Law & Order fürs Auto

US-Vorgaben für IT-Sicherheit und Datenschutz im Auto

Ein neues US-Gesetz regelt Sicherheits- und Privacy-Aspekte der Datenverarbeitung in vernetzten und teilautonomen Fahrzeugen. Der deutsche Gesetzgeber ist bei diesem Thema deutlich laxer unterwegs.

Von Christiane Schulzki-Haddouti

Das US-Repräsentantenhaus hat mit dem „Self-Drive Act“ im September eine Regelung verabschiedet, die strenge Vorgaben für Datenschutz und IT-Sicherheit beim hochautomatisierten und autonomen Fahren setzt. Hierzulande hat der Deutsche Bundestag bereits im März 2017 mit einer Änderung des Straßenverkehrsgesetzes das hochautomatisierte und autonome Fahren in Deutschland ermöglicht. Seine Regelungen zur Datenverarbeitung im Kraftfahrzeug, die eine Speicherung bestimmter Fahrzeugdaten in einer Blackbox für Haftungszwecke vorsehen, sind jedoch im Vergleich zur US-Regelung sehr zurückhaltend formuliert.

So widmet der Self-Drive Act dem Thema Cybersecurity einen eigenen Abschnitt: Demnach müssen Automobilhersteller einen sogenannten „Cybersecurity Plan“ entwickeln, der erläutert, wie Cyber-Attacken sowie falsche oder störende Kontrollkommandos entdeckt und verhindert werden können. Hierfür müssen die Hersteller systematisch Schwachstellen identifizieren, bewerten und entschärfen können. Dazu gehören Intrusion-Detection-und-Prevention-Systeme samt einer Pflicht zu etwaigen Updates bei „veränderten Umständen“. Das Gesetz verpflichtet Automobilhersteller außerdem dazu, einen Cybersecurity-Beauftragten zu bestellen. Eine solche Position haben bislang nur sehr wenige Unternehmen eingerichtet. Das Gesetz verlangt von den Herstellern sogar, den Zugang ihrer Mitarbeiter zu autonomen Fahrzeugsystemen zu kontrollieren.

Datentransparenz

Überdies müssen Automobilhersteller einen Privacy-Plan entwickeln. Das entspricht in weiten Teilen den Plänen des Bundesverkehrsministeriums für einen „Datenausweis“. Er soll transparent machen, welche Daten das Fahrzeug sammelt und wie diese genutzt, geteilt und gespeichert werden. Der Ausweis bezieht sich auf alle Daten, die Rückschlüsse auf den Fahrzeughalter oder die Insassen liefern.

Aus dem Privacy-Plan soll hervorgehen, wie der Automobilhersteller mit solchen Daten umgeht, etwa in Bezug auf Datensparsamkeit, Anonymisierung oder eine etwaige Vorratsdatenspeicherung. Auch soll der Hersteller angeben, mit welchen weiteren Unternehmen er die Daten teilt.

Nach Vorgaben des US-Gesetzgebers sollen die Hersteller klar benennen, welche Wahl- und Interventionsmöglichkeiten die Fahrzeuginhaber oder die Fahrzeuginsassen bezüglich der Erfassung von Informationen erhalten und wie diese Personen über den Privacy-Plan informiert werden sollen. Das Gesetz fordert die Möglichkeit, bestimmte Informationen aus allen Datenspeichern zu löschen, sofern sie keine unmittelbare Sicherheits- und Betriebsfunktionen haben.

Der US-Gesetzgeber hat auch einen Anreiz zu „Privacy by Design“ eingebaut: So muss immer dann kein Privacy-Plan erstellt werden, wenn die Fahrzeugdaten keinem bestimmten Fahrzeug zugeordnet werden können – etwa dank Anonymisierungs- oder Verschlüsselungstechniken.

Von den USA lernen

Die Juristin Jutta Stender-Vorwachs von der Leibniz Universität Hannover, die kürzlich mit einem Kollegen das deutschlandweit erste Buch zu den juristischen Aspekten des autonomen Fahrens herausgegeben hat, sagt: „Das US-Gesetz ist bei der Umsetzung der IT-Sicherheit deutlich wirkungsvoller.“ Sie betont, dass auch ausländische Automobilhersteller in den USA einen umfassenden „Cyber Security Plan“ erstellen und einen Ansprechpartner für dieses Thema im Unternehmen benennen müssen. Sie plädiert dafür, dass der deutsche Gesetzgeber zusätzlich zu den Speicherungsregelungen in Paragraf 63a des Straßenverkehrsgesetzes auch die Fahrzeughersteller selbst in die Pflicht nimmt.

Dass sich Fahrzeughersteller und Zulieferer bereits mit der Thematik auseinandersetzen, zeigte ein Besuch auf der IAA. Continental stellte Ende-zu-Ende-Sicherheitslösungen vor, die Angriffe auf ein Fahrzeug erkennen und abwehren können. Sie setzen an den Kommunikationsschnittstellen des Fahrzeugs nach außen an. Das Fahrzeugsystem intern wird ebenfalls geschützt, indem etwa die Kommunikation auf dem CAN-Bus auf Unregelmäßigkeiten geprüft und der Datenaustausch zwischen einzelnen Steuergeräten verschlüsselt wird.

Im Unterschied zum „Self-Drive Act“ in den USA setzt der deutsche Gesetzgeber weiterhin darauf, dass die Automobilhersteller und ihre Zulieferer von sich aus entsprechende Lösungen anbieten. Konkrete Vorgaben fehlen. Spannend wird die Frage, ob die Automobilhersteller die IT-Sicherheitssysteme, die sie aufgrund des neuen US-Gesetzes einführen müssen, nur für US-Modelle oder – auf freiwilliger Basis – auch auf dem europäischen Markt anbieten werden. *(sha@ct.de)* ct

Link zum US-Gesetz: ct.de/ygf4

In einigen US-Bundesstaaten wie hier in Nevada durften bereits vor vier Jahren Autos mit spezieller Zulassung autonom fahren.