



Bericht Forum „Daten aus dem Auto – wer bestimmt, was damit geschieht?“

Jedes moderne Auto sammelt heute eine Vielzahl an Daten für unterschiedliche Zwecke. Knackpunkt ist, wer diese Daten wie nutzen kann. Pannenhelfer und freie Werkstätten wollen beispielsweise den Zugriff zum Auto nicht verlieren, um ihre Dienste weiter anbieten zu können. Autohersteller wollen und können nicht einfach einen vollständigen Zugriff gewähren, schließlich gelte es Autos cybersicher über die Lebensdauer zu halten. Ein Spagat, der nicht einfach zu lösen ist, wie das GSV-Forum „Daten aus dem Auto – wer bestimmt, was damit geschieht?“ Mitte November 2024 in Wien gezeigt hat.

Die rechtliche Situation ist nicht ganz klar

Christiane Wendehorst, stv. Institutsvorständin Digitalisierung und Recht, Universität Wien, gibt einen Überblick über die rechtliche Situation: Prinzipiell spiele sich alles zwischen dem Dateninhaber (in der Regel der Autohersteller), dem Fahrzeugnutzer (Halter, Mieter) und potentiellen Datenempfängern (andere Wirtschaftsakteure) ab. Wer kann die Daten nutzen, wer soll entsprechenden Zugang haben? Dies müsse man vor dem Hintergrund der europäischen Datenstrategie aus dem Jahr 2020 sehen, wo einige Maßnahmen bereits angekündigt worden sind:

- Zum **europäische Mobilitätsdatenraum** hat es Ende 2023 seitens der EU-Kommission eine kurze Ankündigung gegeben, in der beschrieben wurde, dass es einen besseren Zugang zu Daten brauche und die gemeinsame Nutzung bzw. Weiterverwendung von Daten ausgebaut werden soll. Im Fokus sollen technische Dimensionen bzw. Governance und offenbar keine neue Regulierung stehen.
- Bei der **neuen Datenverordnung** hingegen stehe eine neue Regulierung im Vordergrund. Diese befinde sich seit Ende 2023 im Amtsblatt und sei „mit Rekordtempo durchgedrückt worden.“ Im Artikel 3 stehe beispielsweise, dass nach Möglichkeit Nutzern ein direkter Zugang zu den Fahrzeugdaten und verbundenen Dienstdaten gewährt werden soll. Laut Artikel 4 kann der Nutzer kostenlosen Zugang zu Fahrzeug- und verbundenen Dienstdaten verlangen. Der Dateninhaber hat ihm dann diese Daten auf Verlangen kostenfrei zur Verfügung zu stellen. Artikel 4 sieht auch vor, dass der Autodateninhaber, also der Autohersteller, die Daten nur noch so weit selber nutzen darf, wie es eine vertragliche Vereinbarung mit dem Nutzer erlaubt. Laut Artikel 5 Daten VO kann der Nutzer die Übertragung der Fahrzeug- und verbundenen Dienstdaten auch auf einen Dritten verlangen. Dieser Zugang ist allerdings nicht kostenfrei. Details wie, ob alle erforderlichen Datenkategorien erfasst werden oder Fragen zum Vertragserfordernis (Gibt es Rahmenverträge?) bei Datenbereitstellung an Dritte oder ob Daten generell nur bei Verlangen des Nutzers bereitgestellt werden (Wer ist Nutzer? Mehr als 2 Personen möglicherweise) sind Punkte, die noch ausjudiziert werden müssen.

- **Erweiterung und Überarbeitung der Datenzugangsvorschriften der Typengenehmigungsverordnung:** Im Kapitel XIV geht es um den Zugang zu Fahrzeug-OBD-Informationen und zu Fahrzeugreparatur- und Wartungsinformationen für unabhängige Wirtschaftsakteure gegen angemessene, verhältnismäßige und nicht abschreckende Gebühren. Ziel ist die Verhinderung vertikaler Wettbewerbsbeschränkungen durch Anspruch „unabhängiger Wirtschaftsakteure“ (einschließlich Automobilclubs) auf Zugang zu Fahrzeug-On-Board-Diagnose (OBD)-Informationen und Fahrzeugreparatur- und Fahrzeugwartungsinformationen. Wendehorst: „Das heißt, hier haben wir tatsächlich einen speziellen Anspruch seitens unabhängiger Wirtschaftsakteure gegen den Dateninhaber, Daten zur Verfügung zu stellen. Das ist aus den genannten Gründen, wo die Datenverordnung ein etwas grober Klotz ist, wahrscheinlich die zukunftssträchtigere Variante. Die Frage ist, ob die Typengenehmigungsverordnung wirklich aktuell ist und ob wir sie hier nicht aktualisieren müssen. Dazu hat es 2022 eine Sondierung seitens der EU-Kommission gegeben, das Ergebnis war alles andere als eindeutig. Intern hat die Kommission an einem Entwurf einer neuen Verordnung über die Nutzung von und den Zugang zu Fahrzeugdaten, Funktionen und Ressourcen gearbeitet. Der ist bis heute von allen Seiten sehr umstritten.“

Autohersteller sammeln nicht unendlich Daten

Peter Geffers, Manager Connectivity Solutions Integration & OTA software updates, FORD, beleuchtet das Thema aus Sicht der Hersteller und möchte der medialen Botschaft der Datenkrake Auto entgegenhalten. Geffers: „Ein Fahrzeug sendet nicht permanent von Zündung an bis Zündung aus nur Daten.“ Fahrzeugdaten können für Hersteller wertvolle Aufschlüsse geben, z.B. für die Bauteiloptimierung in der Entwicklung, über die tatsächliche Nutzung einzelner Features oder auch im Aftermarket für Services, Reparaturen etc. Selbstverständlich könne der Datenaustausch hinterfragt werden. Gleichzeitig erwarten die Kunden, Daten für notwendige Services zu erhalten (Navigation, freie Ladesäulen / Parkplätze etc.). Geffers: „Ich glaube, wenn ein Hersteller diese Daten nicht zur Verfügung stellt, dann läuft er Gefahr, aus dem Markt verdrängt zu werden.“ Durch die ePrivacy Directive („TTDSG“) wurde die Nutzung der Daten bei den Herstellern ohnehin bereits extrem eingeschränkt. Geffers: „Mit der Einführung dieser Direktive müssen wir jetzt unsere Kunden explizit fragen, zu welchem Zweck wir die Daten verwenden dürfen. Ohne eine Zustimmung dürfen wir keine Daten mehr verwenden.“ Als Beispiel nennt Geffers Navigationslösungen: Für diesen Dienst ist es erforderlich, dass Daten, Positionsdaten, Ziele etc. ausgetauscht werden. Diese Daten müssen, wenn der Kunde diesen Dienst auch im Fahrzeug aktiviert, übertragen werden. Geffers: „Wir dürfen diese dann aber für keinen anderen weiteren Zweck verwenden. Gleichzeitig existiert etwa in Belgien ein Gesetz, dass wir die Kilometerstände bei vernetzten Fahrzeugen einmal im Quartal übermitteln müssen. Wir sehen da als Hersteller leichte Komplikationen.“

All das Datensammeln sei für Hersteller aufgrund von Mobilfunkverträgen etc. auch kein günstiges Unterfangen. Laut Geffers müsse daher jedenfalls ein konkreter Nutzen dahinterstehen.

Prinzipiell seien Autohersteller auch verpflichtet, die Daten zu teilen. Das Identitätsmodell und Geschäftsmodell von Drittanbietern muss natürlich nicht bekannt gegeben werden. Geffers:

„Wir ermöglichen auch das Schreiben von Servicefunktionen, in diesem Fall möchten wir uns jedoch austauschen, damit der Drittanbieter unsere Fahrzeugarchitektur und die Funktion versteht. Das dient der Sicherheit.“

Cybersecurity ein Fahrzeubleben lang als Herausforderung

Klaus Kainrath, Cybersecurity Manager, Magna Steyr, berichtet über das Thema Cyber Security, welches in der Automobilindustrie seit 2022 für neue Typen und seit 2024 mehr oder weniger für alle Fahrzeuge verpflichtend berücksichtigt werden muss: „Es gibt eine EU-Verordnung, die UNECE R155, die besagt, dass jedes Fahrzeug Cybersecurity by Design implementieren muss, das heißt, das Produkt Auto muss sicher entwickelt werden, man muss ein sogenanntes Cybersecurity Management System in seinem Unternehmen aufbauen und beweisen können, wie das im Produktentwicklungsprozess wirklich implementiert werden kann. Das muss von einer unabhängigen Stelle zertifiziert werden - wir als Magna Steyr haben seit zwei Jahren ein entsprechendes Zertifikat.“

Bei Cybersecurity sei man jedoch nie fertig. Die Regularie besagt, Fahrzeuge müssen bis zum Ende der Lebensdauer (bis zu 20 Jahre!) mit Cybersicherheit versorgt werden – eine Herausforderung. Kainrath: „Auch wenn der OEM selbst dafür bis End of Life verantwortlich ist, aus rationaler Sicht wird man wahrscheinlich dann Verträge abschließen und nach einem gewissen Zeitraum einfach als Best Effort Support ansehen oder im schlimmsten Fall Systeme abschalten müssen.“

ÖAMTC: Sektorspezifische Regelung erforderlich

Oliver Schmerold, Direktor, ÖAMTC, ist aufgrund der Ausführungen von Frau Wendehorst besorgt, dass der Gesetzgeber nicht alles zu Ende gedacht hat, womit die Justiz das letzte Wort hat. 2023 wurde in einem Verfahren gegen einen Hersteller laut Schmerold auch klar festgehalten, dass dieser entgegen der aktuell gültigen Typen-Genehmigungsverordnung agiert und seine Verfahren zu ändern hat, was jedoch nicht passiert ist. Es brauche daher dringend die sektorspezifische Regulierung im Automotive Bereich, also der angesprochenen Typengenehmigungsverordnung.

Schmerold: „Es muss klar sein, dass ein Fahrzeugbesitzer die Möglichkeit haben muss, aus unterschiedlichen Diensten zu wählen und von einem anderen Anbieter auch weiterführende Services zu empfangen. In der Praxis stellt sich bei uns die Frage, ob wir beispielsweise in Zukunft noch Fehlercodes bei Mitgliederfahrzeugen löschen können? Das legitime Interesse der Hersteller an einem geregelten und vor allem geschützten Zugang wollen wir überhaupt nicht in Frage stellen. Es darf aber nicht dazu führen, dass zwischen unterschiedlichen Dienstleistern diskriminiert wird. Wir wollen im Rahmen eines fairen, transparenten, aber auch praxistauglichen Authentifizierungsverfahren die Möglichkeit haben, auch aus der Ferne oder auch vor Ort auf entsprechende Daten zugreifen zu können. Aktuell haben wir den Zugang zu den Daten über die Diagnosegeräte der bekannten Hersteller. Unsere Mitarbeiter haben alle einen persönlichen Account, der mit einer digitalen Signatur abgesichert ist. Dieser Zugriff funktioniert allerdings nur bei einer entsprechend guten stabilen Datenverbindung. Es gibt jedoch immer wieder Einsatzfälle, wo diese Datenverbindung nicht gegeben ist wie Tunnel oder Garagen. Das heißt, eine unserer Minimalforderungen ist, dass ein Pannenhelfer nach

Authentifizierung am Beginn seiner Schicht am Diagnosegerät den ganzen Tag lang Zugang haben muss.“

Aus Cyber Security Sicht ist der letzte Satz laut **Kainrath** genau der kritische Punkt, weil durch einen längeren Offline Zugang immerhin die Gefahr bestehe, dass Schlüsselmaterial in falsche Hände gelangt und in weiterer Folge ganze Flotten kompromittiert werden können.

Schmerold präzisiert, dass es dem ÖAMTC nur um ein gewisses Set an Daten gehe und andere Daten durchaus entsprechend abgesichert werden könnten. Geffers ergänzt, dass Fehlercodes immer auslesbar seien.

Was kann der Kunde daraus ableiten?

Daniela Zimmer, Expertin digitaler Verbraucherschutz, Arbeiterkammer, betont die verschiedenen Typologien von Verbrauchern: „Early Adopters wissen um die vielen Softwarekomponenten im Auto, die Mehrheit weiß es nicht. Bei all dem, was wir bisher gehört habe, bräuchte es eigentlich wie im Telekom Sektor eine sektorspezifische Aufsicht, damit neben den Interessen der verschiedenen Stakeholder auch der Verbraucherschutz nicht zu kurz kommt. Mir erscheint es erstrebenswert, dass sich die EU-Kommission mit ihrer Plattformregulierung, die bislang eigentlich nur große Messengerdienste, Suchmaschinen usw. betroffen hat, eigentlich auch diesem Sektor frühzeitig zuwenden sollte, damit dort nicht dominante Gatekeeper entstehen, wo Verbraucherorganisationen oder Verkehrsclubs möglicherweise nicht auf Augenhöhe wahrgenommen werden. Das ist ein Prozess, der zu moderieren ist, damit er ausbalanciert ist.“ Zimmer schlägt vor, Fact Sheets vor dem Kauf einzuführen, in denen übersichtlich je nach Automarke aufgelistet ist, welcher Anbieter wie intensiv Daten verwendet und welche Hersteller Zugang zu Diagnosedaten für Werkstätten etc. bieten.

Und einem Reifenhersteller?

Christoph Vondenhoff, Head of Public Affairs DACH-Region, Michelin, betont, dass Michelin alleine durch den Einbau von RFID-Chips in die Reifen seit dem letzten Jahrzehnt auch mit dem Thema Daten aus dem Auto zu tun hat. Diese Daten wurden dann weiter in der Entwicklung bzw. Forschung genutzt, um festzustellen, wie die Reifen auf der Strecke geschlagen haben. Daraus wurden Verbesserungen entwickelt. Seit Ende 2023 werden etwa sämtliche LKW Reifen serienmäßig mit RFID Chips ausgestattet und das verspricht auch entsprechende Geschäftsmodelle. Vondenhoff: „Wir wollen auch als Reifenhersteller unsere Geschäftsfelder erweitern unter anderem in Richtung digitaler Dienstleistungen. Daher wäre eine sektorspezifische Regelung zum Thema Daten aus unserer Sicht sehr wünschenswert. Wir unterstützen auch die Verbraucherverbände bei dem Thema, denn wir glauben schon, dass das ein ganz erheblicher Markt ist, den es hier zu heben gibt. Und wenn wir uns als europäische Automobilindustrie nicht darum kümmern, machen das Geschäft womöglich andere. Deswegen ist es gut, wenn man relativ zügig zu klaren Regelungen kommt. Fiat hat vorgerechnet, was passiert oder was volkswirtschaftlich verloren geht, wenn man auf klare Regelungen verzichtet, da wurden bis zum Jahr 2030 29 Milliarden Euro genannt, für 2050 sogar 89 Milliarden.“

Geffers denkt auch, dass es vernünftig ist, Kunden vor der Kaufentscheidung zu informieren, welche Marke welches (digitale) Angebot unterstützt: „Wenn wir uns dann nicht öffnen und die Daten nicht teilen und ein Kunde kann einen After Market Servicedienst nicht bei uns abrufen, dann werden wir, glaube ich, Kundschaft verlieren und das signifikant.“

Schmerold hebt abschließend Ford als wichtigen Partner hervor, der ÖAMTC habe dort bereits direkte Anbindung ans Backend: „Das löst zwar nicht das Authentifizierungs-Thema, aber den technischen Zugriff auf die Daten, den haben wir bei Ford.“

14.11.2024, Bernhard Weiner, GSV