wirtschaftsakteuren besondere Entgelte verlangt wurden. Der Entscheidung des EuGH folgend kann für das Verlangen derartiger Entgelte keine legitime Grundlage bestanden haben, weil der OBD-Port gar nicht erst „verschlossen" werden durfte.

2. Cybersecurity oder Wettbewerb? Cybersecurity und Wettbewerb!

In seinem Urteil hat der EuGH auch die Bedeutung des Themas Cybersecurity berücksichtigt. Mit seiner Entscheidung bestätigt der Gerichtshof, dass Fragen der Cybersecurity von den Fahrzeugherstellern angemessen gehandhabt werden können, ohne dem Kfz-Servicemarkt Einschränkungen aufzuerlegen. Denn der Zugang zum OBD-Port ist für den freien Markt überlebenswichtig: Viele Tätigkeiten einer Kfz-Werkstatt (ob Reparatur oder Wartung) erfordern, dass der Mechatroniker über den OBD-Port Zugriff auf den Datenstrom des Fahrzeugs erhält; Tendenz steigend.

Die Herausforderung wird darin liegen, Fragen der Cybersecurity und des fairen Wettbewerbs im Reparaturmarkt künftig in Einklang zu bringen. Fahrzeughersteller müssen den Vorgaben der General Safety Regulation bzw. der UN-Regelung Nr. 155 in Bezug auf Cybersicherheit genügen können, ohne zugleich gegen ihre Verpflichtungen zur Zugangsgewährung zu verstoßen.

Nach derzeitiger Rechtslage wird nach der UN-Regelung Nr. 155 von den Fahrzeugherstellern gefordert, dass sie ein Cyber Security Management System (CSMS) etablieren und für die Typgenehmigung eines neuen Fahrzeugtyps nachweisen, dass dieses CSMS funktioniert. Gleichzeitig darf der Zugriff auf den OBD-Port nicht eingeschränkt werden.

Sollte sich in Zukunft abzeichnen, dass eine besondere Absicherung des Zugangs zum Fahrzeugdatenstrom oder bestimmten Funktionen erforderlich wird, muss deren Ausgestaltung dem Gesetzgeber vorbehalten bleiben. Durch eine sektorspezifische Gesetzgebung könnten angemessene Maßnahmen getroffen werden, die einen fairen Wettbewerb im Reparaturmarkt unter Einhaltung höchstmöglicher Sicherheitsstandards ermöglichen.

Als erstes Beispiel könnten dabei die neu eingeführten Regelungen für SERMI (Security-Related Vehicle Repair and Maintenance Information) Orientierung bieten. SERMI sieht ein Akkreditierungssystem vor, das für unabhängige Werkstätten und ihre Mitarbeiter eingeführt wird, um Zugang zu sicherheitsrelevanten (gemeint: diebstahlsrelevanten) Informationen von Fahrzeugherstellern zu erhalten. Anstatt einer individuellen Überprüfung des unabhängigen Wirtschaftsakteurs durch jeden Fahrzeughersteller, von dem der Informationszugang beansprucht wird, besteht die Idee hinter SERMI darin, dass eine unabhängige Instanz die Überprüfung vornimmt und die Akkreditierung erteilt.

Mit der Akkreditierung kann ein unabhängiger Betreiber oder Beschäftigter dann Zugang zu allen sicherheitsbezogenen Reparatur- und Wartungsinformationen erhalten. Zwar ist SERMI in seinem Anwendungsbereich auf solche Informationen begrenzt, die der Diebstahlsprävention dienen (und nicht der allgemeinen Fahrzeugsicherheit). Auch müsste die Rolle der Hersteller von Mehrmarken-Diagnosegeräten berücksichtigt werden. Eine Erweiterung des SERMI-Systems als solches würde daher nicht ausreichen. Das zugrundeliegende Konzept einer unabhängigen Akkreditierungsstelle könnte aber in Zukunft möglicherweise als Modell für andere Lösungen dienen.

IV. Zusammenfassung/Summary

Die Entscheidung des EuGH vom 5.10.2023 in der Rechtssache C-296/22 – A.T.U und Carglass/FCA Italy ist sowohl für den Kfz-Markt als auch für den Anschlussmarkt wegweisend. Der Gerichtshof hat unmissverständlich festgehalten, dass sämtliche Bedingungen, an die der Zugang zum Fahrzeug geknüpft wird, unzulässig sind, es sei denn, sie sind ausdrücklich gesetzlich vorgesehen. Die von vielen Herstellern ohne gesetzliche Grundlage eingeführte Praxis, den Zugang zum Fahrzeugdatenstrom durch Verwendung von „Secure Gateways" oder ähnlichen Mechanismen einzuschränken, muss nach dem Urteil unverzüglich aufgegeben werden. Unabhängige Reparaturbetriebe müssen ohne Einschränkungen sowohl im Lese- als auch im Schreibmodus auf die Steuergeräte des Fahrzeugs zugreifen können. Das Argument, die Einschränkungen seien zur Gewährleistung der Cybersicherheit zwingend erforderlich, ließ der EuGH nicht gelten. Dennoch sind Fahrzeughersteller gesetzlich verpflichtet, die Cybersicherheit ihrer Fahrzeuge sicherzustellen. Hersteller sehen sich nun vor der Herausforderung, dieser Verpflichtung Genüge zu tun, ohne dabei den Zugang zum Fahrzeugdatenstrom über den OBD-Port einzuschränken. Mögliche Lösungen können technisch in der Blockierung schädlicher Befehle (statt der generellen Blockade des OBD-Ports) bestehen, organisatorisch in der Einführung einer Zertifizierung seriöser Betriebe durch eine unabhängige Stelle. Hierfür wäre allerdings zunächst eine entsprechende Gesetzesänderung nötig.

The ECJ's decision of 5 October 2023 in Case C-296/22 – A.T.U and Carglass v FCA Italy is groundbreaking for both the motor vehicle market and the aftermarket. The Court clearly stated that any conditions attached to access to the vehicle are unlawful unless they are expressly provided for by law. The practice introduced by many manufacturers without a legal basis of restricting access to the vehicle data stream by using „secure gateways" or similar mechanisms must be abandoned immediately following the judgement. Independent repairers must be able to access the vehicle's control units in both read and write mode without any restrictions. The ECJ did not accept the argument that the restrictions were necessary to ensure cyber security. Nevertheless, vehicle manufacturers are legally obliged to ensure the cyber security of their vehicles. Manufacturers are now faced with the challenge of fulfilling this obligation without restricting access to the vehicle data stream via the OBD port. Possible solutions could include the technical blocking of harmful commands (instead of the general blocking of the OBD port) and the organisational introduction of certification of reputable companies by an independent body. However, this would first require a corresponding change in the law.

What's New Regulatory

RAin Dr. Charlotte Harms, Berlin*

Meldepflichten im Bereich der Cybersicherheit

Im Fahrzeugregulierungsrecht stellt sich regelmäßig die Frage, in welchen Fällen Meldepflichten an die zuständigen Regulierungsbehörden bestehen. Dabei können Spezialregelungen mit allgemeinen Regelungen ineinandergreifen. So auch im Bereich der Cybersicherheit. Spezielle Meldepflichten im Bereich der Cybersicherheit regelt die UN-Regelung 155 (im Folgenden: **UN/ECE R 155**).[1] Zur Konkretisierung der dortigen Meldevorgaben hat das Kraftfahrt-Bundesamt (KBA) Leitlinien zur Berichterstattung veröffentlicht (im Folgenden: **KBA-Leitfaden Berichterstattung**).[2] Generelle Regelungen zu Meldepflichten im Fahrzeugregulierungsrecht finden sich in der Verordnung (EU) 2018/858 über die Genehmigung und Marktüberwachung von Fahrzeugen.[3]

Vor diesem Hintergrund soll ein kurzer Überblick über die Meldepflichten im Bereich der Cybersicherheit gegeben werden.

---

* Mehr über die Autorin erfahren Sie auf S. III.

1 UN-Regelung Nr. 155 – Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems [2021/387]. Für eine Auslegungshilfe vgl. UN/ECE, Proposals for Interpretation Documents for UN Regulation No. 155 (Cyber security and cyber security management system), UN Doc. ECE/TRANS/WP.29/2021/59 Stand: 22.12.2020. Für einen Überblick zur UN/ECE R 155 vgl. *Karn/Sedlmaier*, Cybersecurity im Automotive-Sektor, RAW 2022, 1 ff. Zum risikobasierten Ansatz der UN/ECE R 155 siehe *Harms*, RAW 2022, 153.

2 KBA, Leitlinien zur Berichterstattung der Hersteller an das KBA und den Technischen Dienst im Rahmen der UN-R 155/156, Revision 1.0 final, Stand: 27.6.2022, abrufbar unter https://www.kba.de/DE/Themen/Typgenehmigung/Zum_Herunterladen/ErteilungTypgenehmigungen/CyberSecurity_SoftwareUpdate/berichterstattung_hersteller.pdf?__blob=publicationFile&v=5 (zuletzt abgerufen am 31.1.2024).

3 Verordnung (EU) 2018/858 des europäischen Parlaments und des Rates vom 30.5.2018 über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge, zur Änderung der Verordnung (EG) Nr. 715/2007 und (EG) Nr. 595/2009 und zur Aufhebung der Richtlinie 2007/46/EG.