# Kommentar: Fahrende Verräter

Von Harald Kaier, cen

Der Name klingt nach Vertrauen. „Automotive Trustcenter“ nennt der TÜV-Verband (VdTÜV) eine Art Datenknotenpunkt, in dem die Fahrdaten aller Automobile in Deutschland gebündelt gesammelt werden sollen. Natürlich so, dass kein Fremder darauf Zugriff hat. Es geht um dies: Unzählige Sensoren erheben in modernen Fahrzeugen massenhaft Daten zur Funktionsweise der eingebauten Technik, zum Fahrverhalten und den zurückgelegten Wegen. Das vom VdTÜV im Dezember 2019 präsentierte Konzept für ein „Automotive Trustcenter“ soll einen „diskriminierungsfreien, sicheren und datenschutzkonformen Zugang zu Daten vernetzter Fahrzeuge“ sicherstellen, schrieb der Verband kurz vor Jahresschluss 2019 in einer Mitteilung.

Ein Vorschlag, der super klingt. Doch so selbstlos, wie es scheint, ist das Konzept nicht. Denn sofern diese Idee umgesetzt wird, geht es auch ums Geschäft mit der Sicherung und der Verwaltung dieser höchst sensiblen Daten von zig Millionen Autos. Das Konzept sieht eine im staatlichen Auftrag handelnde Stelle vor, die nur „berechtigte Organisationen“ zum Zug kommen lässt. So sollen zum Beispiel Prüforganisationen (TÜV, Dekra), Versicherungen oder Behörden Fahrzeugdaten nutzen dürfen, um etwa alle drei Jahre (bei Neuwagen) oder alle zwei Jahre (bei Gebrauchtwagen) im Rahmen der Hauptuntersuchung digitale Komponenten prüfen oder Haftungsfragen nach Unfällen klären zu können. Das Trustcenter soll dabei selbst keine Informationen speichern, sondern untergeordnete Treuhänder. Die darüber stehende Instanz erteile dann Zugriffsrechte für bestimmte Datenpakete an die jeweiligen legitimen Nutzer.

Alles halb so schlimm?

Also alles halb so schlimm? Das Thema ist weit brisanter als es zu sein scheint. Ein vordergründig harmloses Beispiel dafür, welche Daten in einem modernen Automobil ständig abgerufen und verarbeitet werden. Es betrifft die Klimaautomatik. Steht ein Seitenfenster einen Spalt offen? Ist das Schiebedach womöglich nicht ganz geschlossen? Wie hoch ist die Außentemperatur? Und könnte der Fahrtwind beim Kühlen der Luft für den Innenraum mithelfen? Diese Daten benötigt der Mikrocomputer der Kühlanlage in jeder Sekunde, um den Passagieren angepasst an die gerade aktuellen Erfordernisse wohl temperierte Luft zufächeln zu können.

Dieses Beispiel zeigt, wie weit die Datenvernetzung in Autos inzwischen fortgeschritten ist. Und es ist beileibe nicht in jedem Fall unwichtig. Sollte sich etwa nach einem Diebstahl des Autos herausstellen, dass ein Fenster leicht geöffnet war und die Täter darüber ins Auto gekommen sein können, dann hat der Besitzer womöglich schlechte Karten. Sofern es herauskommt. Denn auch die Botschaft, dass ein Fenster einen Spalt aufstand, würde verschlüsselt an solch einen Datensammler gemeldet – über die registrierten und abrufbaren Klimadaten.

Solche Angaben sind jedoch nur winzige Schnipsel dessen, was die modernen rollenden Rechenzentren mit inzwischen 80 und mehr solcher Schlauberger erzeugen und bewerten.Steuercomputer wie die für den Airbag, den Schleuderverhinderer ESP oder das Antiblockiersystem ABS wissen zum Beispiel immer:
• wie schnell das Auto gerade ist,
• wie die Vorderräder stehen,
• ob beschleunigt wird,
• welcher Gang eingelegt ist,
• welche Tageszeit herrscht,

• wie hoch die Außentemperatur ist,
• wie das Gas steht,
• welche Sitze belegt und
• welche Gurte angelegt sind,
• sowie auch, ob sich die Querbeschleunigung einem kritischen Wert nähert, an dem automatisch ein Rad gebremst werden muss, um Schleudern und Schlimmeres zu verhindern.

Nur nicht gespeicherte Momentaufnahmen

Mit diesen Informationen müssen die elektronischen Schlauberger ständig gefüttert werden, sollen sie ihre schützende Wirkung in der Tausendstelsekunde entfalten, in der sie gebraucht werden. Nach Darstellung einiger Autohersteller sind diese Daten nur Momentaufnahmen, die nicht dauerhaft gespeichert werden. Glauben muss man das allerdings nicht. Denn Sensoren melden durchgängig fahrdynamische Zustände, Steuergeräte verarbeiten diese Signale und gleichen sie untereinander und mit vorgegebenen Sollwerten ab. Da der reine Abgleich mit Soll-Werten aber nicht ausreicht, müssen Messwerte mal länger, mal kürzer gespeichert werden. Nur so ist ein Vergleich mehrerer Messwerte möglich, der Rückschlüsse erlaubt. Mit anderen Worten: Das ist Vorratsdatenspeicherung.

Schon 2014 hat ein Insider ausgeplaudert, worum es eigentlich geht. Damals hat der ehemalige Ford-Europa-Chef Jim Farley während einer Podiumsdiskussion auf der Computermesse CES in den USA verraten: „Wir kennen jeden Autofahrer, der die Verkehrsregeln bricht. Und weil GPS in den Autos ist, wissen wir, wo und wie jemand das tut.“ Als Farley die Tragweite seiner Worte erkannte, versuchte er sie mit einer Erklärung abzuschwächen. Doch die Äußerung war nicht mehr zurückzuholen. Und sie war entlarvend: Es geht um Überwachung im großen Stil, um die Analyse der gespeicherten Daten sowie um die Möglichkeit, daraus massenhaft Fahrprofile erstellen zu können.

Dürfen Daten weitergegeben werden?

Aber dürfen Daten weitergegeben werden? Eindeutige Antworten sind schwierig bis unmöglich. Die Hersteller versichern zwar, dass sie dieses digitale Wissen nicht weitergeben. Kontrollieren kann das jedoch keiner. Warum machen die das? Hauptsächlich, um sich vor Gewährleistungsansprüchen zu schützen. So dürfte sich der eine oder andere Autofahrer schon darüber gewundert haben, wenn der Hersteller ein Garantiebegehren, zum Beispiel wegen eines defekten Motors, mit Fakten aus diesen Speichern abgelehnt hat. Die führen nämlich auch darüber Buch, wie der Motor behandelt wird. Wer ihn über Wochen im kalten Zustand auf astronomische Drehzahlen jagt und deswegen einen Motorschaden herbeigeführt hat, wird mit seinem Garantieanspruch abgeblockt. Es gibt aber auch einen anderen Grund, weswegen die Autobauer so verfahren: Weil sie es können.
Die wichtigste Frage ist: Wem gehört das verschlüsselte Profil in Bits und Bytes? Was ist mit der Privatsphäre?

Wer ein Auto besitzt, glaubt, dass die darin enthaltenen Daten sein alleiniges Eigentum sind. Also Datenschutz wie etwa das Recht am eigenen Bild. Von wegen. Der Kasseler Juraprofessor Alexander Roßnagel beleuchtete die Rechtsfrage nach dem Eigentum dieser Dinge schon vor Jahren in einem Fachaufsatz mit einem ernüchternden Fazit: „Dingliche Rechte sind nur an körperlichen Gegenständen möglich. Sie können daher nicht an Daten, sondern nur an Datenträgern bestehen. Kfz-Daten sind immaterielle Informationen und unterliegen daher nicht einer Eigentums- oder Besitzordnung.“ Das heißt: Wer die Schlüssel für die Decodierung besitzt, wird sich auch als Eigentümer fühlen und kann damit machen, was er will.

Fluch und Segen der digitalen Welt

Die digitale Welt, in der wir seit Jahren leben, ist Fluch und Segen zugleich. Überall hinterlassen wir mehr oder weniger gleichgültig private Datenspuren: Im Supermarkt am Kreditkartenleser, die Kennung eingeschalteter Mobiltelefone erlaubt ein Bewegungsbild von Funkzelle zu Funkzelle, Apples iPhone speichert sogar (abschaltbar) die Aufenthaltsorte mit Uhrzeit und Datum und die Seitenbesuche im Internet geben den Betreibern Auskünfte über die Produktvorlieben der Benutzer. Längst sind wir gefangen in den Tentakeln internationaler Datenkraken, ohne die – zugegeben – manches auch nicht mehr funktionieren würde. Sie kennen nicht nur unsere Adressen, Familienmitglieder, unsere Kreditwürdigkeit, sie gucken uns auch aus dem Himmel elektronisch auf den Balkon oder auf die Terrasse. Zumeist herrscht Gottvertrauen darauf, dass mit den Daten kein Schindluder getrieben wird.

Im Auto, das wie kaum ein zweites Symbol für Freiheit steht, ist der normale Fahrer inzwischen genauso gläsern wie ein Rennprofi, dessen Können in der Box am Bildschirm überwacht wird – wie und wo er Gas gibt, wann er schaltet, wo er bremst, wie er lenkt. Ab Mai 2022 müssen nach einem Beschluss der EU alle neuen Pkw unter anderem mit folgenden Aufpassern ausgestattet sein: Intelligenter Geschwindigkeitsassistent, Vorrichtung zum Einbau einer alkoholempfindlichen Wegfahrsperre, Warnsystem bei Müdigkeit und nachlassender Aufmerksamkeit des Fahrers, Warnsystem bei nachlassender Konzentration des Fahrers, Notbremslicht, Rückfahrassistent und eine ereignisbezogene Datenerfassung. Letztere meint den altbekannten Unfalldatenschreiber (UDS), der momentan in Deutschland nur auf freiwilliger Basis eingebaut wird, weshalb er nur in sehr wenigen Privatwagen zu finden ist. Grund: Niemand will sich durch objektive Daten bei einer juristischen Auseinandersetzung selbst belasten. In Mietwagenflotten, Feuerwehr- und Polizeiautos hingegen finden sich diese elektronischen Spione zumeist. Beide, der stets mitschreibende Auto-Zentralspeicher wie der UDS, können Retter wie Verräter sein. Denn deren aufgezeichnete Daten können den Fahrer genauso belasten wie entlasten.

Die Datenwelle bekommt Tsunami-Ausmaße

Die langfristigen Aussichten, dass sich etwa die Lage zugunsten des Autofahrers verändert, sind düster. Denn die Datenwelle wird spätestens in 20 Jahren, wenn die ersten autonomen Autos unterwegs sind, Tsunamiausmaße angenommen haben und auch nicht mehr abebben. Wohin die Reise geht, wissen Experten seit Jahren: In Zukunft wird der Fahrer abgeschafft und nur noch tatenloser Passagier sein, um auf diese Weise den fehlbaren Menschen auszuschalten, damit Unfälle künftig so gut wie ausgeschlossen sind. Der Rohstoff für solche vom Rechner gesteuerten Autos sind Daten, Daten, Daten. Ohne das detaillierte Wissen, wer wo wie unterwegs ist, würden sich diese Fahrzeuge heillos verkeilen.

Das bedeutet aber auch, wenn Autos nicht nur zwecks Unfallverhinderung mit anderen Autos, sondern auch mit der sonstigen Umwelt elektronisch kommunizieren und ständig Positionsdaten senden, sind die auf Servern hinterlegten digitalen Spuren für Dritte geschäftlich interessant. Fällt einem vernetzten Rechner bei der automatischen Auswertung der Navigationsdaten etwa auf, dass ein Auto öfter in der Nähe eines Mutter+Kind-Ladens parkt, wird der wegen seiner spezifischen Programmierung daraus die Wahrscheinlichkeit ableiten, dass bald ein Familienauto ins Haus steht. Also wird der Halter oder die Halterin des Fahrzeugs mit Werbung für einen Van oder einen Kombi bombardiert.

Es könnten aber auch die Schnäppchenangebote von Tankstellen, Möbelhäusern, Supermärkten oder Eroscentern auf dieser Grundlage ins Haus flattern oder direkt und in Windeseile auf dem Bildschirm des Bordrechners oder in der Windschutzscheibe

eingeblendet werden, weil der Wagen nur noch wenige hundert Meter von einem Discounter entfernt ist. Und wer will bestreiten, dass nicht auch Autobanken Interesse an fahrerspezifischen Informationen haben? Ist der Wagen geleast oder über Kredit finanziert, kann es gut sein, dass die Finanzdienstleister der großen Autohersteller schon bald wissen möchten, wie mit ihrem Eigentum umgegangen wird.

Überhaupt bahnt sich ein neues Geschäftsfeld an, das die internationale Autobranche zusammen mit der Daten-Wirtschaft weltweit aufbaut. Es wird Big Data genannt und hat die Vernetzung all dieser Informationen zum Zweck. Angeblich zum Wohle des Kunden. Nicht nur, um Werbebotschaften elektronisch an den Mann oder die Frau zu bringen, sondern etwa auch, um das Fahrzeug via Borddisplay vorzeitig zur Wartung in die Werkstatt zu rufen, weil der Fahrer ständig einen heißen Reifen fährt. Oder weil online ein sich ankündigender Defekt früh geortet worden ist und ein rascher Eingriff womöglich einen kapitalen Schaden verhindert. Klingt vernünftig und verlockend. Es geht aber auch umgekehrt. So ist es heute längst möglich, das eine oder andere Elektrofahrzeug auf Knopfdruck stillzulegen, weil der Fahrer seine Leasinggebühr für den verwendeten Akku nicht bezahlt hat.

Oder die Sache mit dem Notrufsystem „eCall“, dessen Einführung in Neuwagen seit 1. April 2018 Pflicht ist. Der von der EU verordnete elektronische Retter ist zugleich auch ein trojanisches Pferd. Zwar ist der im Falle eines Unfalls automatisch auslösende eCall für sich genommen eine prima Sache, weil er für die Rettungskräfte wichtige Daten wie Ort, Zeit und Fahrtrichtung über eine Telefonkarte direkt an eine Leitstelle überträgt.

Doch im Hintergrund von eCall sendet ein zweites System unbeschränkt und permanent Daten übers Netz. Und zwar auf Basis der Navigationsdetails. Diese Erkenntnisse können nicht nur für Fahndungen benutzt werden, scharf auf solche persönlichen Daten sind auch Versicherer, weil sich auf Basis des Fahrprofils maßgeschneiderte Policen anbieten lassen. Diverse Gesellschaften machen dies bereits seit längerem. Nötig dafür ist oft nur ein kleiner elektronischer Kasten im Auto, der von der Versicherung geliefert wird. Dieses unscheinbare Ding hält fest, wo sich das Auto gerade befindet, wie schnell es sich bewegt, wie stark es beschleunigt, er zeichnet hastiges Bremsen auf sowie Nacht- und Stadtfahrten. Motto: Zuckler zahlen weniger, Raser mehr.

Das Auto ist längst Teil der Internets

Bleibt die derzeit unbeantwortbare Frage nach der Datensicherheit. Denn ob man es nun wahrhaben will oder nicht: Das Auto ist im Begriff, ein Teil des Internets zu werden. Es ist inzwischen sogar so, dass sich der Terminkalender des Smartphones mit der Autoelektronik und der des Navigerätes vernetzt und automatisch den Teilnehmern einer bevorstehenden Konferenz mitteilt, dass man sich wegen der Verkehrslage verspäten werde. Das ist zwar ziemlich praktisch, eröffnet geschickten Hackern aber zumindest theoretisch Zugang zu womöglich höchst sensiblen Daten des aktuellen Aufenthaltsortes oder des Ziels einer vielleicht potentiell gefährdeten Person. Und wer weiß, was diese Herrschaften mit den Erkenntnissen anstellen? Solche Computernerds warten nur darauf, der Welt übers Internet zeigen zu können, wozu sie in der Lage sind. Experten gehen davon aus, dass bis 2025 mit 97 Prozent nahezu alle neuen Pkws und Lkws weltweit vernetzt sein werden. Dies dürfte auf mehr als 620 Millionen Kraftfahrzeuge hinauslaufen, die Daten austauschen – und die gehackt werden könnten. (ampnet/hk)

## Bilder zum Artikel

Harald Kaiser.

Foto: Auto-Medienportal.Net/Harald Kaiser