AUTOMATISIERTES, VERNETZTES FAHREN: NICHT OHNE DATENSCHUTZ

Das automatisierte und vernetzte Fahrzeug wird es in Deutschland etwa ab 2020 geben. Es funktioniert, indem eine gigantische Summe von Daten gesammelt und ausgewertet wird. Auf verschiedenen technologischen Wegen kommuniziert das Fahrzeug mit seinem Fahrer, anderen Fahrzeugen sowie mit der gesamten zukünftig auf das vernetzte Fahren ausgerichteten Infrastruktur. Über GPS, Mobilfunk sowie über bestimmte WLAN-Standards werden unzählige Daten ausgetauscht. Hinzu kommt, dass die Kraftfahrer die Fahrzeit in automatisierten Autos zukünftig zu einem Großteil für Online-Aktivitäten nutzen werden. Dadurch fällt auch im Kontext der Fahrzeugnutzung eine weitere Datenmenge an.

Eine Umfrage im Auftrag des Verbraucherzentrale Bundesverbandes hat ergeben, dass ein Fünftel der Bevölkerung autonome Fahrzeuge strikt ablehnt. Viele andere Verbraucher sind irritiert. Für die Bereitschaft der Verbraucher, solch ein Fahrzeug zu nutzen, ist die Transparenz der Datenwege, Speicherorte und Zugriffsbefugnisse durch potentielle Interessenten unerlässlich. Denn nahezu alle im Fahrzeug erzeugten Daten lassen Rückschlüsse auf Fahrer und Fahrverhalten zu und sind somit als personenbeziehbare Daten hochsensibel. Transparenz und Datensparsamkeit sind deshalb entscheidende Gebote, die von der Autoindustrie einzuhalten sind.

Ein automatisiertes, vernetztes Fahrzeug erfasst permanent Daten. Darunter beispielsweise den **Standort** des Fahrzeugs, zahlreiche **technische Fahrzeugdaten** wie die Nutzung von Bremse, Licht, Nebelscheinwerfern und das Aktivieren und Deaktivieren des Fahrzeugassistenzsystems (der Fahrfunktion). Aber auch **Service-Dienste** des Herstellers wie etwa ein persönlicher Internetzugang im Fahrzeug, sowie die Aktualisierung von Navigationskarten im Fahrzeug werden mit erhoben.

Darüber hinaus werden im Rahmen des **eCall-Systems**, das europäische Unfall-Notrufsystem (verpflichtender Einbau in Neufahrzeugen: 31.03.2018), Informationen zum Unfallzeitpunkt, zum Unfallort, der Fahrtrichtung und Co. übermittelt. Die meisten dieser Daten benötigt das Fahrzeug für die Fahrfunktion, allerdings überwiegend jeweils nur für den Fahrmoment. Eine darüberhinausgehende Speicherung ist für die Fahrfunktion technisch nicht erforderlich.

DIE VERBRAUCHERZENTRALE SACHSEN FORDERT:

Datensammlungen sind das Fundament des automatisierten Fahrens. Trotzdem darf der Fahrer nicht gläsern sein. Der Schutz der persönlichen Daten der Fahrzeugnutzer muss gewährleistet werden.

Personenbezogene Daten dürfen im Fahrzeug nur zweckgebunden gespeichert werden, beispielsweise wenn die Daten auf ein abweichendes Verhalten des Fahrzeugs schließen lassen. Es darf zu keiner Permanent-Speicherung unterschiedlicher Fahrdaten kommen.

Personenbezogene Daten dürfen nur mit einer ausdrücklichen und einzelfallbezogenen Einwilligung des Betroffene an Dritte weitergegeben werden, beispielsweise an Versicherungen und andere private Dritte. Die Einwilligung sollte nutzerfreundlich direkt im Fahrzeug erfolgen können.

Daten sollen nicht in der Sphäre des Herstellers gespeichert werden.

Fahrdaten sind permanent zu überschreiben. Ausschließlich kritische Fahrsituationen dürfen gespeichert werden, jedoch nicht länger als 10 Sekunden.

Weitergabe gespeicherter Fahrdaten an Dritte muss strikten Beschränkungen obliegen. Wünschenswert ist, dass ein übergeordnetes, unabhängiges Trust Center im Einzelfall über die Datenweitergabe entscheidet, ohne dass die Daten dadurch dem Anbieter oder dem Staat obliegen.

In einer herstellerübergreifenden Cloud sollen ausschließlich maschinenbezogene Daten gespeichert werden. Davon profitieren alle am automatisierten Fahren beteiligten Personen.

verbraucherzentrale
Sachsen

WIE UND WANN SOLLEN DIE DATEN GESPEICHERT WERDEN?

UMFANG DER ZU SPEICHERNDEN DATEN

Die Regelungen des im Juni 2017 neu gefassten Straßenverkehrsgesetzes definieren und begrenzen nicht, welche Daten im vernetzten Fahrzeug überhaupt gespeichert werden müssen bzw. dürfen. Essentiell zu speichern ist nur, ob die Fahrfunktion eingeschaltet war oder der Fahrer gesteuert hat - inklusive der zugehörigen GPS-Daten. Außerdem ist es wichtig nachvollziehen zu können, wann das Übergabesignal vom System an den Fahrer gegeben wurde - beispielsweise um den Hergang eines Unfalls besser nachvollziehen zu können.

DATENVERARBEITUNG IN EINER CLOUD

Wünschenswert ist, dass Maschinendaten des Fahrsystems in einer herstellerübergreifenden Cloud gespeichert werden. Dort könnten sie zum Nutzen aller Fahrer ausgewertet und in deren Fahrsystem eingespeist werden. Ein Beispiel: Nebelscheinwerfer eingeschaltet ›› Signal an die Cloud ›› Auswertung, dass im entsprechenden Gebiet Nebel herrscht ›› Ausgabe der „Nebelwarnung“ an alle Fahrsysteme im relevanten GPS-Gebiet. Ein solch sinnvolles Datenauswertungssystem in einer übergeordneten, unabhängigen Cloud darf nicht in die Hand eines einziges Anbieters gegeben werden.

FAHRZEUGHALTER HAT RECHT AN DATEN

Im Grundsatz muss der Fahrzeughalter das Recht an seinen Daten haben. Er muss entscheiden können, was mit seinen personenbezogenen, sensiblen Daten geschieht. In diesem Zusammenhang muss transparent werden, welche Daten wann an wen weitergebeben werden. Es muss klar sein, wer die Daten speichert: Der Hersteller, der Fahrzeughalter oder Dritte. Das ist derzeit nicht der Fall.

SPEICHERDAUER

Der Fahrtenschreiber muss die Fahrdaten permanent überschreiben. Erst bei genau definiertem, abweichendem Verhalten des Systems darf eine Datenspeicherung dahingehend zulässig sein, dass etwa die letzten zehn Sekunden aufgezeichnet werden. Diese Daten dürfen nicht ohne Weiteres durch Polizei, Behörden oder Dritte abgerufen werden. Vielmehr sollte ein zwischengeschaltetes Trust Center die Entscheidung über die Weitergabe solcher Daten treffen.

DATENSCHUTZFREUNDLICHE FAHRZEUGSYSTEME, TRANSPARENZ UND TECHNIKAKZEPTANZ

Um den Verbrauchern die Ängste zu nehmen, ihre Akzeptanz bei der Digitalisierung des Verkehrs herzustellen und diese somit voranzutreiben, ist **Transparenz** in diesem Prozess die grundlegende Basis für das Gelingen. Die Verbraucherzentrale Sachsen will sich der Herausforderung der Herstellung von Transparenz für die privaten Endkunden stellen.

Dialoge mit Vertretern aus Forschung und Industrie sollen Brücken zum Endkunden bauen. Ziel ist, die Funktionalität der neuen Systeme aus Endkundenperspektive zu durchdringen und den Verbrauchern die Vorbehalte zu nehmen. Nur so kann sich **Technikakzeptanz** für automatisierte Fahrsysteme etablieren.

Dabei muss transparent sein, welche Daten erfasst und verarbeitetet werden. Für den Nutzer muss klar sein, wo und unter welchen Voraussetzungen **personenbezogene Daten** gespeichert werden können und wer unter welchen Umständen Zugriff diese Daten hat. In diesem Zusammenhang ist es erstrebenswert, Software und Fahrzeugsysteme bereits datenschutzfreundlich zu entwickeln (**privacy by design**). Datenschutz und Privatsphäre wären damit bereits durch die Technik gewährleistet.

Es gilt strikt zu verhindern, dass sich im Zuge der Einführung des automatisierten Fahrens eine **Vorratsdatenspeicherung** etabliert. Hersteller, Anbieter, Versicherungen sowie Polizei und andere staatliche Behörden dürfen nicht ungehindert Zugriff auf die Daten bekommen.

verbraucherzentrale
Sachsen

Verbraucherzentrale Sachsen, Landesgeschäftsstelle
Katharinenstraße 17, 04109 Leipzig
Telefon: 0341 - 696 290
E-Mail: vzs@vzs.de
www.verbraucherzentrale-sachsen.de

Stand: Oktober 2017

Dieses Faktenblatt wird durch Steuermittel auf der Grundlage des von den Abgeordneten des Sächsischen Landtages beschlossenen Haushaltes mitfinanziert.